Host Security Service

User Guide (Kuala Lumpur Region)

Date **2025-10-09**

Contents

1 Introduction 1
1.1 What Is HSS? 1
1.2 Advantages 3
1.3 Scenarios 3
1.4 Features 4
1.5 HSS Permissions Management 49
1.6 Constraints 51
1.7 Related Services 58
1.8 Basic Concepts 59
2 Using IAM to Grant Access to HSS 62
2.1 Creating a User and Granting Permissions 62
2.2 HSS Custom Policies 63
2.3 HSS Actions 64
3 and Accessing HSS 70
3.1 Access Process 70
3.2 Installing the Agent on Servers 70
3.2.1 Installing the Agent on Cloud Platform Servers 71
3.2.2 On-Premises IDCs Accessing HSS Through a Direct Connect and Proxy Servers 80
3.2.2.1 Overview 80
3.2.2.2 Resources 81
3.2.2.3 Process Flow 81
3.2.2.4 Process 82
3.2.2.4.1 Creating a Direct Connect 82
3.2.2.4.2 Creating a Proxy Server 82
3.2.2.4.3 Installing an Agent on the Proxy Server 82
3.2.2.4.4 Installing and Configuring Nginx on the Proxy Server 83
3.2.2.4.5 Creating an Agent Installation Package or Installation Commands Using a Proxy Server 88
3.2.2.4.6 Installing an Agent for an On-premises IDC 91
3.2.3 Installing the HSS Agent Using CBH 92
3.3 Installing the Agent on Containers 94
3.3.1 Installing the Agent in a CCE Cluster 94
3.3.2 Installing the Agent on an Independent Container Node 96

3.4 Enabling Protection 97
3.4.1 Enabling the Basic/Enterprise/Premium Edition 102
3.4.2 Enabling Web Tamper Protection 104
3.4.3 Enabling Container Protection 106
4 Checking the Dashboard 108
5 Asset Management 120
5.1 Asset Overview 120
5.2 Server Fingerprints 121
5.2.1 Collecting Server Asset Fingerprints 121
5.2.2 Viewing Server Asset Fingerprints 125
5.3 Container Fingerprints 127
5.3.1 Collecting Container Asset Fingerprints 127
5.3.2 Viewing Container Asset Fingerprints 131
5.4 Server Management 137
5.4.1 Enabling Server Protection 137
5.4.2 Viewing Server Protection Status 140
5.4.3 Exporting the Server List 142
5.4.4 Deploying a Protection Policy 142
5.4.5 Managing Server Groups 144
5.4.6 Servers Importance Management 146
5.4.7 Ignoring a Server 147
5.4.8 Disabling HSS 148
5.4.8.1 Disabling the Basic/Enterprise/Premium Edition 148
5.4.8.2 Disabling WTP 149
5.5 Container Management 150
5.5.1 Enabling Container Protection 150
5.5.2 Viewing the Container Node Protection Status 153
5.5.3 Exporting the Container Node List 154
5.5.4 Managing Local Images 154
5.5.5 Managing Repository Images 157
5.5.6 Viewing Container Information 165
5.5.7 Handling Unsafe Containers 166
5.5.8 Uninstalling the Agent from a Cluster 167
5.5.9 Disabling Container Protection 168
6 Prediction 170
6.1 Vulnerability Management 170
6.1.1 Vulnerability Management Overview 170
6.1.2 Vulnerability Scan 174
6.1.3 Viewing Vulnerability Details 177
6.1.4 Exporting the Vulnerability List 180
6.1.5 Handling Vulnerabilities 181

6.1.6 Managing the Vulnerability Whitelist 191
6.1.7 Viewing Vulnerability Handling History 192
6.2 Baseline Check 193
6.2.1 Baseline Check Overview 194
6.2.2 Performing a Baseline Check 196
6.2.3 Viewing and Handling Baseline Check Results 200
6.2.4 Exporting a Baseline Check Report 206
6.2.5 Managing Manual Baseline Check Policies 206
6.3 Container Image Security 207
6.3.1 Viewing SWRImage Repository Vulnerabilities 208
6.3.2 Viewing Malicious File Detection Results in Images 208
7 Server Protection 210
7.1 Application Protection 210
7.1.1 Application Protection Overview 210
7.1.2 Enabling Application Protection 215
7.1.3 Viewing Application Protection 216
7.1.4 Managing Application Protection Policies 218
7.1.5 Disabling Application Protection 222
7.2 WTP 222
7.2.1 WTP Overview 222
7.2.2 Enabling Web Tamper Protection 225
7.2.3 Adding a Protected Directory 227
7.2.4 Configuring Remote Backup 231
7.2.5 Enabling Dynamic WTP 233
7.2.6 Viewing WTP Events 234
7.2.7 Adding a Privileged Process 235
7.2.8 Enabling/Disabling Scheduled Static WTP 236
7.3 Ransomware Prevention 237
7.3.1 Ransomware Prevention Overview 237
7.3.2 Enabling Ransomware Prevention 238
7.3.3 Enabling Backup 242
7.3.4 Viewing and Handling Ransomware Prevention Events 244
7.3.5 Managing Ransomware Protection Policies 245
7.3.6 Restoring Server Data 249
7.3.7 Managing Server Backup 251
7.3.8 Disabling Ransomware Prevention 255
7.4 Application Process Control 255
7.4.1 Application Process Control Overview 256
7.4.2 Creating a Whitelist Policy 257
7.4.3 Confirming Learning Outcomes 260
7.4.4 Enabling Application Process Control 261
7.4.5 Checking and Handling Suspicious Processes 262

7.4.6 Extending the Process Whitelist....263
7.4.7 Start Learning on Servers Again....263
7.4.8 Disabling Application Process Control....264
7.5 File Integrity Monitoring....266
7.5.1 File Integrity Management Overview....266
7.5.2 Viewing File Change Records....267
7.6 Virus Scan....269
7.6.1 Virus Scan Overview....269
7.6.2 Scanning for Viruses....271
7.6.3 Viewing and Handling Viruses....279
7.6.4 Managing Custom Antivirus Policies....282
7.6.5 Managing Isolated Files....285
7.7 Dynamic Port Honeypot....286
7.7.1 Dynamic Port Honeypot Overview....286
7.7.2 Creating a Protection Policy for a Dynamic Honeypot Port....288
7.7.3 Viewing and Handling Honeypot Protection Events....290
7.7.4 Managing Dynamic Port Honeypot Protection Policies....293
7.7.5 Managing Associated Servers....295

8 Container Protection....297

8.1 Container Firewalls....297
8.1.1 Container Firewall Overview....297
8.1.2 Configuring a Network Defense Policy (for a Container Tunnel Network)....300
8.1.3 Configuring a Network Defense Policy (for a VPC Network)....303
8.2 Container Cluster Protection....305
8.2.1 Container Cluster Protection Overview....305
8.2.2 Enabling Container Cluster Protection....306
8.2.3 Configuring a Container Cluster Protection Policy....307
8.2.4 Checking Container Cluster Protection Events....309
8.2.5 Disabling Container Cluster Protection....310

9 Detection and Response....312

9.1 HSS Alarms....312
9.1.1 Server Alarms....312
9.1.2 Viewing Server Alarms....328
9.1.3 Handling Server Alarms....334
9.1.4 Exporting Server Alarms....336
9.1.5 Managing Isolated Files....337
9.2 Container Alarms....338
9.2.1 Container Alarm Events....338
9.2.2 Viewing Container Alarms....346
9.2.3 Handling Container Alarms....350
9.2.4 Exporting Container Alarms....352
9.3 Whitelist Management....352

9.3.1 Managing the Login Whitelist ... 352
9.3.2 Managing the Alarm Whitelist ... 354
9.3.3 Managing the System User Whitelist ... 356
10 Security Operations ... 358
10.1 Policy Management ... 358
10.1.1 Policy Management Overview ... 358
10.1.2 Configuring Policies ... 365
10.1.3 Creating a Custom Policy Group ... 391
10.1.4 Deleting a Custom Policy Group ... 393
10.2 Handling History ... 394
10.3 Container Audit ... 394
10.3.1 Container Audit Overview ... 394
10.3.2 Viewing Container Audit Logs ... 395
10.4 Security Report ... 396
10.4.1 Security Report Overview ... 396
10.4.2 Creating a Security Report ... 397
10.4.3 Checking a Security Report ... 398
10.4.4 Managing Security Reports ... 400
10.5 Free Health Check ... 401
11 Installation and Configuration ... 404
11.1 Installation and Configuration on Servers ... 404
11.1.1 Agent Management ... 404
11.1.1.1 Agent Overview ... 404
11.1.1.2 Installing the Agent on a Server ... 405
11.1.1.3 Upgrading the Agent ... 407
11.1.1.4 Uninstalling the Agent ... 408
11.1.2 Security Configurations ... 410
11.1.2.1 Configuring Common Login Locations ... 411
11.1.2.2 Configuring Common Login IP Addresses ... 411
11.1.2.3 Configuring an SSH Login IP Address Whitelist ... 412
11.1.2.4 Isolating and Killing Malicious Programs ... 413
11.1.3 Enabling 2FA ... 414
11.2 Installation and Configuration on Containers ... 415
11.2.1 Cluster Management ... 415
11.2.1.1 Modifying Cluster Agent Installation Information ... 416
11.2.1.2 Upgrading or Uninstalling the Agent from a Cluster ... 417
11.2.1.3 Viewing the Cluster Node List and Permission List ... 418
11.2.2 Independent Node Management ... 419
11.2.2.1 Installing the Agent on an Independent Node ... 419
11.2.2.2 Upgrading or Uninstalling the Agent from an Independent Node ... 421
11.2.3 Connecting to a Third-party Image Repository ... 423
11.3 Alarm Configuration ... 426

11.4 Authorization....436
11.5 Plug-in Settings....438
11.5.1 Plug-Ins Overview....438
11.5.2 Viewing Plug-in Information....439
11.5.3 Installing a Plug-in....440
11.5.4 Uninstalling a Plug-in....441
12 Monitoring and Auditing....443
12.1 Cloud Eye Monitoring....443
12.1.1 HSS Metrics....443
12.1.2 Monitored HSS Events....444
12.1.3 Configuring a Monitoring Alarm Rule....445
12.1.4 Viewing Monitoring Metrics....449
12.2 CTS Auditing....449
12.2.1 HSS Operations Supported by CTS....449
13 FAQs....453
13.1 About HSS....453
13.1.1 What Is Host Security?....453
13.1.2 What Is Container Security?....454
13.1.3 What Is Web Tamper Protection?....454
13.1.4 What Are the Relationships Between Images, Containers, and Applications?....456
13.1.5 Is HSS in Conflict with Any Other Security Software?....456
13.1.6 What Are the Differences Between HSS and WAF?....456
13.1.7 What Is the HSS Agent?....457
13.1.8 Can HSS Automatically Detect and Remove Viruses?....458
13.2 Agent....458
13.2.1 Is the Agent in Conflict with Any Other Security Software?....458
13.2.2 How Do I Uninstall the Agent?....459
13.2.3 What Should I Do If Agent Installation Failed?....461
13.2.4 How Do I Fix an Abnormal Agent?....462
13.2.5 What Is the Default Agent Installation Path?....464
13.2.6 How Many CPU, Memory, and Disk Resources Are Occupied When the Agent Is Running?....464
13.2.7 Do Different HSS Editions Share the Same Agent?....466
13.2.8 How Do I View Servers Where No Agents Have Been Installed?....466
13.2.9 What Can I Do If the Agent Status Is Still "Not installed" After Installation?....466
13.2.10 What Do I Do If the Upgrade Fails?....467
13.2.11 What If I Do Not Upgrade to the New Version?....469
13.2.12 What Do I Do If I Cannot Access the Download Link of the Windows Or Linux Agent?....470
13.2.13 What Do I Do If Agent Upgrade Fails and the Message "File replacement failed" Is Displayed?....470
13.3 Vulnerability Management....471
13.3.1 How Do I Fix Vulnerabilities?....471
13.3.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?....471
13.3.3 Why a Server Displayed in Vulnerability Information Does Not Exist?....472

13.3.4 Do I Need to Restart a Server After Its Vulnerabilities Are Fixed? 472
13.3.5 What Do I Do If Vulnerability Fix Failed? 472
13.3.6 Why Can't I Select a Server During Manual Vulnerability Scanning or Batch Vulnerability Fixing? 482
13.4 Detection & Response 482
13.4.1 What Do I Do If My Servers Are Subjected to a Mining Attack? 483
13.4.2 Why a Process Is Still Isolated After It Was Whitelisted? 486
13.4.3 Why an Attack Is Not Detected by HSS? 487
13.4.4 Can I Unblock an IP Address Blocked by HSS, and How? 487
13.4.5 Why a Blocked IP Address Is Automatically Unblocked? 487
13.4.6 How Often Is Malware Scan and Removal? 487
13.4.7 What Do I Do If an IP Address Is Blocked by HSS? 488
13.4.8 How Do I Defend Against Ransomware Attacks? 488
13.4.9 How Do I Add High-risk Command Execution Alarms to the Whitelist? 488
13.5 Abnormal Logins 489
13.5.1 Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist? 489
13.5.2 How Do I Check the User IP address of a Remote Login? 490
13.5.3 How Do I Cancel the Alarm Notifications of Successful Server Logins? 491
13.5.4 Can I Disable Remote Login Detection? 491
13.5.5 How Do I Know Whether an Intrusion Succeeded? 492
13.6 Brute-force Attack Defense 492
13.6.1 How Does HSS Intercept Brute Force Attacks? 493
13.6.2 How Do I Handle a Brute-force Attack Alarm? 495
13.6.3 How Do I Defend Against Brute-force Attacks? 498
13.6.4 How Do I Unblock an IP Address? 499
13.6.5 What Do I Do If HSS Frequently Reports Brute-force Alarms? 499
13.6.6 What Do I Do If the Port in Brute-force Attack Records Is Not Updated? 501
13.7 Baseline Inspection 501
13.7.1 Why Are Weak Password Alarms Generated After the Weak Password Detection Policy Is Disabled? 501
13.7.2 How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS? 501
13.7.3 How Do I Set a Proper Password Complexity Policy in a Windows OS? 503
13.7.4 How Do I Handle Unsafe Settings? 504
13.7.5 How Do I View Configuration Check Reports? 505
13.7.6 How Do I Handle a Weak Password Alarm? 505
13.7.7 How Do I Set a Secure Password? 507
13.8 Web Tamper Protection 508
13.8.1 Why Do I Need to Add a Protected Directory? 508
13.8.2 How Do I Modify a Protected Directory? 508
13.8.3 What Should I Do If WTP Cannot Be Enabled? 509
13.8.4 How Do I Modify a File After WTP Is Enabled? 509
13.8.5 What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect? 510
13.8.6 What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF? 510

13.9 Container Security 511
13.9.1 How Do I Disable Node Protection? 512
13.9.2 How Do I Enable Node Protection? 512
13.9.3 How Do I Enable the API Server Audit for an On-Premises Kubernetes Container? 513
13.9.4 What Do I Do If the Container Cluster Protection Plug-in Fails to Be Uninstalled? 516
13.10 Security Configurations 519
13.10.1 What Can I Do If I Cannot Remotely Log In to a Server via SSH? 519
13.10.2 How Do I Use 2FA? 520
13.10.3 Why Can't I Receive a Verification Code After 2FA Is Enabled? 521
13.10.4 Why Does My Login Fail After I Enable 2FA? 522
13.10.5 How Do I Add a Mobile Number or Email Address for 2FA? 522
13.10.6 Can I Disable HSS Alarm Notifications? 523
13.10.7 How Do I Modify Alarm Notification Items? 523
13.10.8 How Do I Disable the SELinux Firewall? 524
13.11 Others 525
13.11.1 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Windows Server? 525
13.11.2 How Do I Check HSS Log Files? 525
13.11.3 How Do I Enable Logging for Login Failures? 527
13.11.4 How Do I Enable or Disable the Agent Self-protection Policy? 527
13.11.5 What Do I Do If HSS Self-Protection Cannot Be Disabled? 529
A Change History 530

1 Introduction

1.1 What Is HSS?

HSS is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It provides server security, container security, 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.

Server Security

Host Security Service (HSS) is designed to enhance server security through diverse functions, including asset management, vulnerability detection, baseline checks, intrusion detection, ransomware protection, and web tamper protection (WTP). HSS can comprehensively identify and manage information assets on servers, detect server risks in real time, and prevent intrusions, helping companies build a server security system and reduce 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.

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.

Component	Description
HSS cloud protection center	• 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	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10180 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. • If no agent is installed or the agent installed is abnormal, HSS is unavailable. • The agent can be installed on Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), on-premises IDC servers, and third-party cloud servers. • Web tamper protection, container security, and HSS share the same agent, so 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.

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, BMSs, on-premises IDC servers, and third-party cloud servers 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.

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

Server Security

- 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.

Container Security

- 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 container security 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.

1.4 Features

HSS comes in basic, enterprise, premium, web tamper protection, and container editions. It provides the following functions: **Dashboard**, **Asset Overview**, **Server Management**, **Container Management**, **Server Fingerprints**, **Container Fingerprints**, **Vulnerability Management**, **Baseline Check**, **Application Protection**, **Web Tamper Protection**, **Ransomware Protection**, **File Integrity Management**, **Virus Scanning**, **Dynamic Port Honeypot**, **Container Firewall**, **Application Process Control**, **Container Cluster Protection**, **Server Alarms**, **Container Alarms**, **Whitelist Management**, **Policy Management**, **Handling History**, **Security Reports**, **Container Audit**, **Installation and Configuration on Servers**. The functions supported by each edition are different. You can select a proper edition based on your service requirements.

- To protect test servers or individual users' servers, use the **basic edition. It can protect any number of servers, but only part of the security scan capabilities are available. This edition does not provide protection capabilities**.
- For servers that need to protect websites and key systems from tampering, the **WTP edition** is recommended.
- For containers that need to enhance image security and container runtime security, the container edition is recommended.
- 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 use the **premium or Web Tamper Protection edition**.

NOTE

- 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.
- The meanings of the symbols in the table are as follows:
  - √: supported
  - ×: not supported

Dashboard

Dashboard displays the overall security score and protection configuration of assets on the cloud, helping you learn about asset security status.

Table 1-2 Functions

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Dashboard	You can check the security score, risks, and protection overview of all your assets in real time, including servers and containers.	√	√	√	√	√

Assets

Asset management displays the asset status and their statistics.

Table 1-3 Assets

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Assets	Collect statistics on asset status and usage of all servers, including the agent status, protection status, quota status, and asset fingerprint.	√	√	√	√	√

Servers

Server management allows you to view and manage servers.

Table 1-4 Server management functions

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Servers	Manage all server assets, including their protection statuses, quotas, and policies. You can install agents on all the Linux servers in batches.	√	√	√	√	√

Containers

Container management allows you to view and manage servers in the dimension of the containers deployed on them, and to manage the security risks of container images and instances.

Table 1-5 Containers & Quota

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container node management	Manage all container nodes. You can enable or disable protection for container nodes and deploy protection policies.	×	×	×	×	√
Container images	Scan local images, third-party repository images, and SWR images, and check image scan results, vulnerabilities, and the suggestions for fixing abnormal configurations. Detect and resolve image security risks, so that insecure images will not be deployed in the production environment.	×	×	×	×	√
Container	Check container instance information and isolate or stop insecure container instances.	×	×	×	×	√

Server Fingerprints

Server fingerprints can collect asset information about ports, processes, web applications, web services, web frameworks, and auto-started items on servers. Users can use the server fingerprint function to centrally check asset information on servers and detect unsafe assets in a timely manner.

Table 1-6 Server fingerprint function

Check Item	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Accounts	Check and manage accounts in the current system all in one place. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every hour.	×	√	√	√	√
Open ports	Check open ports all in one place and identify high-risk and unknown ports. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every 30s.	×	√	√	√	√
Processes	Check running applications all in one place and identify malicious applications. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every hour.	×	√	√	√	√
Software	Check and manage server software all in one place and identify insecure versions. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every day.	×	√	√	√	√

Check Item	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Auto-started items	Check auto-started items and collect statistics on their changes in a timely manner. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every hour.	×	√	√	√	√
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. **Supported OSs**: Linux and Windows. **Scan time**: once a week (04:10 a.m. every Monday).	×	√	√	√	√
Web services	Check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux **Scan time**: once a week (04:10 a.m. every Monday).	×	√	√	√	√
Web frameworks	Check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	√	√	√	√

Check Item	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Websites	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. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	√	√	√	√
Middleware	Check information about servers, versions, paths, and processes associated with middleware. **Supported OSs**: Linux and Windows. **Scan time**: once a week (04:10 a.m. every Monday).	×	√	√	√	√
Databases	You can check details about the software that provides data storage, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux and Windows (MySQL only). **Scan time**: once a week (04:10 a.m. every Monday).	×	√	√	√	√

Container Fingerprints

Container fingerprints collect asset information such as accounts, ports, processes, clusters, services, and workloads in containers. You can use the container fingerprint function to centrally check asset information in containers and detect unsafe assets in a timely manner.

Table 1-7 Asset fingerprints

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Accounts	Check and manage container accounts all in one place. **Supported OSs**: Linux. **Scan time**: automatic scan every hour.	×	×	×	×	√
Open ports	Check container open ports all in one place and identify high-risk and unknown ports. **Supported OSs**: Linux. **Scan time**: automatic scan every 30s.	×	×	×	×	√
Process	Check running applications all in one place and identify malicious applications. **Supported OSs**: Linux. **Scan time**: automatic scan every hour.	×	×	×	×	√
Installed software	Check and manage container software all in one place and identify insecure versions. **Supported OSs**: Linux. **Scan time**: automatic scan every day.	×	×	×	×	√
Auto-started items	Check auto-started items and collect statistics on their changes in a timely manner. **Supported OSs**: Linux. **Scan time**: automatic scan every hour.	×	×	×	×	√
Web application	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Web service	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	√
Web frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	√
Website	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. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	√
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Database	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	√
Clusters	Collect statistics on and display cluster details. You can view the type, node, version, and status of all clusters. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	√
Services	Collect statistics on and display details about services and breakpoints. You can view information about all services, such as namespaces and clusters to which the services belong. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	√
Workloads	Collect statistics on and display details about workloads (StatefulSets, deployments, DaemonSets, normal jobs, cron jobs, and container groups). You can view the status, number of instances, and namespace of all workloads. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container instances	Collect statistics on and display container instance details. You can view the status, pods, and clusters of all container instances. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	√

Vulnerability Management

Vulnerability management detects Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities and emergency vulnerabilities, helping users identify potential risks.

Table 1-8 Vulnerabilities

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
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. **Supported OSs**: Linux. **Scan time**: automatic scan (every day by default), scheduled scan (once a week by default, not supported in the basic edition), and manual scan at any time (not supported in the basic edition).	√	√	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Windows vulnerability detection	Detect vulnerabilities in Windows OS based on the official patch releases of Microsoft. **Supported OSs**: Windows. **Scan time**: automatic scan (every day by default), scheduled scan (once a week by default, not supported in the basic edition), and manual scan at any time (not supported in the basic edition).	√	√	√	√	×
Web-CMS vulnerability detection	Scan for Web-CMS vulnerabilities in web directories and files. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan (every day by default), scheduled scan (once a week by default), and manual scan at any time.	×	√	√	√	√
Application vulnerability detection	Detect vulnerabilities in JAR packages, ELF files, and other files of open source software, such as Log4j and spring-core. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan (every Monday by default), scheduled scan (once a week by default), and manual scan at any time.	×	√	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Emergency vulnerability detection	Checks whether the software and any dependencies running on the server have vulnerabilities through version comparison and POC verification. Reports risky vulnerabilities to the console and provides vulnerability alarms for you. **Supported OSs**: Linux and Windows. **Scan time**: scheduled scan (which needs to be manually enabled) and manual scan at any time.	×	√	√	√	√

Baseline Inspection

Baseline inspection can scan risky configurations, weak passwords, and password complexity policies of server systems and key software. The supported detection baselines include security practices. You can customize sub-baseline items and fix vulnerability risks.

Table 1-9 Baseline checks

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Password complexity policies	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security. **Supported OSs**: Linux. **Scan time**: automatic scan in the early morning every day and manual scan at any time.	√	√	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Common weak passwords	Change weak passwords to stronger ones based on HSS scan results and suggestions. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan in the early morning every day and manual scan at any time.	√	√	√	√	√
Baseline check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan in the early morning every day and manual scan at any time.	×	√	√	√	√

Container Image Security

Container image security allows you to scan the image repository and running container images, detect vulnerabilities and malicious files in the images, and provide suggestions to secure your images.

Table 1-10 Container images

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
SWR image repository vulnerabilities	Detect system and application vulnerabilities in SWR image repository based on a vulnerability database and handle critical vulnerabilities in a timely manner. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Viewing Malicious File Detection Results	Scan images for malicious files (such as Trojans, worms, viruses, and adware) and identify risks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Application Protection

Application protection provides security defense for 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.

Table 1-11 Application protection

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
SQL injection	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities. **Supported OSs**: Linux **Scan time**: real-time detection.	×	×	√	√	√
OS command injection	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities. **Supported OSs**: Linux **Scan time**: real-time detection.	×	×	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
XSS	Detect and defend against stored cross-site scripting (XSS) injection attacks. **Supported OSs**: Linux **Scan time**: real-time detection.	×	×	√	√	√
Log4j RCE vulnerability	Detect and defend against remote code execution and intercept attacks. **Supported OSs**: Linux **Scan time**: real-time detection.	×	×	√	√	√
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. **Supported OSs**: Linux **Scan time**: real-time detection.	×	×	√	√	√
Memory injection	Detect and defend against memory injection attacks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
XXE	Detect and defend against XML External Entity Injection (XXE) attacks, and check web applications for related vulnerabilities. **Supported OSs**: Linux **Scan time**: real-time detection.	×	×	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Deserialization input	Detect deserialization attacks that exploit unsafe classes. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
File directory traversal	Check whether sensitive directories or files are accessed. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
Struts2 OGNL	Detect OGNL code execution. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
Command execution using JSP	Detect command execution using JSP. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
File deletion using JSP	Detect file deletion using JSP. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
Database connection exception	Detect authentication and communication exceptions thrown by database connections. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
0-day vulnerability	Check whether the stack hash of a command is in the whitelist of the web application. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Security Manager permission exception	Detect exceptions thrown by SecurityManager. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√

Web Tamper Protection (WTP)

WTP can detect and prevent tampering of files in specified directories, including web pages, documents, and images, and quickly restore them using valid backup files.

Table 1-12 Web Tamper Protection

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Static WTP	Protect the static web page files on website servers from being tampered with. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	×
Dynamic WTP	Provide dynamic web tamper protection for Tomcat. Protect the dynamic web pages in website databases from being tampered with. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	√	×

Ransomware Prevention

Ransomware prevention supports user-defined ransomware prevention policies, using static and dynamic honeypots to identify attacks launched by known and unknown ransomware.

Table 1-13 Ransomware prevention

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Ransomware prevention	Help you identify some unknown ransomware attacks by using static and dynamic honeypot files. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√

Application Process Control

Application process control can detect malicious processes and generate alarms.

Table 1-14 Application process control

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Application Process Control	Learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√

Checking File Integrity

File integrity management checks and records changes to key files.

Table 1-15 File integrity monitoring

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
File integrity monitoring	Check the key files of the Linux system to detect the changes that may be exploited by attacks in a timely manner. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√

Virus Scan

Virus scan can detect virus files on the server, helping users eliminate potential malicious threats.

Table 1-16 Virus scan

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Virus scan	The function uses the virus detection engine to scan virus files on the server. The scanned file types include executable files, compressed files, script files, documents, images, and audio and video files. Users can perform quick scan and full-disk scan on the server as required. Customize scan tasks and handle detected virus files in a timely manner to enhance the virus defense capability of the service system. **Supported OSs**: Linux and Windows. **Scan time**: manual scan at any time.	×	√	√	√	√

Dynamic Port Honeypot

The **dynamic port honeypot** function uses real ports as honeypot ports to induce attackers to access the intranet. In the horizontal penetration scenario, the function can effectively detect attackers' scanning and identify faulty servers.

Table 1-17 Function

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Dynamic port honeypot	The dynamic port honeypot function is a proactive defense measure. It uses a real port as a honeypot port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√

Container Firewalls

Container firewalls protect container runtime.

Table 1-18 Container firewall

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container firewall	Control and intercept network traffic inside and outside a container cluster to prevent malicious access and attacks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Container Cluster Protection

Container cluster protection can detect non-compliant baselines issues, vulnerabilities, and malicious files in images to prevent insecure container images from being deployed in clusters.

Table 1-19 Container cluster protection

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container cluster protection	Check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Server Alarms

Server intrusion detection identifies and prevents intrusion to servers, discover risks in real time, detect and kill malicious programs, and identify web shells and other threats.

Table 1-20 Server alarm function

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojan, mining software, worms, and viruses. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Virus	Check servers in real time and report alarms for viruses detected on servers. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Worm	Detect and kill worms on servers and report alarms. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
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. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Botnet	Detect whether zombie programs that have been spread exist in servers and report alarms immediately after detecting them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Backdoor	Detect backdoors in the server system in real time and report alarms immediately after detecting them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√
Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√
Hacker tool	Check whether non-standard tool used to control the server exist and report alarms immediately after detecting them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Web shell	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. • Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. • You can use the manual detection function to detect web shells on servers. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Mining software	Detect whether mining software exists on servers in real time and report alarms for the detected software. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Remote code execution	Check whether the server is remotely called in real time and report an alarm immediately once remote code execution is detected. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Reverse shell	Monitor user process behaviors in real time to report alarms on and block reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. Currently, the following types of reverse shells can be blocked: exec reverse shell, Perl reverse shell, AWK reverse shell, Python reverse shell.b, Python reverse shell.a, Lua reverse shell, mkfifo/openssl reverse shell, PHP reverse shell, Ruby reverse shell, rssocks reverse proxy, Bash reverse shell, Ncat reverse shell, exec redirection reverse shell, Node reverse shell, Telnet dual-port reverse shell, nc reverse shell, Socat reverse shell, rm/mkfifo/sh/nc reverse shell, and socket/tchsh reverse shell. **Supported OSs**: Linux. **Scan time**: real-time detection. **NOTE** To enable automatic reverse shell blocking, ensure the following conditions are met: 1. In the **HIPS Detection** policy, **Automatic Blocking** is enabled. This function is disabled by default. You need to manually enable it. 2. Ensure the function of isolating and killing malicious programs is enabled. This function is disabled by default. You need to manually enable it.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
File privilege escalation	Check the file privilege escalations in your system. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√
Process privilege escalation	The following process privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√
Important file change	Receive alarms when critical system files are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√
File/ Directory change	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Abnormal process behavior	Check server process information, including the process ID, command line, process path, and behavior. If a process crashes, consumes too many resources, or establishes network connections unexpectedly, an alarm is generated. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
High-risk command execution	Check executed commands in real time and generate alarms if high-risk commands are detected. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
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. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√
Sensitive file access	Detect the unauthorized access to or modifications of sensitive files. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Suspicious crontab 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. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√
System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	×
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. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
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. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	√
System log deletion	An alarm is generated when a command or tool is used to clear system logs. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	×
Suspicious command execution	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Suspicious process execution	Detect and report alarms on unauthenticated or unauthorized application processes. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√
Brute-force attack	Check for brute-force attack attempts and successful brute-force attacks. • Detect password cracking attacks on accounts and block attacking IP addresses to prevent server intrusion. • Trigger an alarm if a user logs in to the server by a brute-force attack. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√
Abnormal login	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√
Invalid account	Scan accounts on servers and list suspicious accounts in a timely manner. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
User account added	Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	√
Password theft	Detect the abnormal obtaining of hash value of system accounts and passwords on servers and report alarms. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Cloud honeypot	An alarm is reported if a connection to the honeypot port of a server is detected. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√
Abnormal outbound connection	Report alarms on suspicious IP addresses that initiate outbound connections. **Supported OSs**: Linux (kernel 5.10 or later). **Scan time**: real-time detection.	×	√	√	√	√
Port forwarding	Report alarms on port forwarding using suspicious tools. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	×
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. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	√	√	√	×
Port scan	Detect scanning or sniffing on specified ports and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√
Server scan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√

Container Alarms

Container alarms can detect intrusion behaviors of Docker and Containerd engines. Scan running containers for malicious programs including miners and ransomware; detect non-compliant security policies, file tampering, and container escape; and provide suggestions.

Table 1-21 Container alarm function

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Unclassified malware	Check and handle malicious programs in a container, including web shells, Trojan, mining software, worms, and viruses. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Ransomware	Check and handle alarms on ransomware in containers. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Hacker tool	Check for non-standard tools used to control containers in the container runtime, and report alarms immediately after detecting them. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√
Web shell	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Vulnerability escape detection	An escape alarm is reported if a container process behavior that matches the behavior of known vulnerabilities is detected. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
File escape detection	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. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Reverse shell	Monitor user process behaviors in a container environment in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
File privilege escalation	Check the file privilege escalations in the container system. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Process privilege escalation	The following process privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Important file change	Receive alarms when critical system files are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Abnormal process behavior	Check container process information, including the process ID, command line, process path, and behavior. If a process crashes, consumes too many resources, or establishes network connections unexpectedly, an alarm is generated. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Abnormal container process	• Malicious container program detection 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 processes The service reports an alarm if it detects that a process not in the whitelist is running in the container. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Abnormal container startup	The service monitors container startups and reports an alarm if it detects that a container with too many permissions is started. Container check items include: ● 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:[...]**) **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
High-risk command execution	Check executed commands in containers and generate alarms if high-risk commands are detected. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
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. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Sensitive file access	The service monitors the container image files associated with file protection policies, and reports an alarm if the files are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
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. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Suspicious command execution	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
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. **Supported OSs**: Linux. **Scan time**: real-time detection. **NOTE** Currently, brute-force attacks can be detected only in the Docker runtime.	×	×	×	×	√
Invalid account	Detect suspicious accounts and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Password theft	Detect the abnormal obtaining of hash value of system accounts and passwords on servers in a container environment and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Abnormal outbound connection	Report alarms on suspicious IP addresses in a container environment that initiate outbound connections. **Supported OSs**: Linux (kernel 5.10 or later). **Scan time**: real-time detection.	×	×	×	×	√

Alarm	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Port forwarding	Report alarms on port forwarding using suspicious tools in a container environment. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Kubernetes event deletion	Detect the deletion of Kubernetes events and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
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. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
User information enumeration	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√
Binding cluster role	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Whitelist Management

The whitelist function includes **Alarm whitelist**, **Login whitelist** and **System user whitelist**. To reduce false alarms, import events to and export events from the whitelist.

Table 1-22 Whitelists

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Alarm whitelist	You can add an alarm to the whitelist when handling it. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√
Login Whitelist	Add IP addresses and usernames to the Login Whitelist as needed. HSS will not report alarms on the access behaviors of these IP addresses and users. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√
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. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√

Policy Management

You can configure **policy management**, customize detection rules, and apply different policies to different servers, containers, or groups, easily adapting to your business scenarios.

Table 1-23 Policies

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Policy Management	You can define and issue different detection policies for different servers or server groups, implementing refined security operations. • Check the policy group list. • Create a policy group based on default and existing policy groups. • Define a policy. • Edit or delete a policy. • Modify or disable policies in a group. • Apply policies to servers in batches on the **Servers** page. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√ (Only the default enterprise policy group is supported.)	√	√	√

Handling History

Handling history displays the handling history of vulnerabilities and security alarms.

Table 1-24 Handling history

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Handling history	Check historical vulnerability and alarm handling records, including the handling time and handlers.	×	√	√	√	√

Security Report

The HSS can generate **Security reports** on user assets on a daily, weekly, or monthly basis.

Table 1-25 Security report

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Security Report	Check weekly or monthly server security trend, key security events, and risks.	×	√	√	√	√

Container Audit

Container audit monitors and records operations and activities of cluster containers and independent containers. You can view and analyze their logs on the HSS console.

Table 1-26 Container audit

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container audit	Keep track of the operations and activities in your container clusters, gaining insight into every phase of the container lifecycle, including creating, starting, stopping, and destroying containers. Find and handle security problems through audit and analysis in a timely manner, ensuring the security and stability of container clusters. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√

Installation and Configuration

Security configuration provides functions such as agent management, common login locations, common login IP addresses, SSH login IP address whitelist,

automatic isolation and removal of malicious programs, two-factor authentication, alarm configuration to meet server and container security requirements in different scenarios.

Table 1-27 Installation and configuration

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Agent management	You can view the agent status of all servers and upgrade, uninstall, and install agents. **Supported OSs**: Linux and Windows.	√	√	√	√	√
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. **Supported OSs**: Linux and Windows.	√	√	√	√	√
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. **Supported OSs**: Linux and Windows.	√	√	√	√	√
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. **Supported OSs**: Linux.	√	√	√	√	√

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Malicious program isolation and removal	HSS automatically isolates and kills identified malicious programs, such as web shells, Trojans, and worms, removing security risks. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√
Two-factor Authentication (2FA)	Prevent brute-force attacks by using password and SMS/email authentication. **Supported OSs**: Linux and Windows.	Pay per use: ×	√	√	√	√
Alarm configurations	After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers, containers, and web pages. **Supported OSs**: Linux and Windows.	√	√	√	√	√
Plug-in management	Install, uninstall, upgrade, and manage plug-ins in a unified manner. **Supported OSs**: Linux.	×	×	×	×	√
Container installation and configuration	Connect your clusters to HSS. Upgrade or uninstall the agent in your clusters or independent containers. **Supported OSs**: Linux.	√	√	√	√	√

HSS Self-protection

Self-protection protects HSS files and processes.

Table 1-28 HSS self-protection

Function	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Self-protection	Protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes. • Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. • Enabling the self-protection policy has the following impacts: – The HSS agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console. – HSS processes cannot be terminated. – In the agent installation path **C:\Program Files\HostGuard**, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded). **Supported OSs**: Windows.	×	×	√	√	×

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 efficiently manage 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 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 1-29 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	This role depends on the **Tenant Guest** and **BSS Administrator** roles.
HSS FullAccess	All HSS permissions	Policy	None
HSS ReadOnlyAccess	Read-only permission for HSS	Policy	None

WTP provides two types of user permissions by default: user management and resource management. User management permissions include permissions for managing users, user groups, and user group permissions. Resource management permissions include permissions for performing operations on cloud resources.

1.6 Constraints

Server Protection Restrictions

HSS can protect cloud servers. The following types of servers can be protected:

- Elastic Cloud Server (ECS)
- Bare Metal Server (BMS)
- On-premises data center (IDC)

OS Restrictions

Currently, the HSS agent and system vulnerability scan functions are not supported in certain OSs.

For details about the OS restrictions of HSS, see:

- **HSS restrictions on Windows (x86)**
- **HSS restrictions on Linux (x86)**
- **HSS restrictions on Linux (Arm)**

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.
- The meanings of the symbols in the table are as follows:
  - √: supported
  - ×: not supported

Table 1-30 HSS restrictions on Windows (x86)

OS	Agent	System Vulnerability Scan
Windows Server 2012 R2 Standard 64-bit English (40 GB)	√	√
Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	√	√
Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	√	√
Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	√	√
Windows Server 2016 Standard 64-bit English (40 GB)	√	√

OS	Agent	System Vulnerability Scan
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 2019 Datacenter 64-bit English (40 GB)	√	√
Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	√	√
Windows Server 2022 Datacenter 64-bit English (40 GB)	√	×
Windows Server 2022 Datacenter 64-bit Chinese (40 GB)	√	×
Windows Server 2022 Standard 64-bit English (40 GB)	√	×
Windows Server 2022 Standard 64-bit Chinese (40 GB)	√	×

Table 1-31 HSS restrictions on Linux (x86)

OS	Agent	System Vulnerability Scan
CentOS 7.4 (64-bit)	√	√
CentOS 7.5 (64-bit)	√	√
CentOS 7.6 (64-bit)	√	√
CentOS 7.7 (64-bit)	√	√
CentOS 7.8 (64-bit)	√	√
CentOS 7.9 (64-bit)	√	√
CentOS 8.1 (64-bit)	√	×
CentOS 8.2 (64-bit)	√	×
CentOS 8 (64-bit)	√	×
Debian 9 (64-bit)	√	√
Debian 10 (64-bit)	√	√
Debian 11 (64-bit)	√	√

OS	Agent	System Vulnerability Scan
Debian 12 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
EulerOS 2.2 (64-bit)	√	√
EulerOS 2.3 (64-bit)	√	√
EulerOS 2.5 (64-bit)	√	√
EulerOS 2.7 (64-bit)	√	×
EulerOS 2.9 (64-bit)	√	√
EulerOS 2.10 (64-bit)	√	√
EulerOS 2.11 (64-bit)	√	√
EulerOS 2.12 (64-bit)	√	√
Fedora 28 (64-bit)	√	×
Fedora 31 (64-bit)	√	×
Fedora 32 (64-bit)	√	×
Fedora 33 (64-bit)	√	×
Fedora 34 (64-bit)	√	×
Ubuntu 16.04 (64-bit)	√	√
Ubuntu 18.04 (64-bit)	√	√
Ubuntu 20.04 (64-bit)	√	√
Ubuntu 22.04 (64-bit)	√	√
Ubuntu 24.04 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
AlmaLinux 8.4 (64-bit)	√	√
AlmaLinux 9.0 (64-bit)	√	×

OS	Agent	System Vulnerability Scan
AlmaLinux 9.2 (64-bit)	√	×
AlmaLinux 9.4 (64-bit)	√	×
Rocky Linux 8.4 (64-bit)	√	×
Rocky Linux 8.5 (64-bit)	√	×
RockyLinux 8.6 (64-bit)	√	√
RockyLinux 8.10 (64-bit)	√	√
Rocky Linux 9.0 (64-bit)	√	×
RockyLinux 9.4 (64-bit)	√	√
RockyLinux 9.5 (64-bit)	√	√
HCE 1.1 CentOS-compatible edition (64-bit)	√	√
HCE 2.0 standard edition (64-bit)	√	√
SUSE Linux Enterprise Server 12 SP5 (64 bit)	√	√
SUSE Linux Enterprise Server 15 (64 bit)	√	×
SUSE Linux Enterprise Server 15 SP1 (64 bit)	√	√
SUSE Linux Enterprise Server 15 SP2 (64 bit)	√	√
SUSE Linux Enterprise Server 15 SP3 (64 bit)	√	×
SUSE Linux Enterprise Server 15.5 (64 bit)	√	×

OS	Agent	System Vulnerability Scan
SUSE Linux Enterprise Server 15 SP6 (64 bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Kylin V10 (64 bit)	√	√
Kylin V10 SP1 (64 bit)	√	√
Kylin V10 SP2 (64 bit)	√	√
Kylin V10 SP3 (64 bit)	√	×
UnionTech OS 1050u2e	√ **NOTE** Currently, file escape detection is not supported.	√

Table 1-32 HSS restrictions on Linux (Arm)

OS	Agent	System Vulnerability Scan
CentOS 7.4 (64-bit)	√	√
CentOS 7.5 (64-bit)	√	√
CentOS 7.6 (64-bit)	√	√
CentOS 7.7 (64-bit)	√	√
CentOS 7.8 (64-bit)	√	√
CentOS 7.9 (64-bit)	√	√
CentOS 8.0 (64-bit)	√	×
CentOS 8.1 (64-bit)	√	×
CentOS 8.2 (64-bit)	√	×
CentOS 9 (64-bit)	√	×
Debian 11 (64-bit)	√	√
Debian 12 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
EulerOS 2.8 (64-bit)	√	√
EulerOS 2.9 (64-bit)	√	√

OS	Agent	System Vulnerability Scan
EulerOS 2.10 (64-bit)	√	√
EulerOS 2.11 (64-bit)	√	√
EulerOS 2.12 (64-bit)	√	√
Fedora 29 (64-bit)	√	×
Ubuntu 18.04 (64-bit)	√	√
Ubuntu 20.04 (64-bit)	√	√
Ubuntu 22.04 (64-bit)	√	√
Ubuntu 24.04 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
NeoKylin Linux Advanced Server Operating System V7 (64-bit)	√	×
Kylin V10 (64 bit)	√	√
Kylin V10 SP1 (64 bit)	√	√
Kylin V10 SP2 (64 bit)	√	√
Kylin V10 SP3 (64 bit)	√	×
HCE 2.0 standard edition (64-bit)	√	√
UnionTech OS V20 (64-bit)	√	√ **NOTE** Only UnionTech OS V20 server editions E and D support system vulnerability scan.
UnionTech OS V20 1050e (64-bit)	√	√
UnionTech OS V20 1060e (64-bit)	√	√
RockyLinux 9.5 (64-bit)	√	√

OS	Agent	System Vulnerability Scan
CTyunOS 3-23.01 (64-bit)	√	√

Agent Restrictions

- If third-party security software is installed on the server, uninstall the software before installing the HSS agent. If the third-party security software is incompatible with the HSS agent, the HSS protection functions will be affected.
- After the agent is installed on the server or container node, the agent may modify the following system files or configurations:
  - Linux system files:
    - /etc/hosts.deny
    - /etc/hosts.allow
    - /etc/rc.local
    - /etc/ssh/sshd_config
    - /etc/pam.d/sshd
    - /etc/docker/daemon.json
    - /etc/sysctl.conf
    - /sys/fs/cgroup/cpu/ (A subdirectory will be created for the HSS process in this directory.)
    - /sys/kernel/debug/tracing/instances (A CSA instance will be created in this directory.)
  - Linux system configurations: iptables rules
  - Windows system configurations:
    - Firewall rules
    - System login event audit policy and the configuration of login security layer and authentication mode
    - Windows Remote Management trusted server list

Restrictions on Brute-force Attack Defense

- Before you enable protection for a Windows server, enable the Windows firewall to block the source IP addresses of brute-force attacks. If the Windows firewall is not enabled, HSS only generates alarms for detected brute-force attacks, but does not block them.
  - After the Windows firewall is enabled, HSS automatically adds firewall rules **hostguard_AllowAnyIn** and **hostguard_AllowAnyOut** to allow all

inbound and outbound traffic, so that the firewall will not affect your services. If HSS detects a brute-force attack, it adds an inbound rule to the firewall to block the attack source IP address. This does not affect your servers.

- Do not disable the Windows firewall when using HSS, or HSS cannot block the source IP addresses of brute-force attacks. Once it is disabled, HSS may fail to block the attack source IP addresses even after you manually enable it again.

- Brute-force attack detection does not support Debian 12, Ubuntu 24.04, or SUSE Linux Enterprise Server 15 SP6.

1.7 Related Services

ECS

The HSS agent can be installed on ECS.

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

Cloud Container Engine (CCE)

CCE can rapidly build a highly reliable container cluster based on cloud servers and add nodes to the cluster for management. HSS can install Hostguard-agent on the nodes to protect the container applications deployed on them.

NOTE

CCE is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily set up a container runtime environment on the cloud. For more information, see the *Cloud Container Engine User Guide*.

Software Repository for Container (SWR)

Software Repository for Container (SWR) is a service that supports lifecycle management for container images. It provides simple, easy-to-use, secure, and reliable image management functions, helping you quickly deploy containerized services. For more information, see *SoftWare Repository for Container User Guide*. HSS scans for vulnerabilities and configurations in container images to help you detect the container environment that cannot be achieved by traditional security software.

Simple Message Notification (SMN)

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

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

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

Identity and Access Management

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

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

Cloud Trace Service (CTS)

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

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

1.8 Basic Concepts

Account Cracking

In account cracking, intruders use diverse methods, such as brute-force attacks and dictionary attacks, to obtain system or application accounts and passwords. Once an account is cracked, intruders may log in to the system without authorization, steal data, and damage the system.

Baseline

A baseline specifies the minimum security configuration requirements for OSs, databases, middleware, and applications in terms of account management, password policy configuration, authorization management, service management, configuration management, network configuration, and permission management.

Weak Password

A weak password can be easily cracked. Once the password is cracked, attackers can directly log in to the system and read, tamper with, or damage system data.

Malicious Program

Malicious programs are designed to attack or remotely control a system. They can be categorized into backdoors, Trojans, worms, and viruses, based on the way they spread. 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. 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.

Alarms

Security alarms refer to the events reported and recorded by HSS when it detects security threats (such as malicious programs and vulnerability exploits) on servers or containers. They notify users of potential security risks in a timely manner and prompt users to take measures to eliminate the risks, thereby improving the overall system security.

Two-Factor Authentication

Two-factor authentication (2FA) refers to user login authentication using both the user password and a verification code. This enhances account security.

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 is a combination of cloud resources, such as cloud servers (nodes) and load balancers, for container running. A cluster can be seen as one or more elastic cloud servers (nodes) in a same subnet. It provides compute resources for running containers.

Node

A node is a server (a VM or PM) that containers run on.

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. During the development, deployment, and running of images, security risks may be introduced, such as known or unknown vulnerabilities and malicious files. If such images are used in the production environment without security check, the system will be highly vulnerable to intrusions, which may cause serious consequences such as data leakage and resource abuse. Therefore, image security is critical to containerized application deployment.

Pod

A pod in Kubernetes is the smallest, basic unit for deploying applications or services. It can contain one or more containers, which typically share storage and networks.

Container

A container is an instance created using an image. Multiple containers can run on a node (host). Containers are essentially processes, but they run in their own separate namespaces, unlike processes that directly run on the host machine.

Container Runtime

Container runtime, one of the most important components of Kubernetes, manages the lifecycle of images and containers. Kubelet interacts with a container runtime through the Container Runtime Interface (CRI) to manage images and containers.

Project

Projects in IAM are used to group and isolate OpenStack resources (computing resources, storage resources, and network resources). Resources in your account must be mounted under projects. A project can be a department or a project team. Multiple projects can be created under an account.

2 Using IAM to Grant Access to HSS

2.1 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.

Prerequisite

Before authorizing permissions to a user group, you need to know which HSS permissions can be added to the user group. **Table 2-1** describes the policy details.

Table 2-1 System-defined permissions supported by HSS

Role/Policy Name	Description	Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS	System-defined role	• It depends on the **Tenant Guest** role. Tenant Guest: A global role, which must be assigned in the global project.
HSS FullAccess	All HSS permissions	System-defined policy	None

Role/Policy Name	Description	Type	Dependency
HSS ReadOnlyAccess	Read-only permission for HSS	System-defined policy	None

Authorization Process

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

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

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

   a. In the service list, choose HSS. The **Dashboard** page is displayed.

   b. Choose a service other than HSS from the service list. A message is displayed indicating that the user does not have the permission.

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

2.2 HSS Custom Policies

Custom policies can be created to supplement the system-defined policies of HSS.

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"
            ]
        },
    ]
}
```

- 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"
            ]
        }
    ]
}
```

2.3 HSS Actions

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

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

You can grant users permissions by using roles and policies. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. IAM uses policies to perform fine-grained authorization. A policy defines

permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

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

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

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

Actions

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

Permission	Action	Related Action
Query the vulnerability list	hss:vuls:list	-
Perform batch operations on vulnerabilities	hss:vuls:operate	-
Query the account list	hss:accounts:list	-
Query the software list	hss:softwares:list	-
Query the web path list	hss:webdirs:list	-
Query the process list	hss:processes:list	-
Query configuration scan reports	hss:configDetects:list	-
Query web shell scan results	hss:Webshells:list	-
Query risky account scan reports	hss:riskyAccounts:list	-
Obtain server risk statistics	hss:riskyDashboard:get	-
Query password complexity policy scan reports	hss:complexityPolicys:list	-
Perform batch operations on malicious programs	hss:maliciousPrograms:operate	-
Perform batch operations on open ports	hss:ports:operate	-
Perform operations on detected unsafe settings	hss:configDetects:operate	-
Perform batch operations on web shells	hss:Webshells:operate	-
Configure common login locations	hss:commonLocations:set	-
Query common login locations	hss:commonLocations:list	-

Permission	Action	Related Action
Configure common login IP addresses	hss:commonIPs:set	-
Query common login IP addresses	hss:commonIPs:list	-
Configure the login IP address whitelist	hss:whiteIps:set	-
Query the login IP address whitelist	hss:whiteIps:list	-
Configure weak passwords	hss:weakPwds:set	-
Query weak passwords	hss:weakPwds:get	-
Configure web paths	hss:webDirs:set	-
Query web paths	hss:webDirs:get	-
Obtain the list of servers where 2FA is enabled	hss:twofactorAuth:list	-
Enable 2FA	hss:twofactorAuth:set	-
Enable or disable automatic isolation and killing of malicious programs	hss:automaticKillMp:set	-
Query the programs that have been automatically isolated and killed	hss:automaticKillMp:get	-
Query the agent download address	hss:installAgent:get	-
Uninstall an agent	hss:agent:uninstall	-
Query HSS alarms	hss:alertConfig:get	-
Configure HSS alarms	hss:alertConfig:set	-
Query the WTP list	hss:wtpHosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Enable or disable WTP	hss:wtpProtect:switch	-
Configure backup servers	hss:wtpBackup:set	-

Permission	Action	Related Action
Query backup servers	hss:wtpBackup:get	-
Configure protected directories	hss:wtpDirectorys:set	-
Query the protected directory list	hss:wtpDirectorys:list	-
Query WTP records	hss:wtpReports:list	-
Configure privileged processes	hss:wtpPrivilegedProcess:set	-
Query the privileged process list	hss:wtpPrivilegedProcess-es:list	-
Configure a protection mode	hss:wtpProtectMode:set	-
Query the protection mode	hss:wtpProtectMode:get	-
Configure a protected file system	hss:wtpFilesystems:set	-
Query the protected file system list	hss:wtpFilesystems:list	-
Configure scheduled protection	hss:wtpScheduledProtec-tions:set	-
Query scheduled protection	hss:wtpScheduledProtec-tions:get	-
Configure WTP alarms	hss:wtpAlertConfig:set	-
Query WTP alarms	hss:wtpAlertConfig:get	-
Query WTP statistics	hss:wtpDashboard:get	-
Query policy group	hss:policy:get	-
Configure a policy group	hss:policy:set	-
Query the detected intrusion list	hss:event:get	-
Perform operations on intrusions	hss:event:set	-
Query server groups	hss:hostGroup:get	-
Configure server groups	hss:hostGroup:set	-
Monitor file integrity	hss:keyfiles:set	-

Permission	Action	Related Action
Query important file change reports	hss:keyfiles:list	-
Query the auto-startup list	hss:launch:list	-

3 and Accessing HSS

3.1 Access Process

This section describes how to connect servers and containers to HSS for protection when you use HSS for the first time.

HSS provides asset management, vulnerability detection, baseline check, intrusion detection, ransomware protection, and web tamper protection functions to comprehensively identify security risks in servers and containers, prevent intrusions, and help you build a secure server and container environment.

Access Process

Perform the following operations to connect a server or container to HSS.

Table 3-1 Access process description

No.	Step	Description
1	• **Installing the Agent on Servers** • **Installing the Agent on Containers**	The HSS agent is a piece of software installed on cloud servers to exchange data between the servers and HSS, implementing security check and protection for servers and containers. You can use HSS only after installing the agent.
2	**Enabling Protection**	

3.2 Installing the Agent on Servers

3.2.1 Installing the Agent on Cloud Platform Servers

Scenario

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

Prerequisites

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

Agent Installation Modes

HSS supports two installation modes. For details about their differences, see **Table 3-2**.

Table 3-2 Installation modes

Agent Installation Mode	Description	Scenario
GUI	It is easy and more efficient than installing the agent using commands. To install the agent in this mode, you simply need to provide HSS with the server username-password pair or key. HSS does not store the password file you upload.	There is at least one server with an online agent in the VPC of the servers where the agent is to be installed.
Commands or script	You need to log in to the server and run commands or a script to install the agent. This method is more complex and slower than installation through the GUI.	• Install the agent for the first time. • There are no servers with an online agent in the VPC of the servers where the agent is to be installed.

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

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

Step 10 Enter a username and password as prompted.

- Linux

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

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

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

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

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

- Windows

  Enter a username and its password.

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

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

----End

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

Step 9 Upload the installation template.

1. Click **Download Template** to download the batch installation template to your local PC.
2. Open the downloaded file, fill in server information as required, and save the file.
3. Click **Select File** and upload the file.

   HSS will automatically match the servers based on IP addresses. If the matching fails, you can click **View Failed Servers** and check the failure cause.

Step 10 Select servers.

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

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

----End

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

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

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

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

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

----End

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

Step 9 Upload the installation template.

1. Click **Download Template** to download the batch installation template to your local PC.
2. Open the downloaded file, fill in server information as required, and save the file.
3. Click **Select File** and upload the file.

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

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

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

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

----End

Using Commands to Install the Agent on a Cloud Platform Linux Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

Step 9 Install the agent as prompted.

1. On the console page, click in the **Install HSS Agent** dialog box to copy the installation command.
2. Log in to the server as the **root** user and paste the installation command.

   If the command output shown in **Figure 3-1** is displayed, the agent has been installed.

   Figure 3-1 Agent installed

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

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

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

----End

Using Commands to Install the Agent on Multiple Cloud Platform Linux Servers

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

Step 9 Install the agent as prompted.

Perform the following operations on any server:

1. On the console, click **linux-host-list.csv** in the **Install HSS Agent** dialog box to download the template.
2. Enter the server information based on the requirements in the **linux-host-list.csv** template and save the template.

   Ensure that the entered server verification information is consistent with the verification mode selected in **Step 8**.
3. Use the **root** account to remotely log in to any target server.
4. Use the SSH client to upload the **linux-host-list.csv** file to the **/tmp** directory on the server.
5. Return to the HSS console. In the **Install HSS Agent** dialog box, click to copy the installation command.
6. Paste and run the installation command on the server to install the agent.

   If the information shown in **Figure 3-2** is displayed, the installation is complete.

Figure 3-2 Agent installed

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

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

----End

Using the Script to Install the Agent on a Cloud Platform Windows Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

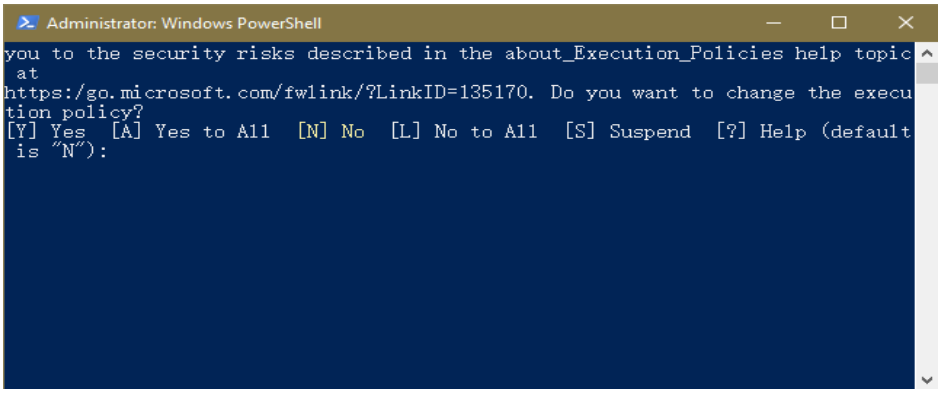
- **Install Mode**: Select **Command**.
- **Server OS**: Select **Windows**.
- **Scale**: Select **Single**.

Step 9 Install the agent as prompted.

1. On the console, click **installAgent.ps1** in the **Install HSS Agent** dialog box to download the installation script.
2. Log in as user **Administrator** to the server where the agent is to be installed.
3. Copy the **installAgent.ps1** file to the **C:\Users** directory of the server where the agent is to be installed.
4. Right-click **installAgent.ps1** and choose **Run with PowerShell**.
5. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

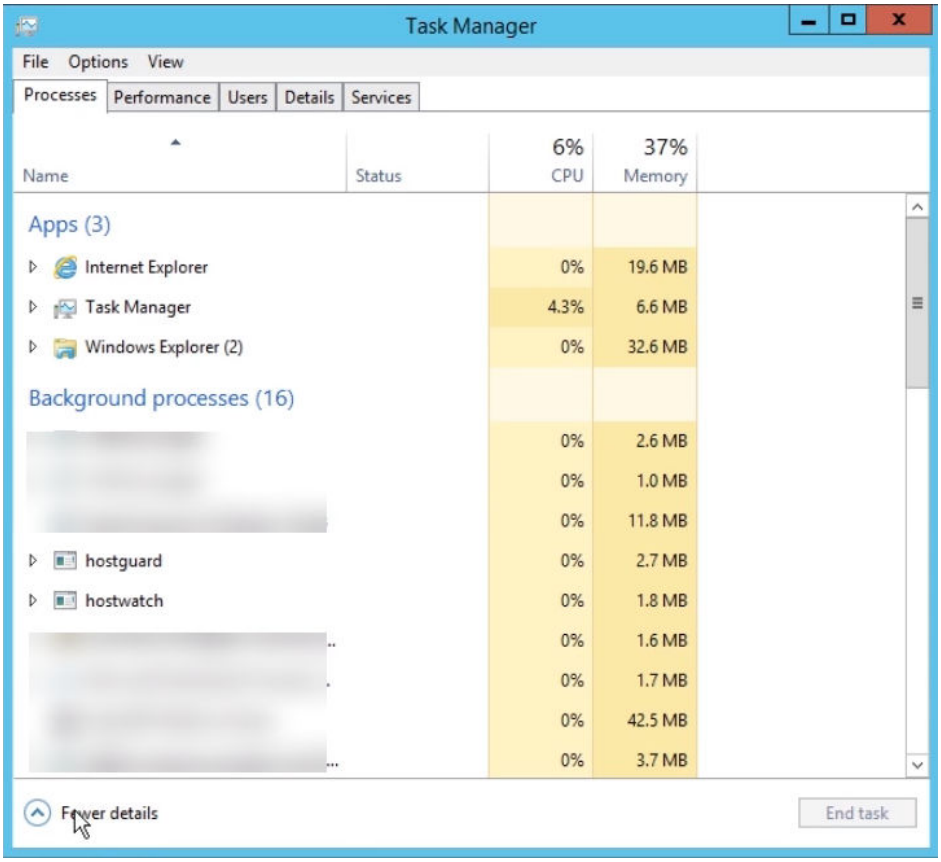
   If no dialog box is displayed, skip this step.

Figure 3-3 Changing the execution policy



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

Figure 3-4 Agent installed



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

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

----End

Using the Script to Install the Agent on Multiple Cloud Platform Windows Servers

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

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

Step 8 Configure installation parameters as follows:

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

Step 9 Install the agent as prompted.

⚠ CAUTION

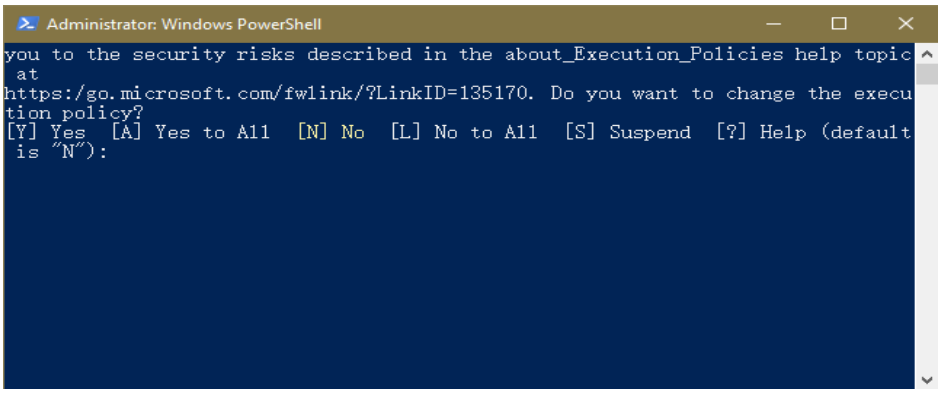
- Perform the following operations on any server.
- To install the agent, the server where the script is executed needs to access the port 5985 on other servers. Modify the inbound rules of the security groups on those servers to allow such access, or HSS will temporarily modify their security group rules while installing the agent. After the agent is installed, the modified settings will be deleted.

---

1. On the console, click **windows-host-list.xlsx** in the **Install HSS Agent** dialog box to download the template to the local PC.
2. Enter server information based on the requirements in the **windows-host-list.xlsx** template and save it.
3. Return to the HSS console and click **BatchInstallAgent.ps1** to download the installation script.
4. Log in as user **Administrator** to a server where the agent is to be installed.
5. Copy the **windows-host-list.xlsx** and **BatchInstallAgent.ps1** files to the **C:\Users** directory of the server where the agent is to be installed.
6. Right-click **BatchInstallAgent.ps1** and choose **Run with PowerShell**.
7. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

Figure 3-5 Changing the execution policy



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

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

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

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

----End

Follow-up Procedure

After the agent is installed on servers, **enable protection**.

3.2.2 On-Premises IDCs Accessing HSS Through a Direct Connect and Proxy Servers

3.2.2.1 Overview

Scenario

With the development of hybrid clouds, there is also a growing need for companies to perform unified security management of on- and off-cloud. HSS supports the access and management of on-premises IDCs. Users are allowed to use the same security policies on different clouds, preventing the risks caused by inconsistent security policies.

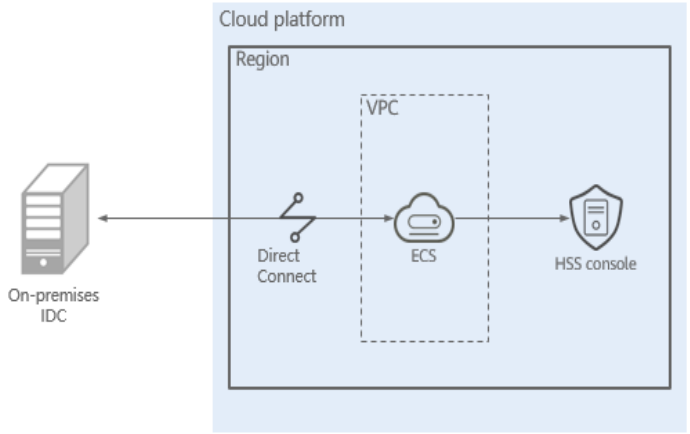
Architecture

On-premises IDCs communicate with VPCs on the cloud through Direct Connect, and then connect to HSS through ECS agent, as shown in **Figure 3-6**.

- Direct Connect establishes a dedicated network connection that features high speed, low latency, stability, and security between your on-premises data center and Cloud VPC. Direct Connect allows you to maximize legacy IT facilities and leverage cloud services to build a flexible, scalable hybrid cloud compute environment.

- Elastic Cloud Server (ECS) is a scalable and on-demand cloud server. It helps you to efficiently set up reliable, secure, and flexible application environments, ensuring stable service running and improving O&M efficiency.

Figure 3-6 On-premises IDCs accessing HSS through direct connect and proxy servers



3.2.2.2 Resources

The following table lists resources in this example.

Table 3-3 Resource description

Resource	Description	Quantity
Direct Connect	Direct Connect is used to connect third-party servers and cloud resources.	1
Elastic Cloud Server (ECS)	ECS, as a proxy server, forwards requests from on-premises IDCs to the HSS.	1

3.2.2.3 Process Flow

The process for on-premises IDC to access HSS through Direct Connect and proxy servers is as follows:

1. **Creating a Direct Connect**

   If an on-premises IDC cannot access the public network, you need to create a Direct Connect to connect to the VPC on the cloud for network interconnection.

2. **Creating a Proxy Server**

   You need to create an on-premises IDC as the proxy server to connect to the third-party server.

3. **Installing an Agent on the Proxy Server**

   Install an agent on the proxy server. Ensure the network is available and configure Nginx.

4. **Installing and Configuring Nginx on the Proxy Server**

   Nginx forwards requests from an on-premises IDC to the HSS management backend.

5. **Creating an Agent Installation Package or Installation Commands Using a Proxy Server**

   Generate the installation command for Linux servers and the package for Windows servers.

6. **Installing the Agent for an On-premises IDC**

   Install an agent for an on-premises IDC and connect the server to HSS for unified management.

3.2.2.4 Process

3.2.2.4.1 Creating a Direct Connect

on-premises IDCs can use Direct Connect to access servers in VPCs on the cloud without using the public network.

For details about how to use Direct Connect to connect an on-premises data center to a VPC on the cloud, see .

3.2.2.4.2 Creating a Proxy Server

Create a server on the cloud to function as a proxy server of the third-party server.

Creating a Proxy Server

Log in to the cloud console and apply for an ECS as a proxy server. For details, see *Elastic Cloud Server User Guide*.

The proxy server must meet the following requirements:

- The CPU architecture of the proxy server must be x86.
- The number of vCPUs of the proxy server must be 4 or greater, and the memory must be 8 GiB or greater.
- The image of the proxy server must be a Linux image that can use the **yum** command.

3.2.2.4.3 Installing an Agent on the Proxy Server

Install an agent on the proxy server. Ensure the network is available and configure Nginx.

Installing an Agent on the Proxy Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select the region and project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 5 Choose **Agents** > **Servers Without Agents**.

Step 6 In the **Operation** column of the target server, click **Install Agent**. The **Install Agent** dialog box is displayed.

Step 7 Select and set the server verification information.

- **Server authentication mode**: Select a mode. In this example, select **Account and password** mode.
- Allow direct connection as user **root**: Depends on whether the server allows direct connection as user **root**. In this example, select this option.
  - **Server Root Password**: Set this parameter based on the server information.
  - **Server Login Port**: Set this parameter based on the actual server login port. In this example, set **22** port.

Step 8 Click **OK** to start installation.

Step 9 Choose **Servers With Agents** page and view the agent status of the target server.

If the **Agent Status** is **Online**, the agent is successfully installed.

----End

3.2.2.4.4 Installing and Configuring Nginx on the Proxy Server

Nginx forwards requests from an on-premises IDC to the HSS management console.

Installing and Configuring Nginx on the Proxy Server

Step 1 Log in to the proxy server.

Step 2 Check the Yum repository.

Check whether the Nginx software package exists in the Yum repository. If the Nginx software package does not exist, configure the Yum repository and bind the public IP address temporarily. After the installation is complete, unbind the public IP address.

Remotely log in to the proxy server and run the following command to check whether the Nginx package exists in the Yum repository:

- For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **yum list nginx** command.
- For OSs that support DEB installation, such as Ubuntu and Debian, run the **apt list nginx** command.

If the information shown in **The Nginx package exists (rpm)** or **The Nginx package exists (deb)** is displayed, the Nginx package exists.

Figure 3-7 The Nginx package exists (rpm)

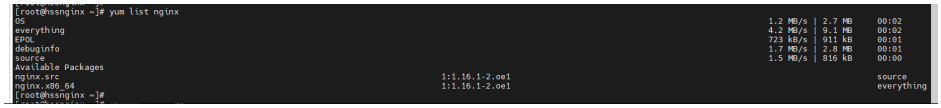
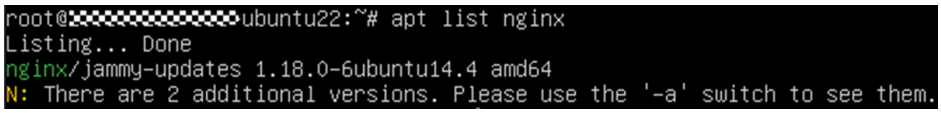


Figure 3-8 The Nginx package exists (deb)



Step 3 Installing Nginx

1. Run the following command to install Nginx using Yum:
   - For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **yum install -y nginx** command.
   - For OSs that support DEB installation, such as Ubuntu and Debian, run the **apt install -y nginx** command.

Figure 3-9 Installing Nginx (yum)

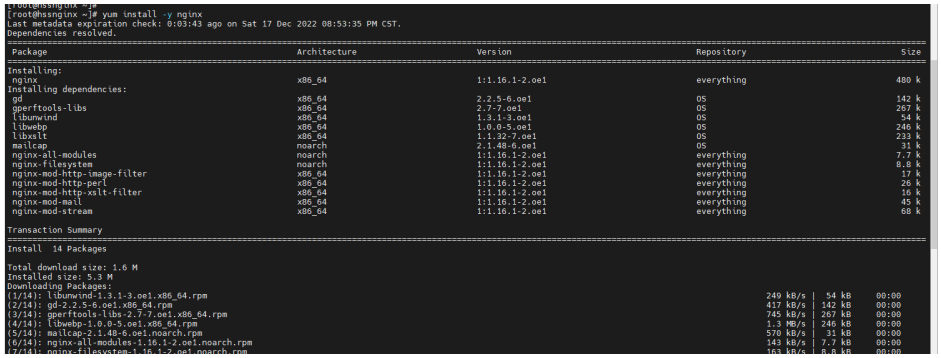
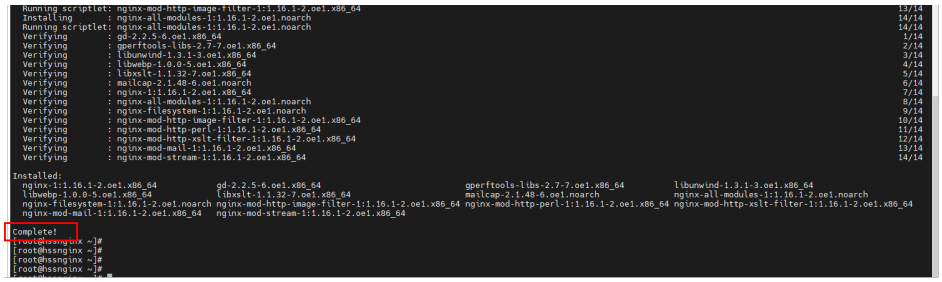


Figure 3-10 Installing Nginx (apt)

2. Check whether the Nginx installation is successful.
   - For OSs that support RPM installation, such as EulerOS, CentOS, and Red Hat:

     The installation is automatically performed. If **Complete!** shown in **Nginx installed successfully (rpm)** is displayed, the installation is successful.

Figure 3-11 Nginx installed successfully (rpm)



- For OSs that support DEB installation, such as Ubuntu and Debian:

  Run the **pkg –l nginx** command. If the command output shown in **Nginx installed successfully (deb)** is displayed, the installation is successful.

Figure 3-12 Nginx installed successfully (deb)

Step 4 Configuring Nginx

1. Run the following command to go to the Nginx directory:

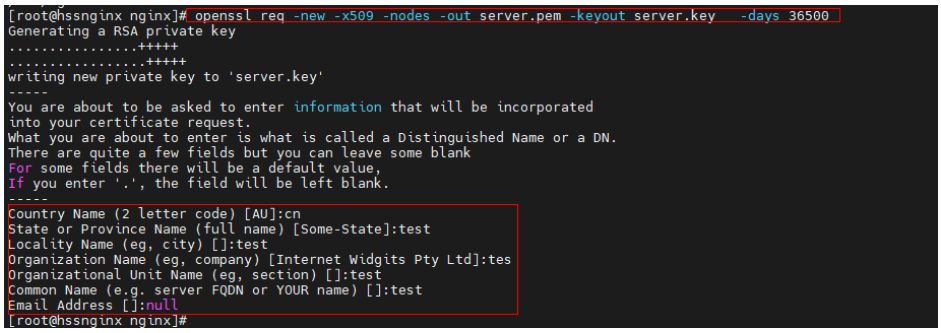
   cd /etc/nginx/

2. Run the following command to sign the certificate:

   openssl req -new -x509 -nodes -out server.pem -keyout server.key -days 36500

   After the command is executed, enter the certificate information. The value of **Country Name** can contain only two characters.

Figure 3-13 Self-signed certificate



3. Run the following command to modify **nginx.conf**:

   a. Run the following commands one by one to modify **nginx.conf**:

      rm -f nginx.conf

      vi nginx.conf

   b. Press **i** to enter the editing mode and copy the following content to the **nginx.conf** file:

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
```

```
pid /run/nginx.pid;

include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # for more information.
    include /etc/nginx/conf.d/*.conf;

    upstream backend_hss {
        server ADDR:10180;
    }

    server {
        listen  10180;

        server_name  ADDR;
        root         /usr/share/nginx/html;

        # Load configuration files for the default server block.
        include /etc/nginx/default.d/*.conf;

        ssl    on;
        ssl_protocols   TLSv1.2;
        ssl_certificate "server.pem";
        ssl_certificate_key "server.key";
        ssl_session_cache shared:SSL:10m;
        ssl_session_timeout  10m;
        ssl_prefer_server_ciphers on;

        location / {

            limit_except GET POST PUT
            {
                deny all;
            }
            proxy_set_header Host ADDR;
            proxy_pass https://backend_hss;

            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "upgrade";

       }

        error_page 404 /404.html;
            location = /40x.html {
        }

        error_page 500 502 503 504 /50x.html;
            location = /50x.html {
```

```
    }
  }
}
```

c. **Optional:** Paste the content, press **Esc**, run the following command, and press **Enter** to exit.

:wq!

d. Run the following command to automatically replace the IP address in the **nginx.conf** file:

sed -i "s#ADDR#`cat /usr/local/hostguard/conf/connect.conf | grep master_address | cut -d '=' -f 2 | cut -d ':' -f 1`#g" nginx.conf

4. Perform the following operations to create the Nginx monitoring script: After the creation is complete, the Nginx running status is checked every minute.

a. Run the following commands one by one to create the Nginx monitoring script:

echo '*/1 * * * * root sh /etc/nginx/nginx_monitor.sh' >> /etc/crontab

vi /etc/nginx/nginx_monitor.sh

Figure 3-14 Creating an Nginx monitoring script

```
[root@hss2 ~]#
[root@hss2 ~]# echo '*/1 * * * * root sh /etc/nginx/nginx_monitor.sh' >> /etc/crontab
[root@hss2 ~]#
[root@hss2 ~]#
[root@hss2 ~]# vi /etc/nginx/nginx_monitor.sh
```

b. Copy the following content to **nginx_monitor.sh**:

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
fi
```

Figure 3-15 Configuring **nginx_monitor.sh**

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
fi
~
~
~
```

c. Paste the content, press **Esc**, run the following command, and press **Enter** to exit.

:wq!

5. Wait 1 minute and run the following command to check whether the Nginx process has been started successfully:

ps -ef | grep nginx

If the command output shown in **Nginx process started successfully** is displayed, the Nginx process is started. Perform the **Creating an Agent Installation Package or Installation Commands Using a Proxy Server**.

Figure 3-16 Nginx process started successfully

```
[root@hss2 ~]#
[root@hss2 ~]# ps -ef | grep nginx
root      5123     1  0 17:47 ?        00:00:00 nginx: master process /usr/sbin/nginx
nginx     5124  5123  0 17:47 ?        00:00:00 nginx: worker process
nginx     5125  5123  0 17:47 ?        00:00:00 nginx: worker process
root      5971  3592  0 17:48 tty1     00:00:00 grep --color=auto nginx
[root@hss2 ~]#
```

----End

3.2.2.4.5 Creating an Agent Installation Package or Installation Commands Using a Proxy Server

Generate the agent installation command for Linux servers and the agent package for Windows servers using a proxy server.

Creating an Agent Installation Commands Using a Proxy Server (Linux)

Step 1 Log in to the proxy server.

Step 2 Run the following command to access the **/tmp** directory:

cd /tmp

Step 3 Run the following commands in sequence to check whether the IP address in **private_ip.conf** is available:

echo `hostname -I` > private_ip.conf

cat private_ip.conf

Figure 3-17 Viewing IP addresses

```
[root@hssnginx tmp]#
[root@hssnginx tmp]# echo `hostname -I` > private_ip.conf
[root@hssnginx tmp]# cat private_ip.conf
192.168.1.63
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

Check whether the IP address in **private_ip.conf** is available for the proxy server. Ensure that the IP address can be connected by on-premises IDCs. If the IP address is not available, manually change it.

Step 4 After confirming that the IP address is available, perform the following operations in sequence to generate the installation command:

1. Run the following commands in sequence to generate the installation commands:
   - x86 RPM software package image:

     echo -e "# for Linux x86 CentOS EulerOS OpenSUSE Fedora\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.x86_64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > x86_rpm_install.sh

- x86 deb software package image:

  echo -e "# for Linux x86 Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > x86_deb_install.sh

- Arm RPM software package image:

  echo -e "# for Linux ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.aarch64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > arm_rpm_install.sh

- Arm deb software package image:

  echo -e "# for Linux ARM Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > arm_deb_install.sh

2. Run the following command to replace the available IP address:

   The command needs to be run without modification.

   sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh

NOTE

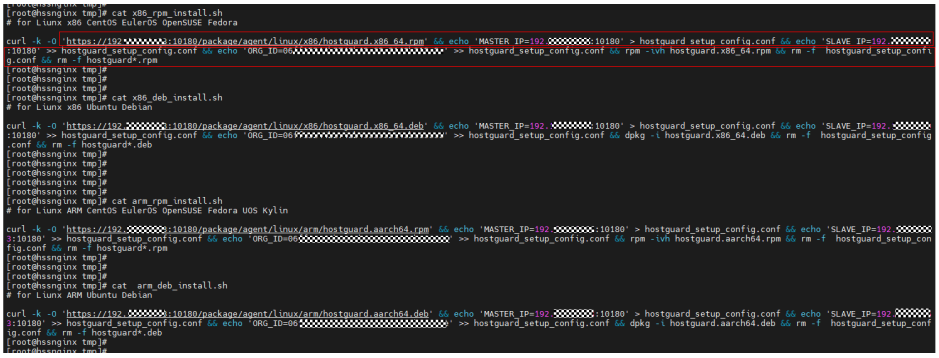
- The installation commands in **x86_rpm_install.sh** are suitable for images managed by the RPM software package in the x86 architecture, such as CentOS, EulerOS, OpenSUSE, and Fedora.
- The installation commands in **x86_deb_install.sh** are suitable for images managed by the .deb software package in the x86 architecture, such as Ubuntu and Debian.
- The installation commands in **arm_rpm_install.sh** are suitable for images managed by the RPM software package in the Arm architecture, such as CentOS, EulerOS, OpenSUSE, Fedora, UOS, and Kylin.
- The installation commands in **arm_deb_install.sh** are suitable for images managed by the .deb software package in the Arm architecture, such as Ubuntu and Debian.

Step 5 Run the following command to view the generated installation command: The generated installation command can be used to install the agent on Linux servers.

- To check the installation command generated for the x86 rpm software package image, run the following command: **cat x86_rpm_install.sh**
- To check the installation command generated for the x86 deb software package image, run the following command: **cat x86_deb_install.sh**

- To check the installation command generated for the Arm rpm software package image, run the following command: **cat arm_rpm_install.sh**
- To check the installation command generated for the Arm deb software package image, run the following command: **cat arm_deb_install.sh**

Figure 3-18 Checking the command generated for the x86 rpm software package image



----End

Creating an Agent Installation Package Using a Proxy Server (Windows)

Step 1 Run the following command to access the **/tmp** directory:

cd /tmp

Step 2 Run the following commands in sequence to generate the agent installation package for Windows servers:

curl -k -O https://`cat private_ip.conf`:10180/package/agent/windows/hostguard_setup.exe && echo '[system]' > hostguard_setup_config.ini && echo 'master=`cat private_ip.conf`:10180' >> hostguard_setup_config.ini && echo 'slave=`cat private_ip.conf`:10180' >> hostguard_setup_config.ini && echo 'orgid='`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2` >> hostguard_setup_config.ini

zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini

NOTE

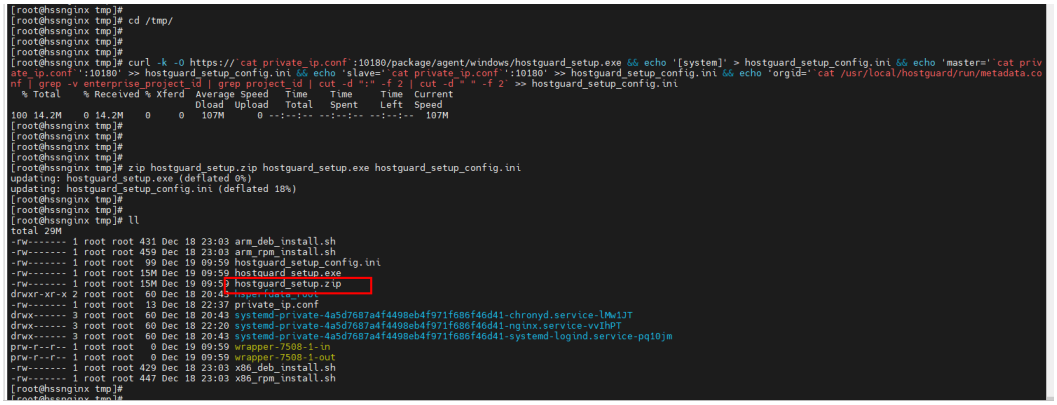
If the proxy server does not have zip commands, run the following command to install the zip plugin:

yum install -y zip

Step 3 View the generated installation package, which will be used to install agents on Windows servers.

ll

Figure 3-19 Windows installation package



----End

3.2.2.4.6 Installing an Agent for an On-premises IDC

Install agents on on-premises IDCs and manage the servers in HSS in a unified manner.

Installing the Agent for a Linux Server

Step 1 Copy the Linux installation commands in **Creating an Agent Installation Commands Using a Proxy Server (Linux)**.

Step 2 Log in to the target Linux server as user **root**, paste and run the Linux installation command.

If the command output shown in **Installing an agent** is displayed, the agent has been installed.

Figure 3-20 Agent installed

Step 3 Wait for about 10 minutes. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The ECS page is displayed.

Step 4 If the target server is displayed in the server list, the connection is successful.

----End

Installing the Agent for a Windows Server

Step 1 Copy the Windows installation package created in section **Creating an Agent Installation Package Using a Proxy Server (Windows)** to the local PC.

Step 2 Upload the installation package to the target Windows server where the agent is to be installed.

Step 3 Log in to the server using the Administrator account.

Step 4 Decompress the installation package, double-click **hostguard_setup.exe**, and install the agent according to the installation wizard.

After the generated .zip installation package is copied to the local PC, you must decompress the package before installing the software. Otherwise, the installation will fail.

Step 5 After the installation is complete, if the **HostGuard.exe** and **HostWatch.exe** processes are displayed in the Windows Task Manager, the agent is successfully installed.

Step 6 Wait for about 10 minutes. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The ECS page is displayed.

Step 7 If the target server is displayed in the server list, the connection is successful.

----End

3.2.3 Installing the HSS Agent Using CBH

Scenario

If you have applied for the Cloud Bastion Host (CBH) professional edition, you can use CBH to install the HSS agent on your server. You do not need to obtain the server account and password or run complex installation commands. You can easily install the agent on one or more servers.

Prerequisites

- You have managed server resources through the CBH.
- The server where the agent is to be installed is a Linux server of the SSH protocol type, and the network connection of the server is normal.
- You have obtained the system administrator account of the CBH.

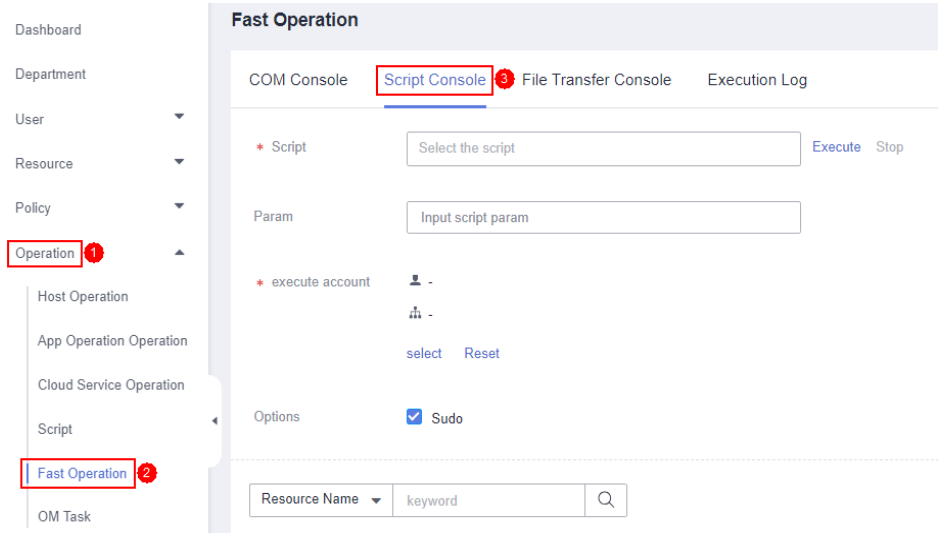
Procedure

Step 1 Use the system administrator account to Log In to the CBH System.

Step 2 In the navigation tree on the left, choose **Operation** > **Fast Operation**. The **Fast Operation** page is displayed.

Step 3 Click the **Script Console** tab.

Figure 3-21 Accessing the Script Console



Step 4 Configure script O&M information. **Script O&M parameters** describes the parameters.

Figure 3-22 Configuring script O&M information

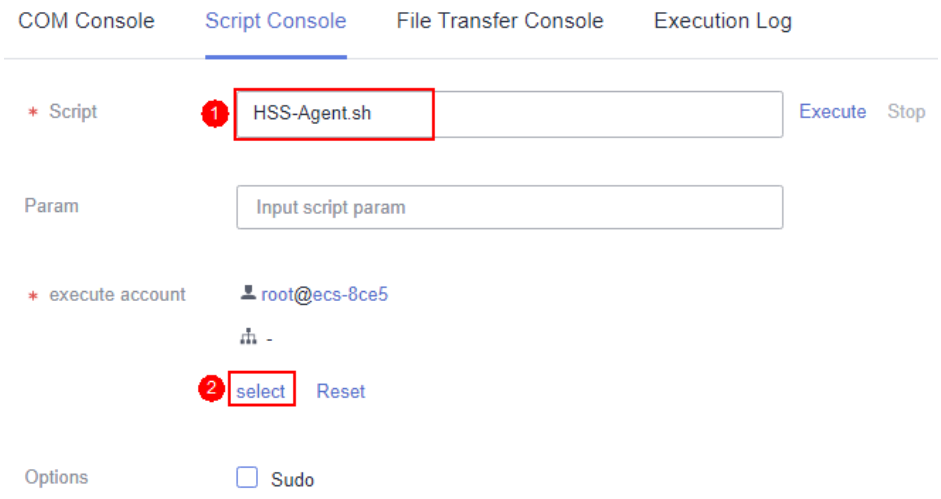


Table 3-4 Script O&M parameters

Parameter	Description
Script	Select the **HSS-Agent.sh** script.
Param	Leave this parameter blank.
Execution account	Click **select**, and select the account or account group of the server where the agent is to be installed.
Options	This parameter is optional. By default, the script task is executed in the Sudoers file on the server. If the server account does not have the execute permission on the file, select **Sudo**.

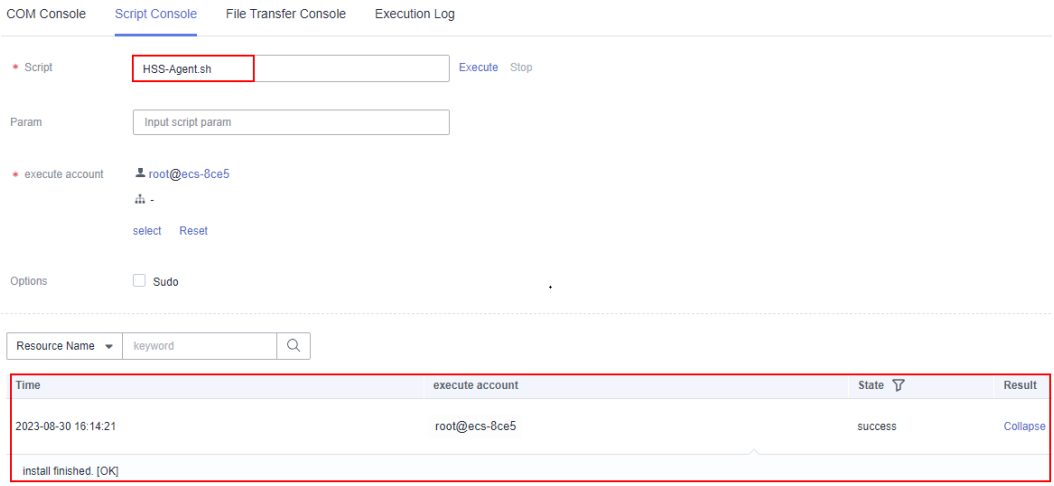
Step 5 Click **Execute**.

Figure 3-23 Executing a script task

Step 6 After the script task is successfully executed, click **Collapse** in the **Result** column to expand the execution result.

If **install finished.[OK]** is displayed, the agent is successfully installed.

Figure 3-24 Successfully executed a script task



Step 7 On the HSS console, confirm the agent installation result.

1. Log in to the HSS console.
2. In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.
3. On the **Servers** tab page, check the agent status of the target server.

   If the agent status is **Online**, the agent is successfully installed.

----End

3.3 Installing the Agent on Containers

3.3.1 Installing the Agent in a CCE Cluster

Scenario

Install the agent in a CCE cluster. After the configuration is complete, HSS automatically installs the agent on existing cluster nodes, installs the agent on new nodes when the cluster is scaled out, and uninstalls the agent from removed nodes when the cluster is scaled in.

Prerequisites

Before installing an agent for a CCE cluster, grant the CCEOperatePolicy permission to HSS. For details, see **Authorization**.

Constraints

- Supported container runtime: Docker and Containerd
- Supported cluster editions: CCE standard and Turbo editions
- Node resource requirements: At least 50 MiB memory and 200m CPU should be available.
- When an agent is installed in a cluster, HSS creates an HSS namespace in the cluster.

Installing the Agent in a CCE Cluster

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 On the **Cluster** tab page, click **Install Container Agent**. The **Container Asset Access and Installation** slide-out panel is displayed.

Step 6 Select **CCE Cluster Installation** and click **Configure Now**.

Step 7 Select a cluster and click **Next**.

Step 8 Configure agent parameters. For more information, see **Table 3-5**.

Table 3-5 Agent parameters

Parameter	Description
Configuration Rules	Select an agent configuration rule. • **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. • **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. **NOTE** • If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. • You are advised to select all runtime types.

Parameter	Description
(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ⌄ to expand advanced configurations. The **Enabling auto upgrade agent** option is selected by default. • **Enabling auto upgrade** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. • **Node Selector Configuration** Set the **Key** and **Value** of tags of the nodes where the agent is to be installed and click **Add**. If no tags are specified, the agent will be installed on all the nodes having no taints. • **Tolerance Configuration** If you added a node whose tag contains a taint in **Node Selector Configuration**, set the **Key**, **Value**, and **Effect** of the taint, and click **Add** to allow agent installation on the node.

Step 9 Click **OK** to start installing the HSS agent.

Step 10 In the cluster list, check the cluster status. If the cluster status is **Running**, the cluster is successfully connected to HSS.

----End

Follow-up Procedure

After the agent is installed in a cluster, **enable protection**.

3.3.2 Installing the Agent on an Independent Container Node

Scenarios

To enable container protection for an independent node, you need to install an agent on the node.

Prerequisites

There is at least one node with an online agent in the VPC of the nodes where the agent is to be installed. Otherwise, install the agent using the command line provided in **Installing the Agent on Servers**.

Installing the Agent on an Independent Container Node

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Independent Nodes** tab.

Step 6 Locate the node where the agent is in the **Not installed** state. Click **Install Agent** in the **Operation** column.

Step 7 On the agent installation page, configure **Server Authentication Mode**.

- **Account and password**
  - If **Allow direct connection with root permissions** is selected:

    The **root** account can be used to log in to the server. Provide the **root** user password and login port. HSS will use your **root** account to install the agent for the server.
  - If **Allow direct connection with root permissions** is not selected:

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

  Only user-created keys are supported. Click **Upload Key** and upload a user-created key file in .pem format.

Step 8 Confirm the information and click **OK**.

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

----End

Follow-up Operations

After the agent is installed on a node, **enable protection**.

3.4 Enabling Protection

Enabling the Enterprise/Premium Edition

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 5 Click **OK**. 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.

Step 6 (Optional) Configure alarm notification, protection policies, server login protection, and malicious program isolation and removal.

- **Configuring alarm notifications**

  After HSS is enabled, alarms are displayed on the console by default. To learn the security risks of servers, containers, or web pages in a timely manner, you can enable alarm notification, and HSS will notify you of risks by SMS or email. For details, see **Alarm Configuration**.

- **Configuring protection policies**

  Each HSS edition provides a group of protection policies preset with default settings. You can enable or disable policies and adjust protection rules as needed. For details, see **Policy Management**.

- **Configuring login protection**

  To enhance server login security, perform the operations in **Enabling 2FA**, **Configuring Common Login Locations**, **Configuring Common Login IP Addresses**, and **Configuring an SSH Login IP Address Whitelist**.

- **Enabling malicious program isolation and removal**

  If this function is enabled, HSS will automatically isolate identified malicious programs, such as backdoors, Trojans, and worms, to help you handle security risks. For details, see **Isolating and Killing Malicious Programs**.

----End

Enabling Web Tamper Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.

Step 5 On the **Add Server** page, click the **Available Servers** tab. Select the target server, and click **Add and Enable Protection**.

Step 6 You can check the server protection status on the **Web Tamper Protection** page.

- Choose **Server Protection** > **Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.

NOTE

- After WTP is enabled for a website, if you need to update the website, add a privileged process or temporarily disable WTP. Enable WTP 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.

----End

Enabling Container Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 5 In the row of a server, click **Enable Protection** in the **Operation** column. The confirmation dialog box is displayed.

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

CAUTION

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

Step 8 Click **OK**. If the **Protection Status** of the node changes to **Protected**, protection has been enabled.

Step 9 (Optional) Configure alarm notification, protection policies, server login protection, and malicious program isolation and removal.

- **Configuring alarm notifications**

  After HSS is enabled, alarms are displayed on the console by default. To learn the security risks of servers, containers, or web pages in a timely manner, you can enable alarm notification, and HSS will notify you of risks by SMS or email. For details, see **Alarm Configuration**.

- **Configuring protection policies**

  Each HSS edition provides a group of protection policies preset with default settings. You can enable or disable policies and adjust protection rules as needed. For details, see **Policy Management**.

- **Configuring login protection**

  To enhance server login security, perform the operations in **Enabling 2FA**, **Configuring Common Login Locations**, **Configuring Common Login IP Addresses**, and **Configuring an SSH Login IP Address Whitelist**.

- **Enabling malicious program isolation and removal**

If this function is enabled, HSS will automatically isolate identified malicious programs, such as backdoors, Trojans, and worms, to help you handle security risks. For details, see **Isolating and Killing Malicious Programs**.

----End

Viewing Scan Details

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

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

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

Table 3-6 Risk status

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

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

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

----End

Advanced Protection

HSS provides a series of advanced defense functions. You can enable or use them as required to enhance the security of your servers and containers. For details, see **Table 3-7**.

Table 3-7 Advanced protection

Function	Description	Version Restriction
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.	Premium, WTP, and container editions

Function	Description	Version Restriction
Ransomware Prevention	The function can detect and defend against ransomware. It can automatically back up data either at a scheduled time, or immediately if ransomware is detected. This can help you defend against ransomware and reduce loss. Ransomware prevention is automatically enabled with the container edition. HSS will deploy honeypot files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy.	Premium, WTP, and container editions
Application Process Control	Application process control helps to enhance the security of applications and processes running on servers. It can automatically identify and analyze application processes, and classify them into trusted, suspicious, and malicious processes. It allows trusted processes to run, and generates alarms for suspicious and malicious processes. This helps to build a secure environment for application processes, and protects servers from untrusted or malicious application processes.	Premium, WTP, and container editions
Virus Scanning and Removal	This function combines cloud-based and local antivirus mechanisms to scan executable files, compressed files, scripts, documents, images, and audiovisual files for viruses. You can perform quick scan, full-disk scan, and custom scans on servers as needed to detect and remove virus files in a timely manner, enhancing the virus defense of the system.	Professional, enterprise, premium, WTP, and container editions
Dynamic Port Honeypot	The dynamic port honeypot function is a proactive defense measure. It uses a real port as a honeypot port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify compromised servers, and protect real user resources.	Premium, WTP, and container editions
Container Firewall	The container firewall can isolate pods, workloads, and nodes in a network to prevent lateral movement and minimize permissions, and enhancing security and stability.	Container edition
Container Cluster Protection	HSS can check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks.	Container edition

3.4.1 Enabling the Basic/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 **Server Protection** > **Web Tamper Protection** > **Server Protection** and then enable it.

NOTE

To enable the WTP edition, choose **Server Protection** > **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 has been installed on the servers to be protected, the agent status is **Online**, and the protection status is **Unprotected**.
- To better protect your containers, you are advised to set security configurations.

Restrictions

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.

Enabling Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Asset Management** > **Servers**. The **Servers** tab is displayed.

Step 5 Select the target server and click **Enable**.

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

NOTE

If the version of the agent installed on the Linux server is 3.2.8 or later or the version of the agent installed on the Windows server is 4.0.16 or later, ransomware prevention is automatically enabled with the premium edition. To enhance ransomware prevention, you can configure specified protected directories. You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Modifying a Protection Policy**.

Step 6 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.

----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 **Unsafe Servers**.

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 Procedure

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

Related Operations

Disabling HSS

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

NOTICE

- Before disabling protection, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent attacks.
- 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.

3.4.2 Enabling Web Tamper Protection

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 3-8 How WTP works

Protection Type	Mechanism
Static web page protection	1. Local directory lock WTP locks files in a web file directory in a drive to prevent attackers from modifying them. Website administrators can update the website content by using privileged processes. 2. Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. 3. Remote backup and restoration After a remote backup server is configured, if a file in a protected directory is changed, HSS will back up the updated file. If the file and backup directory on the local server become invalid, you can log in to the remote backup server, obtain backup files, and manually restore the tampered websites. You can view backup paths on the **Manage Remote Backup Server** page. For details, see **Changing a Remote Backup Server**.
Dynamic web page protection	The proprietary RASP can detect application program behaviors, prevent attackers from tampering with web pages through application programs, and provide self-protection in Tomcat application runtime.

Prerequisites

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

Setting Protected Directories

You can set:

- 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.

Step 5 On the **Add Server** page, click the **Available servers** tab. Select the target server, select a quota from the drop-down list or retain the default value, and click **Add and Enable Protection**.

Step 6 You can check the server protection status on the **Web Tamper Protection** page.

- Choose **Server Protection** > **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 the target server is **Enabled** and the **Edition** of it is **Web Tamper Protection**, the WTP edition is enabled.

----End

NOTICE

- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- If the version of the agent installed on the Linux server is 3.2.8 or later or the version of the agent installed on the Windows server is 4.0.16 or later, ransomware prevention is automatically enabled with the WTP edition. To enhance ransomware prevention, you can configure specified protected directories. You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Modifying a Protection Policy** and **Enabling Ransomware Backup**.
- 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.

Related Operations

Disabling WTP

To disable WTP for a server, choose **Server Protection** > **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.

3.4.3 Enabling Container 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.

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 and Containerd containers.

Prerequisites

- Choose and click the **Container Nodes** tab. The **Agent Status** of the target node is **Online** and the **Protection Status** is **Unprotected**.
- You have created nodes on CCE.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. The **Container Nodes** tab is displayed.

Step 5 In the **Operation** column of the node list, click **Enable Protection**.

Step 6 In the displayed dialog box, confirm the server information.

Step 7 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.
- If the version of the agent installed on the Linux server is 3.2.8 or later or the version of the agent installed on the Windows server is 4.0.16 or later, ransomware prevention is automatically enabled with the container edition. To enhance ransomware prevention, you can configure specified protected directories. You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Modifying a Protection Policy** and **Enabling Ransomware Backup**.

----End

Related Operations

Disabling protection for a node

Choose **Asset Management** > **Containers**. In the node list on the **Container Nodes** tab, click **Disable Protection** in the **Operation** column.

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.

4 Checking the Dashboard

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

Checking the Dashboard

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Overview**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 View asset security information. For details, see **Overview**.

Table 4-1 Overview components

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

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

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

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

----End

Security Scores Criteria and Methods for Improving Scores

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

- No vulnerabilities detected: 20. For details about the score deduction criteria and improvement methods, see **Table 4-2**.
- No compliance risks detected: 20. For details about the score deduction criteria and improvement methods, see **Table 4-3**.
- No intrusion risks detected: 30. For details about the score deduction criteria and improvement methods, see **Table 4-4**.
- No asset risks detected: 10. For details about the score deduction criteria and improvement methods, see **Table 4-5**.

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

Table 4-2 Vulnerability risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled vulnerabilities	Unhandled critical vulnerabilities	All	10	√	Fix vulnerabilities based on the suggestions provided, scan for vulnerabilities again, and update the score. • For details about how to fix vulnerabilities, see **Handling Vulnerabilities**. • For details about how to scan for vulnerabilities, see **Vulnerability Scan**.
	Unhandled high-risk vulnerabilities	All	3	√	
	Unhandled medium-risk vulnerabilities	All	1	√	
	Unhandled low-risk vulnerabilities	All	0.1	√	
No vulnerability scan	No vulnerability scans were performed in the past month.	All	15	×	• The basic edition HSS does not provide vulnerability scan. To use this feature, upgrade HSS to the enterprise or premium edition. • In HSS enterprise, premium, and WTP editions, you are advised to perform vulnerability scans. For details, see **Scanning Vulnerabilities**.

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

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled non-compliance items	Unhandled high-risk non-compliance items	All	10	√	Rectify non-compliance items, perform a baseline check again, and update the score. • For details about how to fix baseline risks, see **Viewing and Processing Baseline Check Results**. • For details about how to perform baseline check, see **Performing Baseline Check**.
	Unhandled medium-risk non-compliance items	All	3	√	
	Unhandled low-risk non-compliance items	All	1	√	
Weak passwords	Weak passwords	All	10	√	Use strong passwords.
Weak password check not enabled	Weak password check policy not enabled	All	10	×	Enable the **Weak Password Detection** policy to check for weak passwords on servers. For details, see **Policy Management Overview**.

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Baseline check not performed	No baseline checks were performed in the past month.	All	10	×	• The HSS basic edition does not provide baseline check. To use this feature, you are advised to upgrade HSS to the enterprise or premium edition. • In HSS professional, enterprise, premium, and WTP editions, you are advised to perform baseline checks. For details, see **Viewing and Editing a Policy**.

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

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

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

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

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

Table 4-5 Asset risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Open ports	Open TCP/UDP high-risk ports	All	1	√	You are advised to disable unnecessary ports. To enable a port, choose **Asset Management** > **Server Fingerprints**, click **Open Ports**, and ignore the port.
Asset discovery not enabled	Asset discovery policy not enabled	All	5	×	• The HSS and enterprise editions do not provide asset discovery. To use this feature, upgrade HSS to the premium edition. • In the HSS premium and WTP editions, you are advised to enable the **Asset Discovery** policy. For details, see **Policy Management Overview**.

Table 4-6 Image risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unsafe images	High-risk images	Container edition	3	√	Re-create an image, scan the image, and update the score.
	Medium-risk images	Container edition	1	√	
	Medium-risk images	Container edition	0.1	√	
Image security scan not performed	No image security scans were performed in the past month.	Container edition	5	×	In the HSS container edition, you are advised to perform image security scans. For details, see: • **Managing Local Images**

Table 4-7 Unprotected assets risks score deduction criteria and improvement methods

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

5 Asset Management

5.1 Asset Overview

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

Constraints

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

Checking the Asset Overview

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Asset Management** > **Assets**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 View assets and their states.

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

corresponding container node list page. For details about how to enable protection, see **Enabling Protection**.

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

----End

5.2 Server Fingerprints

5.2.1 Collecting Server Asset Fingerprints

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

Constraints

The server fingerprint function is available in HSS enterprise, premium, WTP, and container editions.

Server Asset Fingerprint Collection Items

Table 5-1 lists the collection items of server asset fingerprints. Each asset fingerprint is automatically collected periodically. If you are using HSS premium edition or later, you can customize the asset fingerprint collection period. For details, see **Asset Discovery**.

Table 5-1 Asset fingerprints

Item	Description	Supported OS	Automatic Check Frequency
Accounts	Check and manage all accounts on your servers to keep them secure. You can check real-time and historical account information to find suspicious accounts. ● Real-time account information includes the account name, number of servers, server name/IP address, login permission, root permission, user group, user directory, shell started by the user, 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	Automatic check every hour
Open Ports	Check open ports on your servers, including risky and unknown ports. You can easily identify high-risk ports by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● Manually disabling high-risk ports If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary. It is recommended that you handle the ports at the **Dangerous** risk level promptly and handle the ports at the **Unknown** risk level based on the actual service conditions. ● Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.	Linux and Windows	Automatic check every 30 seconds

Item	Description	Supported OS	Automatic Check Frequency
Processes	Check processes on your servers and find abnormal processes. You can easily identify abnormal processes based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Linux and Windows	Automatic check every hour
Installed Software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, 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-started items	Check for auto-startup items and quickly locate Trojans. ● Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, and the last scan time. ● The historical change records of auto-started items include server names, IP addresses, change statuses, paths, file hashes, users, and the last scan time.	Linux and Windows	Automatic check every hour

Item	Description	Supported OS	Automatic Check Frequency
Websites	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.	Linux	Once a week (04:10 a.m. every Monday)
Web Frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Linux	Once a week (04:10 a.m. every Monday)
Middleware	You can check information about servers, versions, paths, and processes associated with middleware.	Linux and Windows	Once a week (04:10 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 (04:10 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 (04:10 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 (04:10 a.m. every Monday)

Manually Collecting the Latest Asset Fingerprints of a Single Server

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Servers**.

Step 7 Click a fingerprint in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

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

Step 8 After the automatic execution is complete, the last scan time is updated and the latest server asset information is displayed.

----End

Follow-up Procedure

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

5.2.2 Viewing Server Asset Fingerprints

HSS can collect server asset fingerprints, including information about ports, processes, web applications, web services, web frameworks, and auto-started items. You can centrally check server asset information and detect risky assets in a timely manner based on the server fingerprints. Asset management only detects risks. You need to manually handle suspicious assets.

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

Constraints

The server fingerprint function is available in HSS enterprise, premium, WTP, and container editions.

Viewing Asset Information of All Servers

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Asset Management** > **Server Fingerprints**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 View the server fingerprints.

Step 7 Click a fingerprint type in the list to view the asset information.

Step 8 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

----End

Viewing the Asset Information of a Single Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Servers**.

Step 7 Click a fingerprint type in the list to view the asset information.

Step 8 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

----End

5.3 Container Fingerprints

5.3.1 Collecting 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 collect container asset fingerprints.

Constraints

Container fingerprints are supported only by the HSS enterprise edition.

Container Asset Fingerprint Collection Items

Table 5-2 lists the collection items of container asset fingerprints. The fingerprint items except clusters, services, workloads, and container instances are automatically collected periodically. You can customize the asset fingerprint collection period. For details, see **Asset Discovery**.

Table 5-2 Container asset fingerprints

Item	Description	Automatic Detection Period
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.	Automatic check every hour

Item	Description	Automatic Detection Period
Open Ports	Check open ports on your containers, including risky and unknown ports. You can easily find high-risk ports on containers by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● Manually disabling high-risk ports If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary. It is recommended that you handle the ports with the **Dangerous** risk level promptly and handle the ports with the **Unknown** risk level based on the actual service conditions. ● Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.	Automatic check every 30 seconds
Processes	Check processes on your containers and find abnormal processes. You can easily identify abnormal processes on your containers based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Automatic check every hour
Installed Software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, 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

Item	Description	Automatic Detection Period
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.	Automatic check every hour
Websites	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 (04:10 a.m. every Monday)
Web Frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Once a week (04:10 a.m. every Monday)
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware.	Once a week (04:10 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 (04:10 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 (04:10 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.	Once a week (04:10 a.m. every Monday)
Clusters	Collect statistics on and display cluster details. You can view the type, node, version, and status of all clusters.	-
Services	Collect statistics on and display details about services and breakpoints. You can view information about all services, such as namespaces and clusters to which the services belong.	-

Item	Description	Automatic Detection Period
Workloads	Collect statistics on and display details about workloads (StatefulSets, deployments, DaemonSets, normal jobs, cron jobs, and container groups). You can view the status, number of instances, and namespace of all workloads.	-
Container Instances	Collect statistics on and display container instance details. You can view the status, pod, and cluster of all container instances.	-

Collecting the Latest Asset Fingerprints of a Single Container

To view the latest data of web applications, web services, web frameworks, websites, middleware, and databases in real time, you can manually collect their fingerprints.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Containers**.

Step 7 Click a fingerprint in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

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

Step 8 After the automatic execution is complete, the last scan time is updated and the latest container asset information is displayed.

----End

Collecting Cluster, Service, Workload, and Container Information

The information about clusters, services, workloads, and containers is not collected automatically. If your assets change, manually collect the latest data referring to this section.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 5 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 6 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

----End

Follow-up Procedure

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

5.3.2 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. For more information, see **Collecting Container Asset Fingerprints**.

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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Asset Management** > **Container Fingerprints** > **Asset Fingerprints**. On the **Asset Fingerprints** page that is displayed, view the fingerprint data of all containers.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click a fingerprint type in the list to view the asset information.

Step 7 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

----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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Containers**.

Step 7 Click a fingerprint type in the list to view the asset information.

Step 8 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

----End

Viewing Cluster Information

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 5 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 6 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 7 On the **Clusters** page, view cluster information.

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

- Searching for the target cluster

  You can enter information such as the cluster name and status in the search box to search for the target cluster.
- Viewing details about the target cluster

  a. Click the name of the target cluster to go to the CCE console.

  b. On the CCE console, view basic cluster information and network information.

----End

Viewing Services

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 5 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 6 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 7 On the **Services** tab page, view the information.

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

- Searching for a service

  You can enter information such as the service name and access mode in the search box 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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 5 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 6 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 7 Choose **Services** > **Endpoints**. View endpoints information.

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

- Searching for an endpoint

  You can enter information such as the endpoint name and namespace in the search box 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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 5 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 6 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 7 Click the **Workloads** tab.

Step 8 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 to search for the target workload.

Table 5-3 Workload information

Workload Type	Item
Deployment	• Workload name • Status • Instances • Namespaces • Created • Image name • Cluster • Cluster Type
StatefulSets	• Workload name • Status • Instances • Namespace • Created • Image name • Cluster • Cluster Type
DaemonSets	• Workload name • Status • Instances • Namespace • Created • Image name • Cluster • Cluster Type
Jobs	• Workload name • Status • Instances • Namespace • Created • Image name • Cluster • Cluster Type

Workload Type	Item
Cron Jobs	• Workload name • Status • Trigger • Running jobs • Namespace • Latest scheduled • Created • Image name • Cluster • Cluster Type
Pods	• Name • Namespace • Cluster • Cluster Type • 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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 5 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 6 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 7 Click the **Container Instances** tab.

The container name, status, pod, cluster name, cluster type, 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 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

5.4 Server Management

5.4.1 Enabling Server Protection

Scenarios

This section describes how to enable the basic, enterprise, or premium edition for a server.

Prerequisites

- Ensure that the agent has been installed on the server and is online. For details, see **Installing the Agent on Cloud Platform Servers**.

Constraints

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

- After the Windows firewall is enabled, HSS automatically adds firewall rules **hostguard_AllowAnyIn** and **hostguard_AllowAnyOut** to allow all inbound and outbound traffic. This ensures that the firewall does not affect your services. If HSS detects a brute-force attack, it adds an inbound rule to the firewall to block the attack source IP address. This does not affect your servers.
- Do not disable the Windows firewall when using HSS, or HSS cannot block the source IP addresses of brute-force attacks. Once it is disabled, HSS may fail to block the attack source IP addresses even after you manually enable it again.

Enabling the Enterprise/Premium Edition

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 5 Click **OK**. 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.

Step 6 (Optional) Configure alarm notification, protection policies, server login protection, and malicious program isolation and removal.

- **Configuring alarm notifications**

  After HSS is enabled, alarms are displayed on the console by default. To learn the security risks of servers, containers, or web pages in a timely manner, you can enable alarm notification, and HSS will notify you of risks by SMS or email. For details, see **Alarm Configuration**.

- **Configuring protection policies**

  Each HSS edition provides a group of protection policies preset with default settings. You can enable or disable policies and adjust protection rules as needed. For details, see **Policy Management**.

- **Configuring login protection**

  To enhance server login security, perform the operations in **Enabling 2FA**, **Configuring Common Login Locations**, **Configuring Common Login IP Addresses**, and **Configuring an SSH Login IP Address Whitelist**.

- **Enabling malicious program isolation and removal**

  If this function is enabled, HSS will automatically isolate identified malicious programs, such as backdoors, Trojans, and worms, to help you handle security risks. For details, see **Isolating and Killing Malicious Programs**.

----End

Viewing Scan Details

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

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

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

Table 5-4 Risk status

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

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

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

----End

Advanced Protection

HSS provides a series of advanced defense functions. You can enable or use them as required to enhance the security protection level of your servers. For details, see **Table 3-7**.

Table 5-5 Advanced protection

Function	Description	Version Restriction
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.	Premium edition
Ransomware Prevention	The function can detect and defend against ransomware. It can automatically back up data either at a scheduled time, or immediately if ransomware is detected. This can help you defend against ransomware and reduce loss. Ransomware prevention is automatically enabled with the container edition. HSS will deploy honeypot files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy.	Premium edition
Application Process Control	Application process control helps to enhance the security of applications and processes running on servers. It can automatically identify and analyze application processes, and classify them into trusted, suspicious, and malicious processes. It allows trusted processes to run, and generates alarms for suspicious and malicious processes. This helps to build a secure environment for application processes, and protects servers from untrusted or malicious application processes.	Premium edition
Virus Scanning and Removal	This function combines cloud-based and local antivirus mechanisms to scan executable files, compressed files, scripts, documents, images, and audiovisual files for viruses. You can perform quick scan, full-disk scan, and custom scans on servers as needed to detect and remove virus files in a timely manner, enhancing the virus defense of the system.	Professional, enterprise, and premium editions

Function	Description	Version Restriction
Dynamic Port Honeypot	The dynamic port honeypot function is a proactive defense measure. It uses a real port as a honeypot port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user.	Premium edition

5.4.2 Viewing Server Protection Status

You are advised to periodically check the server protection status and handle security risks in a timely manner to prevent asset loss.

Viewing Server Protection Status

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 In the server list, view the protection status of servers. For details, see **Server protection status**.

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

- **Searching for a server**

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

- **Viewing servers of a certain type**

  On the left of the server protection list, select a server protection edition or an asset importance category to view the protection status of each type of servers.

- **Viewing server protection information**

  The **Protection Status** column indicates whether a server is protected. The protection status of a server is determined by **Agent Status** and **Server Status**. You can view the server risk detection status in the **Risk Level** column. For details about the preceding parameters, see **Table 5-6**.

Table 5-6 Protection description

Parameter	Description
Server Status	HSS can only protect running servers. If the server is in the **Stopped** or other state, you cannot perform security checks or fix risks on the server.
Agent Status	– **Not installed**: The agent has not been installed or successfully started. Click **Install Agent** and install the agent as prompted. – **Online**: The agent has been installed and running properly. – **Offline**: The agent has been installed, but the agent is disconnected from the HSS remote protection center. In this case, HSS cannot provide protection. For more information, see **How Do I Fix an Abnormal Agent?** – **Installation failed**: An error or problem occurred, leading to an installation failure. Click ? next to the installation failure status to view the cause. Rectify the fault by referring to **What Should I Do If Agent Installation Failed?** – **Installing**: The agent is being installed.
Protection Status	– **Enabled**: The server is fully protected by HSS. – **Unprotected**: HSS is disabled for the server. After the agent is installed, click **Enable** in the **Operation** column to enable protection. – **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled.
Risk Level	Risk status of a server. (Data is updated every 24 hours.) – **Risky**: The server has risks. Hover your cursor over a risk icon to view risk distribution details. Click a risk quantity to go to the risk details page. – **Safe**: No risks are found. – **Pending risk detection**: HSS is not enabled for the server.

----End

Viewing the WTP Status

Step 1 Choose **Server Protection** > **Web Tamper Protection**. The **Servers** tab page is displayed.

Step 2 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 3 Check the server protection status.

Table 5-7 Statuses

Parameter	Description
Dynamic WTP	Status of dynamic WTP, which can be: • : Dynamic WTP is enabled. • : Dynamic WTP is disabled. (After enabling dynamic WTP, restart Tomcat to make this setting take effect.)
Static Tampering Attacks	Number of times that static web page files are attacked and tampered with.
Dynamic Tampering Attacks	Number of web application vulnerability exploits and injection attacks.

----End

5.4.3 Exporting the Server List

This section describes how to export the server protection list to your local PC.

Exporting the Server List to the Local PC

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**. The **Servers** tab is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 In the upper right corner of the server list, click **Export** to export the server list details.

You can also select specified servers in the server list and click **Export**. The details of up to 1000 servers can be exported at a time.

----End

5.4.4 Deploying a Protection Policy

You can quickly configure and start server scans by using policy groups. Simply create a group, add policies to it, and apply this group to servers. The agents deployed on your servers will scan everything specified in the policies.

Precautions

When the enterprise, premium, WTP, or container edition is enabled, the protection policy group of the corresponding edition is deployed by default and applies to servers. You do not need to manually deploy policies. For premium and container editions, you can copy a policy group and customize it as required. To flexibly manage server protection policies, you can replace the default policy group with a custom policy group.

Creating a Policy Group

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 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 7 In the dialog box displayed, enter a policy group name and description, and click **OK**.

- The name of a policy group must be unique, or the group will fail to be created.
- The policy group name and its description can contain only letters, digits, underscores (_), hyphens (-), and spaces, and cannot start or end with a space.

Step 8 Click **OK**.

Step 9 Click the name of the policy group you just created. The policies in the group will be displayed.

Step 10 Click a policy name and modify its settings as required. For details, see **Configuring Policies**.

Step 11 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 In the navigation pane on the left, choose **Asset Management** > **Servers**. The **Servers** tab is displayed.

Step 2 Select one or more servers for which you want to deploy a policy, and click **More** > **Apply Policy**.

NOTE

After protection is enabled for a server, the protection policy of the corresponding protection edition is deployed by default. For servers that use the premium and container editions, you can create and deploy different protection policies.

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

After the policy group is applied, click in the upper right corner of the server list, select **Policy Group** in the **Custom Columns** area, and click **OK**. Then, you can view the policy group of a server in the server list.

NOTE

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

----End

5.4.5 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 On the **Servers** tab page, click **Server Groups**, and click **Create Server Group**.

Step 7 In the **Create Server Group** dialog box, enter a server group name and select the servers to be added to the group.

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

Step 8 Click **OK**.

----End

Adding Servers to Groups

You can add servers to an existing server group. A server can be added to only one server group.

Step 1 Click the **Server** tab.

Step 2 Select one or more servers and click **Add to Group**.

To add a server to a group, you can also locate the row where the server resides, click **More** in the **Operation** column, and choose **Add to Group**.

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

After the allocation is complete, click in the upper right corner of the server list, select **Server Group** in the **Custom Columns** dialog box, and click **OK**. Then, you can view the group that a server belongs to in the server list.

----End

Related Operations

Editing a server group

Step 1 In the navigation pane on the left, choose **Servers & Quota** > **Servers**. On the **Servers** tab, click **Server Groups**.

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

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

Step 4 Click **OK**.

----End

Deleting a server group

Step 1 In the navigation pane on the left, choose **Servers & Quota** > **Servers**. On the **Servers** tab, click **Server Groups**.

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

NOTE

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

----End

5.4.6 Servers Importance Management

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

Assets are classified into the following types:

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

Checking Asset Importance

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**. The **Servers** tab is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 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 In the navigation pane on the left, choose **Asset Management** > **Servers**. The **Servers** tab is displayed.

Step 2 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 3 Select the target servers and click **Configure Asset Importance** above the list.

Step 4 In the dialog box that is displayed, select an asset importance level.

Step 5 Confirm the information and click **OK**.

In the **Asset Importance** area in the lower left corner, select a level and check whether the importance of assets is correct.

----End

5.4.7 Ignoring a Server

You can ignore the servers that do not need to be protected. HSS will neither protect the ignored servers nor synchronize the information changes of the ignored servers.

Ignoring a Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Servers** tab.

Step 7 Set filter criteria to filter unprotected servers.

Step 8 Select the target server and click **More** > **Ignore** above the server list to ignore the server.

In the server type area on the left, click **Ignored Servers** under **Attribute** to view ignored servers.

----End

Unignoring a Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Servers** tab.

Step 7 In the **Attribute** area, choose **Ignored Servers** to view the list of ignored servers.

Step 8 In the row of an ignored server, click **Unignore** in the **Operation** column.

At the top of the server type area on the left, click **All Servers**. You can view the unignored server in the server list.

----End

5.4.8 Disabling HSS

5.4.8.1 Disabling the Basic/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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**. The **Servers** tab is displayed.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 5 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

5.4.8.2 Disabling WTP

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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click the **Servers** tab.

> **NOTE**
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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

You can also select multiple servers, and click **Disable** above the server list to disable protection in batches.

Step 6 In the dialog box that is displayed, confirm the information and click **OK**.

Step 7 Choose **Asset Management** > **Servers** and click the **Servers** tab. If **Protection Status** of the server is **Unprotected**, the protection has been disabled for the server.

CAUTION

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

----End

5.5 Container Management

5.5.1 Enabling Container Protection

Scenarios

The HSS container edition protects containers throughout their lifecycles. This section describes how to enable protection for container nodes.

Prerequisites

- Ensure that the agent has been installed on the container node and is online. For details about how to install the agent on a single node, see **Installing the Agent on Cloud Platform Servers**. For details about how to install the agent on a cluster, see **Installing the Agent on Containers**.

Constraints

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

Enabling the Container Edition

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 5 In the row of a server, click **Enable Protection** in the **Operation** column. The confirmation dialog box is displayed.

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

CAUTION

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

Step 8 Click **OK**. If the **Protection Status** of the node changes to **Protected**, protection has been enabled.

Step 9 (Optional) Configure alarm notification, protection policies, server login protection, and malicious program isolation and removal.

- **Configuring alarm notifications**

  After HSS is enabled, alarms are displayed on the console by default. To learn the security risks of servers, containers, or web pages in a timely manner, you can enable alarm notification, and HSS will notify you of risks by SMS or email. For details, see **Alarm Configuration**.

- **Configuring protection policies**

  Each HSS edition provides a group of protection policies preset with default settings. You can enable or disable policies and adjust protection rules as needed. For details, see **Policy Management**.

- **Configuring login protection**

  To enhance server login security, perform the operations in **Enabling 2FA**, **Configuring Common Login Locations**, **Configuring Common Login IP Addresses**, and **Configuring an SSH Login IP Address Whitelist**.

- **Enabling malicious program isolation and removal**

  If this function is enabled, HSS will automatically isolate identified malicious programs, such as backdoors, Trojans, and worms, to help you handle security risks. For details, see **Isolating and Killing Malicious Programs**.

----End

Viewing Scan Details

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

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

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

Table 5-8 Risk status

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

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

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

----End

Advanced protection

HSS provides a series of advanced defense functions. You can enable or use them as required to enhance the security of your servers and containers. For details, see **Table 3-7**.

Table 5-9 Advanced protection

Function	Description
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.
Ransomware Prevention	The function can detect and defend against ransomware. It can automatically back up data either at a scheduled time, or immediately if ransomware is detected. This can help you defend against ransomware and reduce loss. Ransomware prevention is automatically enabled with the container edition. HSS will deploy honeypot files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy.
Application Process Control	Application process control helps to enhance the security of applications and processes running on servers. It can automatically identify and analyze application processes, and classify them into trusted, suspicious, and malicious processes. It allows trusted processes to run, and generates alarms for suspicious and malicious processes. This helps to build a secure environment for application processes, and protects servers from untrusted or malicious application processes.
Virus Scanning and Removal	This function combines cloud-based and local antivirus mechanisms to scan executable files, compressed files, scripts, documents, images, and audiovisual files for viruses. You can perform quick scan, full-disk scan, and custom scans on servers as needed to detect and remove virus files in a timely manner, enhancing the virus defense of the system.
Dynamic Port Honeypot	The dynamic port honeypot function is a proactive defense measure. It uses a real port as a honeypot port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user.
Container Firewall	The container firewall can isolate pods, workloads, and nodes in a network to prevent lateral movement and minimize permissions, and enhancing security and stability.
Container Cluster Protection	HSS can check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks.

5.5.2 Viewing the Container Node Protection Status

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

Constraints

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

Viewing the Container Node Protection Status

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. Click the **Container Nodes** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 View the node protection status. For details, see **Table 5-10**.

Table 5-10 Parameter description

Parameter	Description
Server Information	Server information, including the server name and IP address. You can hover your cursor over a server name to view the server details, including the server ID, OS, system name, and system version.
Protection Status	Protection status of a node. The options are as follows: • **Unprotected**: HSS is disabled for the server. After the agent is installed, click **Enable** in the **Operation** column to enable protection. • **Enabled**: The server is fully protected by HSS. • **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled.
Server Status	• Running • Unavailable • Normal

Parameter	Description
Agent Status	You can select a status to view the server. • **Online**: The agent is running properly. • **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. • **Not installed**: The agent has not been installed or successfully started.

----End

5.5.3 Exporting the Container Node List

This section describes how to export the container node list to your local PC.

Exporting the Container Node List to the Local PC

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. The container management page is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Choose the **Container Nodes** tab.

Step 7 In the upper part of the container list, click **Export** to export the list.

You can select multiple container nodes and click **Export** to export their container details in batches.

NOTE

The information about up to 1,000 container nodes can be exported at a time.

----End

5.5.4 Managing Local Images

Scenario

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.
- Only the images whose storage drive is OverlayFS or OverlayFS2 can be scanned. Nodes using Device Mapper cannot be scanned.
- Images whose names or versions are **--** cannot be scanned.
- HSS only has the permission to access the default scan directory **/var/run**. If **Docker Root Dir** is not **/var/run/**, HSS cannot scan images. You are advised to perform image scanning on the Containerd server.

Viewing Local Images

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Containers**. The container management page is displayed.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 5 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

  Click the server name of an image. The associated server list 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.
- Viewing image security risks

  You can view the number of risky images and click the value to go to the risk details page.

----End

Scanning Local Images

You can choose all images, multiple images, or a single image and manually start a scan. The duration of a security scan depends on the scanned image size. Generally, scanning an image takes shorter than 3 minutes. After the scan is complete, click **View Report** to check the report.

The following security scan items are supported for local images:

Scan Item	Description
Vulnerability	Detects vulnerabilities in images. System vulnerability scan supports the following OSs: • EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) • CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 (64-bit) • Ubuntu 16.04, 18.04, 20.04, 22.04 (64-bit) • Debian 9, 10, 11 (64-bit) • Kylin V10, V10 SP1, V10 SP2 (64-bit) • HCE 2.0 (64-bit) • SLES 12 SP5, 15 SP1, and 15 SP2 (64-bit) • UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) • Rocky Linux 8.6, 8.10, 9.4, 9.5 (64-bit) • CTyunOS 3-23.01 (64-bit) • AlmaLinux 8.4 (64-bit)
Installed software	Collects software information in an image.

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

Step 2 In the navigation pane, choose **Asset Management** > **Containers**. The container management page is displayed.

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 In the displayed dialog box, click **OK** to start the scan job.

After a full scan task is started, you can move the cursor over the gray **Scan All** button to view the scan progress.

Step 6 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 management console and go to the HSS page.

Step 2 Click the **Container Images** tab and click **Local image**.

Step 3 In the **Operation** column of the target image, click **View Report**. On the displayed page, view vulnerability reports and software information.

----End

Exporting Local Image Vulnerability Reports

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

Step 2 In the navigation pane, choose **Asset Management** > **Containers**. The container management page is displayed.

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**.

Step 5 View the export status in the upper part of the container management page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

5.5.5 Managing Repository Images

Scenario

Repository images include SWR private images, SWR shared images, SWR enterprise images, and third-party images. SWR-related images are synchronized from SWR to HSS. For details about how to access third-party images, see **Connecting to a Third-party Image Repository**.

HSS scans these images for vulnerabilities, malicious files, software information, file information, baseline configuration, sensitive information, software

compliance, and basic image information. For details about the scan items, see **Table 5-11**.

You can periodically scan images to detect and clear security risks in a timely manner, improving image security and keeping your assets away from security threats.

Table 5-11 Image scan items

Item	Description
Vulnerabilities	Detects system and application vulnerabilities in images. • System vulnerability scan supports the following OSs: – EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) – CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 (64-bit) – Ubuntu 16.04, 18.04, 20.04, 22.04 (64-bit) – Debian 9, 10, 11 (64-bit) – Kylin V10, V10 SP1, V10 SP2 (64-bit) – HCE 2.0 (64-bit) – SLES 12 SP5, 15 SP1, and 15 SP2 (64-bit) – UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) – Rocky Linux 8.6, 8.10, 9.4, 9.5 (64-bit) – CTyunOS 3-23.01 (64-bit) – AlmaLinux 8.4 (64-bit) • Application vulnerability scanning supports the following applications: fastjson, log4j-core, log4j-api, spring-core, shiro-core, struts-core, tomcat-embed-el, tomcat-jdbc, tomcat-embed-websocket, tomcat-juli, tomcat-annotations-ap, tomcat-embed-core, spring-jdbc, druid, commons-lang, commons-logging, commons-configuration, commons-collections, spring-cloud-netflix-archaius, mysql-connector-java, tensorflow, bootstrap, json, spring-beans, spring-context, spring-aop and spring-webmvc.
Malicious Files	Detects malicious files in images.
Software Information	Collects software information in an image.
File Information	Collects file information in an image.

Item	Description
Unsafe Settings	• Configuration check: – Checks the images configurations of CentOS 7, Debian 10, EulerOS, and Ubuntu16. – Checks SSH configurations. • Weak password check: detects weak passwords of Linux (SSH) accounts. • Password complexity check: detects insecure password complexity policies in Linux.
Sensitive Information	Detects files that contain sensitive information in images. • The paths that are not checked by default are as follows: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *AnyPath*/node_modules/*AnyPath*/*AnyName*.md – *AnyPath*/node_modules/*AnyPath*/test/*AnyPath* – */service/iam/examples_test.go – *AnyPath*/grafana/public/build/*AnyName*.js **NOTE** • *AnyPath*: indicates that the current path is a customized value and can be any path in the system. • *AnyName*: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system. • On the **View Report** > **Sensitive Information** tab, click **Configure Sensitive File Path** to set the Linux paths of the file that do not need to be checked. A maximum of 20 paths can be added. • No checks are performed in the following scenarios: – The file size is greater than 20 MB. – The file type can be binary, common process, or auto generation.
Software Compliance	Detects software and tools that are not allowed to be used.
Base Images	Detects service images that are not created using base images.

Constraints

- Only the HSS container edition supports this function.
- Security scans can be performed only on Linux images.

Viewing Repository Image 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**. The HSS page is displayed.

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

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click **Container Images** and click **Repository Images**.

Step 5 View the repository image information.

You can view the image version, size, and security risks in the image list.

In addition, you can perform the following operations:

- Synchronizing all images

  Click **Synchronize All Images** to synchronize all types of SWR images. In the upper right corner of the page, click **Manage Task** and click **Image Synchronization** to view the progress of image synchronization tasks.

  NOTE

  Images can be synchronized only after being authorized by SWR. For details, see "SWR Authorization Methods" in *SoftWare Repository for Container (SWR)*.

- Filtering images of the latest version

  If you select **Display latest image versions only**, you can filter the latest images of all images.

- Viewing image details

  Move the pointer over the target image in the **Image** column to view **Organization** and **Repository Type**. Click the image name to go to the image details page and view the image version, security scan status, and more information.

----End

Scanning Repository Images

You can manually scan images or set a scheduled scan policy to scan them periodically. The scan duration depends on the image size. Generally, a scan can complete within 3 minutes.

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**. The HSS page is displayed.

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

Step 4 Click **Container Images** and click **Repository Images**.

Step 5 Scan images.

NOTE

- SWR shared images can be scanned only if they are valid.
- Multi-architecture images do not support manual or scheduled scan.

- **Scanning an image**
  a. In the **Operation** column of an image, click **Scan**.
  b. Confirm the image information and click **OK** to start the scan.
- **Manually scanning images**
  a. In the upper right corner of the page, click **Scan**.
  b. Set manual scan parameters. For more information, see **Table 5-12**.

Table 5-12 Manual scan parameters

Parameter	Description	Example Value
Risk Type	Select the types of risks to be scanned. HSS scans for software information, file information, and base images by default.	Select all
Speed Limit for Third-party Image Repositories	If you have a large number of third-party images to be scanned, but you are worried that too much network bandwidth will be occupied if they are all scanned at once, you can click ⌄ to set the number of images to be scanned per hour.	Unlimited
Scan Tasks	A scan task occupies one pod. You can set the number of scan tasks running in the cluster. For example, if the number of scan tasks is set to 2, only two scan tasks can run in the cluster.	2
Image Scope	Select **All** or specify images. A full scan takes a long time and cannot be stopped after it starts. Exercise caution when performing this operation.	All

  c. Click **OK**.
- **Scheduling image scans**
  a. In the upper right corner of the page, click **Scheduled Scan Policy**.
  b. Set the scheduled scan parameters. For details, see **Table 5-13**.

Table 5-13 Parameters of a scheduled scan policy

Parameter	Description	Example Value
Scheduled Scan Policy	Whether to enable scheduled scan. After this function is enabled, you can view and configure scheduled scan parameters. ■ : disabled ■ : enabled	
Scheduled Scan Period	Click to select the scan period. The scan time range is fixed to 00:00:00 - 07:00:00.	Every 3 days
Risk Type	Select the types of risks to be scanned. HSS scans for software information, file information, and base images by default.	Select all
Speed Limit for Third-party Image Repositories	If you have a large number of images to be scanned, but you are worried that too much network bandwidth will be occupied if they are all scanned at once, you can click to set the number of images to be scanned per hour.	Unlimited
Image Update Time Range	Select a range of image update time. It determines which images will be scanned. For example, if you set the scan time range to **Last 15 days**, HSS scans only the images updated in the last 15 days.	Last 15 days
Scan Tasks	A scan task occupies one pod. You can set the number of scan tasks running in the cluster. For example, if the number of scan tasks is set to 2, only two scan tasks can run in the cluster.	2
Image Repositories	Select the type of the images to be scanned.	Swr-private

c. Click **OK** to start the scan.

Step 6 In the upper right corner of the page, click **Manage Task** and click the **Image Scan** tab to view image scan task status.

----End

Viewing Image Scan Results

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**. The HSS page is displayed.

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

Step 4 Click **Container Images** and click **Repository Images**.

Step 5 In the row containing the target image, click **View Results** in the **Operation** column to go to the image details page.

Step 6 View image security scan results. For more information, see **Table 5-14**.

Table 5-14 Security report parameters

Parameter	Description
Basic Information	Displays basic image information, including the image names, organizations, image tags, image sizes, number of vulnerabilities, last update time of the image tags, and scan status. To rescan image security, click **Scan Again**.
Vulnerability Reports	Displays the scan results of image system vulnerabilities and application vulnerabilities. • Viewing vulnerability details Click a vulnerability name to go to the vulnerability details page and view the basic information and affected images. • Viewing the **CVE ID**, **CVSS Score**, and **Disclosed Time** of a vulnerability Click in front of a vulnerability name to view its CVE ID, CVSS score, and the time when it was disclosed. • Viewing vulnerability solutions In the **Solution** column of a vulnerability, click the solution description to view the vulnerability solution details.
Malicious Files	Displays the scan results of malicious image files, including the malicious file names, paths, and file sizes.
Software Information	Displays the statistical results of image software information, including the software names, types, versions, and number of software vulnerabilities. Click next to a software name to view the software vulnerability name, urgency, and solution.
File Information	Displays the statistical results of image file information, including the total number of files, total file size, and details about the top 50 files.

Parameter	Description
Unsafe Settings	Displays the image baseline check results, including the configuration check, password complexity policy check, and common weak password check results. • Viewing unsafe settings and suggestions 1. On the **Unsafe Configurations** tab page, select a baseline. 2. In the detection item column of a detection item, click **Description** to view the detection item description and modification suggestions. • Customizing common weak passwords 1. Click **Common Weak Password Detection**. 2. Configure weak passwords and click **OK**.
Sensitive Information	Displays the scan result of sensitive image information, including the risk levels, image paths, file paths, and sensitive information. To add the paths of sensitive files that are not detected, choose **Configure Sensitive File Path** and add the paths to be filtered. • Only Linux system file paths can be filtered. • A maximum of 20 paths can be added. Put each path on a separate line. • Example: **/usr/** or **/lib/test.txt**.
Software Compliance	Displays the scan results of non-compliant image software, including the non-compliant software name, software version, path, and image layer information.
Base Images	Displays the scan results of service images that are not built using basic images. The scan results include image names, versions, and image paths.

----End

Exporting an Image Vulnerability Report Report

Vulnerability or baseline report cannot be exported for multi-architecture images.

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**. The HSS page is displayed.

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

Step 4 Click **Container Images** and click **Repository Images**.

Step 5 Click **Export Vulnerability** above the image list and select a report type to export the vulnerability or baseline report.

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

Step 6 View the export status in the upper part of the container management page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

5.5.6 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.

Viewing Container Information

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. The container management page is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Containers** tab. The container page is displayed.

Step 7 View the container information and security status.

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

- View container details.

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

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

Click **Export** in the upper left corner of the list to export the container list to the local PC.

----End

5.5.7 Handling Unsafe Containers

Scenario

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

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

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

Constraints

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

Handling Unsafe Containers

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. The container management page is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Containers** tab. The container page is displayed.

Step 7 In the search box above the container list, choose **Risks** > **Risky** to filter risky containers.

Step 8 In the **Operation** column of the target risky container, select the operation to be performed.

Only the running containers with medium or higher risks can be handled. You can hover your cursor over the Risks column of a container to view its risk distribution. For a container that belongs to a cluster, you can stop it. For an independent container, you can isolate, suspend, or stop it.

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

----End

Related Operations

Restoring a container to the running state

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

NOTE

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

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

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

----End

5.5.8 Uninstalling the Agent from a Cluster

Uninstalling an Agent from a CCE Cluster

Step 1 Log in to the CCE console.

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Computing** > **Cloud Container Engine**. The CCE console is displayed.

Step 3 Click the name of a cluster to enter its details page.

Step 4 In the navigation pane, choose **Workloads**.

Step 5 Click the **DaemonSets** tab. Delete the workload **install-agent-ds**.

In the **Operation** column of the workload, choose **More** > **Delete**.

Step 6 Click ☰ in the upper left corner of the page, select a region, and choose **Security** > **Host Security Service**. The HSS page is displayed.

Step 7 Click 📍 in the upper left corner and select a region or project.

Step 8 In the navigation tree on the left, choose **Installation & Configuration** > **Server Install & Config**.

Step 9 Click the **Agents** tab. Uninstall the agent from all container nodes in the CCE cluster.

For details, see **Uninstalling the Agent**.

----End

Uninstalling an Agent from an On-Premises Cluster

Step 1 Log in to the Kubernetes cluster.

Step 2 Run the following command to delete the workload **install-agent-ds**:

kubectl delete ds install-agent-ds -n default

Step 3 Log in to the management console.

Step 4 Click 📍 in the upper left corner and select a region or project.

Step 5 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 6 In the navigation tree on the left, choose **Installation & Configuration** > **Server Install & Config**.

Step 7 Click the **Agents** tab. Uninstall the agent from all container nodes in the cluster.

For details, see **Uninstalling the Agent**.

----End

5.5.9 Disabling Container Protection

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

Before You Start

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

Disabling the Container Edition

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. Click the **Container Nodes** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 In the **Operation** column of a server, click **Disable Protection**.

To disable protection in batches, select multiple target servers and click **Disable Protection**.

Step 7 In the dialog box that is displayed, confirm the information and click **OK**.

Step 8 After the function is disabled, choose **Asset Management** > **Containers**. On the **Container Nodes** tab, if the **Protection Status** of the server is **Unprotected**, it indicates protection has been disabled.

----End

6 Prediction

6.1 Vulnerability Management

6.1.1 Vulnerability Management Overview

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

NOTE

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

How Vulnerability Scan Works

Table 6-1 describes how different types of vulnerabilities are detected.

Table 6-1 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	HSS detects the vulnerabilities in the software and dependency packages running on servers and container server machines, reports risky vulnerabilities to the console, and displays vulnerability alarms.
Emergency Vulnerabilities	Checks whether the software and any dependencies running on the server have vulnerabilities through version comparison and POC verification. Reports risky vulnerabilities to the console and provides vulnerability alarms for you.

Types of Vulnerabilities That Can Be Scanned and Fixed

For details about the types of vulnerabilities that can be scanned and fixed in different HSS editions, see **Types of vulnerabilities that can be scanned and fixed in each HSS edition**.

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

- √: supported
- ×: not supported

Table 6-2 Types of vulnerabilities that can be scanned and fixed in each HSS edition

Vulnerability Type	Function	Basic Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
Linux vulnerability	Automatic vulnerability scan (daily by default)	√	√	√	√	√
	Scheduled vulnerability scan (once a week by default)	×	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√

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

Vulnerability Type	Function	Basic Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Scheduled vulnerability scan (once a week by default)	×	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×
Application vulnerability	Automatic vulnerability scan (every Monday by default)	×	√	√	√	√
	Scheduled vulnerability scan (once a week by default)	×	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×
Emergency vulnerability	Automatic vulnerability scan	×	×	×	×	×
	Scheduled vulnerability scan (disabled by default)	×	√	√	√	√
	Vulnerability whitelist	×	×	×	×	×

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

NOTE

HSS can scan for Web-CMS vulnerabilities, emergency vulnerabilities, and application vulnerabilities but cannot fix them. You can log in to your server to manually fix the vulnerability by referring to the suggestions displayed on the vulnerability details page.

6.1.2 Vulnerability Scan

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

- Automatic scan

  By default, Linux, Windows, and Web-CMS vulnerabilities are automatically scanned every day. Application vulnerabilities are automatically scanned every Monday. The time of an automatic application vulnerability scan changes with the middleware asset scan time. For details about how to view and set the latter, see **Asset Discovery**.

  If a manual or scheduled vulnerability scan has been performed in a day, HSS will not automatically scan for vulnerabilities on that day.
- Scheduled scan

  By default, a full server vulnerability scan is performed once a week. To protect workloads, you are advised to set a proper scan period and scan server scope to periodically scan server vulnerabilities.
- Manual scan

  If you want to view the vulnerability fixing status or real-time vulnerabilities of a server, you are advised to manually scan for vulnerabilities.

This section describes how to manually scan for vulnerabilities and configure a scheduled scan policy.

Constraints

- If the agent version of the Windows OS is 4.0.18 or later, application vulnerability scan is supported. If the agent version of the Linux OS is 3.2.9 or later, emergency vulnerability scan is supported. For details about how to upgrade the agent, see **Upgrading the Agent**.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. Otherwise, vulnerability scan cannot be performed.

- For details about the types of vulnerabilities that can be scanned by different HSS editions, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.
- For details about the OSs supported by Linux and Windows vulnerability scan, see **Table 6-3**. Emergency vulnerability scan supports x86 Ubuntu, CentOS, EulerOS, Debian, and AlmaLinux.

Table 6-3 OSs supporting vulnerability scan

OS Type	Supported OS
Windows	• Windows Server 2019 Datacenter 64-bit English (40 GB) • Windows Server 2019 Datacenter 64-bit Chinese (40 GB) • Windows Server 2016 Standard 64-bit English (40 GB) • Windows Server 2016 Standard 64-bit Chinese (40 GB) • Windows Server 2016 Datacenter 64-bit English (40 GB) • Windows Server 2016 Datacenter 64-bit Chinese (40 GB) • Windows Server 2012 R2 Standard 64-bit English (40 GB) • Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) • Windows Server 2012 R2 Datacenter 64-bit English (40 GB) • Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)
Linux	• EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) • CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 (64-bit) • Ubuntu 16.04, 18.04, 20.04, 22.04 (64-bit) • Debian 9, 10, 11 (64-bit) • Kylin V10, V10 SP1, V10 SP2 (64-bit) • HCE 2.0 (64-bit) • SLES 12 SP5, 15 SP1, and 15 SP2 (64-bit) • UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) • Rocky Linux 8.6, 8.10, 9.4, 9.5 (64-bit) • CTyunOS 3-23.01 (64-bit) • AlmaLinux 8.4 (64-bit)

Manual Vulnerability Scan

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 Click **Scan** in the upper right corner of the **Vulnerabilities** page.

To scan for emergency vulnerabilities, locate the row of an emergency vulnerability, and click **Scan** in the **Operation** column.

Step 6 In the **Scan for Vulnerability** dialog box displayed, set the vulnerability types and scope to be scanned. For more information, see **Table 6-4**.

Table 6-4 Parameters for manual scan vulnerabilities

Parameter	Description	Example Value
Type	Select one or more types of vulnerabilities to be scanned. Possible values are as follows: • **Linux** • **Windows** • **Web-CMS** • **Application** • **Emergency**	Select all
Scan	Select the servers to be scanned. Possible values are as follows: • **All servers** • **Selected servers** You can select a server group or search for the target server by server name, ID, EIP, or private IP address. The following servers cannot be selected for vulnerability scan: – Servers are protected by basic edition HSS. – Servers that are not in the **Running** state – Servers whose agent status is **Offline**	**All servers**

Step 7 Click **OK**.

Step 8 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 icon 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

Scheduled vulnerability scan

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose Prediction > **Vulnerabilities**.

Step 5 In the upper right corner of the **Vulnerabilities** page, click **Scheduled Scan Policy**. The **Configure Scheduled Scan Policy** dialog box is displayed.

Step 6 In the dialog box, configure parameters such as the period and scope for scheduled vulnerability scanning.

- **Scheduled Vulnerability Scan**: Select whether to enable scheduled vulnerability scan. indicates it is enabled.
- **Type**: Select the types of vulnerabilities to be scanned.
- **Scan Period**: Select **Every day**, **Every three days**, or **Every week**. The default scan duration is **00:00:00 - 07:00:00** and cannot be changed.
- **Servers**: Select the server to be scanned. The following servers cannot be selected for vulnerability scan:
  - Servers that use the HSS basic edition
  - Servers that are not in the **Running** state
  - Servers whose agent status is **Offline**

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

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

----End

6.1.3 Viewing Vulnerability Details

You can view vulnerabilities of your assets on the **Vulnerabilities** page. The **Vulnerabilities** page contains two tabs: **Vulnerabilities view** and **Server view**, helping you analyze vulnerabilities from the vulnerability and server perspectives.

Constraints

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

Viewing Vulnerability Details (Vulnerability View)

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 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 6-5** describes related parameters.

  Table 6-5 Vulnerability scan parameters

Parameter	Description
Critical Vulnerabilities	Click the number in **Critical vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in **Unfixed Vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Click the number in **Servers with Vulnerabilities**. You can view the servers with vulnerabilities in the lower part of the **Vulnerabilities** page.
Servers Fixed and Pending Restart	After Linux kernel vulnerabilities and Windows vulnerabilities are fixed, you need to restart the fixed servers. Otherwise, HSS will probably continue to warn you of these vulnerabilities. Click the number in the **Servers Fixed and Pending Restart** area to view the servers to be restarted.
Vulnerabilities Handled Today/ Total	Number of vulnerabilities handled today and the total number of vulnerabilities handled. You can click the numbers to view details. The total number of vulnerabilities is just the vulnerabilities handled within one year.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.
Total Scans	Displays the number of vulnerability scans. Click **Scan** to manually scan for vulnerabilities on servers.

- Viewing vulnerability details

Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the repair suggestions, CVE details, affected servers, and historical handling records of the vulnerability.

To check affected servers,

- Hover the cursor on the name of an affected server, and you can see the server status and OS version.
- If a server has the associated process, click the server name and check process details in the **Associated Process** column.

- Viewing handled vulnerabilities or vulnerabilities to be handled

  Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities.

----End

Viewing Vulnerability Details (Server View)

The basic edition does not provide the server view.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 In the upper 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 6-6** describes related parameters.

Table 6-6 Vulnerability scan parameters

Parameter	Description
Critical Vulnerabilities	Click the number in **Critical vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in **Unfixed Vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Click the number in **Servers with Vulnerabilities**. You can view the servers with vulnerabilities in the lower part of the **Vulnerabilities** page.

Parameter	Description
Servers Fixed and Pending Restart	After Linux kernel vulnerabilities and Windows vulnerabilities are fixed, you need to restart the fixed servers. Otherwise, HSS will probably continue to warn you of these vulnerabilities. Click the number in the **Servers Fixed and Pending Restart** area to view the servers to be restarted.
Vulnerabilities Handled Today/ Total	Number of vulnerabilities handled today and the total number of vulnerabilities handled. You can click the numbers to view details. The total number of vulnerabilities is just the vulnerabilities handled within one year.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.
Total Scans	Displays the number of vulnerability scans. Click **Scan** to manually scan for vulnerabilities on servers.

- Viewing server details and vulnerabilities on servers
  a. Click the name of a target server. On the server details slide-out panel displayed, you can view details about the server and vulnerabilities on the server.
  b. Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the CVE details, affected servers, and historical handling records of the vulnerability.
- Viewing handled vulnerabilities or vulnerabilities to be handled
  Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities to be handled or that have been handled.

----End

6.1.4 Exporting the Vulnerability List

You can refer to this section to export the vulnerability list.

Prerequisite

The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. For details, see **Viewing Server Protection Status**.

Exporting the Vulnerability List (Server View)

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 In the upper left corner of the **Vulnerabilities** page, click the **Server view** tab.

Step 6 Export the vulnerability list.

- Export vulnerability details: In the upper part of the vulnerability list, click **Export Details** to export the vulnerability list.

  You can select the risk level, vulnerability handling status, or search criteria to filter the vulnerability information of the target server, and click **Export Details** to export the vulnerability details.
- Export a vulnerability report: In the upper part of the vulnerability list, click **Export Report** and select a report format.
  - When exporting a vulnerability report in HTML format, the vulnerability information about up to 100 servers can be exported. In the exported HTML vulnerability report, you can view vulnerability details.
  - When exporting a vulnerability report in PDF format, the vulnerability information about up to 140 servers and vulnerabilities can be exported.
  - To export vulnerability reports of some servers, you can select the servers and click **Export**.

Step 7 View the export status in the upper part of the **Vulnerabilities** page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

6.1.5 Handling Vulnerabilities

If HSS detects a vulnerability on a server, you need to handle the vulnerability in a timely manner based on its severity and your business conditions to prevent the vulnerability from being exploited by intruders.

Vulnerabilities can be handled in the following ways:

- **Fixing vulnerabilities**

  If a vulnerability may harm your services, fix it as soon as possible. For Linux and Windows vulnerabilities, you can let HSS fix them in one-click. Web-CMS vulnerabilities and application vulnerabilities cannot be automatically fixed. Handle them by referring to the suggestions provided on the vulnerability details page.
- **Ignoring vulnerabilities**

  Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. If you can confirm that a vulnerability is harmless, you can ignore it.
- **Adding vulnerabilities to the whitelist**

If you can confirm that a vulnerability does not affect your services and does not need to be fixed, you can add it to the whitelist. After a vulnerability is added to the whitelist, its status will change to **Ignored** in the vulnerability list, and it will not be reported in later scans.

Constraints

- For details about vulnerability handling operations supported by each HSS version, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.
- **The following table** describes the OSs that have reached their end of life (EOL). HSS does not support automatic vulnerability fixing on these OSs. You are advised to use the OSs in active support.

  Table 6-7 OSs that have reached EOS

OS	Description
CentOS 8	It has reached EOL and will no longer maintained. HSS scans them for vulnerabilities based on Red Hat patch notices, but cannot fix them due to the lack of official patches. You are advised to change to the OSs in active support.
Ubuntu 16.04, 18.04, 22.04	They have reached EOL and do not support free patch updates. You need to purchase and configure Ubuntu Pro to install upgrade packages, or vulnerability fix will fail.
Debian 9 and 10	It has officially reached EOL. No official patches are available. You are advised to change to the OSs in active support.
Windows 2012 R2	It has officially reached EOL. No official patches are available. You are advised to change to the OSs in active support.

- Kernel vulnerabilities cannot be fixed on CCE, MRS, and BMS servers, or services may be interrupted.
- To handle vulnerabilities on a server, ensure the server is in the **Running** state, its agent status is **Online**, and its protection status is **Protected**.

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

Vulnerabilities detected by HSS are classified into four priority levels: critical, high, medium, and low. You can refer to the priorities to fix the vulnerabilities that have significant impact on your server first.

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

Vulnerability Display

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

Automatically Fixing Vulnerabilities (Vulnerability View)

You can only fix Linux and Windows vulnerabilities with one-click on the console. A maximum of 1,000 server vulnerabilities can be fixed at a time. If there are more than 1,000 vulnerabilities, fix them in batches.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 Fix Linux and Windows vulnerabilities.

- Fixing a single vulnerability

  Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

- Fixing multiple vulnerabilities

  Select all target vulnerabilities and click **Fix** in the upper left corner of the vulnerability list to fix vulnerabilities in batches.

- Fix all vulnerabilities.

  Click **Fix** in the upper left corner of the vulnerability list to fix all vulnerabilities.

- Fix 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 6 In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

For Linux vulnerabilities, you can click **View details** in the **Fix** dialog box to view the name of the component to be fixed.

Step 7 (Optional) Back up servers.

Before fixing vulnerabilities, use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

1. In the **Fix** dialog box, click to enable backup.

   NOTE

   - After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up.
   - If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

2. Choose **Select Server to Scan**. The backup creation dialog box is displayed.
3. In the **Create Backup** dialog box, set a backup file name, and click **OK**.

Step 8 In the **Fix** dialog box displayed, select **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.** and click **Auto Fix**.

If you have manually fixed the vulnerability, click **Manual handling** in the **Fix** dialog box. After the vulnerability is manually handled, its status changes to **Fixed**. If the vulnerability is not successfully fixed, it will still be displayed in the vulnerability list after the next vulnerability scan completes.

Step 9 Click a vulnerability name.

Step 10 Click the **Handling History** tab to view the fix status of the target vulnerability in the **Status** column. **Table 6-8** describes vulnerability fix statuses.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

Table 6-8 Vulnerability fix statuses

Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.

Status	Description
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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 In the upper left corner of the page, select **Server View**.

Step 6 Fix Linux and Windows vulnerabilities.

- Fixing all Linux or Windows vulnerabilities on a server
  a. Locate the row containing a target server and click **Fix** in the **Operation** column.

     You can also select multiple servers and click **Fix** in the upper part of the vulnerability list. To fix all server vulnerabilities, you just need to click **Fix** with no need of selecting servers.
  b. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

     For Linux vulnerabilities, you can view fix commands in the dialog box to view the name of the component to be fixed.
  c. (Optional) Back up servers.

Before fixing vulnerabilities, use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

i. In the **Fix** dialog box, click to enable backup.

NOTE

- After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up.
- If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

ii. Choose **Select Server to Scan**. The backup creation dialog box is displayed.

iii. In the **Create Backup** dialog box, set a backup file name, and click **OK**.

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

Only Linux and Windows vulnerabilities can be automatically fixed with one-click. Web-CMS and application vulnerabilities need to be manually fixed by logging in to the server.

e. Click the server name. On the server details slide-out panel displayed, view the vulnerability fix status. **Table 6-9** describes vulnerability fix statuses.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

- Fixing one or more vulnerabilities on a server

a. Click the name of a target server. The server details slide-out panel is displayed.

b. Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

Alternatively, you can select all target vulnerabilities and click **Fix** above the vulnerability list to fix vulnerabilities in batches. To fix all vulnerabilities, click **Fix** with no need of selecting any servers.

c. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

For Linux vulnerabilities, you can view fix commands in the dialog box to view the name of the component to be fixed.

d. (Optional) Back up servers.

Before fixing vulnerabilities, you can use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

i. In the **Fix** dialog box, click to enable backup.

NOTE

- After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up.
- If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

ii. Choose **Select Server to Scan**. The backup creation dialog box is displayed.

iii. In the **Create Backup** dialog box, set a backup file name, and click **OK**.

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

If you have manually fixed the vulnerability, click **Manual handling** in the **Fix** dialog box. After the vulnerability is manually handled, its status changes to **Fixed**. If the vulnerability is not successfully fixed, it will still be displayed in the vulnerability list after the next vulnerability scan completes.

f. In the **Status** column of the target vulnerability, view the fix status of the vulnerability. **Table 6-9** describes vulnerability fix statuses.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

Table 6-9 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.

Status	Description
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Manually Fixing Vulnerabilities

HSS cannot automatically fix Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities in one click. You can log in to the server to manually fix them by referring to the fix suggestions on the vulnerability details slide-out panel.

NOTE

- Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.
- Fix the vulnerabilities in sequence based on the suggestions.
- If multiple software packages on the same server have the same vulnerability, you only need to fix the vulnerability once.

Viewing vulnerability fix suggestions

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 Click the name of a target vulnerability to access the vulnerability details slide-out panel and view the fix suggestions.

----End

Fixing vulnerabilities by referring to vulnerability fix suggestions

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

- Method 1: Create a new VM to fix the vulnerability.

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

  a. Create an image for the ECS to be fixed.

  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.

  Use this method if you have fixed the vulnerability on similar servers before.

  a. Create a backup for the ECS whose vulnerabilities need to be fixed.
  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

Ignoring a Vulnerability

Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. Such vulnerabilities can be ignored. HSS will not generate alarms for ignored vulnerabilities.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 Locate the row containing a target vulnerability and click **Ignore** in the **Operation** column.

Step 6 In the dialog box displayed, click **OK**.

----End

Adding a Vulnerability Whitelist Item

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 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 a vulnerability, choose **More** > **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 **Vulnerability Whitelist**.

  b. In the **Vulnerability Whitelist** area, click **Add Rule**.

  c. Configure a whitelist rule according to **Table 6-10**.

Table 6-10 Vulnerability whitelist rule parameters

Parameter	Description
Type	Select the type of vulnerabilities to be whitelisted. Possible values are as follows: ▪ **Linux Vulnerabilities** ▪ **Windows Vulnerabilities** ▪ **Web-CMS Vulnerabilities** ▪ **Application Vulnerabilities** ▪ **Emergency Vulnerabilities**
Vulnerability	Select one or more vulnerabilities to be whitelisted.

Parameter	Description
Rule Scope	Select the servers affected by the vulnerabilities. Possible values are as follows: ▪ **All servers** HSS will ignore the vulnerability when scanning for vulnerabilities on all servers. ▪ **Selected servers** Select one or more target servers. HSS will ignore the vulnerabilities when scanning for vulnerabilities on these servers. You can search for a target server by server name, ID, EIP, or private IP address.
Remarks (Optional)	Enter the remarks.

d. Click **OK**.

----End

Verifying the Vulnerability Fix

After you manually fix vulnerabilities, you are advised to verify the fixing result.

- **Method 1**: On the **Affected** tab page of the vulnerability details page, choose **More** > **Verify** to verify the vulnerability fix. This method has the following restrictions:
  - The fix of emergency vulnerabilities cannot be verified.
  - Only the fix of the application vulnerabilities of the JAR package can be verified. The application vulnerabilities of non-JAR packages are automatically filtered out and not verified.
- **Method 2**: Ensure the software has been upgraded to the latest version. The following table provides the commands to check the software upgrade result.

Table 6-11 Verification commands

OS	Command
CentOS/Fedora /Euler/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*

6.1.6 Managing the Vulnerability Whitelist

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

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

This section describes how to modify and remove an item in the vulnerability whitelist.

Editing a Vulnerability Whitelist

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 In the upper right corner of the **Vulnerabilities** page, click **Vulnerability Whitelist**.

Step 6 In the row containing the desired vulnerability whitelist rule, click **Edit** in the **Operation** column.

Step 7 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 In the upper right corner of the **Vulnerabilities** page, click **Vulnerability Whitelist**.

Step 6 In the row containing the desired vulnerability whitelist rule, click **Delete** in the **Operation** column.

Step 7 In the dialog box displayed, confirm the information and click **OK**.

----End

6.1.7 Viewing Vulnerability Handling History

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

Constraints

- The basic edition does not support this function.
- Handling history can be retained for a maximum of 180 days.

Viewing the Handling History of a Vulnerability

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 In the list of handled vulnerabilities, click a vulnerability name. The vulnerability details slide-out panel is displayed.

Step 6 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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Handling History**. The **Handling History** page is displayed.

Step 5 On the **Vulnerabilities** tab page displayed, view the handling history of all vulnerabilities.

- Viewing the vulnerability handling history of a specified enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project for **Enterprise Project** to view the handling history of server vulnerabilities in the enterprise project.

- Viewing the vulnerability handling history of a specified property

  In the search box above the vulnerability handling history list, select an attribute or enter a keyword to search for the handling records of a specified attribute.

----End

6.2 Baseline Check

6.2.1 Baseline Check Overview

What Is a Baseline Check?

Baselines specify the recommended security configurations for OSs, databases, middleware, and applications. They include the configurations of permissions, services, network, password security, and DJCP MLPS compliance.

HSS can check password complexity policies, common weak passwords, and other settings to detect insecure passwords and the configuration risks in systems and critical software. It also provides suggestions to help users correctly handle unsafe settings on servers.

Baseline Check Content

Check Item	Description	Supported HSS Edition
Baseline check	Check the unsafe Tomcat, Nginx, SSH login, and system configurations found by HSS. The following systems, databases, and applications can be checked: ● For Linux, – Cloud security practices: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, EulerOS, EulerOS_ext, Kubernetes-Node, Kubernetes-Master, HCE 1.1, HCE 2.0. – DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu12, Ubuntu14, Ubuntu16, Ubuntu18, SUSE 12, SUSE 15, HCE1.1, and Alma. – General security standard: HCE 1.1 **NOTE** The MySQL baseline detection of Linux OS is based on the MySQL 5 security configuration specifications. If MySQL 8 is installed on your server, the following check items are not displayed in the detection results, because they are discarded in that version. The detection results are displayed only on the server whose MySQL version is 5. ● Rule: Do not set **old_passwords** to **1**. ● Rule: Set secure_auth to **1** or **ON**. ● Rule: Do not set **skip_secure_auth**. ● Rule: Set **log_warnings** to **2**. ● Rule: Configure the MySQL binlog clearing policy. ● Rule: The **sql_mode** parameter contains **NO_AUTO_CREATE_USER**. ● Rule: Use the MySQL audit plug-in. ● For Windows, – Cloud security practices: MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016, Windows_2019, and SQL Server.	Enterprise, premium, WTP, and container editions
Password complexity policies	Check whether your password complexity policy of Linux system account is proper and modify it based on suggestions provided by HSS, improving password security.	All

Check Item	Description	Supported HSS Edition
Common weak passwords	Weak passwords defined in the common weak password library. You can check for the weak passwords used by accounts and remind users to change them. Linux supports weak password detection for MySQL, FTP, Redis, and system accounts. Windows supports weak password detection for system accounts.	All

Usage Process

Table 6-12 Usage process

No.	Operation	Description
1	**Performing a Baseline Check**	The baseline inspection supports automatic and manual baseline checks. • Automatic baseline check: automatically performs a baseline check on all servers **at 01:00 every day**. The server configurations, password complexity policies, and common weak passwords are checked. The premium, WTP, and container editions allow you to customize the automatic configuration check period. For details, see **Configuration Check**. For HSS enterprise, premium, WTP, and container editions, you can customize weak passwords and configure the automatic scan period. For details, see **Weak Password Detection**. • Manual baseline inspection: To view the real-time baseline risks of a specified server, you can manually perform a baseline inspection.
2	**Viewing and processing baseline inspection results**	After the baseline inspection is complete, you need to view and handle baseline configuration risks.

6.2.2 Performing a Baseline Check

Scenarios

The baseline checks can be performed automatically or manually.

- Automatic baseline check: The server settings, password complexity policies, and common weak passwords are checked periodically.
- Manual baseline check: To view the real-time baseline risks of specific servers, you can manually perform a baseline check. If multiple baseline check policies are configured for a server, the system displays only the latest baseline check result.

Automatic Baseline Checks

By default, automatically checks the configurations, password complexity policies, and common weak passwords of all servers at about **01:00 in the early morning** every day. After the check is complete, you can view and handle the risk items in your assets.

In the premium, WTP, and container editions, you can customize the automatic check period. For details, see **Configuration Check**.

For HSS enterprise, premium, WTP, and container editions, you can customize weak passwords and configure the automatic scan period. For details, see **Weak Password Detection**.

Manually Performing a Baseline Check

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 5 (Optional) Create a manual baseline check policy.

Before manually checking the baseline policy, you need to create a manual baseline check policy for the target server. If you have created a policy for the target server, skip this step.

1. Click **Policies** in the upper right corner of the page.
2. Click **Create Policy** and configure the policy information by referring to **Table 6-13**.

   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 6-13 Baseline policy parameters

Parameter	Description	Example Value
Policy	Policy name	default_linux_security_check_policy
OS	OS that will be checked. – Linux – Windows	Linux

Parameter	Description	Example Value
Baseline	Baseline used for a check. Check items are as follows: – For Linux, ▪ Cloud security practices: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, EulerOS, EulerOS_ext, Kubernetes-Node, Kubernetes-Master, HCE 1.1, HCE 2.0. ▪ DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu12, Ubuntu14, Ubuntu16, Ubuntu18, SUSE 12, SUSE 15, HCE1.1, and Alma. ▪ General security standard: HCE 1.1 **NOTE** The MySQL baseline detection of Linux OS is based on the MySQL 5 security configuration specifications. If MySQL 8 is installed on your server, the following check items are not displayed in the detection results, because they are discarded in that version. The detection results are displayed only on the server whose MySQL version is 5. ▪ Rule: Do not set **old_passwords** to **1**. ▪ Rule: Set secure_auth to **1** or **ON**. ▪ Rule: Do not set **skip_secure_auth**. ▪ Rule: Set **log_warnings** to **2**. ▪ Rule: Configure the MySQL binlog clearing policy. ▪ Rule: The **sql_mode** parameter contains **NO_AUTO_CREATE_USER**. ▪ Rule: Use the MySQL audit plug-in. – For Windows, ▪ Cloud security practices: MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008,	**Cloud security practices**: Select all.

Parameter	Description	Example Value
	Windows_2012, Windows_2016, Windows_2019, and SQL Server.	

3. 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.
4. Confirm the information and click **OK**. The baseline policy will be displayed in the policy list.

Step 6 In the upper left corner of the **Baseline Inspection** page, select the target baseline inspection policy.

Step 7 Click **Scan** in the upper right corner of the page.

Step 8 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 and Handling Baseline Check Results**.

----End

6.2.3 Viewing and Handling Baseline Check Results

Scenarios

You can check for and fix unsafe baseline settings, weak passwords, and insecure password complexity policies on your servers.

If multiple baseline check policies are configured for a server, the system displays only the latest baseline check result.

Constraints

Only the HSS enterprise, premium, WTP, and container editions support baseline configuration checks.

Detection Description

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

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

Viewing Baseline Check Overview Information

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click different tabs on the displayed page to check the detected unsafe settings. **Table 6-14** lists the corresponding parameters.

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

Table 6-14 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 scanned 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.

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

----End

Viewing and Handling Configuration Check Results

Step 1 Click the **Unsafe Configurations** tab to view the risk items. For more information, see **Table 6-15**.

Table 6-15 Parameter description

Parameter	Description
Risk Level	Level of a detection result. • High • Low • Medium • Secure
Baseline Name	Name of the baseline that is checked.
Type	Policy type of the baseline that has been checked. • **Cloud security practices** • **DJCP MLPS** • **General Security Standard**
Check Item	Total number of configuration items that are checked.
Risky Item	Total number of the risky configurations.
Affected Servers	Total number of servers affected by the detected risks in a baseline.

Parameter	Description
Description	Description of a baseline.

Step 2 Click a baseline name in the list to view the baseline description, affected servers, and details about all check items.

Step 3 Handle risk items.

- **Ignoring risks**

  After a risk is ignored, it will be displayed in the ignored item list. It will no longer be reported in the HSS baseline checks on servers.

  a. Click **Ignore** in the **Operation** column of a check item to ignore it. Select multiple check items and click **Ignore** to ignore them at a time.

  b. In the displayed dialog box, click **OK**.

  You can click **Ignored** above the check item list to view the ignored items.

- **Fixing risks**

  a. Click **View Details** in the **Operation** column of a risk item.

  b. View the content in the **Audit Description**, **Suggestion**, and **Affected Servers**. Rectify the unsafe settings.

  NOTE

  - Currently, one-click fixing is supported for some EulerOS baseline configurations and CentOS 8 baseline configurations. You can simply click **Fix** in the **Operation** column of the target EulerOS or CentOS check item to fix the unsafe settings. If some parameters need to be configured during restoration, retain the default values.
  - You are advised to fix the settings with high severity immediately and fix those with medium or low severity.

  c. After the repair is complete, click **Verify** on the **Affected Servers** tab page to verify the result.

  If a failed check item has been fixed, you can update its status through verification. The restrictions are as follows:

  - Currently, baseline verification is not supported for Windows OSs.
  - The agent status of the target server must be online.
  - Only one risk item can be verified at a time. Other risk items can be verified only after the risk items are verified.
  - Baseline checks are supported for the following Linux OSs: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, SUSE 12, SUSE 15, HCE 1.1, and HCE 2.0.

  d. Click **OK** to start the verification.

e. Return to the check item list page and view the status of the risk item.

The status changes to **Verifying**. The system starts automatic verification. After the verification is complete, check the status. If a check item failed to be fixed, click **View Cause** to view the cause. Then, fix it again.

----End

Checking and Handling Password Complexity Policy Detection Results

Step 1 Click the **Password Complexity Policy Detection** tab to view the risk statistical items and handling suggestions. For more information, see **Table 6-16**.

Table 6-16 Parameter description

Parameter	Description
Server Name	Name and public/private IP address of the scanned server.
Password Length	Whether the password length policy of the target server meets the requirement. • Passed • Failed
Uppercase Letters	Whether the uppercase letter policy used for passwords on the target server meets the requirement. • Passed • Failed
Lowercase Letters	Whether the lowercase letter policy used for passwords on the target server meets the requirement. • Passed • Failed
Digits	Whether the number policy used for passwords on the target server meets the requirement. • Passed • Failed
Special Characters	Whether the special character policy used for passwords on the target server meets the requirement. • Passed • Failed
Suggestion	Suggestion for the password complexity policy of the target server.

Step 2 Modify the password complexity policy on the server as recommended.

- 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?**

Step 3 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.

----End

Viewing and Handling Common Weak Password Detection Results

Step 1 Click the **Common Weak Password Detection** tab to view the statistics of risky weak password accounts on the server. For more information, see **Viewing common weak password detection**.

Table 6-17 Parameter description

Parameter	Description
Server Name	Name and public/private IP address of the scanned server.
Account Name	Accounts with weak passwords that are detected on the target server.
Account Type	Type of an account.
Usage Duration (Days)	Duration a weak password is used.

Step 2 Log in to the server and change the weak password.

NOTE

- To enhance server security, you are advised to modify the accounts with weak passwords in a timely manner, such as SSH accounts.
- To protect internal data of your server, you are advised to modify software accounts that use weak passwords, such as MySQL accounts and FTP accounts.
- A password should contain more than eight characters, including uppercase letters, lowercase letters, digits, and special characters.

Step 3 After the weak password is changed, perform a manual check in the upper part of the **Baseline Checks** page to verify the result.

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

----End

6.2.4 Exporting a Baseline Check Report

Scenarios

Yon can export the baseline check results to your local PC.

Constraints

Only the HSS enterprise, premium, WTP, and container editions support baseline configuration checks.

Exporting a Baseline Check Report

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

Step 5 Perform the following operations to export the detection result based on the baseline check type:

- Unsafe configurations

  Click the **Unsafe Configurations** tab, and click **Export** in the upper left corner of the list. In the displayed dialog box, set the export scope and click **OK** to export the configuration check results.

- Password complexity policies

  Click the **Password Complexity Policy Detection** tab. In the upper left corner of the list, click **Export** > **Export all data to an XLSX file** to export the result.

- Common weak passwords

  Click the **Common Weak Password Detection** tab. In the upper right corner of the list, click to export the result.

  You can enter the server name, IP address, or account name in the upper right corner of the list, and click to search for the target content and download it.

----End

6.2.5 Managing Manual Baseline Check Policies

This section describes how to modify a created manual baseline check policy.

Editing a Manual Baseline Check Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 5 Click **Policies** in the upper right corner of the page.

Step 6 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 7 Confirm the configuration, click **Next**, and select servers.

Step 8 Confirm the information and click **OK**. You can view the updated policy in the policy list.

----End

Deleting a Manual Baseline Check Policy

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**. The HSS page is displayed.

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

NOTE

Only user-defined policies can be deleted. Default policies **default_linux_security_check_policy** and **default_windows_security_check_policy** cannot be deleted.

----End

6.3 Container Image Security

6.3.1 Viewing SWRImage Repository Vulnerabilities

This section describes how to view SWR image repository vulnerabilities and fix the vulnerabilities as prompted.

Prerequisites

Container node protection has been enabled.

Constraints

Only vulnerabilities in Linux images can be checked.

Viewing Vulnerabilities in SWR Images

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Prediction** > **Container Images**.

Step 5 Click the **SWR Image Repository Vulnerability** tab to view the system and application vulnerability lists. For details about the vulnerability list, see **SWR image repository vulnerability parameters**

Table 6-18 SWR image repository vulnerability parameters

Parameter	Description
Vulnerability Name	You can click a vulnerability name to view basic information about a vulnerability and the images affected by the vulnerability.
Repair Urgency	You are advised to fix vulnerabilities of the high and medium levels.
Historically Affected Images	Images affected by the vulnerability.
Solution	HSS provides a recommended solution to the vulnerability. Click the solution description to go to the details page.

----End

6.3.2 Viewing Malicious File Detection Results in Images

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.

Constraints

- This function is available only in the HSS container edition.
- Only malicious files in Linux images can be detected.

Viewing Malicious File Detection Results in Images

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Prediction** > **Container Images**.

Step 5 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

7 Server Protection

7.1 Application Protection

7.1.1 Application Protection Overview

What Is Application Protection?

Based on runtime application self-protection (RASP), the application protection feature provides security check and protection for running applications. You do not need to modify application files. You simply need to inject probes to the applications on servers or containers to enjoy powerful security protection capabilities.

Technical Principles

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

Detection Capabilities

Table 7-1 describes the types of attacks that can be detected by application protection.

Table 7-1 Attack types detected by application protection

Attack Type	Description	Detection Rule ID	Description
SQL injection	SQL injection is an attack technology. Attackers exploit the vulnerabilities of dynamic SQL query in web applications to insert malicious code into user input fields and trick the database into executing SQL commands to steal, tamper with, or damage sensitive data, or run dangerous system-level commands on the database server. Most websites and web applications need to use SQL databases. Therefore, SQL injection attacks become one of the oldest and most widely launched network attacks.	SQLI	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities.
OS command injection	OS command injection is a web program vulnerability that is usually found in applications that require user input. If there is no effective filtering and verification mechanism for user input, this vulnerability may be exploited. It allows attackers to execute arbitrary OS commands on the server where an application is running.	CMDI	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities.
XSS	Cross-site scripting (XSS) is a typical web program vulnerability exploit attack. Attackers can inject executable malicious scripts into websites or web applications where web programs do not check user input. When users access web pages, the malicious scripts are executed to steal users' personal data, display advertisements, or even tamper with web page content.	XSS	Detect and defend against stored XSS attacks.

Attack Type	Description	Detection Rule ID	Description
Log4j RCE vulnerability	Log4j RCE is a major security vulnerability in Apache Log4j 2.x. This vulnerability allows attackers to inject and execute remote code through Java Naming and Directory Interface (JNDI).	Log4jRCE	Detect and defend against remote code execution and intercept attacks.
Web shell upload	Uploading web shells is a network attack method. Attackers upload malicious code such as web shells to a server through vulnerability exploit or other methods to obtain the control permission for the server.	WebShellUpload	Detect and defend against attacks of uploading dangerous files (mainly web shells in JSP format) or renaming existing files to dangerous file name extensions (mainly web shells in JSP format), and check whether web applications have corresponding vulnerabilities.
Memory injection	Memory injection is an advanced network attack technology. Attackers inject malicious code into the memory, bypassing the traditional security defense mechanism and controlling the target system.	FilelessWebshell	Detect various types of fileless Java web shells.
XXE	XXE refers to the XML External Entity Injection vulnerability. If external entity reference is not disabled when an application parses XML files, attackers can construct malicious XML content to read arbitrary files and execute system commands.	XXE	Detect and defend against XXE injection attacks, and check web applications for related vulnerabilities.

Attack Type	Description	Detection Rule ID	Description
Deserialization input	Deserialization is a process of restoring serialized data (such as strings and byte streams) to original objects. In the process of generating a deserialized object, an attacker may construct specific serialized data input to control the generated object and launch attacks.	UntrustedDeserialization	Detect deserialization attacks that exploit unsafe classes.
File directory traversal	File directory traversal means that an attacker accesses or reads any file or folder on a server by modifying URLs or using special characters to bypass the security check of an application.	FileDirAccess	Check whether sensitive directories or files are accessed.
Struts2 OGNL	Struts2 OGNL refers to the Object-Graph Navigation Language (OGNL) in Struts2 in the Java web framework. If OGNL expressions are externally controllable, attackers can construct malicious OGNL expressions to make programs perform malicious operations.	Struts2OGNL	Detect OGNL code execution.
Command execution using JSP	Java Server Pages (JSP) is a technology for developing dynamic web pages. Attackers may exploit JSP security vulnerabilities to execute invalid OS commands, causing data leakage and service interruption.	SuspiciousBehavior	Detect command execution using JSP.
File deletion using JSP	Attackers may exploit JSP security vulnerabilities to delete files from a server.	SuspiciousBehavior	Detect file deletion using JSP.

Attack Type	Description	Detection Rule ID	Description
Database connection exception	Database connection exceptions include but are not limited to network exceptions, configuration errors, and permission exceptions. These exceptions may indicate that applications are being attacked.	SuspiciousException	Detect authentication and communication exceptions thrown by database connections.
0-day vulnerability	0-day vulnerabilities, also called zero-day attacks, usually refers to security vulnerabilities that have not been patched. If such vulnerabilities are detected, hackers can exploit these vulnerabilities to launch zero-day attacks.	• ZeroDay • ZeroDayDetect	• Check whether a command stack is similar to some typical stacks of the 0-day vulnerability. • Check whether the stack hash of a command is in the whitelist of the web application.
SecurityManager permission exception	SecurityManager is a Java security manager class that manages and controls the security of applications. When the SecurityManager detects that the code performs an operation that is not allowed, an exception is thrown.	SuspiciousException	Detect exceptions thrown by SecurityManager.

Application Scenarios and Advantages

- Context awareness: Application protection can provide accurate detection results based on application context.
- Complementary with WAF: Application protection can detect the data written in the memory and unauthorized database access when applications are running.
- 0-day vulnerability defense: Application protection can dynamically detect and defend against attacks in real time when applications are running, blocking 0-day vulnerability exploits.

Constraints

- Application protection is available in HSS premium, WTP, and container editions.

Process of Using Application Protection

Figure 7-1 Usage process

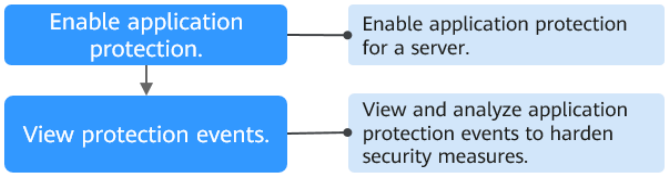


Table 7-2 Process description

Operation	Description
Enabling Application Protection	Enable application protection for a server to assess application security in real time.
Viewing Application Protection Events	Analyze triggered events, harden application protection measures, and improve application security.

7.1.2 Enabling Application Protection

Scenario

To protect Java applications on Linux servers, enable application protection for the servers. HSS will install the RASP plug-in on the servers, and you will need to configure startup parameters.

Enabling Application Protection

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **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

7.1.3 Viewing Application Protection

Scenario

After application protection is enabled, you can view the protection status and events on the **Application Protection** page. You can analyze the events and harden your applications accordingly.

Checking the Protection Status

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Application Protection**. Click the **Protected Servers** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 View the service protection status. For details, see **Table 7-3**.

Table 7-3 Parameters for protection settings

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Private IP address and EIP of the server
OS	Server OS
Server Group	Group that the server belongs to
Policy	Detection policies bound to the target server.
Protection Status	Agent status of a server. • Protected: The agent is online. • Unprotected: The agent is offline.

Parameter	Description
Microservice Protection	Microservice protection status. Its value can be: • Effective: The microservice protection is enabled successfully. • Installing: The microservice RASP protection software is being installed and protection is disabled. • Installed but not configured: The microservice RASP protection software is successfully installed, but microservice startup parameters are not configured and protection is disabled. • Installation failed: The microservice RASP protection software fails to be installed.
RASP Protection.	RASP protection status. Its value can be: If the following information is displayed, protection is not enabled. Check whether there are operations that are not handled by referring to **Enabling Application Protection**. • Installing: The microservice RASP protection software is being installed and protection is disabled. • Installed but not configured: The microservice RASP protection software is successfully installed, but microservice startup parameters are not configured and protection is disabled. • Installation failed: The microservice RASP protection software fails to be installed.
Detected Attacks	Number of attacks detected by RASP.

----End

Viewing Events

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Application Protection** and click the **Events** tab. For more information, see **Table 7-4**.

To view the events of a server, click **View Report** in the **Operation** column of the server.

Table 7-4 Event parameters

Parameter	Description
Severity	Alarm severity. You can search for servers by alarm severities. • **Critical** • **High** • **Medium** • **Low**
Server Name	Server that triggers an alarm
Alarm Name	Alarm name
Alarm Time	Time when an alarm is reported
Attack Source IP Address	IP address of the server that triggers the alarm
Attack Source URL	URL of the server that triggers the alarm

Step 5 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

7.1.4 Managing Application Protection Policies

Scenario

Application protection policies can be added, edited, and deleted in the following scenarios:

- Addition: HSS provides a default policy, which contains all the rules for application protection. If you need to customize the policy for a server, you can add a protection policy and customize the rules and configurations in the policy.
- Editing: You can edit a custom protection policy.
- Deletion: You can delete a custom protection policy that is not associated with any server.

Adding a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Application Protection** and click **Protection Policies**. For more information, see **Table 7-5**.

Table 7-5 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 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click **Add Policy**. In the dialog box that is displayed, configure the parameters by referring to **Table 7-6**.

Table 7-6 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name
Enabled	Whether to enable a rule for the current policy. You can select rules to enable them as required.
Detection Rule ID	ID of a rule.
Action	Action of a rule. • **Detect**: Detects objects based on the target rule and reports alarms for detected risk events. • **Detect and block**: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. **WARNING** Blocking or interception may interrupt services. Exercise caution when enabling this function.
Description	Description about the detected object and behavior of the target protection policy.

Step 7 Click **Configure** in the **Operation** column of a rule to modify the rule content. **Table 7-7** describes the supported rules.

Table 7-7 Detection rules that can be configured only

Rule	Description	Example
XXE	User-defined XXE blacklist protocol	.xml;.dtd;

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

Step 8 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 Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Application Protection** and click **Protection Policies**. For more information, see **Table 7-8**.

Table 7-8 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 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click **Edit** in the **Operation** column of a policy to configure the policy name, supported rules, and rule content.

Table 7-9 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name
Enabled	Whether to enable a rule for the current policy. You can select rules to enable them as required.

Parameter	Description
Detection Rule ID	ID of a rule.
Action	Action of a rule. • **Detect**: Detects objects based on the target rule and reports alarms for detected risk events. • **Detect and block**: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. **NOTICE** Blocking or interception may interrupt services. Exercise caution when enabling this function
Description	Description about the detected object and behavior of the target protection policy.

Step 7 Confirm the rule settings and check items, and click **OK**. You can check whether the rule has been modified on the **Policies** page.

----End

Deleting a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Application Protection** and click **Protection Policies**. For more information, see **Table 7-10**.

Table 7-10 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 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click **Delete** in the **Operation** column of a policy. In the dialog box that is displayed, confirm the policy information and click **OK**.

NOTICE

Only the policies that are not associated with any server can be deleted.

----End

7.1.5 Disabling Application Protection

Scenario

You can disable application protection if it is no longer needed.

Disabling Application Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Application Protection**. Click the **Protected Servers** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Toggle off the switch in the **RASP Protection** column or click **Disable Protection** in the **Operation** column.

Step 7 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

7.2 WTP

7.2.1 WTP Overview

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.

How WTP Prevents Web Page Tampering

WTP supports static and dynamic web page protection. **How WTP works** shows the protection mechanism.

Table 7-11 How WTP works

Protection Type	Mechanism
Static web page protection	1. Local directory lock WTP locks files in a web file directory in a drive to prevent attackers from modifying them. Website administrators can update the website content by using privileged processes. 2. Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. 3. Remote backup and restoration After a remote backup server is configured, if a file in a protected directory is changed, HSS will back up the updated file. If the file and backup directory on the local server become invalid, you can log in to the remote backup server, obtain backup files, and manually restore the tampered websites. You can view backup paths on the **Manage Remote Backup Server** page. For details, see **Changing a Remote Backup Server**.
Dynamic web page protection	The proprietary RASP can detect application program behaviors, prevent attackers from tampering with web pages through application programs, and provide self-protection in Tomcat application runtime.

Constraints

- Web tamper protection is available only in the HSS WTP edition.
- Currently, dynamic WTP can only protect Tomcat applications using JDK 8, JDK 11, and JDK 17.
- After WTP is enabled, the files and folders in the protected directory are set to read-only to prevent unauthorized modification. You can configure privileged processes to modify them. The privileged process function is compatible with Linux and Windows. However, Linux only supports kernel versions 5.10 or later.

Process of Using WTP

Figure 7-2 Usage process

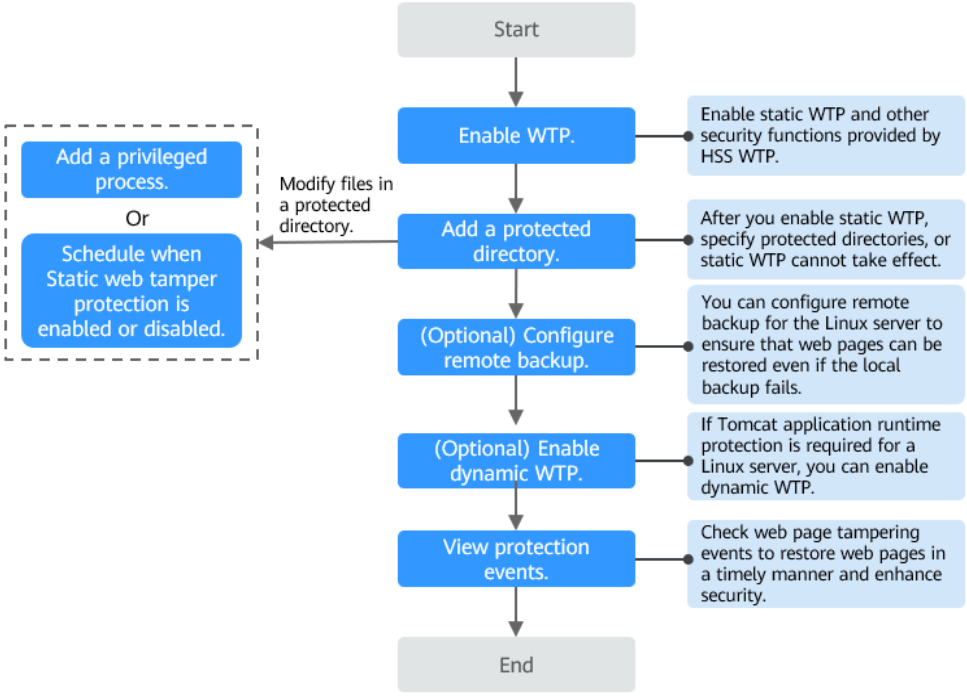


Table 7-12 Process of using WTP

Operation	Description
Enabling Web Tamper Protection	After the WTP edition is enabled, static WTP and other protection functions are enabled automatically.
Adding a Protected Directory	Static WTP protects specified directories. You need to configure static WTP directories.
(Optional) **Configuring Remote Backup**	By default, for Linux servers, HSS backs up files in the protected directories to the local backup paths you specified when adding protected directories. To prevent the local backup from being damaged by attackers, you can configure remote backup to protect web page backup data.
(Optional) **Enabling Dynamic WTP**	For Linux servers, HSS provides runtime application self-protection (RASP) for Tomcat applications. You can enable dynamic WTP for Tomcat applications as required.
Viewing WTP Events	Tamper events that occur during web tamper protection are recorded and displayed in the event list.
Adding a Privileged Process	After static WTP is enabled, the content in the protected directory is read-only and cannot be modified. To modify a protected file, you can add a privileged process.

Operation	Description
Enabling/ Disabling Scheduled Static WTP	Not all OS kernel versions support privileged processes and each server can add up to 10 privileged processes. For OSs that do not support privileged processes, you can set periodic static WTP and update websites while WTP is automatically disabled.

7.2.2 Enabling Web Tamper Protection

Scenarios

The HSS web tamper protection (WTP) edition can protect dynamic and static web pages from being tampered with, enhancing the security and integrity of website content. It also includes the server protection capabilities of the premium edition, such as asset management, vulnerability detection, baseline check, intrusion detection, and ransomware protection, to detect attacks on servers.

This section describes how to enable WTP.

Prerequisites

- Ensure that the agent has been installed on the server and is online. For details, see **Installing the Agent on Cloud Platform Servers**.

Constraints

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

- After the Windows firewall is enabled, HSS automatically adds firewall rules **hostguard_AllowAnyIn** and **hostguard_AllowAnyOut** to allow all inbound and outbound traffic. This ensures that the firewall does not affect your services. If HSS detects a brute-force attack, it adds an inbound rule to the firewall to block the attack source IP address. This does not affect your servers.
- Do not disable the Windows firewall when using HSS, or HSS cannot block the source IP addresses of brute-force attacks. Once it is disabled, HSS may fail to block the attack source IP addresses even after you manually enable it again.

Enabling Web Tamper Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.

Step 5 On the **Add Server** page, click the **Available Servers** tab. Select the target server, and click **Add and Enable Protection**.

Step 6 You can check the server protection status on the **Web Tamper Protection** page.

- Choose **Server Protection** > **Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.

NOTE

- After WTP is enabled for a website, if you need to update the website, add a privileged process or temporarily disable WTP. Enable WTP 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.

----End

Advanced Defense Functions

HSS provides a series of advanced defense functions. You can enable or use them as required to enhance the security protection level of your servers. For details, see **Table 3-7**.

Table 7-13 Advanced defense functions

Function	Description
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.
Ransomware Prevention	The function can detect and defend against ransomware. It can automatically back up data either at a scheduled time, or immediately if ransomware is detected. This can help you defend against ransomware and reduce loss. Ransomware prevention is automatically enabled with the container edition. HSS will deploy honeypot files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy.
Application Process Control	Application process control helps to enhance the security of applications and processes running on servers. It can automatically identify and analyze application processes, and classify them into trusted, suspicious, and malicious processes. It allows trusted processes to run, and generates alarms for suspicious and malicious processes. This helps to build a secure environment for application processes, and protects servers from untrusted or malicious application processes.

Function	Description
Virus Scanning and Removal	This function combines cloud-based and local antivirus mechanisms to scan executable files, compressed files, scripts, documents, images, and audiovisual files for viruses. You can perform quick scan, full-disk scan, and custom scans on servers as needed to detect and remove virus files in a timely manner, enhancing the virus defense of the system.
Dynamic Port Honeypot	The dynamic port honeypot function is a proactive defense measure. It uses a real port as a honeypot port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user.

7.2.3 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.

Constraints

- 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 Click ☰ in the upper left corner of the page, select a region, and choose **Security** > **Host Security Service**. The HSS page is displayed.

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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 7-14**.

Table 7-14 Parameters for adding a protected directory

Parameter	Description	Example Value
Protected Directory	Directory to be protected. – Only one protected directory can be added. The directory length cannot exceed 256 characters. – Do not add an OS directory as a protected directory. – After a directory is added, the files and folders in the protected directory are read-only and cannot be modified directly.	– Linux: **/etc/lesuo** – Windows: **d:\web**
Excluded Subdirectory	Subdirectories that do not need to be protected in the protected directory, such as temporary file directories. A maximum of 10 subdirectories can be added. Separate multiple subdirectories with semicolons (;). Each subdirectory can contain a maximum of 256 characters.	– Linux: **lesuo/test** – Windows: **web \test**

Parameter	Description	Example Value
Excluded File Types	Types of files that do not need to be protected in the protected directory, such as log files. – The file type can contain only letters and numbers. A maximum of 10 file types can be added. Each file type can contain a maximum of 10 characters. Multiple file types are separated by 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.	log;pid;text
Local Backup Path	Set this parameter if your server runs the Linux OS. Set a local backup path for files in protected directories. After WTP is enabled, files in the protected directory are automatically backed up to the local backup path. The backup rules are described as follows: – The local backup path must be valid and cannot overlap with the protected directory path. – Excluded subdirectories and types of files are not backed up. – Generally, the backup completes within 10 minutes. The actual duration depends on the size of files in the protected directory. – If WTP detects that a file in a protected directory is tampered with, it immediately uses the backup file on the local server to restore the file.	/etc/backup

Parameter	Description	Example Value
Excluded File Path	Set this parameter if your server runs the Linux OS. Files that do not need to be protected in the protected directory. A maximum of 50 paths can be added. Separate multiple paths with semicolons (;). Each path can contain a maximum of 256 characters.	lesuo/data;lesuo/list

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 .

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

Related Operations

- 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.

7.2.4 Configuring Remote Backup

After a remote backup server is configured, if a file in a protected directory is changed, HSS will back up the updated file. By default, HSS backs up files in the protected directory to the local backup path configured in the **Add Protected Directory** dialog box. (Excluded subdirectories and file types will not be backed up). Enable remote backup to prevent local backup files from being damaged by attackers.

If the file and backup directory on the local server become invalid, you can log in to the remote backup server, obtain backup files, and manually restore the tampered websites. You can view backup paths on the **Manage Remote Backup Server** page. For details, see **Changing a Remote Backup Server**.

Constraints

- Only Linux servers support remote backup.
- The server used for remote backup must meet the following requirements:
  - Cloud platform Linux servers
  - The server status is **Running**.
  - The HSS agent has been installed on the server and its **Agent Status** is **Online**.

NOTICE

- The remote backup function can be used when the Linux backup server is connected to the protected cloud server. To ensure 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 Click ☰ in the upper left corner of the page, select a region, and choose **Security** > **Host Security Service**. The HSS page is displayed.

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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**.

Table 7-15 Backup server parameters

Parameter	Description	Example Value
Address	This address is the private network address of the server.	192.168.0.249
Port	Ensure that the port is not blocked by any security group or firewall or occupied.	8080
Backup Path	Path of remote backup files. • If the protected directories of multiple servers are backed up to the same remote backup server, the data will be stored in separate folders named after agent IDs. Assume the protected directories of the two servers are **/hss01** and **hss02**, and the agent IDs of the two servers are **f1fdbabc-6cdc-43af-acab-e4e6f086625f** and **f2ddbabc-6cdc-43af-abcd-e4e6f086626f**, and the remote backup path is **/hss01**. The corresponding backup paths are **/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f** and **/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f**. • If WTP is enabled for the remote backup server, do not set the remote backup path to any directories protected by WTP. Otherwise, remote backup will fail.	/hss01

Step 6 Click **OK**.

----End

Setting remote backup

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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

Changing a Remote Backup Server

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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

Step 5 Click **Manage Remote Backup Servers**. The **Manage Remote Backup Servers** page is displayed. Click **Edit** in the **Operation** column to modify the information about the remote backup server.

Step 6 Click **OK**.

----End

Related Operations

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.

7.2.5 Enabling Dynamic WTP

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

Constraints

- Only the servers that are protected by the HSS WTP edition support the operations described in this section.
- Dynamic WTP can be provided only for Tomcat running JDK 8.

Prerequisites

You are using a server running the Linux OS.

Enabling Dynamic WTP

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**. The HSS page is displayed.

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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

7.2.6 Viewing WTP Events

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

Prerequisites

Agent Status of the server is **Online**, and its **WTP Status** is **Enabled**. For more information, see **Viewing Server Protection Status**.

Viewing WTP Events

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Web Tamper Protection** and click **Events** to view the tampering records of protected files on servers.

----End

7.2.7 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 OSs, 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 **Server Protection** > **Web Tamper Protection**. Click the **Servers** tab.

Adding a Privileged Process

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**. The HSS page is displayed.

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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**.

----End

Related Operations

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.

7.2.8 Enabling/Disabling Scheduled Static WTP

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.

Rules for Setting an Unprotected Period

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

Enabling/Disabling Scheduled Static WTP

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**. The HSS page is displayed.

Step 3 Choose **Server Protection** > **Web Tamper Protection**. Click **Configure Protection** in the **Operation** column.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

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 >= 5 minutes
- Unprotected period < 24 hours
- Periods (except for those starting at 00:00 or ending at 23:59) cannot overlap and must have at least a 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

7.3 Ransomware Prevention

7.3.1 Ransomware Prevention Overview

Ransomware can intrude a server, encrypt data, and ask for ransom, causing service interruption, data leakage, or data loss. Attackers may not unlock the data even after receiving the ransom. HSS provides static and dynamic ransomware prevention. You can periodically back up server data to reduce potential losses.

Constraints

- Only the HSS premium, WTP, and container editions support ransomware prevention.
- If the agent of version 3.2.10 or later is installed on a Linux server, or the agent of version 4.0.22 or later is installed on a Windows server, and the HSS premium, WTP, or container edition is enabled for the server, HSS will **automatically** enable **ransomware prevention** for the server, but will not automatically enable ransomware backup. You can enable it as needed. If the agent version installed on the server is not in the preceding range, you need to manually enable ransomware prevention and backup.
- Ransomware prevention is a systematic project that involves multiple aspects, including security management and technical defense. As an important part of ransomware prevention, HSS helps to identify and block ransomware, but it cannot defend against all ransomware. To minimize the loss caused by ransomware, you are advised to build a systematic protection solution, including but not limited to reducing exposure to the the Internet, strengthening network access control, strictly managing account permissions, and building a highly reliable service architecture. In addition, you are advised to periodically back up important service data, so that services can be quickly

restored through backup if a ransomware attack occurs, thus reducing interruptions.

Process of Using Ransomware Prevention

Table 7-16 Usage process

Operation	Description
Enabling Ransomware Prevention	Enable ransomware prevention for a server, deploy static and dynamic honeypots, and detect ransomware attacks in real time. **CAUTION** If you find suspicious files on a server after enabling ransomware prevention, contact technical support and check whether the files are the honeypots deployed by HSS. Honeypot files are used to detect ransomware attacks. They do not affect your services, do not contain any malicious content, and cannot be manually deleted. • If the agent of version 3.2.10 or later is installed on a Linux server, or the agent of version 4.0.22 or later is installed on a Windows server, and the HSS premium, WTP, or container edition is enabled for the server, HSS will **automatically** enable **ransomware prevention** for the server. You can modify the default protection policy settings (including protected directories and actions) as needed. For details, see **Managing Ransomware Protection Policies**. • If the version of the agent installed on the server is not one of the preceding versions, you need to manually enable ransomware prevention.
Viewing and Handling Ransomware Prevention Events	Once a ransomware attack is detected during ransomware protection, analyze and isolate the ransomware in a timely manner, and fix the security weaknesses of the system.

7.3.2 Enabling Ransomware Prevention

Scenarios

Ransomware prevention can detect and defend against known and unknown ransomware in real time. You are advised to enable it for every server.

If the agent version of a server is one of the following versions, and you enable the HSS premium, WTP, or container security edition for it, HSS will automatically **enable ransomware prevention for the server**, deploy honeypot files on the server, and automatically isolate suspicious processes. (There is a low probability that some normal processes are incorrectly isolated.) After ransomware prevention is automatically enabled, you can modify the default protection policy settings (including protected directories and actions) as needed. For details, see **Managing Ransomware Protection Policies**.

- Linux: The agent version is 3.2.10 or later.
- Windows: The agent version is 4.0.22 or later.

If the agent version of a server is not one of the preceding versions, or ransomware prevention has been disabled, you can perform the operations in this section to enable it.

CAUTION

If you find suspicious files on a server after enabling ransomware prevention, contact technical support and check whether the files are the honeypots deployed by HSS. Honeypot files are used to detect ransomware attacks. They do not affect your services, do not contain any malicious content, and cannot be manually deleted.

Step 1: Creating a Protection Policy

Before enabling ransomware prevention, create a ransomware protection policy and configure honeypot protection directories, protected file types, and protection actions.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Ransomware Prevention**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Policies** tab and click **Add Policy**.

Step 7 Configure policy parameters. For more information, see **Table 7-17**.

Table 7-17 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name.	Anti_Ransomware

Parameter	Description	Example Value
Action	How an event is handled. • **Report alarm and isolate**: If a ransomware attack is detected, an alarm will be generated, and the process that attempts to encrypt files will be blocked. • **Report alarm**: If a ransomware attack is detected, only an alarm will be reported.	**Report alarm and isolate**
Dynamic Honeypot Protection	A honeypot is a file that simulates actual service files. It can induce attackers and capture ransomware encryption behaviors in real time. Generally, dynamic and static honeypots are used together for comprehensive protection. After honeypot protection is enabled, the system will deploy honeypot files in honeypot directories and other random locations. (Honeypot files will not be deployed in the excluded directories specified by users). The honeypot files deployed in random locations are automatically deleted every 12 hours and then randomly deployed again. A honeypot file occupies a few server resources. You can configure excluded directories, and the honeypot files will not be deployed in them. Dynamic honeypots are more flexible and can better detect ransomware attacks. This parameter is mandatory only for Linux servers.	Enabled

Parameter	Description	Example Value
Honeypot File Directories	Static honeypots are deployed in specified directories. You can add important service directories or data directories as protected directories. Honeypot files will be deployed in these specified directories (excluding their subdirectories). They can distract attackers and slow down their attacks on real resources. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	• Linux: /root;/home;/opt;/var;/etc • Windows: C:\software
Excluded Directory (Optional)	Directory that does not need to be protected by honeypot files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	• Linux: /bin;/boot;/lib;/lib32;/lib64;/lost+found;/proc;/run;/sbin;/selinux;/srv;/sys;/usr/bin;/usr/local/bin;/usr/local/sbin;/usr/sbin;/var/lib/container;/var/lib/kubelet;/var/lib/ntp/proc • Windows: C:\software\test
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory only for Linux servers.	Select all

Step 8 Click **OK**.

If the added protection policy is displayed in the protection policy list, the policy has been added.

----End

Step 2: Enabling Ransomware Prevention

After a protection policy is created, you can enable ransomware prevention by referring to this section.

Step 1 On the **Ransomware Prevention** page, click the **Protected Servers** tab.

Step 2 In the **Ransomware Prevention Status** column of a server, click **Enable**.

You can also select multiple servers and click **Enable Ransomware Prevention** above the server list.

Step 3 In the **Enable Ransomware Prevention** dialog box, confirm the server information and select a protection policy.

Step 4 Click **OK**.

If the **Ransomware Prevention Status** of the server changes to **Enabled**, ransomware protection is enabled successfully. For details about the ransomware prevention status, see **Table 7-18**.

Table 7-18 Protection status description

Ransomware prevention status	Description
Protected	Ransomware prevention has been enabled.
Disabled	Ransomware prevention is not enabled.
Enabling	Ransomware prevention is being enabled.
Disabling	Ransomware prevention is being disabled.
Protection failed	Ransomware prevention failed.
Protection degraded	Honeypot files failed to be deployed in some protected directories. As a result, the protection is degraded. Check whether the **System** group has full control permissions on the protected directories.

----End

Follow-up Operations

So far, no tools can defend against all ransomware. You are advised to enable backup for servers, so that their data can be restored in a timely manner in the case of a ransomware attack. For details, see **Enabling Backup**.

7.3.3 Enabling Backup

Scenarios

So far, no tools can defend against all ransomware. You can enable backup for servers, so that their data can be restored in a timely manner in the case of a ransomware attack.

Ransomware backup can be performed in two modes: **scheduled backup** and **immediate backup upon ransomware detection**. You can create a custom scheduled backup policy to periodically back up servers. If HSS detects a suspected

ransomware attack, it will immediately trigger a backup to ensure service data is stored as much as possible.

This section describes how to enable ransomware backup.

(Optional) Step 1: Purchasing a Backup Vault

You can purchase a backup vault on the HSS console by referring to this section, or on the CBR console.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Ransomware Prevention**.

Step 5 Toggle on ransomware backup. In the dialog box that is displayed, click **Next**.

Step 6 In the displayed dialog box, set the vault parameters.

Table 7-19 Parameters for purchasing backup capacity

Parameter	Description
Billing Mode	The default billing mode is pay-per-use. 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.
Price	Fees are generated by default based on the backup capacity.

Step 7 Click **OK**.

----End

Step 2: Enabling Ransomware Backup

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Ransomware Prevention**.

Step 5 Click the **Protected Servers** tab.

Step 6 Select a server and click **Enable Backup**.

Step 7 In the **Enable Backup** dialog box, select a vault.

A vault that meets the following conditions can be bound:

- The vault is in **Available** or **Locked** state.
- The backup policy is in **Enabled** state.
- The vault has backup capacity available.
- The vault is bound to fewer than 256 servers.

Step 8 Click **OK**.

If the binding status of the repository on the target server is **Bound**, the ransomware backup is enabled.

----End

Related Operations

Ransomware backup can only be used to restore data after a ransomware attack to reduce some losses. To detect and defend against ransomware attacks in real time, enable ransomware prevention. For details, see **Enabling Ransomware Prevention**.

7.3.4 Viewing and Handling Ransomware Prevention Events

Scenarios

After ransomware protection is enabled, if a ransomware attack event occurs on the server, the event will be recorded and displayed in the ransomware event list. You can handle the events based on your service requirements.

Constraints

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

Viewing and Handling Ransomware Prevention Events

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Ransomware Prevention**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Events** tab and check events.

To check alarm details, click an alarm name.

Step 7 After confirming the severity of an event, click **Handle** in the **Operation** column of the target event to handle the event.

You can also select multiple events and click **Batch Handle** above the list to handle events in batches.

Step 8 In the **Handle Event** dialog box, select an action. For details, see **Table 7-20**.

Table 7-20 Alarm handling methods

Parameter	Description
Action	• **Mark as handled** For a manually handled event, you can add remarks to record the details about the event. • **Ignore** Ignore the current alarm. Any new alarms of the same type will still be reported by HSS. • **Add to alarm whitelist** Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. • **Isolate and kill** If a program is isolated and killed, its executable file status will change to read-only, and the program will be terminated immediately. To avoid impact on services, exercise caution when performing this operation. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** in the upper right corner to check the files. For details, see **Managing Isolated Files**.
Batch Handle	If this option is selected, the same alarms triggered at different time are handled in batches. If no duplicate alarm is displayed after you select it, it indicates no duplicate alarms have been generated.
Remarks	You can add remarks for convenient backtracking.

Step 9 Click **OK**.

----End

7.3.5 Managing Ransomware Protection Policies

Scenarios

After ransomware prevention is enabled, you can manage its policies as needed. Supported operations include:

- **Changing a Policy**: If the current protection policy bound to a server cannot meet your requirements, you can bind another policy to the server.

- **Modifying a Policy**: If you need to modify specific settings (such as the honeypot protection directories or excluded directories), you can modify them in an existing protection policy. When HSS automatically enables ransomware prevention, a protection policy is configured by default. (The default policy for Linux is **tenant_linux_anti_default_policy**, and that for Windows is **tenant_Windows_anti_default_policy**.) You can modify them as needed.
- **Deleting a Policy**: If a protection policy is discarded and not associated with any servers, you can delete the policy.

Constraints

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

Changing a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Ransomware Prevention**.

Step 5 Click the **Protected Servers** tab.

Step 6 Select a server and click **Change Policy**.

You can also choose **More** > **Change Policy** in the **Operation** column of a server.

Step 7 In the **Change Policy** dialog box, select a protection policy.

Step 8 Click **OK**.

----End

Modifying a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Policies** tab.

Step 5 Click **Edit** in the **Operation** column of a policy. Edit the policy configurations and associated servers. For more information, see .

The following uses a Linux server as an example. On the **Protected Servers** tab, you can also click the name of the policy associated with the server to edit the policy.

Table 7-21 Protection policy parameters

Parameter	Description	Example Value
Policy	Policy name.	Anti_Ransomware
Action	How an event is handled. • **Report alarm and isolate**: If a ransomware attack is detected, an alarm will be generated, and the process that attempts to encrypt files will be blocked. • **Report alarm**: If a ransomware attack is detected, only an alarm will be reported.	Report alarm and isolate
Dynamic Honeypot Protection	A honeypot is a file that simulates actual service files. It can induce attackers and capture ransomware encryption behaviors in real time. Generally, dynamic and static honeypots are used together for comprehensive protection. After honeypot protection is enabled, the system will deploy honeypot files in honeypot directories and other random locations. (Honeypot files will not be deployed in the excluded directories specified by users). The honeypot files deployed in random locations are automatically deleted every 12 hours and then randomly deployed again. A honeypot file occupies a few server resources. You can configure excluded directories, and the honeypot files will not be deployed in them. Dynamic honeypots are more flexible and can better detect ransomware attacks. This parameter is mandatory only for Linux servers.	Enabled

Parameter	Description	Example Value
Honeypot File Directories	Static honeypots are deployed in specified directories. You can add important service directories or data directories as protected directories. Honeypot files will be deployed in these specified directories (excluding their subdirectories). They can distract attackers and slow down their attacks on real resources. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	• Linux: /root;/home;/opt;/var;/etc • Windows: C:\software
Excluded Directory (Optional)	Directory that does not need to be protected by honeypot files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	• Linux: /bin;/boot;/lib;/lib32;/lib64;/lost+found;/proc;/run;/sbin;/selinux;/srv;/sys;/usr/bin;/usr/local/bin;/usr/local/sbin;/usr/sbin;/var/lib/container;/var/lib/kubelet;/var/lib/ntp/proc • Windows: C:\software\test
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. **This parameter is mandatory only for Linux servers.**	Select all
(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.**	-

Parameter	Description	Example Value
Associate Servers	Information about the server associated with the policy. If you want to disassociate the server (disable ransomware protection), you can delete the policy.	-

Step 6 Confirm the policy information and click **OK**.

----End

Deleting a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Policies** tab.

Step 5 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 6 Confirm the policy information and click **OK**.

----End

7.3.6 Restoring Server Data

Scenarios

If ransomware backup is enabled for a server, and the server is intruded by ransomware, you can use the backup to restore the server data and minimize losses. Before using the backup for server restoration, check whether the backup is normal. If it is, use it to restore service-critical systems first.

Prerequisites

The backup function has been enabled. For details, see **Enabling Backup**.

Restoring Server Data

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Protected Servers** tab. In the **Operation** column of a server, click **Restore Data**.

Step 5 In the displayed dialog box, view the information about the target server. Search for the backup data source to be restored by backup status and backup name. For details about the parameters, see **Table 7-22**.

Table 7-22 Backup data source parameters

Parameter	Description	Example Value
Backup Name	Name of a backup file.	-
Status	Backup status. It can be: • **Available**: The backup data source is normal and can be used for restoration. • **Creating**: The backup is being created. • **Deleting**: The backup is being deleted. • **Restoring**: The backup is being used for restoration. • **Error**: Backup error.	Available
Purpose	Backup purpose. It can be: • **Periodic execution**: Data is automatically backed up based on the backup period configured in the backup policy. • **Ransomware protection**: Data is backed up immediately when a server is attacked by ransomware.	Periodic execution
Execution Time	Time when the data source was backed up.	-

Step 6 In the **Operation** column of a backup, click **Restore Data**.

Step 7 In the displayed dialog box, confirm the server information and click **OK**.

Step 8 In the **Backup Statistics** column, click the value of **Backup and Restoration Task** to view the backup and restoration progress.

----End

Related Operations

Deleting a backup

You can delete the backup data of a server if it is no longer required. A deleted backup cannot be restored. Exercise caution when performing this operation.

1. In the **Backups** column of a server, click the number. The backup list is displayed.
2. In the **Operation** column of a backup, click **Delete**. The backup deletion dialog box is displayed.
3. Confirm the backup information and click **OK**.

7.3.7 Managing Server Backup

Scenarios

After ransomware backup is enabled for a server, the backup vault backs up the server periodically based on a backup policy. If HSS detects a ransomware attack, the vault will back up the server immediately.

- If no backup policy is bound to the vault, it cannot perform periodic backups. You need to perform the operations in **Binding to a Backup Policy**.
- If the vault capacity is insufficient, backup cannot be performed. In this case, perform the operations in **Increasing the Backup Capacity**.
- If the backup period and backup retention rule of a backup policy do not meet your requirements, perform the operations in **Modifying a Backup Policy**.

Prerequisites

Ransomware backup has been enabled. For details, see **Enabling Backup**.

Binding to a Backup Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Prevention** > **Ransomware Prevention**.

Step 5 In the **Backup Policy Status** column of a server, click **Bind Backup Policy**.

Step 6 In the **Backup Policy** drop-down list, select a policy.

If no backup policies are available or you want to create a backup policy for the vault, click **Create Policy in CBR**. After the backup policy is created, return to the HSS console and select the new policy.

Step 7 Click **OK**.

If the **Backup Policy Status** of the server is **Enabled** and the policy name is the one you selected, the backup policy has been bound.

----End

Increasing the Backup Capacity

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Server Protection** > **Ransomware Prevention**.

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

Step 6 In the displayed dialog box, configure the capacity.

Step 7 If the information is correct, click **OK**. The payment page is displayed. After the payment is complete, return to the **Protected Server** tab page to view the storage capacity of the target server.

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

----End

Modifying a Backup Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Server Protection** > **Ransomware Prevention**.

Step 5 Click the policy name in the **Backup Policy Status** column of a server. The **Modify Policy** dialog box is displayed.

Step 6 In the dialog box, modify the backup rule. For details, see **Policy parameters**.

Table 7-23 Parameters for modifying a backup rule

Parameter	Description	Example Value
Backup Frequency	Data can be automatically backed up on specific days in a week, or at a fixed interval. • **Weekly**: Specifies on which days of each week the backup will be executed. You can select multiple days. • **Day based**: Specifies the interval (every 1 to 30 days) for executing the backup. If you select **Day based**, the first backup time is supposed to be on the day when the backup policy is created. If the execution time on the day you create the backup policy has passed, the first backup will be executed in the next backup cycle.	Every 1 day
Execution Time	Time when a backup task is executed. Backups can only be scheduled on the hour. You can select multiple hours. It is recommended that backups be performed during off-peak hours or when no services are running. Backup rule examples: • Rule 1: Set **Backup Frequency** to **Weekly** (**Wednesday** and **Saturday**) and **Execution Time** to **00:00** and **13:00**. The backup task will be executed at 00:00 and 13:00 every Wednesday and Saturday. • Rule 2: Set **Backup Frequency** to **Day based** and set the interval to two days. Set **Execution Time** to **02:00** and **14:00**. The backup task will be executed at 02:00 and 14:00 every two days from the date when the backup rule is set.	00:00, 07:00
Timezone	Select the time zone of the backup time.	UTC+08:00

Step 7 Confirm the settings and click **Next**. Configure the backup retention rule.

- **Type**: **Backup quantity**

  Table 7-24 describes the parameters for configuring a backup rule.

Table 7-24 Parameters for data retention by quantity

Parameter	Description	Example Value
Rule	The total number of backups retained for a single cloud server. The value range is 2 to 99,999. This setting takes effect no matter how you configure advanced options. For example, if the rule is configured to keep the most recent 30 backups, and **Advanced Options** are configured to keep the latest backups in the last 3 months (90 days), the latest 30 backups will be retained.	30
(Optional) Advanced Options	Long-term retention rule. This rule and the quantity-based backup retention rules do not conflict. They will both be applied. – **Daily Based**: The latest backup from each of the last N days is retained. N ranges from 0 to 100. – **Weekly**: The latest backup from each of the last M weeks is retained. M ranges from 0 to 100. – **Monthly**: The latest backup from each of the last P months is retained. P ranges from 0 to 100. – **Yearly**: The latest backup from each of the last Q years is retained. Q ranges from 0 to 100.	Keep the most recent backup from each of the last three months

- **Type**: **Time period**

  Table 7-25 describes the parameters for configuring a backup rule.

Table 7-25 Parameters for data retention by time period

Parameter	Description	Example Value
Rule	You can set the backup retention period to 1 month, 3 months, 6 months, 1 year, or a custom period. The custom retention period ranges from 2 to 99,999 days. If the retention period of a backup exceeds the specified period, the backup will be automatically deleted.	3 months

- **Type**: **Permanent**

  Backup data will be permanently stored.

  NOTE

  If the **Retention Type** of a rule is changed from **Time period** to another, historical backups will still be deleted based on the **Time period** settings.

Step 8 Click **OK**.

----End

7.3.8 Disabling Ransomware Prevention

Scenario

You can disable ransomware protection as needed. After protection is disabled, your server may be intruded by ransomware. Exercise caution when performing this operation.

Disabling Ransomware Prevention

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Protected Servers** tab.

Step 5 Choose **More** > **Disable Protection** in the **Operation** column of the target server.

Step 6 Confirm the information and click **OK**.

----End

7.4 Application Process Control

7.4.1 Application Process Control Overview

HSS can learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.

Constraints

- Application process control is available only in HSS premium, WTP, and container editions.
- To use application process control, ensure the agent installed on the server falls within the following range. For details about how to upgrade the agent, see **Upgrading the Agent**.
  - Linux: 3.2.7 or later
  - Windows: 4.0.19 or later

Process of Using Application Process Control

Figure 7-3 Usage process

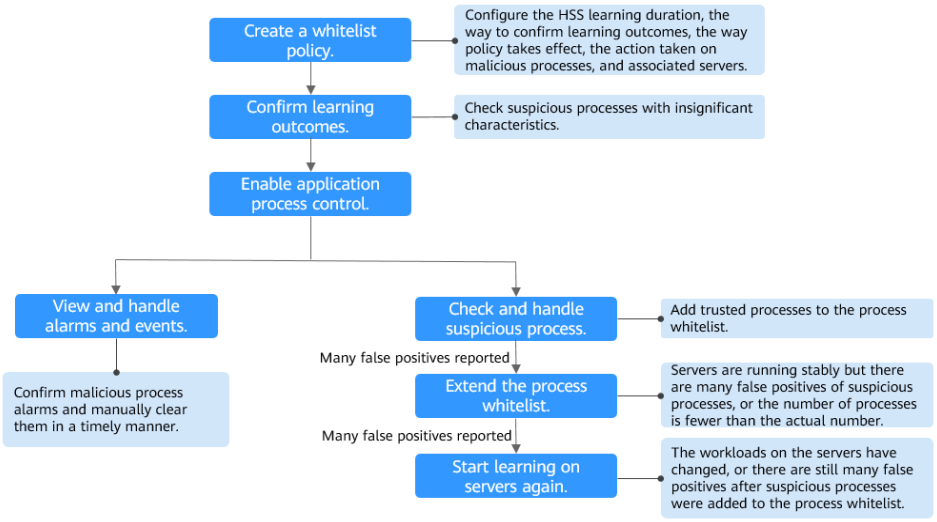


Table 7-26 Process of using application process control

Operation	Description
Create a whitelist policy.	A whitelist policy specifies how HSS learns server behaviors and protect application processes. Application process protection can be enabled only for servers associated with a whitelist policy.
Confirm learning outcomes.	After the HSS learns the application processes on servers, there may be some suspicious application processes with insignificant characteristics, and HSS cannot determine whether they are malicious or trustworthy. In this case, you need to confirm the learning outcomes.

Operation	Description
Enable application process control.	Enable application process control on the servers associated with a policy.
Check and handle suspicious processes.	HSS cannot determine whether some suspicious application processes with insignificant characteristics are trustworthy. You need to check their process details, determine whether they are trustworthy, and add them to the process whitelist.
Check and handle malicious process alarms.	HSS reports an alarm once it detects a malicious process. Choose **Detection & Response** > **Alarms**, check and handle the alarms on the **Server Alarms** tab page, and clear malicious processes in a timely manner.
(Optional) **Add items to the process whitelist.**	After HSS completes learning, if you think the number of application processes it learned is fewer than the number of process fingerprints collected by the asset fingerprint function, or if it regarded many trustworthy application processes as suspicious, you can extend the HSS process whitelist. HSS will compare the application processes it already learned with the collected process fingerprints to enrich the HSS application process intelligence library and extend the trusted process whitelist.
(Optional) **Start learning on the servers again.**	If you have added trustworthy processes to the whitelist but there are still many false positives reported, you can let HSS start learning again on the servers.

7.4.2 Creating a Whitelist Policy

Scenarios

Before enabling application process control, you need to create a whitelist policy and configure the HSS learning duration, the way to confirm learning outcomes, the way policy takes effect, and the action taken on malicious processes. HSS will manage application processes based on your policies.

Creating a Whitelist Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab. Click **Create Policy**.

Step 6 In the **Create Policy** dialog box, configure policy parameters. For details about related parameters, see **Table 7-27**.

Table 7-27 Whitelist policy parameters

Parameter	Description	Example Value
Policy Mode	Mode of the application process control policy. The conservative mode is used by default. Trustworthy and suspicious processes are allowed to run. Alarms are generated only for malicious processes.	-
Policy Name	A whitelist policy name is generated by default. You are advised to set a custom name to facilitate management.	test
Intelligent Learning Period	Number of days that HSS learns the application processes on servers. A long learning period indicates accurate learning outcomes.	7
Confirm Learning Outcomes	The way to confirm suspicious processes with insignificant characteristics after HSS completes learning on the servers associated with the policy. • **Automatically**: HSS automatically marks suspicious application processes with insignificant characteristics based on the application process signature database. • **Manually**: After HSS finishes learning based on policy configurations, choose **Application Process Control** > **Whitelist Policies**. Click a policy name. On the policy details page, click the **Process Files** tab and filter processes in the **To be confirmed** state. Manually mark suspicious processes with insignificant characteristics.	Automatically
Apply Policy After Learning	The way application process control is enabled after HSS completes learning on the servers associated with the policy. • **Automatically**: Application process control is automatically enabled after HSS completes learning on the servers associated with the policy. • **Manually**: Manually enable application process control as needed after HSS completes learning. For more information, see **Enabling Application Process Control**.	Automatically
Action	Action taken when a malicious process is detected. Alarms are generated for malicious processes.	Report alarm

Parameter	Description	Example Value
Servers	Servers to be protected. The agent version falls within the following scope. For details about how to upgrade the agent, see **Viewing Server Protection Status**.	-

Step 7 Click **OK**.

You can view the created policy and its status in the policy list. For more information, see **Table 7-28**.

Table 7-28 Policy status description

Policy Status	Description
Learning	HSS is learning the characteristics of the application processes on servers. Please wait.
Learning complete but not in effect	The server characteristics associated with the policy have been learned. Confirm the learning outcomes. For details, see **Confirming Learning Outcomes**.
Learning complete and in effect	Application process control protection has been enabled for servers.

----End

Related Operations

Editing a whitelist policy

You can modify the policy mode, action, or protected servers in a whitelist policy.

Step 1 In the row of a policy, click **Edit** in the **Operation** column.

Step 2 In the **Edit Policy** dialog box, modify parameters and click **OK**.

----End

Deleting a whitelist policy

If you no longer need HSS to provide application process control for the servers associated with a policy and do not need to retain the application process information learned by HSS, you can delete the whitelist policy. If you need to enable application process control for the servers after the deletion, HSS will need to start learning again. Exercise caution when performing this operation.

Step 1 In the row of a policy, click **Delete** in the **Operation** column.

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

----End

7.4.3 Confirming Learning Outcomes

Scenarios

After HSS completes learning on the servers associated with a whitelist, there may be some suspicious processes with insignificant characteristics that need to be confirmed. You can manually or let HSS automatically mark them as suspicious, malicious, or trusted processes.

You can configure how to confirm learning outcomes only when **creating a whitelist policy**. The value of **Confirm Learning Outcomes** can be:

- **Automatically**: Suspicious processes are automatically marked based on the application process intelligence.
- **Manually**: You need to manually check and mark suspicious processes. This section describes the detailed procedure.

Prerequisites

A policy has been created and its status is **Learning complete but not in effect**. For details, see **Creating a Whitelist Policy**.

Confirming Learning Outcomes

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab.

Step 6 Click the name of a policy whose **Policy Status** is **Learning complete but not in effect**. The **Policy Details** page is displayed.

Step 7 Click the **Process Files** tab.

Step 8 Click the number of processes to be confirmed.

Step 9 Check whether the application processes are trustworthy based on their names and file paths.

Step 10 In the row of a process, click **Mark** in the **Operation** column.

You can also select all application processes and click **Batch Mark** above the process list.

Step 11 In the **Mark** dialog box, set **Trust Status**.

Select **Suspicious**, **Trusted**, or **Malicious**.

Step 12 Click **OK**.

----End

Follow-up Operations

After the learning outcomes are confirmed, you can enable application process protection. For details, see **Enabling Application Process Control**.

7.4.4 Enabling Application Process Control

Scenarios

HSS can control different types of application processes on servers. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.

You can configure how to enable application process control when **creating a whitelist policy**. The value of **Apply Policy After Learning** can be:

- **Automatically**: Application process control is automatically enabled after HSS completes learning on the servers associated with the policy.
- **Manually**: Manually enable application process control as needed after HSS completes learning. This section describes the detailed procedure.

Prerequisites

A whitelist policy has been created and the policy learning outcomes have been confirmed. For details, see **Creating a Whitelist Policy** and **Confirming Learning Outcomes**.

Enabling Application Process Control

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab.

Step 6 In the **Operation** column of a policy, click **Enable Protection**.

You can also select multiple policies and click **Enable Protection** above the policy list.

Step 7 In the **Enable Protection** dialog box, click **OK**.

Step 8 Check the policy status. If **Policy Status** is **Learning complete and in effect**, application protection has been enabled.

----End

Follow-up Operations

After application process control protection is enabled, alarms will be reported for suspicious and malicious processes running on servers.

- For details about how to handle running suspicious processes, see **Checking and Handling Suspicious Processes**.
- For details about how to handle running malicious processes, see **Handling Server Alarms**.

7.4.5 Checking and Handling Suspicious Processes

Scenarios

If a new application process is started after application process control was enabled, HSS will display it in the suspicious process list. In this case, determine whether the process can be trusted. If it is a normal process, add it to the process whitelist.

Checking and Handling Suspicious Processes

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Suspicious Processes** tab.

Step 6 Determine whether a suspicious process can be trusted based on its information, such as the hash value and file path.

- If the process can be trusted, go to **Step 7**.
- If the process cannot be trusted, manually clear it.

Step 7 In the row of a process, click **Handle** in the **Operation** column.

You can also select multiple suspicious processes and click **Batch Handle** above the list.

Step 8 In the dialog box that is displayed, select an action.

Select **Add to process whitelist**.

Step 9 Click **OK**.

----End

Related Operations

HSS reports an alarm once it detects a running malicious process. Choose **Detection & Response** > **Alarms**, check and handle the alarms on the **Server Alarms** tab page, and clear malicious processes in a timely manner. For details, see **Handling Server Alarms**.

7.4.6 Extending the Process Whitelist

Scenarios

After HSS completes learning the whitelist policy, if you think the number of application processes it learned is fewer than the number of process fingerprints collected by the asset fingerprint function, or if it regarded many trustworthy application processes as suspicious, you can extend the process whitelist. HSS will compare the application processes it already learned with the collected process fingerprints to enrich the HSS application process intelligence library and extend the trusted process whitelist.

For details about how to confirm the learning results of the application process whitelist, see **Confirming Learning Outcomes**. For details about how to view the process fingerprints, see **Viewing Server Asset Fingerprints**.

Extending the Process Whitelist

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab.

Step 6 Click a policy name. The **Policy Details** page is displayed.

Step 7 Click the **Associated Servers** tab.

Step 8 In the row of a server, choose **More** > **Add to Whitelist** in the **Operation** column.

Step 9 Click **Compare** to compare the server process fingerprints with the application processes learned by the whitelist.

Step 10 Select trusted processes and click **Add**.

Click the **Process Files** tab.

----End

7.4.7 Start Learning on Servers Again

Scenarios

If you have **extended the process whitelist** but there are still many false positives reported, or if your server workloads changed, you can let HSS start learning again on the servers and calibrate its application process intelligence library to reduce false positives.

Start Learning on Servers Again

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab.

Step 6 Click a policy name. The **Policy Details** page is displayed.

Step 7 Click the **Associated Servers** tab.

Step 8 Select servers and click **Learn Again** above the list.

Step 9 In the dialog box that is displayed, click **OK**.

The relearning is performed according to the intelligent learning time specified in the policy. After the learning is complete, confirm the learning results in a timely manner. For details, see **Confirming Learning Outcomes**.

----End

7.4.8 Disabling Application Process Control

Scenarios

You can disable application process control for one or multiple servers at a time.

Disabling Protection for Servers Associated with a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab.

Step 6 Disable application process control.

- Disable protection but retain the application process characteristics learned by HSS.
  a. In the **Operation** column of a policy, click **Disable Protection**. Alternatively, select multiple policies and click **Disable** above the policy list.
  b. Click **OK**.
- Disable protection and delete the application process characteristics learned by HSS.

a. In the row of a policy, click **Delete** in the **Operation** column.
b. Click **OK**.

Step 7 Check the policy list.

- Disable protection but retain the application process characteristics learned by HSS.

  If the **Policy Status** of the policy is **Learning complete but not in effect**, application process control has been disabled.
- Disable protection and delete the application process characteristics learned by HSS.

  If the policy is deleted from the policy list, application process control has been disabled.

----End

Disabling Protection for a Single Server

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 5 Click the **Whitelist Policies** tab.

Step 6 Click a policy name. The **Policy Details** page is displayed.

Step 7 Click the **Associated Servers** tab.

Step 8 Disable application process control.

- Disable protection but retain the association between the server and the policy.
  a. In the **Operation** column of a policy, click **Disable Protection**. Alternatively, select multiple policies and click **Disable** above the policy list.
  b. Click **OK**.
- Disable protection and disassociate the server from the policy.

  NOTE

  To change the protection policy associated with a server, remove the server from the policy settings, and then create or edit another protection policy to associate with the server.

  a. In the row containing the desired instance, click **Delete** in the **Operation** column.
  b. Click **OK**.

Step 9 Check the server list.

- Disable protection but retain the association between the server and the policy.

If the **Policy Status** of the server is **Learning complete but not in effect**, application process control has been disabled.

- Disable protection and disassociate the server from the policy.

  If the server is deleted from the list, application process control has been disabled.

----End

7.5 File Integrity Monitoring

7.5.1 File Integrity Management Overview

File integrity monitoring (FIM) monitors key files on Linux servers in real time; records file addition, modification, and deletion; and reports alarms, helping you detect suspicious changes in a timely manner.

File Integrity Monitoring Principles

HSS checks for suspicious changes by comparing the previous and current statuses of a file.

File Integrity Monitoring Scope

Some file monitoring paths are preconfigured in HSS. For details, see **Table 7-29**.

To add or remove monitored files, you can modify parameters in the **File Integrity** area in the **File Protection** policy. For details, see **Configuring Policies**.

Table 7-29 Default file monitoring paths

Type	File Path
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

7.5.2 Viewing File Change Records

File integrity monitoring provides change statistics, change types, and file change records, helping you learn about file changes in real time and detect malicious changes in a timely manner.

Viewing File Change Overview

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **File Integrity Monitoring**. Check the file change overview.

Table 7-30 File change overview parameters

Parameter	Description
Overview	Number of servers where files are changed.
Changes	• **Total Changes**: total number of file and registry changes. • **File Changes**: number of all file changes. • **Registry Changes**: number of registry changes.
Action	• **Modify**: total number of file and registry changes. • **Create**: total number of file and registry creations. • **Delete**: total number of file and registry deletions.

----End

Viewing the File Change Records of a Single Server

Step 1 In the server list, you can view the number of files and registry changes on a servers and the time when they were last changed.

Step 2 Click a server name to go to the server change details page. You can view the file change details of the server.

Table 7-31 Server file change parameters

Parameter	Description	Example Value
File Name	Name of a modified file.	du
Path	Path of a modified file.	-

Parameter	Description	Example Value
Change Description	Description of the change. To view the change details, hover the cursor over the change content.	**SHA2560ba0c4b5e48e55a6** is changed to **4f6079f5b37d1513**.
Type	Type of a modified file. Its value can be: • **File** • **Registry**	File
Action	How a file was modified. • Create • Modify • Delete	Modify
Last Modified	The last time when a file was modified.	-

----End

Viewing the File Change Records of All Servers

In the modified file list, you can view all file change records. For details, see **Table 7-31**.

Suggestions for Handling File Changes

The file changes of servers protected by HSS will be recorded and displayed on the **File Integrity Monitoring** page, helping you trace the behavior of attackers. If a file change is displayed on the **File Integrity Monitoring** page, check whether it is a normal event in a timely manner.

- If the file change is an abnormal event, manually block the related process and isolate the file – on condition that these operations do not affect services.
- If the file change is a normal event, ignore it or modify the file integrity monitoring scope. For details, see **File Integrity** in the **File Protection** policy in **Configuring Policies**.

A file change will also trigger a **File/Directory changes** alarm. You are advised to handle it too. The procedure is as follows:

1. On the **File Integrity Monitoring** page, copy the name of the server where the file change was made.
2. In the navigation pane, choose **Detection & Response** > **Alarms**.
3. On the **Server Alarms** tab page, select the alarm whose **Alarm Type** is **Abnormal System Behavior** > **File/Directory changes**.
4. In the search box on the right, paste and search for the server name to find its **File/Directory changes** alarm.

5. Click the alarm name to view details. Check whether the file change is abnormal based on these details and the file change information on the **File Integrity Monitoring** page.
6. Select a handling method at the bottom of the alarm details page.

   The change records on the **File Integrity Monitoring** page will be retained, no matter how you handle the alarm.

   a. **Mark as handled**: You have manually blocked related processes and isolated the modified files. The risk has been eliminated.
   b. **Ignore**: The file change has no impact and the alarm can be ignored.
   c. **Add to whitelist**: The file change is made by normal service operations. It needs to be whitelisted so that it will not trigger alarms.

7.6 Virus Scan

7.6.1 Virus Scan Overview

What Is Virus Scan?

Viruses are self-replicable instructions or program codes compiled independently or embedded in server systems to adversely affect the servers by damaging their functions or data. Once a virus infiltrates a server, it can cause a range of damages – from occupying the system memory and slowing down operations to important data loss, data leaks, and system breakdown, causing immeasurable losses.

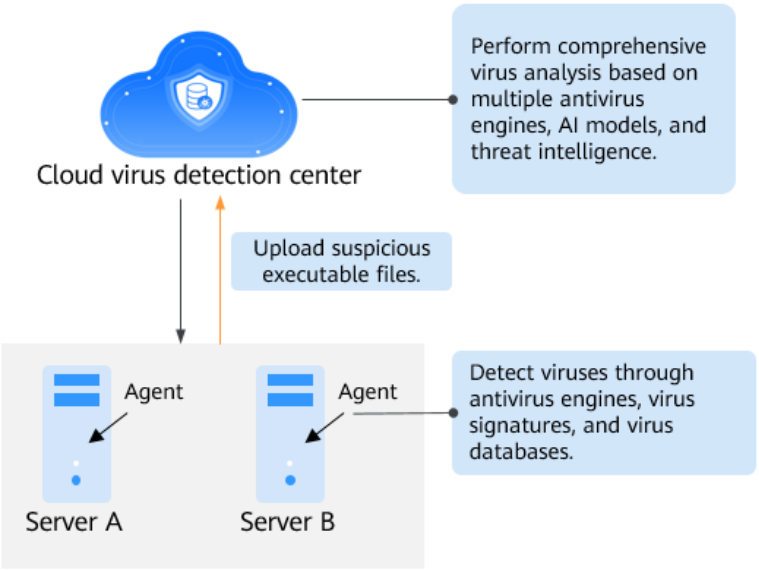
HSS can help you detect and remove viruses to protect your servers.

HSS combines cloud-based and local antivirus mechanisms to scan executable files, compressed files, scripts, documents, images, and audiovisual files for viruses. You can perform quick scan, full-disk scan, and custom scans on servers as needed to detect and remove virus files in a timely manner, enhancing the virus defense of the system.

Virus Scan and Removal Principles

The HSS antivirus combines cloud-based and local antivirus mechanisms. On servers, it uses the virus signature database and agent-side antivirus engine to quickly scan all static files. A malicious file is isolated once it is detected. A suspicious executable file can be uploaded to the cloud virus detection center. This center uses multiple antivirus engines, AI models, and threat intelligence technologies to further evaluate suspicious files and remove viruses.

Figure 7-4 Virus scan and removal principles



Detectable and Removable Viruses

Antivirus can scan for and remove ransomware, mining programs, DDoS Trojans, Trojan programs, backdoors, malicious programs, high-risk programs, worms, suspicious programs, and self-mutating Trojans.

Advantages of Virus Scan and Removal

- **Fast and accurate file type identification**

  This function integrates dedicated file type identification algorithms to check the real content of files and effectively detect fake file suffixes or content. Hundreds of file types can be quickly and accurately identified.

- **In-depth parsing of malicious files**

  The Cloud+Local collaborative virus detection mechanism analyzes binary files, compound documents, and diverse scripts. It can restore complete file content and deeply identify potential malicious behaviors.

Constraints

- This function is available in HSS enterprise, premium, WTP, and container editions.
  - Professional edition: quick scan and removal
  - Enterprise edition and other editions: quick, full-disk, and customized scan and removal
- To use virus scan and removal, ensure the agent installed on the server falls within the following ranges. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.9 or later
  - Windows: 4.0.20 or later
- To use virus scan and removal, ensure the **AV Detection** policy is enabled. For details, see **Configuring Policies**.

Process of Virus Scan

Figure 7-5 Process of Virus Scan

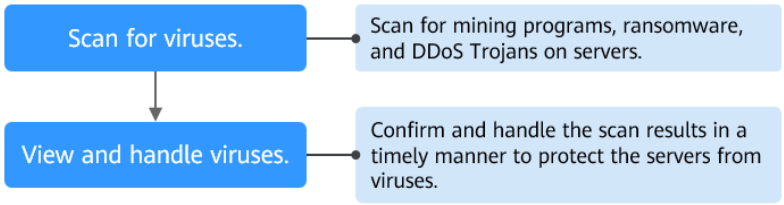


Table 7-32 Virus scan and removal process

Operation	Description
Scanning for Viruses	You can perform quick scans, full scans, or custom scans to check your servers for viruses, including mining programs, ransomware, and DDoS Trojans.
Viewing and Handling Viruses	HSS allows you to isolate, remove, whitelist, or ignore virus-infected files. You can isolate and remove different types of viruses. To protect servers from viruses, you are advised to view and handle the scan results in a timely manner after the scan is complete.

7.6.2 Scanning for Viruses

Scenarios

Once a static virus file is started, it may become a malicious process and become a security risk of servers. You are advised to scan for and clear viruses on servers in a timely manner.

HSS supports quick scans, full-disk scans, and custom scans. For details, see **Table 7-33**.

Table 7-33 Virus scan methods

Method	Description	File Type	Directory Scope
Quick Scan	Quick virus scan tasks can save time and costs. This function scans and removes preset key system files and directories.	• Windows Processes (active processes, hidden processes, and Docker processes), kernel modules, installed programs, dynamic library hijacking, services, scheduled tasks, auto-started items, sensitive directories, Office files, images, videos, scripts, and compressed packages • Linux Processes (active processes, hidden processes, and Docker processes), kernel modules, installed programs, dynamic library hijacking, services, scheduled tasks, auto-started items, sensitive directories,	• Windows – User desktop, downloaded files, and document directories – Startup items in the Start menu – System directories **C:\Windows\System**, **C:\Windows\System32**, **C:\Windows\SysWOW64** – Temporary directories **C:\Users***[Username]***\AppData\Local\Temp**, **C:\Temp**, **C:\Windows\Temp** – Download directories of browsers Google Chrome, Microsoft Edge, and Mozilla Firefox • Linux – Standard system directories **/bin**, **/sbin**, **/lib**, **/lib64**, **/usr/bin**, **/usr/sbin**, **/usr/lib**, **/usr/lib64**, **/usr/local/lib**, **/usr/local/lib64**, **/usr/local/bin**, **/usr/local/sbin** – Other important directories **/tmp**, **/root**, **/home**, **/boot**, **/opt**, **/data**, **/var/tmp**, **/var/run**, **/var/lib**, **/dev/shm**, **/etc**, **/etc/sysconfig**, **/usr/local/src**, **/usr/share**, and the root directory – Directories of the executable files corresponding to the startup items **/etc/rc.d**, **/etc/init.d**

Method	Description	File Type	Directory Scope
		Office files, images, videos, scripts, and compressed packages	
Full-disk Scan	A time-consuming full-disk virus scan can comprehensively check servers for viruses.	• **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files • **Compressed**: installation packages or other compressed packages, such as .zip, .rar, and .tar files • **Script**: script files, such as .bat, .py, and .ps1 files • **Document**: document files, such as .txt, .doc, and .pdf files • **Image**: image files, such as .bmp, .jpg, and .gif files • **Audio & Video**: audiovisual files, such as .mp3, .mp4, and .flv files	All directories except network directories. The reasons for not scanning network directories are as follows: • Inefficient scan A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. • Network bandwidth consumption Accessing a network directory consumes network bandwidth. A large-scale scan may fully occupy the network bandwidth and affect your workloads. For example, the access speed may slow down and the network latency may increase. You can create a custom scan task to scan network directories.
Custom Scan	You can create a custom virus scan task as needed.	You can scan executable, compressed, script, document, image, or audiovisual files.	User-defined

Constraints

- A virus scan uses a lot of memory, CPU, and I/O resources. Perform this operation during off-peak hours.
- A full-disk scan does not check network directories.

Quick Scan

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Click **Quick Scan**. The dialog box is displayed.

Step 6 Set parameters related to the quick scan task as prompted.

Table 7-34 Quick scan parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Quick Scan-20250425173536
Select Server	Select the servers where you want to perform a quick scan. You can select and scan servers that meet all the following conditions: • Have online agent (Windows agent 4.0.20 or later, or Linux agent 3.2.9 or later) For details about how to install the agent, see **Installing the Agent on Servers**. • The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. • The server is not being scanned.	-

Parameter	Description	Example Value
Handling Policy	Action to be taken on the detected virus-infected files. • **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. • **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 7 Click **Scan** and start the scan task.

----End

Full-disk Scan

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Click **Full-disk Scan**. The dialog box is displayed.

Step 6 Set parameters related to the full-disk scan task as prompted.

Table 7-35 Full-disk scan parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Full-disk Scan-20250425174038

Parameter	Description	Example Value
Select Server	Select the servers where you want to perform a full scan. You can select and scan servers that meet all the following conditions: • Have online agent (Windows agent 4.0.20 or later, or Linux agent 3.2.9 or later) For details about how to install the agent, see **Installing the Agent on Servers**. • The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. • The server is not being scanned.	-
Handling Policy	Action to be taken on the detected virus-infected files. • **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. • **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 7 Click **Scan** and start the scan task.

----End

Custom Scan

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Click **Custom Scan**.

Step 6 Set the parameters of the **Custom Scan** policy as prompted. For details about the parameters, see **Custom antivirus policy parameters**.

Table 7-36 Custom antivirus policy parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Custom Scan-20250425180036
Startup Type	Scan task execution type. • **Scan Now**: Start a scan immediately. • **Scan Later**: Start a scan at the specified time. • **Periodic Start**: Start a scan periodically based on your settings.	Scan Later
Start	If **Startup Type** is set to **Scan Later**, configure this parameter to set the start time of the scan. You can set the start time to a time within one month.	2025/04/25 18:10
Schedule	If **Startup Type** is set to **Periodic Start**, configure this parameter to set the scan period.	-
File Type	Type of the file to be scanned. Currently, the following types of files can be scanned: • **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files • **Compressed**: installation packages or other compressed packages, such as .zip, .rar, and .tar files • **Script**: script files, such as .bat, .py, and .ps1 files • **Document**: document files, such as .txt, .doc, and .pdf files • **Image**: image files, such as .bmp, .jpg, and .gif files • **Audio & Video**: audiovisual files, such as .mp3, .mp4, and .flv files	Select All

Parameter	Description	Example Value
(Optional) Directory Settings	Directory where virus-infected files need to be scanned. If this parameter is not set, full scan is performed by default. Full scan does not cover network directories. **WARNING** The reasons for not scanning network directories are as follows: • Inefficient scan A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. • Network bandwidth consumption Accessing a network directory consumes network bandwidth. A large-scale scan may fully occupy the network bandwidth and affect your workloads. For example, the access speed may slow down and the network latency may increase.	-
(Optional) Exclude Specified Directories	Directories that do not require virus scan.	-
Select Server	Select the servers to be scanned. You can select and scan servers that meet all the following conditions: • Have online agent (Windows agent 4.0.20 or later, or Linux agent 3.2.9 or later) For details about how to install the agent, see **Installing the Agent on Servers**. • The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. • The task start conditions required by the corresponding policy are met: – Policy whose **Startup Type** is **Scan Now**: The server is not being scanned. – Policy whose **Startup Type** is **Scan Later**: No other custom scan policies using the same startup time as the current policy are bound to the server. – Policy whose **Startup Type** is **Periodic Start**: No other custom policies whose **Startup Type** is **Periodic Start** are bound to the server.	-

Parameter	Description	Example Value
Handling Policy	Action to be taken on the detected virus-infected files. • **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. • **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 7 Click **Scan** and start the scan task.

----End

Follow-up Operations

- View the execution status of a scan job
  a. On the **Virus Scan** page, click the **Scan tasks** to view the execution status of virus scan tasks.
     To stop an ongoing scan task, click **Cancel** in the **Operation** column of the target scan task.
  b. Click ⌄ to view the scan status and number of scanned files of each server.
     Click **Cancel** in the **Operation** column of the target server to stop scanning the server.
- View and handle viruses
  After a virus scan task is complete, you can manually handle the detected virus-infected files based on service requirements. For details, see **Viewing and Handling Viruses**.

7.6.3 Viewing and Handling Viruses

Scenarios

After the virus scanning is complete, HSS handles the virus-infected files based on the handling policy selected. The handling policies are as follows:

- Automatic handling: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled.

- Manual handling: Alarms are generated for the detected virus-infected files. You need to manually confirm the files before handling them.

No matter which handling policy you choose, you need to confirm and handle the scan results in a timely manner to protect your servers from viruses.

The section describes how to check and manually handle virus-infected files.

Prerequisites

A virus scanning task has been executed. For details, see **Scanning for Viruses**.

Viewing and Handling Viruses

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

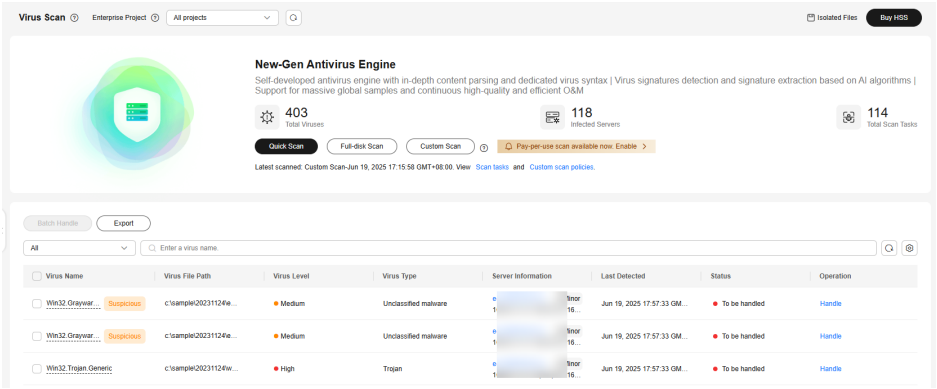
Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 View the scanned virus files.

Hover the cursor over a virus name to view its file path, file hash, owner, attribute, size, and creation time.

Figure 7-6 Virus-infected file list



Step 6 In the **Operation** column of a virus file, click **Handle**.

You can also select multiple virus files and click **Batch Handle** above the list to handle them in batches.

Step 7 In the **Handle Infected Files** dialog box, select a virus-infected file handling method. For more information, see **Virus-infected file handling methods**.

Table 7-37 Virus-infected file handling methods

Parameter	Description
Mark as handled	You can manually handle the virus-infected file on the server.
Ignore	Ignore the virus-infected file alarm. If this file is detected again, HSS generates an alarm.
Add to alarm whitelist	If you confirm that the virus file is falsely reported, you can add it to the alarm whitelist. After a file is added to whitelist, HSS will not generate alarms for the file.
Isolating files manually	Isolate virus-infected files. After a file is isolated, it will become read-only. To avoid impact on services, exercise caution when performing this operation. Isolated files are added to the **Isolated Files** and cannot harm your server. You can restore or delete isolated files as required. For details, see **Isolated Files**.

Step 8 Click **OK**.

After the alarm is handled, the status of the virus file alarm event changes to **Handled**.

----End

Exporting Virus Alarms

Export virus alarms to a local PC.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Above the virus-infected file alarm event list, click **Export** to export all virus-infected file alarm events to the local PC.

Step 6 View the export status in the upper part of the virus scan page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

7.6.4 Managing Custom Antivirus Policies

Scenarios

A custom antivirus policy is generated for each custom antivirus task that starts periodically or at a specified time point. You can modify or delete such policies as needed.

The policy of a task scheduled to be executed at a specified time point will expire after execution, and will be marked with an expiration tag. You can change the startup time of the policy and enable it again.

Editing a Custom Scan Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Choose **Custom scan policies** to view existing user-defined antivirus policies.

Step 6 In the **Operation** column of a policy, click **Edit**. Modify the policy on the edit page. For more information, see **Table 7-38**.

Table 7-38 Custom antivirus policy parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Custom Scan-20250425180036
Startup Type	Scan task execution type. • **Scan Now**: Start a scan immediately. • **Scan Later**: Start a scan at the specified time. • **Periodic Start**: Start a scan periodically based on your settings.	Scan Later
Start	If **Startup Type** is set to **Scan Later**, configure this parameter to set the start time of the scan. You can set the start time to a time within one month.	2025/04/25 18:10
Schedule	If **Startup Type** is set to **Periodic Start**, configure this parameter to set the scan period.	-

Parameter	Description	Example Value
File Type	Type of the file to be scanned. Currently, the following types of files can be scanned: • **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files • **Compressed**: installation packages or other compressed packages, such as .zip, .rar, and .tar files • **Script**: script files, such as .bat, .py, and .ps1 files • **Document**: document files, such as .txt, .doc, and .pdf files • **Image**: image files, such as .bmp, .jpg, and .gif files • **Audio & Video**: audiovisual files, such as .mp3, .mp4, and .flv files	Select All
(Optional) Directory Settings	Directory where virus-infected files need to be scanned. If this parameter is not set, full scan is performed by default. Full scan does not cover network directories. **WARNING** The reasons for not scanning network directories are as follows: • Inefficient scan A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. • Network bandwidth consumption Accessing a network directory consumes network bandwidth. A large-scale scan may fully occupy the network bandwidth and affect your workloads. For example, the access speed may slow down and the network latency may increase.	-
(Optional) Exclude Specified Directories	Directories that do not require virus scan.	-

Parameter	Description	Example Value
Select Server	Select the servers to be scanned. You can select and scan servers that meet all the following conditions: • Have online agent (Windows agent 4.0.20 or later, or Linux agent 3.2.9 or later) For details about how to install the agent, see **Installing the Agent on Servers**. • The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. • The task start conditions required by the corresponding policy are met: – Policy whose **Startup Type** is **Scan Now**: The server is not being scanned. – Policy whose **Startup Type** is **Scan Later**: No other custom scan policies using the same startup time as the current policy are bound to the server. – Policy whose **Startup Type** is **Periodic Start**: No other custom policies whose **Startup Type** is **Periodic Start** are bound to the server.	-
Handling Policy	Action to be taken on the detected virus-infected files. • **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. • **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 7 Click **OK**.

----End

Deleting a Custom Scan Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Choose **Custom scan policies** to view existing user-defined antivirus policies.

Step 6 Click **Delete** in the **Operation** column of a policy.

To delete policies in batches, you can also select multiple policies and click **Delete** in the upper left corner of the list.

Step 7 Click **OK**.

----End

7.6.5 Managing Isolated Files

Scenarios

Isolated files are added to the **Isolated Files** and cannot harm your server. You can also refer to this section to restore or delete isolated files as required.

- **Restoring Isolated Files**: If an isolated file is a normal service file and not infected by any viruses, you can restore the file.
- **Deleting Isolated Files**: If an isolated file is infected by a virus, delete the file to completely remove the virus.

Restoring Isolated Files

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Click **Isolated Files** in the upper right corner of the page. The dialog box is displayed.

Step 6 Click **Restore** in the **Operation** column of the list. The dialog box is displayed.

Step 7 Click **OK**.

If the file can be used after being restored, the restoration is successful.

----End

Deleting Isolated Files

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Virus Scan**.

Step 5 Click **Isolated Files** in the upper right corner of the page. The dialog box is displayed.

Step 6 Click **Delete** in the **Operation** column of the list. The dialog box is displayed.

To delete isolated files in batches, select multiple isolated files and click **Delete** in the upper left corner of the list.

Step 7 Click **OK**.

If the file cannot be found on the **Isolated Files** page, deletion is successful.

----End

7.7 Dynamic Port Honeypot

7.7.1 Dynamic Port Honeypot Overview

What is Dynamic Port Honeypot?

The dynamic port honeypot function is a proactive defense measure. It uses a real port as a honeypot port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user.

You can enable the dynamic port honeypot using recommended ports or user-defined ports to deceive compromised servers and reduce the risk of resources intrusion.

Principles of Dynamic Port Honeypot Protection

Figure 7-7 shows the principles of dynamic port honeypot protection. The process is as follows:

1. Create a protection policy.

   Select a target server and set a honeypot port. Generally, select a common service port that is not used in actual services.

2. Listen to the honeypot port.

   HSS starts real-time listening on the honeypot port.

3. Connect to the honeypot port.

   If an attacker scans the network or attempts to connect to the honeypot port, HSS records the connection event and rejects the connection.

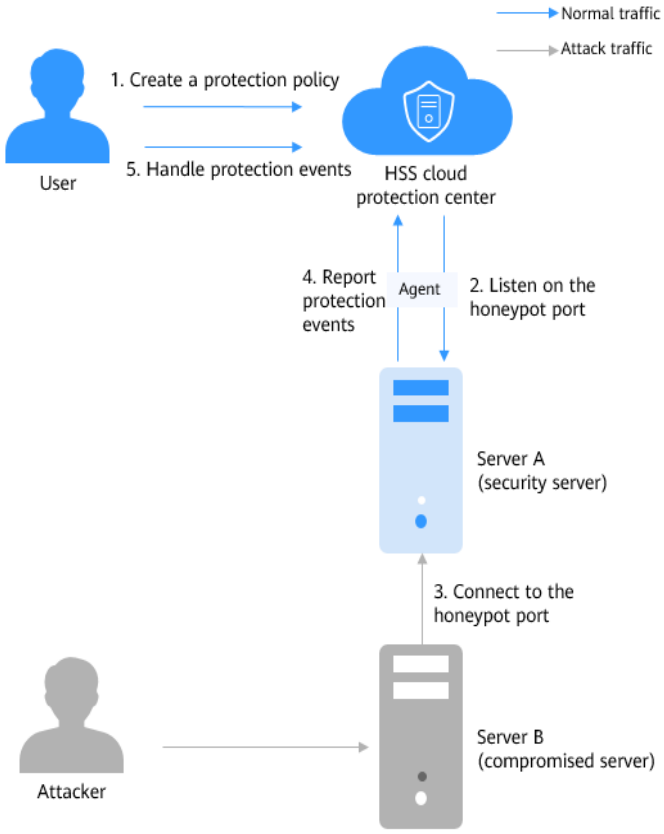
4. Report protection events.

   Once the honeypot port is connected, HSS immediately generates an alarm and displays the event information in the protection event list.

5. Handle alarms.

   Check whether there are compromised servers on the intranet based on the honeypot port protection events or other related events.

Figure 7-7 Principles of dynamic port honeypot protection



Application Scenarios of Dynamic Port Honeypot

Unlike traditional security technologies that focus on defense, dynamic port honeypot proactively lures attackers in the intranet. It not only detects compromised servers in a timely manner, but also deceives and delays attackers.

How Do I Use Dynamic Port Honeypot?

Table 7-39 Process of using the dynamic port honeypot

No.	Operation	Description
1	**Creating a Protection Policy for a Dynamic Honeypot Port**	Configure the honeypot port, the source IP address whitelist, and associated servers. (Only the servers not bound to any EIPs are supported.)
2	**Viewing and Handling Honeypot Protection Events**	The dynamic port honeypot function reports an alarm when a potentially compromised server proactively connects to a honeypot port. You can handle the alarm as needed.

Constraints

- Dynamic port honeypots apply only to servers that are not bound to EIPs.
- Dynamic port honeypots are available only in HSS premium, web tamper protection, and container editions.
- To use the dynamic port honeypots, ensure that the agent installed on the server falls within the following ranges. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.10 or later.
  - Windows: 4.0.22 or later.

7.7.2 Creating a Protection Policy for a Dynamic Honeypot Port

Scenario

The dynamic port honeypot function uses a real port as a honeypot port to induce attackers to access the port. When enabling the dynamic port honeypot, you need to create a protection policy and add a port as a honeypot port.

This chapter describes how to create a dynamic port honeypot protection policy.

Constraints

- A maximum of 50 honeypot ports can be added to a server.
- A honeypot port can be bound to only one protocol. Both TCP and TCP6 are supported.

Creating a Protection Policy for a Dynamic Honeypot Port

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 On the **Servers** tab, click **Create a Protection Policy**. The dialog box is displayed.

Step 7 Create a protection policy as prompted.

1. Configure the policy and click **Next**. For details about related parameters, see **Table 7-40**

   Table 7-40 Parameters for creating a protection policy

Parameter	Description
Policy Name	You can retain the default name or enter a name that is easy to identify.
OS Type	Select the OS type of the server where you want to add the port honeypot.
Protected Port	Set the honeypot port. HSS provides some common ports by default. For Linux OSs, common Windows ports are provided by default. For Windows OSs, common Linux ports are provided by default. You can modify them as needed. **NOTE** Ensure that the port to be added is not occupied by other services. If the port is occupied, the dynamic port honeypot function fails to be enabled.
(Optional) Source IP address whitelist	By default, the servers that proactively connect to the dynamic honeypot port are compromised intranet servers. Once a suspicious connection behavior is detected, an alarm is reported. Therefore, if a trusted server may connect to the port, you are advised to add the IP address to the source IP address whitelist. You can enter IP addresses or CIDR blocks. A maximum of 50 values can be added. Multiple values are separated by commas (,).

2. Select the target server and click **Save and Enable**.

   Note that the dynamic port honeypot can be selected only for the servers that meet all the following conditions:

   - The HSS premium edition or higher has been enabled on the server.
   - The server agent is online. The Windows agent version is 4.0.22 or later, and the Linux agent version is 3.2.10 or later.

- No dynamic port honeypot policies have been bound to the server.
- The OS type of the server is the same as that specified in **Step 7.1**.
- No EIPs have been bound to the server.

Step 8 In the **Associated Servers** column of the created target policy, click the value. The dialog box is displayed.

Step 9 In the **Port Status** column of the associated server, check the port status.

If a port fails to be enabled, you need to manually enable it. Click **Edit Policy**, deselect associated servers, and save the policy. Then, click **Edit Policy**, select servers, and save the policy again. For details about how to edit a policy, see **Editing a Policy**.

----End

FAQs

What can I do if the port fails to be enabled?

- Possible cause 1: The port is occupied by other services.

  Solution: Add other idle ports by editing the policy.
- Possible cause 2: System resources are insufficient.

  Solution: Free up some system resources. Click **Edit Policy**, deselect associated servers, and save the policy. Then, click **Edit Policy**, select servers, and save the policy again. For details about how to edit a policy, see **Editing a Policy**.

7.7.3 Viewing and Handling Honeypot Protection Events

Scenario

By default, the servers that proactively connect to the dynamic honeypot port are compromised intranet servers. Once a suspicious connection behavior is detected, a honeypot protection event will be reported. The event contains the server IP address that initiates the connection, but does not contain process details. You can check for and locate compromised servers based on honeypot protection and other event.

This section describes how to view and handle honeypot protection events.

Viewing and Handling Honeypot Protection Events

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 Under the introductions, view the protection overview.

- You can view the number of protection policies, protected servers, and protection events.

- You can enable the **Automatically apply default policies to newly add servers**. If is displayed, the function is enabled.

Step 6 Click the **Protection Events** tab to view honeypot protection events. For details about the parameters in the event list, see **Table 7-41**.

Table 7-41 Parameters in the event list

Parameter	Description
Alarm Name	The name of an alarm event. Click an alarm name to view the details. For details, see **Table 7-43**.
Alert Severity	Alarm threat level. Honeypot protection events are classified into the following two levels: • High risk: The remote server connects to the honeypot port for multiple times. • Medium risk: The remote server is connected to the honeypot port.
Alarm Summary	Summary of alarm events. Based on the information, you can learn about the server that may have been compromised and the connection between the server and the port.
Affected Asset	Dynamic port server connected to the server that may have been compromised.
Alarm Reported	Time when an alarm occurred.
Status	Alarm handling status, which can be **Handled** or **To be handled**.

Step 7 After confirming the alarm information, click **Handle** in the **Operation** column of the event whose **Status** is **To be handled**. The **Handle Alarm** dialog box is displayed.

If you need to handle multiple alarm events in batches, click **Batch Handle** in the upper left corner of the list.

Step 8 Select a solution. For details about the solution, see **Table 7-42**.

Table 7-42 Parameters for handling alarm events

Parameter	Description
Action	• **Ignore**: Ignore the alarm event. The alarm is still generated when the next threat event occurs. • **Mark as handled**: You can manually isolate ports for the compromised server. • **Add to alarm whitelist**: Add the trusted server that triggers an alarm to the whitelist so that no alarm will be generated when similar events occur.

Parameter	Description
Batch Handle	If you need to handle the same alarm event at the same time, you can select the parameter.
(Optional) Remarks	To facilitate identification of the current processing, supplementary description can be provided.

Step 9 Click **OK**.

----End

Alarm Details Parameters

For details about the parameters on the alarm details, see **Table 7-43**.

Table 7-43 Alarm details parameters

Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an alarm was generated for the first time.
Alarm ID	Unique ID of an alarm
ATT&CK Phase	Attack model used by attackers in each phase.
Last Occurred	Time when an alarm was generated for the last time.
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.
Forensics	The dynamic port honeypot function checks the network forensics information of the attack source.
Similar Alarms	Alarms that are similar to the current alarm event. You can handle the alarm according to the handling method of the similar alarms.

Filtering Events in Different Handling Statuses

Select an event in the target status from the drop-down list.

7.7.4 Managing Dynamic Port Honeypot Protection Policies

Scenario

After a policy is created, you can manage the policy based on your protection requirements.

- **Disabling a policy**: Disable the dynamic port honeypot function temporarily.
- **Enabling a policy**: Re-enable the disabled dynamic port honeypot policy.
- **Editing a policy**: Modify the protection policy information of dynamic port honeypot, for example, adding or deleting ports, and unbinding or binding servers.
- **Deleting a policy**: Delete the dynamic port honeypot protection policy and disable the function.

Constraints

The default policy cannot be deleted.

Disabling a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 In the row containing the target policy, click **Disable Policy** in the **Operation** column. The dialog box is displayed.

Step 7 Confirm the information and click **OK**.

----End

Enabling a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 In the row containing the target policy, click **Enable Policy** in the **Operation** column. The dialog box is displayed.

Step 7 Confirm the information and click **OK**.

----End

Editing a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 In the row containing the target policy, click **Edit Policy** in the **Operation** column. The dialog box is displayed.

Step 7 Configure a policy.

You can modify the policy name, protected port, and source IP address whitelist.

Step 8 Click **Next**.

Step 9 Select a server to be bound.

Step 10 Click **OK**.

----End

Delete a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 In the row containing the target policy, click **Delete** in the **Operation** column. The **Delete Policy** dialog box is displayed.

Step 7 Ensure that all information is correct and click **OK**.

----End

7.7.5 Managing Associated Servers

Scenario

For servers associated with a protection policy, you can **switch the protection policy** for servers or **unbind the protection policy** from the servers.

Changing a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 In the **Associated Servers** column of the target policy, click the value. The dialog box is displayed.

Step 7 Click **Change Policy** in the **Operation** column. The **Change Policy** dialog box is displayed.

To switch protection policies for multiple servers, select all target servers and click **Change Policy** in the upper left corner of the list.

Step 8 Select a protection policy as prompted.

Step 9 Click **OK**.

----End

Unbinding a Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 In the **Associated Servers** column of the target policy, click the value. The dialog box is displayed.

Step 7 Click **Unbind** in the **Operation** column. The **Unbind** dialog box is displayed.

To unbind multiple servers, select all target servers and click **Unbind** in the upper left corner of the list.

Step 8 Confirm the information and click **OK**.

----End

8 Container Protection

8.1 Container Firewalls

8.1.1 Container Firewall Overview

What Is a Container Firewall?

Containers are more lightweight, efficient, and portable than traditional VMs. Dozens, even hundreds of containers can run on a single node. As a result, the security boundaries of containers are blurred, and traditional security measures cannot identify or control the incoming or outgoing traffic of containers. Lateral movement, permission abuse, and data leakage may occur.

To address these challenges, HSS provides the container firewall. The container firewall can isolate pods, workloads, and nodes in a network to prevent lateral movement and minimize permissions, and enhancing security and stability.

Container Firewall Principles and Restrictions

The container firewall is provided by the HSS container edition.

For details about the container firewall principles and restrictions, see **Table 8-1**.

Table 8-1 Container firewall principles and restrictions

Cluster Type	**CCE Standard Cluster**		**CCE Turbo Cluster**	**Third-party Kubernetes Cluster**
Container Network	**Container Tunnel Network**	**VPC Network**	**Cloud Native Network 2.0**	**Kubernetes Native Network**
Container firewall protection principles	Kubernetes network policies restrict the communication between pods and the access from pods to the external network.	Security groups control the traffic to and from nodes, thereby indirectly protecting pods.	You can bind a security group to a workload, and configure security group rules to control the traffic to and from the workload, implementing network isolation for the workload.	Kubernetes network policies can be used to restrict the communication between pods and the access from pods to the external network.
Cluster versions supporting inbound rules	All	All	v1.19 and later	All
Cluster versions supporting outbound rules	v1.23 and later	All	v1.19 and later	v1.23 and later
Selectors for inbound rules	• namespaceSelector • podSelector	N/A	N/A	• namespaceSelector • podSelector
Selectors for outbound rules	• namespaceSelector • podSelector • ipBlock	N/A	N/A	• namespaceSelector • podSelector • ipBlock
Supported OSs	• EulerOS • CentOS • HCE 2.0	None	None	None
Support for IPv6 network policies	No	N/A	N/A	No

Cluster Type	CCE Standard Cluster		CCE Turbo Cluster	Third-party Kubernetes Cluster
Container Network	**Container Tunnel Network**	**VPC Network**	**Cloud Native Network 2.0**	**Kubernetes Native Network**
Support for limiting ClusterIP access through workload labels	No	N/A	N/A	No
Dependencies	To operate resource objects in a cluster, you need to obtain either of the following operation permissions: • IAM permissions: Tenant Administrator or CCE Administrator. • Namespace permissions (authorized by Kubernetes RBAC): O&M permissions.			None

Concepts

- **Network policy**

  A network policy is a Kubernetes resource object that defines network access control rules for pods in a cluster. It uses label selectors (such as podSelector) to specify target pods and defines ingress and egress rules to allow or deny inbound or outbound traffic.

- **Security group**

  A security group is a collection of access control rules for instances, such as cloud servers, containers, and databases, that have the same security requirements and that are mutually trusted within a VPC. A security group can have inbound and outbound rules. You need to specify the source, port, and protocol for each inbound rule and specify the destination, port, and protocol for each outbound rule to control the inbound and outbound traffic to and from the instances in the security group.

- **namespaceSelector**

  namespaceSelector is a label selector used to select specific namespaces. A network policy can use namespaceSelector to allow or deny traffic to or from all pods in these namespaces.

- **podSelector**

  podSelector is a label selector. It is used to select pods. A network policy uses podSelector to specify target pods and define rules for allowing or denying traffic.

- **ipBlock**

  ipBlock is used to specify an IP address range (in CIDR format). Traffic from or to the IP address range will be allowed or denied.

Related Operations

- Configuring a Network Defense Policy (for a Container Tunnel Network)
- Configuring a Network Defense Policy (for a VPC Network)

8.1.2 Configuring a Network Defense Policy (for a Container Tunnel Network)

Scenarios

If no network defense policies are configured for a pod, all traffic is allowed to enter and leave the pod by default. In this case, pods can communicate with each other and access the external network, which poses security risks.

To improve the security of a cluster using the container tunnel network model, you can configure a network defense policy for the cluster to restrict the communication between pods and the access from pods to the external network.

Constraints

- Currently, the container firewall only supports network policies for pods running on nodes with the following OSs: EulerOS, CentOS, HCE 2.0
- The CCE standard clusters of v1.23 and later support inbound and outbound rules. CCE standard clusters earlier than v1.23 only support inbound rules.
- Network isolation is not supported for IPv6 addresses.
- ClusterIP access cannot be restricted by workload labels.

Creating a Network Policy from YAML

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose > **Container Firewalls**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click in the upper right corner of the list to refresh and view the latest data.

Step 7 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 8 Click **Create from YAML** above the policy list.

Step 9 On the YAML creation page, enter content or click **Import**.

The following is an example of a network policy created using YAML. The network policy requires that a pod can only be accessed by pods with specific labels and can only access specific pods.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: access-demo4
  namespace: default
spec:
  policyTypes:
  - Ingress
  - Egress
  podSelector:              # The rule takes effect for pods with the role=db label.
    matchLabels:
      role: db
  ingress:                  # Ingress rule
  - from:
    - podSelector:          # Only allow the access of the pods labeled with role=frontend.
        matchLabels:
          role: frontend
    ports:                  # Only TCP can be used to access port 6379.
    - protocol: TCP
      port: 6379
  egress:                   # Egress rule
  - to:
    - podSelector:          # Only pods with the role=web label can be accessed.
        matchLabels:
          role: web
```

Step 10 Click **OK**.

You can view the new policy in the policy management list.

----End

Creating a Network Policy on the GUI

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose > **Container Firewalls**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click in the upper right corner of the list to refresh and view the latest data.

Step 7 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 8 Click **Create Network Policy** above the network policy list.

- **Policy Name**: Enter a network policy name.

- **Namespace**: Select the namespace of the network policy.
- **Selector**: Enter a key and a value to set the pod to be associated, and click **Add**. You can also click **Reference Workload Label** to reference the label of an existing workload.
- Inbound rule: Click **Add Rule** in the **Inbound Rules** area. For more information, see **Table 8-2**.

Table 8-2 Adding an inbound rule

Parameter	Description
Protocol & Port	Enter the inbound protocol type and port number of the pods to be associated. Currently, TCP and UDP are supported. If this parameter is not specified, all access traffic is allowed.
Source Namespace	Select a namespace whose objects can be accessed. If this parameter is not specified, access to the objects that belong to the same namespace as the current policy is allowed.
Source Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

- Outbound rule: Click **Add Rule** in the **Outbound Rules** area. For more information, see **Table 8-3**.

Table 8-3 Adding an outbound rule

Parameter	Description
Protocol & Port	Enter the port and protocol of destination objects. If this parameter is not specified, access is not limited.
Destination CIDR Block	Configure CIDR blocks. This parameter allows requests to be routed to a specified CIDR block (and not to the exception CIDR blocks). Separate the destination and exception CIDR blocks by vertical bars (|), and separate multiple exception CIDR blocks by commas (,). For example, 172.17.0.0/16|172.17.1.0/24,172.17.2.0/24 indicates that 172.17.0.0/16 is accessible, but not for 172.17.1.0/24 or 172.17.2.0/24.
Destination Namespace	Namespace where the destination object is located. If not specified, the object belongs to the same namespace as the current policy.
Destination Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

Step 9 Click **OK**.

You can view the new policy in the policy management list.

----End

Related Operations

Modifying or deleting a network policy

Step 1 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 2 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 3 Click **Synchronize** above the network policy list.

The synchronization takes about 1 to 2 minutes. Wait for a while and click in the upper right corner of the list to refresh and view the latest data.

Step 4 Manage policies as needed.

- Modifying a policy
  - In the **Operation** column of a policy, click **Edit YAML**. On the YAML page, modify the YAML content and click **OK**.
  - In the **Operation** column of a policy, click **Update**. Modify the network policy information and click **OK**.
- Deleting a policy
  - In the **Operation** column of a policy, click **Delete**. In the confirmation dialog box, click **OK**.
  - Select one or multiple policies and click **Delete** above the policy list. In the displayed dialog box, click **OK**.

----End

8.1.3 Configuring a Network Defense Policy (for a VPC Network)

Scenarios

If no network defense policies are configured for a pod, all traffic is allowed to enter and leave the pod by default. In this case, pods can communicate with each other and access the external network, which poses security risks.

This section describes how to configure network defense policies for clusters using the VPC network model to control the inbound and outbound traffic of nodes, thereby enhancing cluster network security.

Creating a Network Defense Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose > **Container Firewalls**.

Step 5 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 6 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click in the upper right corner of the list to refresh and view the latest data.

Step 7 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 8 In the **Operation** column of a node, click **Configure Policy**.

Step 9 In the displayed dialog box, click **OK** to go to the cloud server console.

Step 10 Click the **Security Groups** tab and view security group rules.

Step 11 Click the security group ID. The system automatically switches to the security group page.

Step 12 Configure inbound and outbound rules.

For details, see "Adding a Security Group Rule" in *Virtual Private Cloud User Guide*.

----End

Related Operations

Modifying or deleting a network defense policy

Step 1 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 2 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 3 Click **Synchronize** above the node list to synchronize node information.

The synchronization takes about 1 to 2 minutes. Wait for a while and click in the upper right corner of the list to refresh and view the latest data.

Step 4 In the **Operation** column of a node, click **Configure Policy**.

Step 5 In the displayed dialog box, click **OK** to go to the cloud server console.

Step 6 Click the **Security Groups** tab and view security group rules.

Step 7 Click **Manage Rule**. The security group page is displayed.

Step 8 Click a rule tab and manage rules as needed.

- Modifying a rule

  In the **Operation** column of a rule, click **Modify**. Modify the rule and click **OK**.
- Deleting a rule

  In the **Operation** column of a rule, click **Delete**. In the confirmation dialog box, click **OK**.

----End

8.2 Container Cluster Protection

8.2.1 Container Cluster Protection Overview

HSS can check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks.

You can configure container cluster protection policies to block images with vulnerabilities, malicious files, non-compliant baselines, or other threats, hardening cluster security.

Constraints

- You have applied for a CCE cluster in version 1.20 or later.
- Container cluster protection is available only in the HSS container edition.

Process of Using Container Cluster Protection

Figure 8-1 Usage process

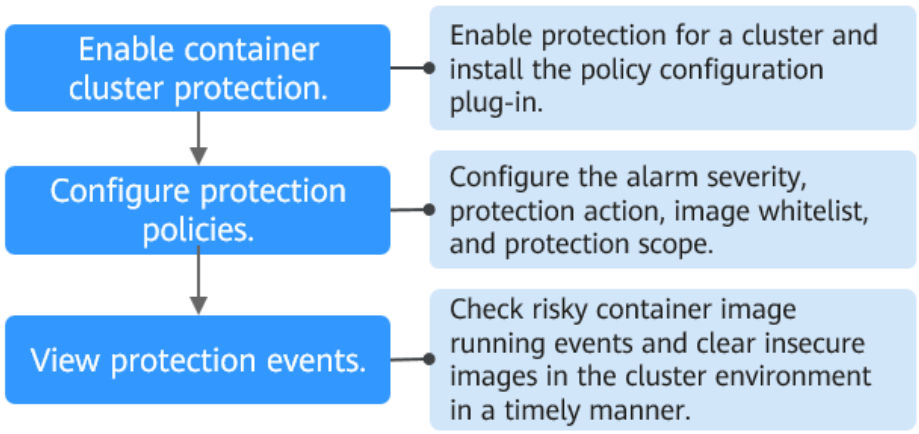


Table 8-4 Process of using container cluster protection

Operation	Description
Enable container cluster protection.	Enable protection for a cluster to protect its workloads and critical data. When protection is enabled, HSS automatically installs the policy management plug-in on the cluster.
Configure a protection policy.	Configure the severity of baseline, vulnerability, and malicious file risks that trigger alarms; container cluster protection scope; image whitelist; and actions to be taken on alarms.
Check container cluster protection events.	On the HSS console, you can view unauthorized or high-risk container image running events that are reported or blocked, and check and clear insecure container images in a timely manner.

8.2.2 Enabling Container Cluster Protection

Container cluster protection can detect risks in baselines, vulnerabilities, and malicious files; and can report alarms on or block insecure container images. You can enable protection to enhance cluster defense and protect containers.

Constraints

After container cluster protection is enabled, you need to configure a policy to make the protection take effect. For more information, see **Configuring a Container Cluster Protection Policy**.

Enabling Container Cluster Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose > **Container Cluster Protection**.

Step 5 Click the **Protected Clusters** tab.

Step 6 Click **Synchronize** to synchronize clusters.

Step 7 Click **Enable** in the **Operation** column of a cluster.

To enable protection for clusters in batches, select clusters and click **Enable Protection** in the upper left corner of the cluster list.

CAUTION

- After container cluster protection is enabled for a cluster, the policy management plug-in will be installed in the cluster and occupy some cluster resources.
- When enabling protection for a container cluster, do not perform any operation on the cluster. Otherwise, protection will fail to be enabled.

Step 8 Click **OK**.

If the **Protection Status** of the container cluster is **Enabled but not configured**, it indicates protection has been configured for the cluster and the policy management plug-in has been installed, but HSS has not started to protect your cluster. In this case, you need to configure a protection policy. For more information, see **Configuring a Container Cluster Protection Policy**.

----End

8.2.3 Configuring a Container Cluster Protection Policy

You can configure container cluster protection policies to specify the level of risks (unsafe baselines, vulnerabilities, or malicious files) that trigger alarms, cluster protection scope, image whitelist, and the actions taken on an alarm.

Creating a Protection Policy

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose > **Container Cluster Protection**.

Step 5 Click the **Protection Policies** tab and click **Create Policy**.

Step 6 In the **Create Policy** dialog box, set policy parameters. For details about related parameters, see **Table 8-5**.

Table 8-5 Container cluster protection policy parameters

Parameter	Description	Example Value
Policy Template	Select a policy template. The procedure is as follows: 1. Click **Select Template**. 2. Select a policy template and click **OK**. You can select a policy template based on the policy description. After selecting a policy template, configure policy parameters based on the policy template requirements. You can refer to the parameter description.	K8sPSPPrivilegedContainer
Policy Name	Enter a policy name. The name can only contain letters, numbers, commas (,), periods (.), spaces, underscores (_), and hyphens (-).	test
Policy Description	Enter policy description. The description can only contain letters, numbers, commas (,), periods (.), spaces, underscores (_), and hyphens (-).	Test
Action	Action taken by HSS if it detects that an image to be started contains specified unsafe baseline items, vulnerabilities, or malicious scripts. ● **Alarm**: Generate an event whose **Action** is **Alarm** on the **Protection Events** tab of the **Container Cluster Protection** page. ● **Block**: Block an unsafe image and generate an event whose **Action** is **Block** on the **Protection Events** tab of the **Container Cluster Protection** page. ● **Allow**: Generate an event whose **Action** is **Allow** on the **Protection Events** tab of the **Container Cluster Protection** page.	Block
Protection Scope	Configure the protection scope of clusters. If you select the image blocking policy, you need to set the images and tags to specify the protection scope.	-

Parameter	Description	Example Value
(Optional) Whitelist	Images to be added to the whitelist. HSS does not check whitelisted images when they are started. Enter values in *ImageName*:*ImageVersion* format. An image name can contain only numbers, letters, underscores (_), hyphens (-), and periods (.). Each image name occupies a separate line. Example: • A single image **image:1.0** • Multiple images **image1:1.0** **image2:1.0**	-

Step 7 Click **OK**.

You can view the protection policy in the policy list.

----End

Editing or Deleting a Cluster Protection Policy

Step 1 Choose **Container Cluster Protection** and click the **Protection Policies** tab.

Step 2 In the **Operation** column of a policy, click a button as required.

- **View YAML**: View the protection policy content in YAML format.
- **Edit**: Modify a protection policy.
- **Delete**: Delete a protection policy. After a policy is deleted, the container clusters associated with it will no be protected. Exercise caution when performing this operation.

Step 3 Click **OK**.

----End

8.2.4 Checking Container Cluster Protection Events

HSS detects risks and displays security events in the protection event list. This section describes how to check the events.

Checking Container Cluster Protection Events

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose > **Container Cluster Protection**.

Step 5 Click the **Protection Events** tab and check events in the cluster.

To export events to your local PC, click **Export** in the upper left corner of the event list.

Step 6 Click an alarm name to view affected resources.

----End

8.2.5 Disabling Container Cluster Protection

If you no longer need HSS to protect your container clusters, you can disable container cluster protection.

Disabling Container Cluster Protection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose > **Container Cluster Protection**.

Step 5 Click the **Protected Clusters** tab.

Step 6 In the **Operation** column of a cluster, click **Disable Protection**.

To disable protection for clusters in batches, select clusters and click **Disable Protection** in the upper left corner of the cluster list.

Step 7 In the dialog box that is displayed, determine whether to select the **Delete policy plug-in of the cluster** check box.

- If you select it, container cluster protection policies and the policy configuration plug-in will be deleted. If you enable protection again, you will need to install the policy configuration plug-in and configure protection policies again.
- If you deselect it, container cluster protection policies will be deleted but the policy configuration plug-in will be retained. If you enable protection again, you only need to configure protection policies. If you want to delete the policy configuration plug-in later, repeat the preceding steps to disable protection and select **Delete policy plug-in of the cluster**.

Step 8 Click **OK**.

- If you did not select **Delete policy plug-in of the cluster** and the **Protection Status** of the cluster changes to **Enabled but not configured**, it indicates protection has been disabled.
- If you selected **Delete policy plug-in of the cluster** and the **Protection Status** of the cluster changes to **Unprotected**, it indicates protection has been disabled.

----End

FAQ

If the cluster network is abnormal or the plug-in is working, you will probably fail to uninstall the plug-in on the HSS console. In this case, you can refer to the content below: **What Do I Do If the Container Cluster Protection Plug-in Fails to Be Uninstalled?**

9 Detection and Response

9.1 HSS Alarms

9.1.1 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	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
Malware	Unclassified malware	Malicious programs include Trojans and web shells implanted by hackers to steal your data or control your servers. For example, hackers will probably use your servers as miners or DDoS zombies. This occupies a large number of CPU and network resources, affecting service stability. Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one-click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.	×	√	√	√	√	√
	Viruses	Detect viruses in server assets, report alarms, and support automatic or manual viruses isolation and killing based on the alarms.	×	√	√	√	√	√
	Worms	Detect and kill worms on servers and report alarms.	×	√	√	√	√	√
	Trojans	Detect and remove Trojan and viruses on servers and report alarms.	×	√	√	√	√	√
	Botnets	Detect and kill botnets on servers and report alarms.	×	√	√	√	√	√

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	Backdoors	Detect backdoors in servers and reports alarms.	×	√	√	√	√	√
	rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	×	√	√	√	√	×
	Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.	×	×	√	√	√	√ (Partially supported)
	Hacker tools	Detect and kill hacker tools on servers and reports alarms.	×	√	√	√	√	√

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	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**. **Isolation and removal**: automated or manual	×	×	√	√	√	×
	Mining	Detect, scan, and remove mining software on servers, and report alarms.	×	√	√	√	√	√
Vulnerability Exploits	Remote code execution	Detect and report alarms on server intrusions that exploit vulnerabilities in real time.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
Abnormal System Behavior	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.	×	×	√	√	√	×
	File privilege escalations	Detect file privilege escalation operations and generate alarms.	×	√	√	√	√	×
	Process privilege escalations	Detect the privilege escalation operations of the following processes and generate alarms: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	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.	×	√	√	√	√	×
	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.	×	√	√	√	√	×
	Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: • Abnormal CPU usage • Processes accessing malicious IP addresses • Abnormal increase in concurrent process connections	×	√	√	√	√	x (Partially supported)

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	High-risk command executions	You can configure what commands will trigger alarms in the **High-risk Command Scan** rule on the **Policies** page. HSS checks executed commands in real time and generates alarms if high-risk commands are detected.	×	√	√	√	√	×
	Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You can configure the abnormal shell detection rule in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	Sensitive file access detection	Detect the unauthorized access to or modifications of sensitive files.	×	√	√	√	√	×
	Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.	×	×	√	√	√	×
	System protection disabling	Detect the preparations for ransomware encryption, such as disabling the real-time protection of Windows defender through the registry. Once such an operation is detected, an alarm is reported immediately.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	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.	×	√	√	√	√	×
	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.	×	√	√	√	√	×
	System log deletions	An alarm is generated when a command or tool is used to clear system logs.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	Suspicious command executions	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution.	×	√	√	√	√	×
	Suspicious process execution	Detect and report alarms on unauthenticated or unauthorized application processes.	×	√	√	√	√	×
	Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
Abnormal User Behavior	Brute-force attacks	If hackers log in to your servers through brute-force attacks, they can obtain the control permissions of the servers and perform malicious operations, such as steal user data; implant ransomware, miners, or Trojans; encrypt data; or use your servers as zombies to perform DDoS attacks. Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. ● 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. The default blocking duration is 12 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.	√	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	Abnormal logins	Detect abnormal login behavior, such as remote login and brute-force attacks. If abnormal logins are reported, your servers may have been intruded by hackers. • Check and handle remote logins. You can check the blocked login IP addresses, and who used them to log in to which server at what time. If a user's login location is not any common login location, an alarm will be triggered. • Trigger an alarm if a user logs in to the server by a brute-force attack.	√	√	√	√	√	×
	Invalid accounts	Hackers can probably crack unsafe accounts on your servers and control the servers. HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them.	×	√	√	√	√	×
	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.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	Password theft	Detect the abnormal obtaining of system accounts and password hashes on servers and report alarms.	×	√	√	√	√	×
Abnormal Network Access	Cloud honeypot	An alarm is reported if a connection to the honeypot port of a server is detected.	×	×	√	√	√	×
	Abnormal outbound connection	Report alarms on suspicious IP addresses that initiate outbound connections.	×	√	√	√	√	×
	Port forwarding	Report alarms on port forwarding performed using suspicious tools.	×	√	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
	Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected.	×	√	√	√	√	×
	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.	×	√	√	√	√	×
Reconnaissance	Port scan	Detect scanning or sniffing on specified ports and report alarms.	×	×	√	√	×	×
	Host scan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms.	×	×	√	√	√	×

Event Type	Alarm Name	Description	Basic Edition	Enterprise Edition	Premium Edition	WTP Edition	Add to Alarm Whitelist	Isolate and Kill
Fileless Attacks	Process injection	Scan for malicious code injection into running processes and report alarms.	×	√	√	√	√	×
	Dynamic library injection	Scan for the payloads injected by hijacking functions in the dynamic link library (DLL) and report alarms.	×	√	√	√	√	×
	Memory file process	Scan for the behaviors of creating an anonymous malicious file that exists only in the RAM through the memfd_create system call and executing the file, and report alarms on such behaviors.	×	√	√	√	√	×

Security Alarm Severities

HSS alarm severities indicate alarm impact on service systems. It can be Critical, High, Medium, or Low. For details, see **Table 9-1**.

Table 9-1 Security alarm severities

Alarm Severity	Description
Critical	A critical alarm indicates that the system is severely attacked, which may cause data loss, system breakdown, or long service interruption. For example, such alarms are generated if ransomware encryption behaviors or malicious programs are detected. You are advised to handle the alarms immediately to avoid severe system damage.
High	A high-risk alarm indicates that the system may be under an attack that has not caused serious damage. For example, such alarms are generated if unauthorized login attempts are detected or unsafe commands (for deleting critical system files or modifying system settings) are executed. You are advised to investigate and take measures in a timely manner to prevent attacks from spreading.
Medium	A medium-risk alarm indicates that the system has potential security threats, but there are no obvious signs of being attacked. For example, if abnormal modifications of a file or directory are detected, there may be potential attack paths or configuration errors in the system. You are advised to further analyze and take proper preventive measures to enhance system security.
Low	A low-risk alarm indicates that a minor security threat exists in the system but does not have significant impact on your system. For example, such alarms are generated if port scans are detected, indicating that there may be attackers trying to find system vulnerabilities. These alarms do not require immediate emergency measures. If you have high requirements on asset security, pay attention to the security alarms of this level.

Monitored Important File Paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login

Type	Linux
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

9.1.2 Viewing Server Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, servers with alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarm events generated in the last 30 days. You can manually handle the alarmed items.

The status of a handled event changes from **Unhandled** to **Handled**.

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

- To skip the checks on high-risk command execution, privilege escalations, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. HSS will not check the servers associated with disabled policies.
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

Viewing Server Alarms

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Check server alarms.

Table 9-2 Alarm statistics

Parameter	Description
Enterprise Project	Select an enterprise project and view alarm details by enterprise project.
Time range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: • Last 24 hours • Last 3 days • Last 7 days • Last 30 days
Urgent Alarms	Number of urgent alarms that need to be handled.
Total Alarms	Total number of alarms on your assets.
Affected Servers	Number of servers for which alarms are generated. When checking alarms generated in the last 24 hours, you can click the number of servers to go to the **Servers & Quota** page and check the corresponding servers.
Handled Alarms	Number of handled alarms.

Parameter	Description
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** • The agent of Linux 3.2.10 or later supports IPv6 blocking. The agent of any earlier version can use TCP Wrapper for blocking, but cannot use iptables for IPv6 blocking. • After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address. • A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be clocked for MySQL and vsftp. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.
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**.

- **Viewing the alarms of a certain type or ATT&CK phase**

  In the **Alarms to Be Handled** area, you can select an alarm type and an ATT&CK phase to view the alarms of the selected type. For details, see **ATT&CK attack phase description**.

  NOTE

  Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a framework that helps organizations understand the cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle.

  Table 9-3 ATT&CK phases

ATT&CK Phase	Description
Reconnaissance	Attackers seek vulnerabilities in your system or network.
Initial Access	Attacker try to enter your system or network.

ATT&CK Phase	Description
Execution	Attackers try to run malicious code.
Persistence	Attackers try to maintain their foothold.
Privilege Escalation	Attackers try to obtain higher permissions.
Defense Evasion	Attackers try to avoid being detected.
Credential Access	Attackers try to steal account names and passwords.
Command and Control	Attackers try to communicate with compromised machines to control them.
Impact	Attackers try to manipulate, interrupt, or destroy your system or data.

- **Viewing the details of a server alarm**

  You can click the alarm name of an event to view the alarm details. **Table 9-4** describes the alarm parameters.

  NOTE

  - For some HSS alarms that have been determined as malware alarms, the alarm source files are saved in the cloud center and you can download them. You can download the alarm source files to your local PC for analysis. The password for decompressing the files is **unlock**.
  - For unacknowledged malware alarms, alarm source files cannot be downloaded. Check the actual service conditions and determine whether the files are malicious files.

  Table 9-4 Alarm detail parameters

Parameter	Description
Protection Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm was first generated
Alarm ID	Unique ID of an alarm
ATT&CK Phase	For details about the attack technology models used by attackers in each phase, see **Table 9-3**.
Last Occurred	Time when an attack alarm was last generated

Parameter	Description
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.

Parameter	Description
Forensics	HSS investigates information such as the attack triggering path or virus type based on the alarm type, helping you quickly trace and locate the attack source. – **Process Tree**: If an alarm event contains process information, you can check the process ID, process file path, process command line, process startup time, and process file hash on the **Forensics** tab page. You can locate malicious processes based on such information. – **File Forensics**: If an alarm event contains file information, the file forensics information is displayed on the **Forensics** tab page. File forensics information includes the file path, file hash. You can locate a file based on the information. – Network Forensics: If an alarm event contains file information, the network forensics information is displayed on the **Forensics** tab page. Network forensics information includes the local IP address, local port, remote IP address, remote port, and protocol. You can determine whether the access is unauthorized based on such information. – User Forensics: If an alarm event contains user behavior information, the user forensics information is displayed on the **Forensics** tab page. User forensics information includes the username, login IP address, login service type, login service port, last login event, and number of login failures. You can determine whether the access is unauthorized based on such information. – **Registry Forensics**: If an alarm event contains registry information, you can check the registry keys and values on the **Forensics** tab page. You can locate registry risks based on such information. – **Abnormal Login Forensics**: If an alarm event contains abnormal login information, you can check the login IP address and port number on the **Forensics** tab page. You can determine whether the login is trusted based on such information. – **Malware Forensics**: If an alarm event contains malware information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. – **Auto-started Item Forensics**: If an alarm event contains self-startup item information, you can check the user, command, self-startup item information, and process file command line information on the **Forensics** tab page. You can locate the auto-boot item based on the auto-started item forensics information. – **Kernel Forensics**: If an alarm event contains kernel information, you can check system functions and kernel functions on the **Forensics** tab page. You can locate kernel risks based on the information.

Parameter	Description
Similar Alarms	Alarm whose server and event type are the same as those of this alarm. You can handle the alarm according to the handling method of the similar alarms.

----End

9.1.3 Handling Server Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, servers with alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarms generated in the last 30 days.

The status of a handled alarm changes from **Unhandled** to **Handled**.

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

- To skip the checks on high-risk command execution, privilege escalations, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. HSS will not check the servers associated with disabled policies.
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

Handling Server Alarms

This section describes how you should handle alarms to enhance server security.

NOTE

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click an alarm name to view the alarm details and suggestions.

Step 7 Handle alarms.

Check and handle alarms as needed. The status of a handled alarm changes from **Unhandled** to **Handled**.

- Handling a single alarm

  In the **Operation** column of an alarm, click **Handle**.
- Handling alarms in batches

  Select all alarms and click **Batch Handle** above the alarm list.
- Handling all alarms

  In the **Alarms to be Handled** area on the left pane of the alarm list, select an alarm type and click **Handle All** above the alarm list.

Step 8 In the **Handle Event** dialog box, select an action. For details about the alarm handling actions, see **Table 9-5**.

When you handle one or multiple alarm events, you can select **Handle duplicate alarms in batches** in the **Handle Event** dialog box.

Table 9-5 Alarm handling methods

Action	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check the files. For details, see **Managing Isolated Files**. For details about events that can be isolated and killed, see **Server Alarms**. **NOTE** When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any).
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.
Add to process whitelist	If you can confirm that a process triggering an alarm can be trusted, you can add it to the process whitelist. HSS will no longer report alarms on whitelisted processes.

Action	Description
Add to Login Whitelist	Add false alarmed items of the **Brute-force attack** and **Abnormal login** types to the Login Whitelist. HSS will no longer report alarm on the Login Whitelist. A whitelisted login event will not trigger alarms. The following alarm events can be added: • Brute-force attacks • Abnormal logins
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. After adding an alarm to the alarm whitelist, you can customize a whitelist rule. The custom rule types vary depending on the alarm types, including the file path, process path, process command line, remote IP address, and user name. If a detected alarm event hit the rule you specified, HSS does not generate an alarm. For details about events that can be isolated and killed, see **Server Alarms**.

Step 9 Click **OK**.

You check handled alarms. For details, see **Handling History**.

----End

Canceling Handled Server Alarms

You can cancel the processing of a handled alarm event.

Step 1 In the alarm event list, filter handled alarms.

Step 2 In the **Operation** column of an alarm, click **Handle**.

Step 3 In the **Handle Alarm Event** dialog box, click **OK** to cancel the last handling.

----End

9.1.4 Exporting Server Alarms

You can export server alarms and events to a local PC.

Exporting Server Alarms

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Detection & Response** > **Alarms**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Server Alarms** tab.

Step 7 Click **Export** above the alarm list to export all security events.

Step 8 View the export status in the upper part of the alarms page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

9.1.5 Managing Isolated Files

HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page. You can click **Isolated Files** on the upper right corner to check them, and can recover or delete isolated files anytime.

For details about events that can be isolated and killed, see **Server Alarms**.

Constraints

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

Isolation and Killing Operations

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 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 7 Click **OK** and isolate and kill the target alarm event.

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

----End

Checking Isolated Files

Step 1 In the alarm statistics area on the **Server Alarms** page, click the number above **Isolated Files** to check the isolated files.

Step 2 Check the servers, names, paths, and modification time of the isolated files.

----End

Restoring Isolated Files

If you want to de-isolate an isolated file, you can restore it by referring to the following steps. The permissions for this file will be restored to what they were before it was isolated. Exercise caution when performing this operation.

Step 1 Click **Restore** in the **Operation** column of the list. The dialog box is displayed.

Step 2 Click **OK**.

----End

Deleting Isolated Files

If you want to permanently delete an isolated file, you can perform the deletion operation by referring to the following steps.

Step 1 Click **Delete** in the **Operation** column of the list. The dialog box is displayed.

To delete isolated files in batches, select multiple isolated files and click **Delete** in the upper left corner of the list.

Step 2 Click **OK**.

----End

9.2 Container Alarms

9.2.1 Container Alarm Events

After node protection is enabled, an agent is deployed on each container host to monitor the running status of containers in real time. The agents support escape detection, high-risk system calls, abnormal processes, abnormal files, and container environment detection. You can learn alarm events comprehensively on the **Container Alarms** page, and eliminate security risks in your assets in a timely manner.

Constraints

- Only the HSS container edition supports container security alarms.

Container Security Alarms

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.
	Hacker tools	Report alarms on the malicious behaviors that exploit vulnerabilities or are performed using hacker tools.
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 report alarms on and block reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. You can configure the reverse shell detection rule and automatic blocking in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. You can also configure automatic blocking of reverse shells in the **HIPS Detection** rule on the **Policies** page.
	File privilege escalation	Report alarms on root privilege escalations exploiting SUID and SGID program vulnerabilities.

Event Type	Alarm Name	Mechanism
	Process privilege escalations	After hackers intrude containers, they will try exploiting vulnerabilities to grant themselves the root permissions or add permissions for files. In this way, they can illegally create system accounts, modify account permissions, and tamper with files. HSS can detect the following abnormal privilege escalation operations: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities • File privilege escalation
	Important file changes	Monitor important system files (such as ls, ps, login, and top) in real time and generate alarms if these files are modified. For more information, see **Monitored important file paths**. HSS reports all the changes on important files, regardless of whether the changes are performed manually or by processes.
	Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: • Abnormal CPU usage • Processes accessing malicious IP addresses • Abnormal increase in concurrent process connections
	High-risk system calls	Users run tasks in kernels through Linux system calls. HSS 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.

Event Type	Alarm Name	Mechanism
	Abnormal container processes	• Malicious container program HSS monitors container process behavior and process file fingerprints. It reports an alarm if it detects a process whose behavior characteristics match those of a predefined malicious program. • Abnormal processes 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	HSS monitors container startups and reports an alarm if it detects that a container with too many permissions is started. This alarm does not indicate an actual attack. Attacks exploiting this risk will trigger other HSS container alarms. HSS container check items include: ● Privileged container startup (**privileged:true**) Alarms are triggered by the containers started with the maximum permissions (similar to OS root permissions). Settings that can trigger such alarms include the **–privileged=true** parameter in the **docker run** command, and **privileged: true** in the **securityContext** of the container in a Kubernetes pod. If the alarm name is **Container Security Options** and the alarm content contains **privileged:true**, it indicates that the container is started in privileged container mode. ● Too many container capabilities (**capability:[xxx]**) In Linux OSs, system permissions are divided into groups before assigned to containers. A container only has a limited number of permissions, and the impact scope of this container is limited in the case of an incident. However, malicious users can grant all the system permissions to a container by modifying its startup configurations. If the alarm name is **Container Security Options** and the alarm content contains **capabilities:[xxx]**, it indicates that the container is started with an overlarge capability set, which poses risks. ● Seccomp not enabled (**seccomp=unconfined**) Secure computing mode (seccomp) is a Linux kernel feature. It can restrict system calls invoked by processes to reduce the attack surface of the kernel. If **seccomp=unconfined** is configured when a container is started, system calls will not be restricted for the container. If the alarm name is **Container Security Options** and the alarm content contains **seccomp=unconfined**, it indicates that the container is started without seccomp, which poses risks. **NOTE** If seccomp is enabled, permissions will be verified for every system call. The verifications will probably affect services if system calls are frequent. Before you decide whether to enable seccomp, you are advised to test-enable it and analyze the impact on your services. ● Container privilege escalation (**no-new-privileges:false**)

Event Type	Alarm Name	Mechanism
		HSS reports an alarm if it detects that a process attempts to escalate permissions by running the **sudo** command and using the SUID or SGID bit. If **–no-new-privileges=false** is specified when a container is started, the container can escalate privileges. If the alarm name is **Container Security Options** and the alarm content contains **no-new-privileges:false**, it indicates that privilege escalation restriction is disabled for the container, which poses risks. • High-risk directory mapping (**mounts:[...]**) For convenience purposes, when a container is started on a server, the directories of the server can be mapped to the container. In this way, services in the container can directly read and write resources on the server. However, this mapping incurs security risks. If any critical directory in the server OS is mapped to the container, improper operations in the container will probably damage the server OS. HSS reports an alarm if it detects that a critical server path (**/boot**, **/dev**, **/etc**, **/sys**, and **/var/run**) is mounted during container startup. If the alarm name is **Container Mount Point** and the alarm content contains **mounts: [{"source":"xxx","destination":"yyy"...]**, it indicates that a file path mapped to the container is unsafe. In this case, check for risky directory mappings. You can configure the mount paths that are considered secure in the container information collection policy. **NOTE** Alarms will not be triggered for the files that need to be frequently accessed by Docker containers, such as **/etc/hosts** and **/etc/resolv.conf**. • Startup of containers in the **host** namespace The namespace of a container must be isolated from that of a server. If a container and a server use the same namespace, the container can access and modify the content on the server, which incurs container escape risks. To prevent such problems, HSS checks the container PID, network, and whether the container IPC namespace is **host**. If the alarm name is **Container Namespace** and the alarm content contains **Container PID Namespace Mode**, **Container IPC Namespace Mode**, or **Container Network Namespace Mode**, it indicates that a container whose namespace is **host** is started. In this case, check the container startup options based

Event Type	Alarm Name	Mechanism
		on the alarm information. If you are sure that the container can be trusted, you can ignore the alarm.
	Container Image blocking	If a Docker container contains insecure images specified in the **Suspicious Image Behaviors**, before the container is started, an alarm will be generated for the insecure images. **NOTE** You need to **install the Docker plug-in**.
	Suspicious command executions	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution.
Abnormal User Behaviors	Invalid accounts	Hackers can probably crack unsafe accounts on your containers and control the containers. HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them.
	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.
	Password thefts	Report alarms on user key theft.
Abnormal Network Access	Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections.
	Port forwarding	Report alarms on port forwarding using suspicious tools.
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.

Event Type	Alarm Name	Mechanism
	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.

Security Alarm Severities

HSS alarm severities indicate alarm impact on service systems. It can be Critical, High, Medium, or Low. For details, see **Table 9-6**.

Table 9-6 Security alarm severities

Alarm Severity	Description
Critical	A critical alarm indicates that the system is severely attacked, which may cause data loss, system breakdown, or long service interruption. For example, such alarms are generated if ransomware encryption behaviors or malicious programs are detected. You are advised to handle the alarms immediately to avoid severe system damage.
High	A high-risk alarm indicates that the system may be under an attack that has not caused serious damage. For example, such alarms are generated if unauthorized login attempts are detected or unsafe commands (for deleting critical system files or modifying system settings) are executed. You are advised to investigate and take measures in a timely manner to prevent attacks from spreading.
Medium	A medium-risk alarm indicates that the system has potential security threats, but there are no obvious signs of being attacked. For example, if abnormal modifications of a file or directory are detected, there may be potential attack paths or configuration errors in the system. You are advised to further analyze and take proper preventive measures to enhance system security.
Low	A low-risk alarm indicates that a minor security threat exists in the system but does not have significant impact on your system. For example, such alarms are generated if port scans are detected, indicating that there may be attackers trying to find system vulnerabilities. These alarms do not require immediate emergency measures. If you have high requirements on asset security, pay attention to the security alarms of this level.

Monitored important file paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

9.2.2 Viewing Container Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, containers with alarms, and handled alarms.

The **Events** page displays the alarm events generated in the last 30 days.

The status of a handled event changes from **Unhandled** to **Handled**.

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.

Viewing Container Alarms

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Detection & Response** > **Alarms** and click the **Container Alarms** tab to view container alarms and events.

Table 9-7 Container alarm statistics

Parameter	Description
Urgent Alarms	Number of alarms that need to be handled immediately. You can click a value to view the corresponding alarm events.
Total Alarms	Total number of alarms reported on your assets. You can click the number to view all alarms.
Containers with Alarms	Number of containers for which alarms are generated.
Handled Alarms	Number of handled alarms

- **Viewing the alarms of a certain type or ATT&CK phase**

  In the **Alarms to Be Handled** area, select an alarm type or att&ck phase. For details, see **ATT&CK attack phase description**.

  NOTE

  Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a framework that helps organizations understand the cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle.

  Table 9-8 ATT&CK phases

ATT&CK Phase	Description
Reconnaissance	Attackers seek vulnerabilities in your system or network.
Initial Access	Attacker try to enter your system or network.
Execution	Attackers try to run malicious code.
Persistence	Attackers try to maintain their foothold.
Privilege Escalation	Attackers try to obtain higher permissions.
Defense Evasion	Attackers try to avoid being detected.
Credential Access	Attackers try to steal account names and passwords.
Command and Control	Attackers try to communicate with compromised machines to control them.
Impact	Attackers try to manipulate, interrupt, or destroy your system or data.

- **Viewing details about container alarms and events**

  Click an alarm name to go to its details page. You can view the alarm description, handling suggestion, alarm path and address in HSS forensics,

and the handling history of similar alarms. **Table 9-9** describes the details of alarm information.

NOTE

For some HSS alarms that have been determined as malware alarms, the alarm source files are saved in the cloud center and you can download them. You can download the alarm source files to your local PC for analysis. The password for decompressing the files is **unlock**.

For unacknowledged malware alarms, alarm source files cannot be downloaded. Check the actual service conditions and determine whether the files are malicious files.

Table 9-9 Alarm detail parameters

Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm was first generated
Alarm ID	Unique ID of an alarm
ATT&CK Phase	For details about the attack technology models used by attackers in each phase, see **Table 9-8**.
Last Occurred	Time when an attack alarm was last generated
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.

Parameter	Description
Forensics	HSS investigates information such as the attack triggering path or virus type based on the alarm type, helping you quickly trace and locate the attack source. – **Process Tree**: If an alarm event contains process information, you can check the process ID, process file path, process command line, process startup time, and process file hash on the **Forensics** tab page. You can locate malicious processes based on such information. – **File Forensics**: If an alarm event contains file information, the file forensics information is displayed on the **Forensics** tab page. File forensics information includes the file path, file hash. You can locate a file change based on the information. – Network Forensics: If an alarm event contains network-related information, you can check the local IP address, local port, remote IP address, remote port, and protocol on the **Forensics** tab. You can determine whether a user is unauthorized based on such information. – User Forensics: If an alarm event contains user-related information, you can check the user name, login IP address, login service type, login service port, last login event, and number of login failures on the **Forensics** tab. You can determine whether the access is unauthorized based on such information. – **Registry Forensics**: If an alarm event contains registry information, you can check the registry keys and values on the **Forensics** tab page. You can locate registry risks based on such information. – **Abnormal Login Forensics**: If an alarm event contains abnormal login information, you can check the login IP address and port number on the **Forensics** tab page. You can determine whether the login is trusted based on such information. – **Malware Forensics**: If an alarm event contains malware information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. – **Auto-started Item Forensics**: If an alarm event contains self-startup item information, you can check the user, command, self-startup item information, and process file command line information on the **Forensics** tab page. You can locate the auto-started items based on such information. – **Kernel Forensics**: If an alarm event contains kernel information, you can check system functions and kernel functions on the **Forensics** tab page. You can locate kernel risks based on the information.

Parameter	Description
	– **Container Forensics**: If an alarm event contains container information, you can check the container name and image ID on the **Forensics** tab page. You can locate container risks based on such information.
Similar Alarms	Alarm whose server and event type are the same as those of this alarm. You can handle the alarm according to the handling method of the similar alarms.

- **Viewing the pod details of a container alarm event**

  Click the pod name of the target alarm event to view the pod details, including the node IP address, namespace, pod IP address, pod label, and container list.

----End

9.2.3 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.

Handling Container Alarms

This section describes how you should handle alarms to enhance server security.

NOTE

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

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Alarms**, and click **Container Alarms**.

Step 5 Click an alarm name to view the alarm details and suggestions.

Step 6 Handle alarms.

Check and handle alarms as needed. The status of a handled alarm changes from **Unhandled** to **Handled**.

- Handling a single alarm

  In the **Operation** column of an alarm, click **Handle**.
- Handling alarms in batches

  Select all alarms and click **Batch Handle** above the alarm list.
- Handling all alarms

  In the **Alarms to be Handled** area on the left pane of the alarm list, select an alarm type and click **Handle All** above the alarm list.

Step 7 In the **Handle Event** dialog box, select an action. For details about the processing modes, see **Table 9-10**.

When handling a single alarm event or handling alarms in batches, you can select **Handle duplicate alarms in batches** in the **Handle Event** dialog box.

Table 9-10 Alarm handling methods

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.
Add to Login Whitelist	Add false alarmed items of the **Brute-force attack** and **Abnormal login** types to the Login Whitelist. HSS will no longer report alarm on the Login Whitelist. A whitelisted login event will not trigger alarms. The following alarm events can be added: • Brute-force attacks • Abnormal logins
Add to process whitelist	If you can confirm that a process triggering an alarm can be trusted, you can add it to the process whitelist.
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. For details about events that can be isolated and killed, see **Container Alarm Events**.

Step 8 Click **OK**.

You check handled alarms. For details, see **Historical Records**.

----End

Canceling Handled Container Alarms

You can cancel the processing of a handled alarm event.

Step 1 In the alarm event list, filter handled alarms.

Step 2 In the **Operation** column of an alarm, click **Handle**.

Step 3 In the **Handle Alarm Event** dialog box, click **OK** to cancel the last handling.

----End

9.2.4 Exporting Container Alarms

You can export container alarms and events to a local PC.

Exporting Container Alarms

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Detection & Response** > **Alarms**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

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

Step 7 Click **Export** above the alarm list to export all security events.

To export the alarms of a certain type or ATT&CK attack phase, select the type or phase in the **Alarms to Be Handled** area and click **to export**.

Step 8 View the export status in the upper part of the alarms page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

9.3 Whitelist Management

9.3.1 Managing the Login Whitelist

You can configure the IP addresses of destination servers, login IP addresses, login usernames, and user behaviors on the **Login Whitelist** tab page.

You can:

- Add the false alarms of the **Brute-force attack** and **Abnormal login** types to the whitelist. For details, see **Viewing Server Alarms**.
- Add whitelist items on the **Login Whitelist** tab page.

Constraints

- If the destination server IP address, login IP address, and username of a login are all whitelisted, this login will be allowed without checking.
- After an IP address is added to a whitelist by following the instructions in **Add an Item 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 Server Alarms**.
- To unblock IP addresses, add the IP address to the whitelist of the login security detection policy. For details, see **Login Security Check**.

Add an Item to the Login Whitelist

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Detection & Response** > **Whitelists**. Click **Login Whitelist** and click **Add**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 On the displayed page, enter the server IP address, login IP address, and login username.

Table 9-11 Login Whitelist parameters

Parameter	Description	Example Value
Server IP Address	IP address or subnet mask of the destination server. • IP address: for example, **192.168.1.1** or **16A0::1** • IP subnet mask: for example, **192.168.7.0/24** or **16A0:10:AB00:1E::/64**	192.168.1.1
Login IP Address		
Login Username	Current login username	hss_test
Remarks	Custom whitelist description	Test
Handle historical alarms	After this option is selected, login alarms that have been generated will be synchronized.	Selected

Step 7 Click **OK**.

----End

Deleting an Item from the Login Whitelist

To delete an item from the Login Whitelist, select it and click **Delete** above the list, or click **Delete** in its **Operation** column.

9.3.2 Managing the Alarm Whitelist

You can configure the alarm whitelist to reduce false alarms. Events can be deleted from the whitelist.

Whitelisted events will not trigger alarms.

On the **Alarms** page, you can add falsely reported alarms to the alarm whitelist. After an alarm is added to the whitelist, HSS will not generate alarms on it.

Adding Events to the Alarm Whitelist

Table 9-12 Adding alarm whitelist items

Method	Description
Add to alarm whitelist	Choose to add the alarm to the whitelist when handling it. The following types of events can be added to the alarm whitelist: • 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Whitelists**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Alarm Whitelist** tab to view the whitelist. For more information, see **Alarm whitelist parameters**.

Table 9-13 Alarm whitelist parameters

Parameter Name	Description
Alarm Type	Name of the alarm whitelist type.
Whitelist Field	Whitelisted file field
Wildcard	Logic used by a whitelisted rule, which can be equal or include.
Description	Description of the whitelist.
Whitelist Rule	Whitelisted rule ID
Added	Time when an alarm is added to the whitelist.
Enterprise Project	Enterprise project
Occurrences Today	Number of times that alarm events meet the whitelist conditions today.
Total Occurrences	Total number of times that alarm events meet the whitelist conditions. By default, this parameter is not displayed.

----End

Removing an Alarm from the Whitelist

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 & Response** > **Alarms**, click **Handle** in the **Operation** column of an event, and select **Remove from whitelist**.

9.3.3 Managing the System User Whitelist

HSS generates risky account alarms when non-root users are added to the root user group. You can add the trusted non-root users to the system user whitelist. HSS does not generate risky account alarms for users in the system user whitelist.

Adding an Item to the System User Whitelist

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Whitelists**.

Step 5 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 6 Click the **System User Whitelist** tab and click **Add**.

Step 7 On the **Add to System User Whitelist** page, enter the server ID, system username, and remarks.

Step 8 Click **OK**.

----End

Modifying the System User Whitelist

Step 1 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 2 In the row of the target system user whitelist, click **Modify** in the **Operation** column.

Step 3 In the **Modify System User Whitelist** dialog box, modify the information and click **OK**.

----End

Removing an Item from the System User Whitelist

Step 1 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 2 In the row of the target system user whitelist, click **Delete** in the **Operation** column.

You can also select multiple system user whitelist items and click **Delete** above the system user whitelist.

Step 3 In the dialog box displayed, click **OK**.

----End

10 Security Operations

10.1 Policy Management

10.1.1 Policy Management Overview

What Is a Policy Group?

HSS comes in multiple editions, including basic, enterprise, premium, WTP, and container editions. Except for the basic edition, they each have a default protection policy group. A policy group is a collection of policies. These policies can be applied to servers to centrally manage and configure the sensitivity, rules, and scope of HSS detection and protection.

You can create custom policy groups for HSS premium and container editions. If you have multiple servers protected by the premium or container edition but have different protection requirements for them, you can create custom policy groups for different servers and deploy different policy groups. For details, see **Creating a Custom Policy Group**.

What Policies Are Does a Policy Group Contain?

Policy groups vary by edition, as shown in **Table 10-1**. You can customize policies for asset management, baseline inspection, and intrusion detection as needed. For details, see **Configuring Policies**.

Table 10-1 Policies

Function Type	Policy	Description	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Asset management	Asset discovery	Scan and display all software in one place, including software name, path, and major applications, helping you identify abnormal assets.	Linux and Windows	×	√	√	√
Baseline Inspection	Weak password detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.	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	×	×	×	√
	Configuration check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	Linux and Windows	×	√	√	√
Intrusion detection	Antivirus	Check server assets and report, isolate, and kill the detected viruses. The generated alarms are displayed under **Detection & Response** > **Alarms** > **Server Alarms** > **Event Types** > **Malware**. After antivirus is enabled, the resource usage is as follows: The CPU usage does not exceed 40% of a single vCPU. The actual CPU usage depends on the server status.	Linux and Windows	√	√	√	×

Function Type	Policy	Description	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	Container 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	×	×	×	√
	Container information module	You can configure a trusted container whitelist based on the container name, organization name to which the image belongs, and namespace. The container whitelist does not detect or generate alarms.	Linux	×	×	×	√
	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 process whitelist	Check for process startups that violate security policies.	Linux	×	×	×	√

Function Type	Policy	Description	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Suspicious image behaviors	Configure the blacklist and whitelist and customize permissions to ignore abnormal behaviors or report alarms.	Linux	×	×	×	√
	Fileless attack detection	Scan for process injection, dynamic library injection, and memory file process behavior in user assets.	Linux	√	√	√	√
	HIPS detection	Check registries, files, and processes, and report alarms for operations such as abnormal changes.	Linux and Windows	√	√	√	√
	File protection	Check the files in the Linux OS, applications, and other components to detect tampering.	Linux and Windows	√	√	√	√

Function Type	Policy	Description	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Login security check	Detect brute-force attacks on SSH, FTP, and MySQL accounts. 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. 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.	Linux and Windows	√	√	√	√
	Malicious file detection	• Reverse shell: Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. • Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Linux	√	√	√	√
	Port scan detection	Detect scanning or sniffing on specified ports and report alarms.	Linux	×	√	√	√

Function Type	Policy	Description	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Abnormal process behaviors	All the running processes on all your servers are monitored for you. You can create a process whitelist to ignore alarms on trusted processes, and can receive alarms on unauthorized process behavior and intrusions.	Linux	√	√	√	√
	Root privilege escalation	Detect the root privilege escalation for files in the current system.	Linux	√	√	√	√
	Real-time process	Monitor the executed commands in real time and generate 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	√	√	√	√

Function Type	Policy	Description	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Self-protection	Self-protection	Protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes. ● Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. ● Enabling the self-protection policy has the following impacts: – The HSS agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console. – HSS processes cannot be terminated. – In the agent installation path **C:\Program Files\HostGuard**, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).	Windows	×	√	√	×

10.1.2 Configuring Policies

Scenario

After HSS is enabled, you can configure HSS policies based on your service requirements.

Constraints

- The enterprise, premium, WTP, or container edition is enabled.
- For the default policy groups, you are advised to retain their default configurations.
- Modifications on a policy take effect only in the group it belongs to.

Accessing the Policies Page

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Security Operation** > **Policies**. On the displayed page, **Policy group parameters** describes the fields.

Table 10-2 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group The preset policy group names are as follows: • **tenant_linux_container_default_policy_group**: preset Linux policy of the container edition. You can copy this policy group and create a new one based on it. • **tenant_linux_enterprise_default_policy_group** is the default Linux policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. • **tenant_windows_enterprise_default_policy_group**: preset Windows policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. • **tenant_linux_premium_default_policy_group**: preset Linux policy of the premium edition. You can create a policy group by copying this default group and modify the copy. • **tenant_windows_premium_default_policy_group**: preset Windows policy of the premium edition. You can create a policy group by copying this default group and modify the copy.
ID	Unique ID of a policy group
Description	Detailed description of a policy group.
Supported Version	HSS edition supported by a policy group.
Supported OS	OS supported by a policy group.
Associated Servers	To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

- If **All projects** is selected, the policy change will apply to the servers under all enterprise projects.
- If a specific enterprise project is selected, the policy change will only apply to the servers under this project.

Step 6 Click the name of a policy group to access the policy detail list.

Step 7 In the row of the policy, click **Enable** or **Disable** in the **Operation** column.

After a policy is disabled, HSS does not check for security issues based on the policy.

Step 8 Click the name of a policy to modify it. The following sections describe the policies.

----End

Asset Discovery

Step 1 Click **Asset Discovery**.

Step 2 On the displayed page, modify the settings as required. For more information, see **Table 10-3**.

Table 10-3 Parameter description

Parameter	Description
Scan Time	Fixed time for automatic assets scan. Offset time is the automatic adjust ahead of or behind the specified scan time. • Accounts: Linux accounts are automatically checked every hour, and Windows accounts are checked in real time. • Open ports are automatically checked every 30 seconds. • Processes are automatically checked every hour. • Installed software is automatically checked once a day. • Auto-started items are automatically checked every hour. • Middleware/Web framework: You can select the scan date and time together. • Kernel modules: You can set the scan date and time as required. • Web applications/Websites/Web services/Databases: You can select the scan date and time together.
Scanned Web Directories	Specifies a web directory to be scanned.
Scanned Web Directory Depth	Specifies the level depth for web directory scanning.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Weak Password Detection

Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no fewer 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 10-4**.

Table 10-4 Parameter description

Parameter	Description
Scan Time	Time when scans are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time of the weak password based on **Scan Time**. The value range is 0 to 7,200s.
Scan Days	Days in a week when weak passwords are scanned. You can select one or multiple days.
User-defined Weak Passwords	You can add a password that may have been leaked to this weak password text box to prevent server accounts from using the password. Enter only one weak password per line. Up to 300 weak passwords can be added.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Configuration Check

Step 1 Click **Configuration Check**.

Step 2 On the **Configure Check**, modify the policy.

Table 10-5 Parameter description

Parameter	Description
Scan Time	Time when scans are performed. It can be accurate to the minute.

Parameter	Description
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 scan is performed. You can select any days from Monday to Sunday.
System Default Baseline Library	The scan baseline has been configured in the system. You only need to select the baseline you want to scan. All parameters are in their default values and cannot be modified.

----End

Web Shell Detection

If **User-defined Scan Paths** is not specified, the website paths in your assets are scanned by default. If **User-defined Scan Paths** is specified, website paths and the specified paths are scanned.

Step 1 Click **Web Shell Detection**.

Step 2 On the **Web Shell Detection** page, modify the settings as required. For more information, see **Table 10-6**.

Table 10-6 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. The value ranges from 0 to 7,200s.
Scan Days	Days in a week when web shells are scanned. You can select one or more days.

Parameter	Description
User-defined Scan Paths	Web paths to be scanned. A file path must: • Start with a slash (/) and end with no slashes (/). • Occupy a separate line and cannot contain spaces. **Do not add network directories as protected directories.** HSS does not scan them even if they are added. The reasons are as follows: • Inefficient detection A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. • Network bandwidth consumption Accessing a network directory consumes network bandwidth. A large-scale scan may fully occupy the network bandwidth and affect your workloads. For example, the access speed may slow down and the network latency may increase.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

File Protection

Step 1 Click **File Protection**.

Step 2 On the **File Protection** page, modify the policy. For more information, see **Table 10-7**.

The following figure uses the Linux policy as an example.

Table 10-7 Parameter description

Parameter	Description
File Privilege Escalation	• Detects privilege escalation. – : enabled – : disabled • **Ignored File Path**: Files to be ignored. Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names.

Parameter	Description
File Integrity	• Checks the integrity of key files. – : enabled – : disabled • **File Paths**: Configure the file paths.
Important File Directory Change	• Detects the directory change of key files. – : enabled – : disabled • **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. – : enabled – : disabled • **Session IP Whitelist**: If the file process belongs to the sessions of the listed IP addresses, no audit applies. • **Unmonitored File Types**: File types that do not need to be monitored. • **Unmonitored File Paths**: File paths that do not need to be monitored. • **Monitoring Login Keys**: monitors login keys. – : enabled – : disabled
Directory Monitoring Mode	• Directory monitoring mode. • Some file or directory monitoring paths are preset in the system. You can modify the file change type to be detected and add the file or directory paths to be monitored. – **File or Directory Path**: path of the file or directory to be monitored. Up to 50 paths can be added. Ensure the specified paths are valid. – **Alias**: alias of a file or directory path. You can enter a name that is easy to distinguish. – **Monitor Subdirectory**: If this option is selected, all files in the corresponding subdirectories are monitored. If it is not selected, subdirectories are not monitored. – **Monitor Creation**, **Monitor Deletion**, **Monitor Movement**, and **Monitor Modification**: Select them as needed.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

HIPS Detection

Step 1 Click **HIPS Detection**.

Step 2 Modify the policy content. For more information, see **Table 10-8**.

Table 10-8 Parameter description

Parameter	Description
Auto Blocking	If this function is enabled, abnormal changes on registries, files, and processes will be automatically blocked to prevent reverse shells and high-risk commands. • : enabled • : disabled
Trusted Processes	Paths of trusted processes. You can click **Add** to add a path and click **Delete** to delete it.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Login Security Check

Step 1 Click **Login Security Check**.

Step 2 On the displayed **Login Security Check** page, modify the policy content. **Table 10-9** describes the parameters.

Table 10-9 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.

Parameter	Description
Check Whether the Audit Login Is Successful	• After this function is enabled, HSS reports successful logins. – : enabled – : disabled
Block Non-whitelisted Attack IP Address	After this function is enabled, HSS blocks the login of brute force IP addresses (non-whitelisted IP addresses).
Report Alarm on Brute-force Attack from Whitelisted IP Address	• After this function is enabled, HSS generates alarms for brute force attacks from whitelisted IP addresses. – : enabled – : disabled
Whitelist	After an IP address is added to the whitelist, HSS does not block brute force attacks from the IP address in the whitelist. A maximum of 50 IP addresses or network segments can be added to the whitelist. Both IPv4 and IPv6 addresses are supported.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Malicious File Detection

Step 1 Click **Malicious File Detection**.

Step 2 On the displayed page, modify the policy. For more information, see **Table 10-10**.

Table 10-10 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.
Ignored Reverse Shell Local Port	Local ports that do not need to be scanned for reverse shells.
Ignored Reverse Shell Remote Address	Remote addresses that do not need to be scanned for reverse shells.

Parameter	Description
Detect Reverse Shells	
Auto-block Reverse Shells	Specifies whether to enable automatic blocking of reverse shells. You are advised to enable this function. • : enabled
Abnormal Shell Detection	• Whether to enable abnormal shell detection. It checks for actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You are advised to enable this function. – : enabled – : disabled

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Abnormal Process Behavior

Step 1 Click **Abnormal process behaviors**.

Step 2 In the displayed area, modify the settings as required. For more information, see **Table 10-11**.

Table 10-11 Parameter description

Parameter	Description	Example Value
Detection Mode	Select a mode for abnormal process behavior detection. • **Sensitive**: In-depth full scans are performed on all processes, which may cause false positives. Suitable for cyber protection drills and key event assurance drills. • **Balanced**: All processes are scanned. The scan result accuracy and the abnormal process detection rate are balanced. Suitable for routine protection. • **Conservative**: All processes are 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**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

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 10-12**.

Table 10-12 Parameter description

Parameter	Description
Ignored Process File Path	Ignored process file path Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Real-time Process

Step 1 Click **Real-time Process**.

Step 2 On the displayed page, modify the settings as required. For more information, see **Table 10-13**.

Table 10-13 Parameters for real-time process policy settings

Parameter	Description
High-Risk Commands	High-risk commands that contain keywords. The command can contain only letters, numbers, hyphens (-), spaces, and the following special characters: /* \=>.:'"+- Currently, built-in shell commands cannot be detected.
Whitelist (Do Not Record Logs)	Paths or programs that are allowed or ignored during detection. You can enter the regular expression of the command to be added to the whitelist. The command regular expression is optional. Example: • Full path or program name of a process: /usr/bin/sleep • Command regular expression: ^[A-Za-z0-9[:space:]* \\.\\\":_'\\(>=-]+$

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Rootkit Detection

Step 1 Click **Rootkit Detection**.

Step 2 On the rootkit detection page, modify the policy content.

Table 10-14 Parameter description

Parameter	Description	Example Value
Kernel Module Whitelist	Add the kernel modules that can be ignored during the detection. Up to 10 kernel modules can be added. Each module occupies a line.	xt_conntrack virtio_scsi tun

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

AV Detection

Step 1 Click **AV Detection**.

Step 2 On the **AV Detection** slide pane that is displayed, modify the settings as required. For details, see **Table 10-15**.

Table 10-15 Parameter description

Parameter	Description	Example Value
Real-Time Protection	After this function is enabled, AV detection is performed in real time when the current policy is executed. You are advised to enable this function. • : enabled • : disabled	: enabled
Protected File Type	Type of the files to be checked in real time. • **All**: Select all file types. • **Executable**: Executable file types such as EXE, DLL, and SYS. • **Compressed**: Compressed file types such as ZIP, RAR, and JAR. • **Text**: Text file types such as PHP, JSP, HTML, and Bash. • **OLE**: Composite file types such as Microsoft Office files (PPT and DOC) and saved email files (MSG). • **Other**: File types except the preceding types.	All
Action	Handling method for the object detection alarms. • **Automated handling**: Isolate high-risk virus files by default. Report other virus files but do not isolate them. • **Manual handling**: All the detected virus-infected files are reported but not automatically isolated.	Automatic handling

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Information Collection

Step 1 Click **Container Information Collection**.

Step 2 On the **Container Information Collection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 10-16**.

Table 10-16 Container information collection policy parameters

Parameter	Description	Example Value
Mount Path Whitelist	Enter the directory that can be mounted. The whitelist has a higher priority than blacklist. If a directory is specified in both the whitelist and blacklist, it is regarded as a whitelisted item.	/test/docker or /root/* Note: If a directory ends with an asterisk (*), it indicates all the sub-directories under the directory (excluding the main directory). For example, if **/var/test/*** is specified in the whitelist, all sub-directories in **/var/test/** are whitelisted, excluding the **test** directory.
Mount Path Blacklist	Enter the directories that cannot be mounted. For example, **user** and **bin**, the directories of key host information files, are not advised being mounted. Otherwise, important information may be exposed.	

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Cluster Intrusion Detection

Step 1 Click **Cluster Intrusion Detection**.

Step 2 On the **Cluster Intrusion Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 10-17**.

Table 10-17 Cluster intrusion detection policy parameters

Parameter	Description	Example Value
Basic Detection Cases	You can select check items as needed. The options are as follows: • **High-privilege RoleBinding**: Check for high-privilege role binding behaviors. **RoleBinding** binds an account to a role. Hackers can bind a common account to a high-privilege role to obtain permissions. • **High-privilege ClusterRoleBinding**: Check for high-privilege cluster role binding behaviors. **ClusterRoleBinding** binds an account to a cluster role. Hackers can bind a common account to a high-privilege role to obtain permissions. • **ServiceAccount creations**: Checks for the creation of service accounts. Service accounts are important Kubernetes credentials. Hackers can create service accounts and bind them to high-privilege roles to control clusters. • **List Secrets operations**: Check for List Secrets operations. Kubernetes Secret is an object that allows users to store and manage sensitive information (such as passwords and connection strings) in a cluster. List Secrets can be referenced in the pod configuration. Attackers who have the permission to retrieve secrets from the API server (for example, by using the service account of the pod) can access sensitive information, which may include the credentials of diverse services. • **DaemonSet creations**: Check for DaemonSet creations. Attacker may attempt to run their code in a cluster by creating a new container. DaemonSet is the best way to control all nodes in Kubernetes. • **Cronjob creation**: Check for Cronjob creations. Kubernetes jobs can be used to run containers that execute	Select all

Parameter	Description	Example Value
	batch processing tasks. These tasks are usually limited. • **Interactive shell used for exec in pods**: Check for the exec using an interactive shell in a pod. Hackers may use interactive shell programs such as bash and sh to perform operations in containers. • **Privileged pod creations**: Check for privileged pod creations. Creating a privileged container and escaping from it is one of the most common escape methods. • **Pods created with sensitive directory**: Check for the creation of pods containing sensitive directories. Hackers may mount sensitive directories, such as **/**, **/root**, and **/etc**, to servers to escalate permissions. • **Pods created with host network namespace**: Check for the creation of pods with a host network namespace. Hackers may create containers that use the host network to escape or listen to traffic. • **Pods created with host PID space**: Check for the creation of pods with a server PID space. Hackers may create containers with a server PID namespace to escape. • **Unauthorized access to API server**: Check for unauthorized access to the API server. Hackers may send API requests to probe the cluster and obtain information about containers, secrets, and other resources in the cluster. These probing behaviors usually trigger alarms for unauthorized access to the API server. • **Access to API Server with curl**: Check for the use of curl to access the API server. Generally, tools like kubectl are unlikely to exist in containers. Using curl to intrude pods and probe API servers is one of the most common attack methods.	

Parameter	Description	Example Value
	• **Exec in system management space**: Check for the **exec** command used for management components such as kube-apiserver. • **Ingress vulnerability**: Check for ingress vulnerabilities. Users who can create or update ingress objects can use custom fragments to obtain all the secrets in the cluster. • **Ingress-alias**: Check for ingress aliases. Users who have the permissions to create or update ingress objects can use the **spec.rules[].http.paths[].path** field in an ingress object (in the **networking.k8s.io** or **extensions** API group) to obtain the credential of the ingress-nginx controller. By default, the credential has access to all confidential information in the cluster. • **SelfSubjectRulesReview**: Check for the behaviors of querying SelfSubjectRulesReview. When a hacker enters a pod, the hacker needs to check the service account (SA) rights of the pod or the token rights stolen through the pod. • **Pods created in management space**: Check for the pod creations in the system management space. Generally, after a Kubernetes cluster becomes stable, the resources in the kube-system namespace will not be created or deleted randomly. Attackers usually forge management components to implement persistence operations. • **Static pod creations**: Check for static pod creations. Hackers may use static pods to achieve a certain purpose because static pods cannot be deleted through the API server. • **Man-in-the-middle attack**: Check for man-in-the-middle (MITM) attacks and medium-risk vulnerabilities (such as CVE-2020-8554).	

Parameter	Description	Example Value
	• **Worm, mining, or Trojan**: Check for the pods created using the images infected with worms, mining software, or Trojans. • **K8s event deletion**: Check for Kubernetes event deletions. Kubernetes events help to identify changes that have occurred in a cluster. Attackers may want to delete these events (for example, by using the **kubectl delete events --all** command) so that their activities in the cluster cannot be detected.	
Whitelist	You can customize the types and values that need to be ignored during the detection. You can add and delete types and values as required. The following types are supported: • IP address filter • Pod name filter • Image name filter • User filter • Pod tag filter • Namespace filter	Type: IP address filtering Value: 192.168.x.x

Step 3 Click **OK**.

- If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same edition.
- After this policy is configured, you need to enable log audit and deploy the HSS agent on the management node (node where the APIServer is located) of the cluster to apply the policy.

----End

Container Escape Detection

Step 1 Click **Container Escape**. The container escape policy details page is displayed.

Step 2 On the container escape page that is displayed, edit the policy content. For details about the parameters, see **Table 10-18**.

If no image, process, or POD needs to be added to the whitelist, leave the whitelist blank.

Table 10-18 Container escape detection policy parameters

Parameter	Description
Image Whitelist	Enter the names of the images that do not need to perform container escape behavior detection. An image name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 image names are allowed.
Process Whitelist	Enter the full paths of processes that do not need to perform container escape behavior detection. A process path can contain only letters, numbers, underscores (_), and hyphens (-), and each path needs to be on a separate line. Up to 100 process paths are allowed.
Pod Name Whitelist	Enter the names of pods that do not need to perform container escape behavior detection. A pod name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 pod names are allowed.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Information Module

Step 1 Click **Container Information Collection**.

Step 2 Modify the policy content as prompted. For details about the parameters related to the policy, see **Table 10-19**.

Table 10-19 Container information module policy parameters

Parameter	Description
Custom Container Whitelist	Enter the container name that can be ignored during the detection. • Simple names of containers can be configured based on Docker. HSS automatically performs fuzzy match. Other containers perform exact match based on their names. • Each container name needs to be on a separate line. Up to 100 whitelist items are allowed.

Parameter	Description
Custom Image Organization Whitelist	Enter the organization name that can be ignored during the detection. Each organization name needs to be on a separate line. Up to 100 whitelist items are allowed.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container File Monitoring

If a monitored file path is under the mount path rather than the writable layer of the container on the server, changes on the file cannot trigger container file modification alarms. To protect such files, configure a **file protection policy**.

Step 1 Click **Container File Monitoring**.

Step 2 On the **Container File Monitoring** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 10-20**.

Table 10-20 Container file monitoring policy parameters

Parameter	Description	Example Value
Fuzzy Match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be checked	test_bj4
Image ID	ID of the target image to be checked	-
File	Name of the file in the target image to be checked	/tmp/testw.txt

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Process Whitelist

Step 1 Click **Container Process Whitelist**.

Step 2 On the **Container Process Whitelist** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 10-21**.

Table 10-21 Container process whitelist policy parameters

Parameter	Description	Example Value
Dynamic Whitelist	If it is enabled, HSS assumes that a container only runs the process commands configured in its startup parameters. When a container is started, HSS identifies its entrypoint configuration to determine its main process. If other processes are detected running in the container, an alarm will be triggered.	
Fuzzy Match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be checked	test_bj4
Image ID	ID of the target image to be checked	sha256:732aab547cfe56841c02fb83921db4b91f04a1e636cc2cad76e224897056f140
Process	Full path of the file in the target image to be checked	/tmp/testw

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Suspicious Image Behaviors

Step 1 Click **Suspicious Image Behaviors**.

Step 2 On the **Suspicious Image Behaviors** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 10-22**.

Table 10-22 Suspicious image behaviors policy parameters

Parameter	Description	Example Value
Rule Name	Name of a rule	-
Description	Brief description of a rule	-
Template	• Configure templates based on different rules. The supported rules are as follows: – Image whitelist – Image blacklist – Image tag whitelist – Image tag blacklist – Create container whitelist – Create container blacklist – Container mount proc whitelist – Container seccomp unconfined – Container privilege whitelist – Container capability whitelist • The parameters are described as follows: – **Exact match**: Enter the names of the images you want to check. Use semicolons (;) to separate multiple names. A maximum of 20 names can be entered. – **RegEx match**: Use regular expressions to match images. Use semicolons (;) to separate multiple expressions. A maximum of 20 expressions can be entered. – **Prefix match**: Enter the prefixes of the images you want to check. Multiple prefixes are separated by semicolons (;). A maximum of 20 prefixes can be entered. – **Tag Name**: Enter the tag and value of the images you want to check. A maximum of 20 tags can be added. – **Permission Type**: Specify permissions to be checked or ignored. For details about permissions, see **Table 10-23**.	-

Table 10-23 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).
IPC_OWNER	Bypass permission checks for operations on System V IPC objects.
LEASE	Establish leases on arbitrary files

Permissions Name	Description
LINUX_IMMUTABLE	Set the FS_APPEND_FL and FS_IMMUTABLE_FL i-node flags.
MAC_ADMIN	Allow MAC configuration or state changes.
MAC_OVERRIDE	Override Mandatory Access Control (MAC).
NET_ADMIN	Perform various network-related operations.
NET_BROADCAST	Make socket broadcasts, and listen to multicasts.
PERFMON	Allow privileged system performance and observability operations using perf_events, i915_perf and other kernel subsystems.
SYS_ADMIN	Perform a range of system administration operations.
SYS_BOOT	Use reboot and kexec_load. Reboot and load a new kernel for later execution.
SYS_MODULE	Load and unload kernel modules.
SYS_NICE	Raise process nice value (nice, set priority) and change the nice value for arbitrary processes.
SYS_PACCT	Enable or disable process accounting.
SYS_PTRACE	Trace arbitrary processes using ptrace.
SYS_RAWIO	Perform I/O port operations (ipl and ioperm).
SYS_RESOURCE	Override resource limits.
SYS_TIME	Set the system clock (settimeofday, stime, and adjtimex) and real-time (hardware) clock.
SYS_TTY_CONFIG	Use vhangup. Employ various privileged ioctl operations on virtual terminals.
SYSLOG	Perform privileged syslog operations.
WAKE_ALARM	Trigger something that will wake up the system.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Port Scan Detection

Step 1 Click **Port Scan Detection**.

Step 2 On the **Port Scan Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 10-24**.

Table 10-24 Port scan detection policy parameters

Parameter	Description	Example Value
Source IP Address Whitelist	Enter one or multiple IP addresses or IP address ranges. Use commas (,) to separate multiple values. Example: **192.168.0.1,192.168.0.2,192.168.10-192.168.100**	192.168.0.1
Ports to Scan	Details about the port number and protocol type to be detected	-

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Fileless Attack Detection

Step 1 Click **Fileless attack detection**.

Step 2 On the policy details page, view or modify the policy. The following table describes the parameters.

Table 10-25 Parameters of a fileless attack detection policy

Parameter	Description	Example Value
Process injection	• **Process Injection**: Enable or disable process injection detection. – : enabled – : disabled • **Trustlist Matching Specifications**: Configure how to match the user-defined path trustlist. Click to select a match mode. The options are as follows: – Full match, case sensitive – Full match, case-insensitive – Fuzzy matching • **Path trustlist**: Enter the paths that do not need to be checked for process injection. Enter one path on each line.	• • Fuzzy matching • /usr/sbin/hald
LD hijacking	• **LD hijacking**: Enable or disable LD hijacking detection. – : enabled – : disabled • **Full process detection**: Enable or disable LD hijacking threat detection for all processes. – : enabled – : disabled • **Trustlist Matching Specifications**: Configure how to match the user-defined path trustlist. Click to select a match mode. The options are as follows: – Full match, case sensitive – Full match, case-insensitive – Fuzzy matching • **Path trustlist**: Enter the paths that do not need to be checked for LD highjacking. Enter one path on each line.	• • • Fuzzy matching • /usr/sbin/hald

Parameter	Description	Example Value
Memory-based process	• **Memory-based process**: Enable or disable memory process detection. – : enabled – : disabled • **Full process detection**: Enable or disable memory-based process threat detection for all processes. – : enabled – : disabled • **Trustlist Matching Specifications**: Configure how to match the user-defined path trustlist. Click to select a match mode. The options are as follows: – Full match, case sensitive – Full match, case-insensitive – Fuzzy matching • **Path trustlist**: Enter the paths that do not need to be checked for memory-based processes. Enter one path on each line.	• • • Fuzzy matching • /usr/sbin/hald

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Self-protection

The self-protection policy protects HSS software, processes, and files from being damaged by malicious programs. You cannot customize the policy content.

10.1.3 Creating a Custom Policy Group

Scenario

For premium and container editions, you can copy a policy group and customize it as required to meet server security requirements in different application scenarios.

Creating a Custom Policy Group

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Security Operation** > **Policies**. On the displayed page, **Policy group parameters** describes the fields.

Table 10-26 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group The preset policy group names are as follows: • **tenant_linux_container_default_policy_group**: preset Linux policy of the container edition. You can copy this policy group and create a new one based on it. • **tenant_linux_enterprise_default_policy_group** is the default Linux policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. • **tenant_windows_enterprise_default_policy_group**: preset Windows policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. • **tenant_linux_premium_default_policy_group**: preset Linux policy of the premium edition. You can create a policy group by copying this default group and modify the copy. • **tenant_windows_premium_default_policy_group**: preset Windows policy of the premium edition. You can create a policy group by copying this default group and modify the copy.
ID	Unique ID of a policy group
Description	Detailed description of a policy group.
Supported Version	HSS edition supported by a policy group.
Supported OS	OS supported by a policy group.
Associated Servers	To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Select a premium or container edition policy group and click **Copy** in the **Operation** column of the policy group.

Step 7 In the dialog box displayed, enter a policy group name and description, and click **OK**.

- The name of a policy group must be unique, or the group will fail to be created.
- The policy group name and its description can contain only letters, numbers, underscores (_), hyphens (-), and spaces, and cannot start or end with a space.

Step 8 Click **OK**.

After a policy group is created, you can configure rules for each policy in the policy group. For details, see **Configuring Policies**.

----End

Follow-up Procedure

After creating a policy group and configuring policies, you can apply the new policy group to servers. For details, see **Deploying a Protection Policy**.

10.1.4 Deleting a Custom Policy Group

Scenario

Preset policy groups cannot be deleted. You can delete custom policy groups of premium and container editions.

Precautions

After a policy group is deleted, the **Policy Group** column of the servers that were associated with the group will be blank. You need to deploy a policy group for a server again by referring to **Deploying a Protection Policy**.

Deleting a Policy Group

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 5 Click **Delete** in the **Operation** column of the target policy.

You can also select multiple policies and click **Delete** in the upper left corner of the policy list to delete multiple policy groups in batches.

Step 6 Click **OK**.

----End

10.2 Handling History

You can check the handling history of vulnerabilities and alarms, including their handlers and handling time.

Viewing the Handling History

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Handling History**.

Step 5 Click a tab and view the corresponding historical handling records.

- Viewing the handling history of a specified enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project for **Enterprise Project** to view the handling history under the enterprise project.

- Viewing the handling history of a specified attribute

  In the search box above the list, select an attribute or enter a keyword to search for the handling records of a specified attribute.

----End

10.3 Container Audit

10.3.1 Container Audit Overview

What Is Container Audit?

Keep track of the operations and activities in your container clusters and gain insight into every phase of the container lifecycle, including creating, starting, stopping, and destroying containers; as well as the communication and transmission between containers. Find and handle security problems through audit and analysis in a timely manner, ensuring the security and stability of container clusters.

Audit Objects

- Cluster container: Kubernetes audit logs, Kubernetes events, container logs, and container commands
- Independent container: container logs and container commands
- SWR image repository: image repository logs

Scenario

If an abnormal operation or activity occurs in the container environment, you can analyze container audit logs to locate the occurrence time, track the event, and work out a solution.

Constraints

The cluster container or independent container is protected by the container edition.

Description

To enable container audit, the following conditions must be met:

1. The cluster container or independent container has been connected to HSS, and is protected by the container edition.

   For more information, see **Installing the Agent on Containers** and **Enabling Container Protection**.
2. Meet the prerequisites for certain audit objects, as shown in **Table 10-27**.

Table 10-27 Audit prerequisites

Object	Audit Object	Audit Prerequisite
Cloud CCE clusters	Kubernetes audit logs	On the CCE console, enable the collection of Kubernetes events, Kubernetes audit logs, and container logs.
	Kubernetes audit events	
	Container logs	
SWR private image repository	Image repository logs	You have used SWR and granted the operation permission (**CTSOperatePolicy**) for HSS. For details, see **Authorization**.

After container audit is enabled, operation and activity logs in the cluster are recorded on the HSS console. For details about how to view audit logs, see **Viewing Container Audit Logs**.

10.3.2 Viewing Container Audit Logs

Scenario

This section describes how to view container audit logs.

Viewing Container Audit Logs

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Security Operations** > **Container Audit**.

Step 5 Perform the following operations to view different types of audit logs:

- Viewing cluster container audit logs
  a. Click the **Cluster Containers** tab.
  b. Click the name of a cluster. On the audit details page, view container command records.
- Viewing container instances
  a. Click the **Container Instances** tab.
  b. Click the name of a container instance. On the audit details page, view container logs and container command records.
- Viewing image repository logs
  Click the **Image Repository Logs** tab to view the audit logs of image repositories.

----End

10.4 Security Report

10.4.1 Security Report Overview

HSS provides daily, weekly, and monthly security reports, and allows you to customize the report period. The reports show the statistics on the security trend, key events, and risks of protected servers.

Constraints

- Security reports are available in HSS professional, enterprise, premium, WTP, and container editions.
- A report will be retained for six months after generation.

Security Report Description

By default, weekly and monthly reports are preconfigured in HSS. After protection is enabled for your assets, reports are automatically generated by default. The report content and generation time are as follows:

- Report content:
  - Security overview: risk trend, risk distribution, top 5 unsafe servers, and top 5 brute-force attack sources
  - Risk management: vulnerability statistics, asset account change records, dangerous open ports, and weak passwords
  - Intrusion detection: unsafe accounts, remote login, malicious programs, web shells, account cracking, and key file changes
- Report generation time:

- A default weekly security report is generated between 06:00 and 12:00 every Monday. It contains the statistics of a week, from 00:00 on Monday to 24:00 on Sunday.
- A default monthly security report is generated between 06:00 and 12:00 every Monday. It contains the statistics generated from 00:00 on the first day to 24:00 on the last day of a month.

You can view security reports. For details, see **Checking a Security Report**.

If the default report does not meet your requirements, you can create a custom report or edit the default report. For details, see **Creating a Security Report** and **Editing a Report**.

10.4.2 Creating a Security Report

If the type and content of the existing report template cannot meet your requirements, you can customize a report.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Creating a Security Report

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 5 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 6 Edit basic information of a report. For more information, see **Table 10-28**.

Table 10-28 Parameter description

Parameter	Description	Example Value
Report Name	Default report name	ecs security report

Parameter	Description	Example Value
Report Type	Statistical period type of a report: • **Daily**: 00:00 to 24:00 every day • **Weekly Reports**: 00:00 on Monday to 24:00 on Sunday • **Monthly Reports**: 00:00 on the first day to 24:00 on the last day of each month • **Custom**: custom statistical period, which ranges from one day to three months • All types of reports will be sent to the recipients the day after it is generated.	Monthly Reports
Schedule Delivery	Time when a report is automatically sent	-
Send Report To	Security report recipients. • **Recipients specified in SMN topic**: If you use SMN topic settings, you can create a topic and specify recipients for HSS. • **No need to send to email**: The report is not sent to the specified email address.	Recipients specified in SMN topic
Report Logo	Logo used in the report. • **None**: The report does not use any logo. • **Default** logo: Cloud logo is used by default. • **Custom**: Upload a custom logo image. The image cannot exceed 20 KB. Only JPG, PNG, JPEG, and BMP are supported.	None

Step 7 After confirming that the information is correct, click **Next** in the lower right corner of the page to configure the report.

Step 8 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

10.4.3 Checking a Security Report

You can check **daily**, weekly, monthly, and **custom** reports. The reports show your server security trends and key security events and risks.

This section describes how to view the generated reports.

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 and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 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 10-29**.

Table 10-29 Parameter description

Parameter	Description
Report Name	Name of a sent report.
Statistical Period	Statistical period of a sent report.
Report Type	Statistical period type of a sent report. • Weekly Reports • Monthly Reports • Daily Reports • Custom Reports
Sent	Time when the report is sent.

Step 3 Click **Download** in the **Operation** column to check historical reports. You can also preview and download the reports.

----End

10.4.4 Managing Security Reports

You can modify, cancel, or unsubscribe to a report.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Editing a Report

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 5 Click **Edit** in the lower right corner of the target report.

Step 6 Edit basic information of a report. For more information, see **Table 10-30**.

Table 10-30 Parameter description

Parameter	Description	Example Value
Report Name	Default report name.	**default monthly security report**
Report Type	Name of the statistical period type of a report, which cannot be edited.	**Monthly Reports**
Schedule Delivery	Time when a report is automatically sent.	-
Send Report To	Security report recipients. • **Recipients specified in 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 7 Confirm the information and click **Next** in the lower right corner of the page to configure the report.

Step 8 Select or deselect the report items in the pane on the left. You can preview the report items on the right. After confirming the report items, click **Save**. The report is changed successfully.

----End

Enabling or Disabling Subscription

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 5 Click the switch in the upper right corner of a report to enable or disable the subscription.

- : The subscription is disabled and no reports will be generated.
- : The subscription is enabled and reports will be generated on time.

----End

Deleting a Report

Default security report templates **default monthly security report** and **default weekly security report** cannot be deleted.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 5 Click **Delete** in the lower right corner of the target report.

----End

10.5 Free Health Check

Servers that are not protected by HSS are scanned for free. A security report on their vulnerabilities, unsafe passwords, and asset risks will be generated.

- Free server health check

This function checks for the vulnerabilities, unsafe passwords, and asset risks on ECSs and generates reports.

To enjoy advanced features like vulnerability management, baseline inspection, application protection, web tamper protection, ransomware protection, intrusion detection, file integrity management, and virus scanning, you can enable the professional edition or higher.

- Free container health check

  This function checks for image vulnerabilities, cluster configurations, privileged container risks and ports, and software information in CCE clusters, and generates reports.

  To enjoy advanced features like asset management, image security scanning, container firewall, and container cluster protection, enable the container edition.

Free Health Check

- ECSs that are not protected by HSS are scanned for free at 05:00 in the early morning on the first day of each month. (The time is subject to the time zone of the server.)
- In a free server check report, up to five results can be displayed for each check item. If a check item has fewer than five results, only half of them will be displayed.
- A free health check report is generated on the first day of each month. You can only view the report online but cannot download it.

Viewing the Free Health Checks of Servers

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

Step 5 Click the **Free Health Check** tab and click **Free Server Health Check** to view the health check results of the servers that are not protected by HSS.

Step 6 In the **Operation** column of a server, click **View Report** to view the health check report online.

----End

Viewing the Free Health Check Results of Containers

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

Step 5 Click the **Free Health Check** tab and click **Free Container Health Check** to view the health check results of the container clusters that are not protected by HSS.

Step 6 In the **Operation** column of a cluster, click **View Report** to view the health check report online.

----End

11 Installation and Configuration

11.1 Installation and Configuration on Servers

11.1.1 Agent Management

11.1.1.1 Agent Overview

What Is an Agent?

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

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

Supported OSs

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

Processes When the Agent Is Running

- **Linux**

  The account of the agent is **root**. **Table 11-1** lists the running processes on a Linux server.

Table 11-1 Agent running process on a Linux server

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

- **Windows**

  The account of the agent is **system**. Table 11-2 lists the running processes on a Windows server.

  Table 11-2 Agent running process on a Windows server

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

11.1.1.2 Installing the Agent on a Server

Scenarios

The HSS agent is a piece of software installed on servers to exchange data between the servers and HSS, implementing security detection and protection. You can use the HSS only after installing the agent.

Step 1: Prepare the Installation Environment

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

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

Step 2 Ensure the server is running properly.

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

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

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

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

Step 4 Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 CIDR block. (This is the default setting.)

This port is used to communicate with the HSS server. For details about how to view and modify an outbound security group rule, see .

Step 5 Uninstall third-party security software.

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

Step 6 (Optional) For a Linux server, disable the SELinux firewall.

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

----End

Step 2: Install the Agent on Servers

HSS can protect cloud servers and third-party servers. For details about how to install the agent on the servers, see:

- **Installing the Agent on Cloud Platform Servers**

Modifying a Security Group

To install the agent, ensure the security group of the server allows outbound access to port 10180 of the 100.125.0.0/16 CIDR block. This section describes how to view and modify ECS security group rules.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the management console and choose **Compute** > **Elastic Cloud Server**.

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

Step 5 On the ECS details page, click the **Security Groups** tab, click , and click the security group ID.

Step 6 Click the **Outbound Rules** tab and add a rule, as shown in **Security group rules**.

Table 11-3 Security group rules

Protocol	Port Range or ICMP Type	Type	Destination	Description
TCP	10180	IPv4	• IP Address • 100.125.0.0/16	Communicates with the HSS server.

----End

11.1.1.3 Upgrading the Agent

HSS keeps improving its service capabilities, including but not limited to new features and defect fixes. Please upgrade your agent to the latest version in a timely manner to enjoy better service.

About the Upgrade

- Agent upgrade is free of charge.
- The upgrade does not affect the workloads on your cloud servers.
- You are advised to perform the upgrade during off-peak hours.

Manually Upgrading the Agent

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. The **Agents** page is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click the **Servers with Agents** tab and filter the servers where the agent needs to be upgraded.

Step 7 In the **Operation** column of a server, click **Upgrade Agent**.

You can also select target servers in batches and click **Upgrade Agent** in the upper left corner of the server list to upgrade agents for the servers in batches.

Step 8 In the displayed dialog box, confirm the server whose agent is to be upgraded and click **OK** to start the automatic upgrade.

Step 9 After the upgrade completes, check the agent version. If the latest version agent is used, the upgrade is successful.

----End

Automatically Upgrading Agents

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. The agent management page is displayed.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 Click to enable automatic agent upgrade.

After this function is enabled, HSS checks the agent to be upgraded from 00:00 to 06:00 every day and automatically upgrades the agent to the latest version. The automatic upgrade can be performed only when the agent status is **Online**.

----End

11.1.1.4 Uninstalling the Agent

If you no longer need to use HSS, uninstall its agent from your servers. After the agent is uninstalled, HSS will not protect your servers or detect risks.

Uninstallation Methods

You can uninstall the agent in either of the following ways:

- One-click uninstallation: Uninstall the agent on the HSS console. For details, see **Uninstalling the Agent on the HSS Console**.
- Manual uninstallation: Uninstall the agent on the server. For details, see **Manually Uninstalling the Agent from a Server**.

You are advised to uninstall the agent in one-click mode, simple and efficient. If the agent is in **Offline** state and cannot be uninstalled on the HSS console, you can manually uninstall it.

Uninstalling the Agent on the HSS Console

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. Click the **Agents** tab.

Step 5 Click the **Servers with Agents** tab and filter the servers with online agents.

Step 6 Click **Uninstall Agent** in the **Operation** column of a server. In the dialog box that is displayed, confirm the uninstallation information and click **OK**.

If you need to uninstall the agent in batches, you can select servers and click **Uninstall Agent** above the list.

----End

Manually Uninstalling the Agent from a Server

- **Uninstalling the Linux agent**

  a. Log in to the server from which you want to uninstall the agent and run the following command to switch to user root:

  su - root

  b. In any directory, run the following command to uninstall the agent:

  Do not run the uninstallation command in the **/usr/local/hostguard/** directory. You can run the uninstallation command in any other directory.

  - For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **rpm -e hostguard** command.
  - For Ubuntu and Debian OSs, or other OSs that support DEB installation, run the **dpkg -P hostguard** command.

  If the information similar to the following is displayed, the agent has been uninstalled. No further action is required. Wait for about 15 minutes. The agent status of the server on the HSS console will change to **Uninstalled** or **Offline**. If the uninstallation fails, go to the **c**.

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

  c. (Optional) If the agent fails to be uninstalled in **b**, perform the following operations to uninstall the agent:

  - For OSs that support RPM installation, such as EulerOS, CentOS, and Red Hat:
    1) Run the following command to delete the installation record:

       rpm -e --justdb hostguard

    2) Run the following command to check whether there are hostguard processes:

       ps -ef | grep hostguard

       If there are residual processes, run the **kill -9 PID** command to stop all residual processes.

    3) Run the following command to check whether the **/usr/local/hostguard** directory exists:

       ll /usr/local/hostguard

       If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.

    4) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

       ll /etc/init.d/hostguard

If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

- For OSs that support DEB installation, such as Ubuntu and Debian:
  1) Run the following command to check whether there are hostguard processes:

     ps -ef | grep hostguard

     If there are residual processes, run the **kill -9 PID** command to stop all residual processes.
  2) Run the following command to check whether the **/usr/local/hostguard** directory exists:

     ll /usr/local/hostguard

     If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.
  3) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

     ll /etc/init.d/hostguard

     If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

- **Uninstalling the Windows agent**
  a. 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 **C:\Program Files\HostGuard** directory and double-click **unins000.exe** to uninstall the program.
     - If you have created a folder for storing the agent shortcut under the **Start** menu when installing the agent, you can also choose **Start** > **HostGuard** > **Uninstall HostGuard** to uninstall HostGuard.

  c. In the **Uninstall HostGuard** dialog box, click **Yes**.
  d. (Optional) Restart the server.

     - If you have enabled WTP, you need to restart the server after uninstalling the agent. In the **Uninstall HostGuard** dialog box, click **Yes** to restart the server.
     - If you have not enabled WTP, you do not need to restart the server. In the **Uninstall HostGuard** dialog box, click **No** to skip server restart.

11.1.2 Security Configurations

11.1.2.1 Configuring Common Login Locations

Scenarios

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.

Configuring Common Login Locations

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Installation & Configuration** > **Server Install & Config** and click the **Security Configuration** tab. Click **Common Login Locations** and click **Add Common Login Location**.

Step 5 In the dialog box that is displayed, select a geographical location and select servers. Confirm the information and click **OK**.

Step 6 Return to the **Common Login Locations** sub-tab and check the added common login locations. If they are displayed, the addition succeeded.

----End

11.1.2.2 Configuring Common Login IP Addresses

Scenarios

Common Login IP addresses are the IP addresses of the devices where normal users often log in to servers. After you configure common IP addresses, HSS will generate alarms on the logins from other IP addresses.

Configuring Common Login IP Addresses

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Installation & Configuration** > **Server Install & Config** and click the **Security Configuration** tab. Click **Common Login IP Addresses** and click **Add Common Login IP Address**.

Step 5 In the dialog box that is displayed, enter a common login IP address and select servers. Confirm the information and click **OK**. For more information, see **Table 11-4**.

Table 11-4 Parameters for adding a protected directory

Parameter	Description
Enter a common login IP address.	Enter an IP address or CIDR block. The requirements are as follows: ● You can add only one IP address or CIDR block at a time. To add multiple values, repeat the operation. Example: – IP address: **192.78.10.3** or **fe80::1** – CIDR block: **192.78.10.0/255.255.255.0**, **192.78.10.0/24**, or **fe80::1:0/112** ● You can add a maximum of 20 login IP addresses.
Select the servers configured with the common login IP address.	Select the servers where you wish to apply the common login IP addresses. You can select multiple servers at a time.

Step 6 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

11.1.2.3 Configuring an SSH Login IP Address Whitelist

Scenarios

The SSH login IP address whitelist helps to prevent brute-force attacks by restricting the IP addresses that can log in to servers via SSH. After an SSH login IP address whitelist is configured for a server, only the whitelisted IP addresses can log in to the server using SSH.

Constraints

- An account can have up to 10 SSH login IP addresses in the whitelist.
- If your server does not need to accept SSH logins, you do not need to configure the SSH login IP address whitelist.
- Ensure all the IP addresses that need to log in to the server through SSH are added 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.

Configuring an SSH Login IP Address Whitelist

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 Choose **Installation & Configuration** > **Server Install & Config** and click the **Security Configuration** tab. Click **SSH IP Whitelist** and click **Add IP Address**.

Step 5 In the dialog box that is displayed, enter a whitelisted login IP address and select servers. Confirm the information and click **OK**. For more information, see **Table 11-5**.

Table 11-5 Parameters for adding an SSH login IP address whitelist

Parameter	Description
Enter an IP address to be added to the whitelist.	Enter an IP address or CIDR block. The requirements are as follows: • You can add only one IP address or CIDR block at a time. To add multiple values, repeat the operation. Example: – IP address: **192.78.10.3** or **fe80::1** – CIDR block: **192.78.10.0/255.255.255.0**, **192.78.10.0/24**, or **fe80::1:0/112** • You can add up to 10 IP addresses to the whitelist.
Select the servers that the IP address or subnet will be whitelisted for.	Select the servers where you wish to apply the whitelisted SSH login IP addresses. You can select multiple servers at a time.

Step 6 Return to the **SSH IP Whitelist** sub-tab and check the added IP addresses. If they are displayed, the addition succeeded.

----End

11.1.2.4 Isolating and Killing Malicious Programs

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

NOTE

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

Isolating and Killing Malicious Programs

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 Choose **Installation & Configuration** > **Server Install and Config** and click the **Security Configuration** tab.Click the **Isolation and Killing of Malicious Programs** tab and enable **Isolate and Kill Malicious Programs**.

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 5 In the confirmation dialog box, click **OK** to enable the isolation and killing of malicious programs.

Automatic isolation and killing may cause false positives. To check isolated malicious programs, click **Isolated Files** on the **Detection & Response** > **Alarms** page on the HSS console. You can cancel the isolation or ignore misreported malicious programs. For details, see **Viewing Server Alarms**.

NOTE

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

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

----End

11.1.3 Enabling 2FA

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

Prerequisites

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

Constraints

- If 2FA is enabled, it can be used only in following scenarios:
  - Linux: The SSH password is used to log in to an ECS, and the OpenSSH version is earlier than 8.
  - Windows: The RDP file is used to log in to a Windows ECS.

- When two-factor authentication is enabled for Windows ECSs, the **User must change password at next logon** function is not allowed. To use this function, disable two-factor authentication.

Enabling 2FA

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Installation & Configuration** > **Server Install & Config** and click **Two-Factor Authentication**.

Step 5 Select servers and click **Enable 2FA** above the list, or select a server and click **Enable 2FA** in the **Operation** column.

Step 6 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 the mobile numbers and email addresses that do not need to receive verification messages.

Step 7 Click **OK**. After 2FA is enabled, it takes about 5 minutes for the configuration to take effect.

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

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

----End

11.2 Installation and Configuration on Containers

11.2.1 Cluster Management

11.2.1.1 Modifying Cluster Agent Installation Information

Scenario

You can modify the access information in the following cases:

- You need to modify the scope of cluster nodes where the agent is to be installed. After the modification, the agent on all cluster nodes will be automatically uninstalled, and then the agent will be reinstalled on specified nodes.
- The container runtime type and sock address need to be modified. After the modification, the agent on all cluster nodes will be automatically uninstalled, and then the agent will be reinstalled on specified nodes.
- Automatic agent upgrade needs to be enabled or disabled.

Modifying Access Information

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Cluster** tab.

Step 6 In the row of a cluster, click **Edit Access Information** in the **Operation** column. The **Edit Access Information** dialog box is displayed.

Step 7 Modify access information. For details about the parameters that can be modified, see **Table 11-6**.

Table 11-6 Modifiable access parameters

Parameter	Description
Configuration Rules	Select an agent configuration rule. • **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. • **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. **NOTE** • If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. • You are advised to select all runtime types.

Parameter	Description
(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ⌄ to expand all advanced configuration items. • **Enabling auto upgrade agent** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. • **Node Selector Configuration** Select the tag of the nodes where the agent is to be installed. If this parameter is not specified, the agent will be installed on all nodes having no taints by default. • **Tolerance Configuration** If the taint tag is selected in **Node Selector Configuration** and the agent needs to be installed on the taint node, you can configure taint toleration.

Step 8 Click **Complete**.

If the container runtime type, container runtime sock address, node selection configuration, or tolerance configuration is modified, the agent on all cluster nodes will be automatically uninstalled and then reinstalled. Wait until the agent installation is complete.

----End

11.2.1.2 Upgrading or Uninstalling the Agent from a Cluster

Scenarios

You can upgrade the agent or uninstall it from a cluster.

Prerequisites

The cluster is running.

Upgrading the Cluster Agent

HSS is periodically updated to improve its capabilities. You are advised to upgrade the agent to the latest version in a timely manner.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Cluster** tab.

Step 6 In the **Operation** column of a cluster, click **Upgrade Agent**.

To upgrade the agent on CCE clusters in batches, select all target CCE clusters and click **Upgrade Agent**.

Step 7 Confirm the upgrade information and click **OK**.

Wait for 5 to 10 minutes. If the agent version in the cluster list is the latest and the **Upgrade Agent** button is grayed out, the upgrade is successful.

----End

Uninstalling the Agent from a Cluster

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Cluster** tab.

Step 6 In the **Operation** column of a cluster, click **Uninstall Cluster**.

To uninstall CCE clusters in batches, select all target clusters and click **Uninstall Agent**. Clusters of other types cannot be uninstalled in batches.

Step 7 Confirm the uninstallation information and click **OK**.

Wait for 5 to 10 minutes. If the cluster is not displayed in the cluster list, the agent has been uninstalled.

----End

11.2.1.3 Viewing the Cluster Node List and Permission List

Scenarios

You can view the cluster node list and permission list.

Viewing the Cluster Node and Permission Lists

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Cluster** tab.

Step 6 Click **Synchronize Access Status** to refresh the cluster access status.

Step 7 Click **Synchronize the Latest Assets**.

Step 8 Check the cluster access status.

To export the cluster list, click **Export** above the list.

Step 9 Click the name of a cluster to go to the cluster node details page and view the node and permission lists.

- Node list

  The node list displays the information about all nodes and the agent status and version.

- Permission list

  The permission list displays the container-related functions and features provided by HSS, and whether the cluster has the permission to use the functions. CCE clusters have no permission lists.

----End

11.2.2 Independent Node Management

11.2.2.1 Installing the Agent on an Independent Node

Scenarios

The HSS agent is a piece of software installed on servers to exchange data between the servers and HSS, implementing security detection and protection. You can use the HSS only after installing the agent.

Prerequisites

There is at least one node with an online agent in the VPC of the nodes where the agent is to be installed. Otherwise, install the agent using the command line provided in **Installing the Agent on Servers**.

Step 1: Prepare the Installation Environment

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

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

Step 2 Ensure the server is running properly.

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

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

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

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

Step 4 Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 CIDR block. (This is the default setting.)

This port is used to communicate with the HSS server. For details about how to view and modify an outbound security group rule, see .

Step 5 Uninstall third-party security software.

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

Step 6 (Optional) For a Linux server, disable the SELinux firewall.

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

----End

Step 2: Install the Agent on an Independent Node

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Independent Nodes** tab.

Step 6 Locate the node where the agent is in the **Not installed** state. Click **Install Agent** in the **Operation** column.

Step 7 On the agent installation page, configure **Server Authentication Mode**.

- **Account and password**
  - If **Allow direct connection with root permissions** is selected:

    The **root** account can be used to log in to the server. Provide the **root** user password and login port. HSS will use your **root** account to install the agent for the server.
  - If **Allow direct connection with root permissions** is not selected:

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

  Only user-created keys are supported. Click **Upload Key** and upload a user-created key file in .pem format.

Step 8 Confirm the information and click **OK**.

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

----End

Follow-up Operations

After installing the agent on an independent node, **enable protection** for the node.

Modifying a Security Group

To install the agent, ensure the security group of the server allows outbound access to port 10180 of the 100.125.0.0/16 CIDR block. This section describes how to view and modify ECS security group rules.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the management console and choose **Compute** > **Elastic Cloud Server**.

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

Step 5 On the ECS details page, click the **Security Groups** tab, click , and click the security group ID.

Step 6 Click the **Outbound Rules** tab and add a rule, as shown in **Security group rules**.

Table 11-7 Security group rules

Protocol	Port Range or ICMP Type	Type	Destination	Description
TCP	10180	IPv4	• IP Address • 100.125.0.0/16	Communicates with the HSS server.

----End

11.2.2.2 Upgrading or Uninstalling the Agent from an Independent Node

Scenarios

You can upgrade the agent or uninstall it from an independent node.

Prerequisites

The agent of a node is online.

Upgrading the Agent on an Independent Node

HSS is periodically updated to improve its capabilities. You are advised to upgrade the agent to the latest version in a timely manner.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Non-cluster Node** tab.

Step 6 Upgrade the agent using either of the following methods:

- Automatic upgrade

  In the upper right corner of the node list, click to enable automatic upgrade. After this function is enabled, HSS automatically upgrades all agents to the latest version between 00:00 and 06:00 every day. You can view the agent version of a node after 06:00 the next day to check whether the upgrade is successful.

- Manual upgrade

  a. In the **Operation** column of a cluster, click **Upgrade Agent**.

  To upgrade the agent on CCE clusters in batches, select all target nodes and click **Upgrade Agent**.

  b. Confirm the upgrade information and click **OK**.

  Wait for 5 to 10 minutes. If the agent version of the target node is the latest, the upgrade is successful.

----End

Uninstalling the Agent from an Independent Node

Uninstall the HSS agent if you no longer need it. This section describes how to uninstall an online agent. If the agent status is offline, perform the operations in **Manually Uninstalling the Agent from a Server**.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Non-cluster Node** tab.

Step 6 In the **Operation** column of a node, click **Uninstall Agent**.

To uninstall the agent from nodes in batches, select all target nodes and click **Uninstall Agent**.

Step 7 Confirm the uninstallation information and click **OK**.

Wait for 5 to 10 minutes. If the agent status of the target node is **Not installed**, the uninstallation is successful.

----End

11.2.3 Connecting to a Third-party Image Repository

HSS can connect to third-party image repositories and provides security detection and management capabilities for vulnerabilities, baselines, and malicious files, helping you detect security risks in images in a timely manner. This section describes how to connect a third-party image repository to HSS.

Prerequisite

The repository cluster (cluster where the repository is deployed) has been connected to HSS and is in the **Running** state. For details, see **Installing the Agent on Containers**.

Connecting to a Third-party Image Repository

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 5 Click the **Third-Party Image Repository** tab.

Step 6 Click **Connect to Third-Party Image Repository**.

Step 7 Enter the required information as prompted. For details about the parameters, see **Table 11-8**.

Table 11-8 Parameters for accessing an image repository

Parameter	Description	Example Value
Jump Cluster	Select the cluster that carries the image repository.	cluster01

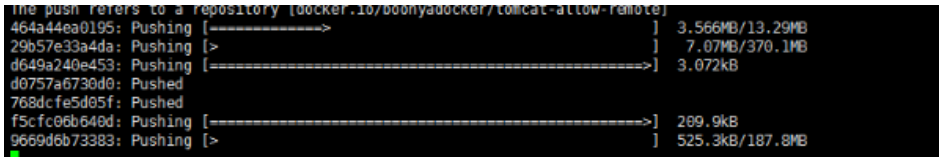
Parameter	Description	Example Value
Scan Component Source	The image scan component is used to pull images, scan and analyze required metadata, and transmit the metadata to the server. The server performs security detection on the metadata, such as vulnerabilities, baselines, malicious files, and sensitive information. The image scan component needs to be uploaded to the image repository. You can obtain the image scan component in either of the following ways: • **SWR**: The cluster can communicate with SWR and obtain image scan components from SWR. • **Manually uploaded**: If the network between the cluster and SWR is disconnected, you need to manually upload the image scan component to the image repository.	SWR
Image Repository Name	Enter the full name of an image repository.	test
Image Repository Type	Click ⌄ and select the type of the image repository.	Harbor
Image Repository API Version	Click ⌄ and select the interface version of the image repository.	V1
Image Repository Project	If you select **Manually uploaded** and the image repository type is **Harbor**, you need to enter image repository project information.	-
Communication Type	Select the communication protocol type of the image repository. • **HTTP** • **HTTPS**	HTTPS

Parameter	Description	Example Value
Image Repository Address	Enter the image repository address. You can enter the **website address** or *IP address*:*port number* of the image repository. Example: myharbor.com	myharbor.com
Username	Enter the login username.	-
Password	Enter the password of the login user.	-

Step 8 (Optional) If you select **Manually uploaded** for the scan component, perform the following operations to configure the scan components after entering the access information:

1. In the **Connect to Third-Party Image Repository** dialog box, click **Generate Command**.
2. In the **Connect to Third-party Image Repository** dialog box, click **Copy the image pull command**.
3. Log in to any Linux server that can access the Internet, paste and run the command copied in **Step 8.2** to download the scan component image.
4. Copy the downloaded scan component image to any node in the repository cluster.
5. In the **Connect to Third-party Image Repository** dialog box, click **Copy the following command**. Run the copied command on the cluster node where the scan component is located. The scan component will be uploaded to the image repository.
6. If the information shown in **Figure 11-1** is displayed, the scan component is uploaded successfully.

Figure 11-1 Scan component uploaded



Step 9 Click **OK** to connect to the image repository.

Step 10 On the **Third-party Image Repositories** tab page, view the access result in the **Image Repository Status** column of the target image repository.

----End

11.3 Alarm Configuration

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

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

Enabling Alarm Notifications

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Alarm Notifications**.

Step 5 (Optional) If your servers are managed by enterprise projects, you can select an enterprise project to configure alarm notifications.

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

Step 6 Configure the alarm notification parameters as prompted. For more information, see **Table 11-9**.

Table 11-9 Alarm configurations

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

Step 7 Select the alarm notification mode.

- **Use SMN topic settings**

  Select an available topic from the drop-down list or click **View Topics** and create a topic. Alarm notifications are sent to message topic recipients through SMS and email.

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

a. Create a topic.

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

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

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

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

Step 8 Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

----End

Alarm Notifications

- **Daily Alarm Notifications**

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

  Table 11-10 Daily alarm notification

Type	Item	Description
Assets	Dangerous ports	Check for high-risk open ports and unnecessary ports.
	Agent not installed	Check for servers with no HSS agent installed, and remind you to install the agent on these servers in a timely manner.
Vulnerabilities	Critical vulnerabilities	Detect critical vulnerabilities and fix them in a timely manner.
Baseline check	Unsafe Configurations	Detect unsafe settings of key applications that will probably be exploited by hackers to intrude servers.
	Common weak passwords	Detect weak passwords in MySQL, FTP, and system accounts.
Intrusions	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojans, mining software, worms, and viruses.
	rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.

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

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

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

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

- **Real-Time Alarm Notifications**

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

  Table 11-11 Real-time alarm notification

Type	Item	Description
Intrusions	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojans, mining software, worms, and viruses.
	rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.
	Ransomware	Check for ransomware in media such as web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.

Type	Item	Description
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. • Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. • You can use the manual detection function to detect web shells on servers.
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.
	File privilege escalations	Check the file privilege escalations in your system.
	Process privilege escalations	The following process privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities
	Important file changes	Receive alarms when critical system files are modified.
	File/ Directory changes	System files and directories are monitored. When a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.

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

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

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

11.4 Authorization

Scenario

Some HSS functions depend on other cloud service resources. To use these functions, you need to delegate HSS to perform operations on related cloud service resources, such as task scheduling and resource O&M.

Table 11-12 describes the cloud service resource permissions that HSS needs you to assign.

Table 11-12 Required permissions on other cloud service resources

Function	Required Permission	Cloud Service Permission		Usage
		Permission	Action	
Container audit (image repository audit)	CTSOperatePolicy	Query audit events	cts:trace:list	Obtain image operation logs (CTS logs of SWR).

Function	Required Permission	Cloud Service Permission		Usage
		Permission	Action	
Installation and configuration on servers	VPCOperatePolicy	Create a port	vpc:ports:create	Create network interface cards (NICs) and modify security groups to ensure that the port used for installing the agent is accessible.
		Delete a port	vpc:ports:delete	
		Create a security group rule	vpc:securityGroupRules:create	
		Delete a security group rule	vpc:securityGroupRules:delete	
		Query the port list or the details about a port	vpc:ports:get	
		Query the network list or the details about a network	vpc:networks:get	
		Query the subnet list or the details about a subnet	vpc:subnets:get	
	VPCEPOperatePolicy	Create an endpoint	vpcep:endpoints:create	Maintain the network channel between the agent and the HSS cloud protection center (master).
		Query the endpoint list	vpcep:endpoints:list	
		Delete an endpoint	vpcep:endpoints:delete	
Installation and configuration on containers	CCEOperatePolicy	Query cluster information	cce:cluster:get	Manage the lifecycle of HSS-Daemonset and Configmap in a CCE cluster.
		Query clusters in a project	cce:cluster:list	
		Query agencies based on specified conditions	iam:agencies:listAgencies	

Assigning Cloud Service Resource Permissions

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Permissions Management**.

Step 5 Click **Assign**. The **Assign** dialog box is displayed.

Step 6 Select permissions and click **OK**.

----End

Deleting Cloud Service Resource Permissions

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Permissions Management**.

Step 5 Locate a permission and click **Remove** in the **Operation** column. The **Remove Permissions** dialog box is displayed.

Alternatively, select multiple permissions and click **Remove** above the list.

Step 6 Confirm the permission information, enter **DELETE** in the dialog box, and click **OK**.

If the permission is no longer displayed in the permission list, it indicates the permission has been removed.

----End

11.5 Plug-in Settings

11.5.1 Plug-Ins Overview

If container protection is enabled and you want to use the image blocking function, you need to **install the Docker plug-in**.

The Docker plug-in provides the image blocking capability. It can prevent the startup of container images that have high-risk vulnerabilities or do not comply with security standards in the Docker environment.

You can configure image blocking in the following scenarios:

- To enhance the security of container images and prevent the risks caused by the use of untrusted or outdated images, you can configure an **image blocking policy** to specify the level of vulnerabilities to be blocked or the whitelist.
- If you need to comply with the security requirements of certain industries or regulations, such as PCI DSS and CIS, you can **configure an image blocking policy** to specify the security baseline or compliance check items to be blocked.
- If you need to implement the best practices of container DevSecOps and embed security check and defense into each phase of the container lifecycle, you can **configure an image blocking policy** to enhance security from source to devices.

Constraints

The constraints for installing the Docker plug-in are as follows:

- The HSS container edition has been enabled.
- Only Docker containers can use this plug-in.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.

11.5.2 Viewing Plug-in Information

The plug-in configuration page displays the server list and the plug-in information of the servers. If no plug-ins are installed on a server, the corresponding plug-in information is empty. You can view the plug-in information of a server to determine the servers where plug-ins need to be installed.

Viewing Plug-in Information

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Installation & Configuration** > **Plug-in Settings**.View plug-in details on the plug-in settings page. For more information, see **Table 11-13**.

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 11-13 Docker plug-in list parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Server IP address
OS	Type of the OS running on the server
Plug-in Name	Name of the plug-in installed on the server.
Plug-in Version	Name of the plug-in installed on the server.
Plug-in Status	Current status of the plug-in. • **Created**: The plug-in has been created but has not been started. • **Running**: The plug-in is running properly. • **Paused**: The plug-in is paused. • **Restarting**: The plug-in is being restarted. • **Removing**: The plug-in is being deleted. • **Exited**: The plug-in has been stopped. • **Dead**: The plug-in cannot be started or has been deleted.
Plug-in Upgrade Status	Plug-in upgrade status. • **Not upgraded**: The plug-in has not been upgraded to the latest version. • **Upgrading**: The plug-in is being upgraded. • **Upgraded**: The plug-in has been upgraded. • **Upgrade failed**: The plug-in failed to be upgraded.

----End

11.5.3 Installing a Plug-in

If container protection is enabled and you want to use the image blocking function, install the Docker plug-in by following the instructions provided in this section.

Installing a Plug-in

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Installation & Configuration** > **Plug-in Settings**.Click **Plug-In Installation Guide**. In the slide-out panel, copy the commands in the **Installation Commands** section.

Step 5 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 6 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 7 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 8 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 9 Copy the batch installation commands to the command terminal and press **Enter**.

If the installation package cannot be downloaded, check to ensure the DNS can resolve the domain name in the installation commands.

Step 10 If **remote_install finished. [OK]** is displayed, the installation is successful. Wait for 3 to 5 minutes and check the Docker plug-in status of the panel server.

```
remote_install finished. [OK]
```

----End

11.5.4 Uninstalling a Plug-in

Uninstall the Docker plug-in if you do not need to use the image blocking function.

Uninstalling a Docker Plug-in

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Installation & Configuration** > **Plug-in Settings**.Click **Plug-In Uninstallation Guide**. In the slide-out panel, copy the commands in the **Uninstallation Commands** section.

Step 5 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 6 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 7 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.

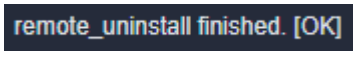
Example:

```
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 8 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 9 Copy the batch uninstallation commands to the command box and press **Enter**. The uninstallation starts automatically.

Step 10 If **remote_uninstall finished. [OK]** is displayed, the uninstallation is successful. Wait for 3 to 5 minutes and check the Docker plug-in status of the server.



----End

12 Monitoring and Auditing

12.1 Cloud Eye Monitoring

12.1.1 HSS Metrics

Feature Description

This section describes the HSS namespaces, function metrics, and dimensions reported to Cloud Eye. You can view HSS function metrics and alarms by using the Cloud Eye console or calling APIs.

Namespace

SYS.HSS

Metrics

Table 12-1 HSS monitoring metrics

ID	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
host_num	Total Servers	Total number of servers	≥0	Count	N/A	Enterprise Project	300s
unprotected_host_num	Unprotected Servers	Servers for which protection is not enabled	≥0	Count	N/A	Enterprise Project	300s

ID	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
risky_host_num	Unsafe Servers	Number of servers where risks are detected	≥0	Count	N/A	Enterprise Project	300s
uninstalled_or_offline_agent_num	Servers Without Agent Running	Number of servers where no agent is installed or the agent is offline	≥0	Count	N/A	Enterprise Project	300s

Dimensions

Table 12-2 Dimension list

key	Value
hss_enterprise_project_id	Enterprise project ID.

12.1.2 Monitored HSS Events

Feature Description

You can monitor the agent status using Cloud Eye. If the agent is offline unexpectedly or the agent protection status is abnormal, an alarm will be generated, notifying you of the HSS protection status in a timely manner.

After alarm notifications are enabled, you can view details about the reported alarms and events on the **Event Monitoring** page of the Cloud Eye console.

Namespace

SYS.HSS

Monitored Events

Table 12-3 Monitored HSS events

Event Name	Event ID	Severity	Description	Suggestion	Impact
HSS agent disconnected	hssAgentAbnormalOffline	Major	The communication between the agent and the server is abnormal, or the agent process on the server is abnormal.	Fix your network connection. If the agent is still offline for a long time after the network recovers, the agent process may be abnormal. In this case, log in to the server and restart the agent process.	Service interruption
Abnormal HSS agent status	hssAgentAbnormalProtection	Major	The agent is abnormal probably because it does not have sufficient resources.	Log in to the server and check your resources. If the usage of memory or other system resources is too high, increase their capacity first. If the resources are sufficient but the fault persists after the agent process is restarted, submit a service ticket to the O&M personnel.	Service interruption

12.1.3 Configuring a Monitoring Alarm Rule

You can configure HSS alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, threshold, monitoring period, and whether to send notifications. This helps you learn the HSS protection status in a timely manner.

You can use Cloud Eye to monitor HSS metrics and events. This section describes how to create alarm rules for monitoring metrics and events.

Creating an Alarm Rule for Metric Monitoring

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Management & Deployment** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rule**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Enter the alarm rule information as prompted. For more information, see **Table 12-4**.

Table 12-4 Parameters for creating an alarm rule for metric monitoring

Parameter	Description	Example Value
Name	Alarm rule name. The system generates a random name, and you can change it if needed.	alarm-hss
Description	Alarm rule description. This parameter is optional.	-
Alarm Type	Type of the alarm rule. The value can be **Metric** or **Event**.	Metric
Cloud Product	Select the cloud product you want to monitor. This parameter is available only when you set **Alarm Type** to **Metric**. In the drop-down list, select **Host Security Service - Host Security** or **Host Security Service - Server**. • **Host Security Service - Host Security**: The monitoring metrics of an enterprise project, including **Total Servers**, **Unprotected Servers**, **Unsafe Servers**, and **Servers Without Agent Running**. • **Host Security Service - Server**: The monitoring metrics of servers, including **Protection Status** and **Agent Status**.	Host Security Service - Host Security

Parameter	Description	Example Value
Resource Level	Resource level of the monitored object. The resource level of the alarm rule. This parameter is available only when you set **Alarm Type** to **Metric**. You can select **Cloud product** or **Specific dimension**. **Cloud product** is recommended.	Cloud product
Monitoring Scope	Monitoring scope the alarm rule applies to. • **All resources**: An alarm will be triggered if a resource of the current cloud product meets the alarm policy. To exclude resources that do not need to be monitored, click **Select Resources to Exclude**. • **Resource groups**: An alarm will be triggered if any resource in the resource group meets the alarm policy. To exclude resources that do not need to be monitored, click **Select Resources to Exclude**. • If you select **Specific resources**, click **Select Specific Resources** and select resources.	All resources
Method	Select **Associate template** or **Configure manually**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.	Configure manually
Alarm Policy	Set this parameter if **Method** is set to **Configure manually**.	-
Alarm Notifications	Set whether to send notifications when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.	Enabled
Notified By	Set the method and recipients of alarm notifications.	Notification policies

Step 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

Creating an Alarm Rule for Event Monitoring

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Management & Deployment** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rule**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Enter the alarm rule information as prompted. For more information, see **Table 12-5**.

Table 12-5 Parameters for creating an event rule for metric monitoring

Parameter	Description	Example Value
Name	Alarm rule name. The system generates a random name, and you can change it if needed.	alarm-hss
Description	Alarm rule description. This parameter is optional.	-
Alarm Type	Type of the alarm rule. The value can be **Metric** or **Event**.	Event
Event Type	Set this parameter if **Alarm Type** is set to **Event**. You can select **System event** or **Custom event**.	Host Security Service - Host Security
Event Source	Set this parameter if **Alarm Type** is set to **Event**. • If **Event Type** is set to **System event**, select the cloud service that generates the event from the drop-down list. • If **Event Type** is set to **Custom event**, the event source must be the same as the reported field and written in the *<Service>.<Item>* format.	System event
Method	Select **Associate template** or **Configure manually**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.	Configure manually
Alarm Policy	Set this parameter if **Method** is set to **Configure manually**.	-
Alarm Notifications	Set whether to send notifications when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.	Enabled

Parameter	Description	Example Value
Notified By	Set the method and recipients of alarm notifications.	Notification policies

Step 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

12.1.4 Viewing Monitoring Metrics

You can view the monitoring metrics of HSS on the management console to learn the HSS protection status in a timely manner.

Viewing Monitoring Metrics

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Mgmt & Deployment** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Host Security Service**.

Step 5 In the **Operation** column of an enterprise project ID, click **View Metric** to view the server protection metric details of the project.

----End

12.2 CTS Auditing

12.2.1 HSS Operations Supported by CTS

Cloud Trace Service (CTS) records all operations on HSS, including the requests initiated from the management console or open APIs and the responses to the requests. You can query the records for auditing and tracing.

Table 12-6 describes the HSS operations recorded by CTS.

Table 12-6 HSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Unignore a port	hss	notIgnorePortStatus
Ignore a port	hss	ignorePortStatus
Unignore configuration check items	hss	notIgnoreCheckRuleStat

Operation	Resource Type	Trace Name
Ignore configuration check items	hss	ignoreCheckRuleStat
Retry a baseline check	hss	runBaselineDetect
Unbind quota	hss	cancelHostsQuota
Disable container protection	hss	closeContainerProtect-Status
Enable container protection	hss	openContainerProtect-Status
Unblock an IP address	hss	changeBlockedIp
Handle an event	hss	changeEvent
Cancel the isolation of a file	hss	changeIsolatedFile
Remove an alarm from whitelist	hss	removeAlarmWhiteList
Add an item to the Login Whitelist	hss	addLoginWhiteList
Remove an item from the Login Whitelist	hss	removeLoginWhiteList
Add a server group	hss	addHostsGroup
Add servers to a group	hss	associateHostsGroup
Modify a server group	hss	changeHostsGroup
Delete a server group	hss	deleteHostsGroup
Disable HSS	hss	closeHostsProtectStatus
Enable HSS	hss	openHostsProtectStatus
Uninstall an agent	hss	uninstallAgents
Scan an image	hss	runImageScan
Synchronize the image list from SWR	hss	runImageSynchronize-Task
Update and scan an SWR image	hss	runSwrImageScan
Perform a security check again	hss	resetRiskScore
Add a policy group	hss	addPolicyGroup
Remove a policy group	hss	deletePolicyGroup
Apply a policy group	hss	deployPolicyGroup
Modify a policy	hss	modifyPolicyDetail
Modify a policy group	hss	modifyPolicyGroup

Operation	Resource Type	Trace Name
Disable automatic isolation and killing	hss	closeAutoKillVirusStatus
Enable automatic isolation and killing	hss	openAutoKillVirusStatus
Configure common login IP addresses	hss	modifyLoginCommonIp
Configure common login locations	hss	modifyLoginCommonLocation
Configure the SSH login whitelist	hss	modifyLoginWhiteIp
Fix a vulnerability	hss	changeVulStatus
Add a protected directory	hss	addHostProtectDirInfo
Add a privileged process	hss	addPrivilegedProcessInfo
Add a scheduled protection setting	hss	addTimingOffConfigInfo
Remove a remote backup server	hss	deleteBackupHostInfo
Remove a protected directory	hss	deleteHostProtectDirInfo
Remove a privileged process	hss	deletePrivilegedProcessInfo
Delete scheduled protection settings	hss	deleteTimingOffConfigInfo
Configure the scheduled protection period	hss	setDateOffConfigInfo
Modify the status of a protected directory	hss	setProtectDirSwitchInfo
Enable or disable dynamic WTP	hss	setRaspSwitch
Configure a remote backup server	hss	setRemoteBackupInfo
Enable or disable scheduled protection	hss	setTimingOffSwitchInfo
Disable WTP	hss	closeWtpProtectionStatus
Enable WTP	hss	openWtpProtectionStatus
Modify a remote backup server	hss	updateBackupHostInfo
Modify a protected directory	hss	updateHostProtectDirInfo

Operation	Resource Type	Trace Name
Modify a privileged process	hss	updatePrivilegedProcessInfo
Modify the Tomcat bin directory	hss	updateRaspPathInfo
Modify the scheduled protection period	hss	updateTimingOffConfigInfo

13 FAQs

13.1 About HSS

13.1.1 What Is 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.

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.

The functions and working processes of HSS components are described as follows:

Table 13-1 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	• 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	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10180 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. • If no agent is installed or the agent installed is abnormal, HSS is unavailable. • The agent can be installed on Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), on-premises IDC servers, and third-party cloud servers. • Web tamper protection, container security, and HSS share the same agent, so you only need to install the agent once on the same server.

13.1.2 What Is Container Security?

Container security refers to the protection provided by the HSS container edition.

The HSS container edition offers asset management, image security scan, cluster protection, runtime intrusion detection, and more capabilities. It provides lifecycle protection for containers and helps companies eliminate the container environment risks that cannot be detected by traditional security software, and enhancing container runtime security.

- During image deployment, HSS can scan the image repository for vulnerabilities, malicious files, and unsafe configurations, and can provide rectification guidance to help you enhance image security.
- During container running, HSS provides real-time monitoring and log management to detect and respond to abnormal activities in a timely manner. It also uses the intrusion detection system and automated response mechanism to cope with potential security threats. In addition, HSS provides the container firewall. You can customize network policies and isolation measures for containers to effectively prevent east-west network risks in clusters and ensure secure communication between containers.

13.1.3 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.

Table 13-2 WTP operation process and function description

Type	Operation	Description
Preparations	Purchase a quota	You can enable WTP only after you purchase a quota.
	Install the 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.
Enable WTP	Configure 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.
	Enable protection	Allocate a quota to a server and enable HSS for the server.
Configure WTP	Add 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.
	Add 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.
	Schedule WTP protection	You can schedule WTP protection to allow website updates in specific periods.
	Enable 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.

13.1.4 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.

13.1.5 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.

13.1.6 What Are the Differences Between HSS and WAF?

HSS and Web Application Firewall (WAF) are provided by 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 13-3 Differences Between HSS and WAF

Service Name	Category	Protected Object	Function
HSS (HSS)	Infrastructure security	Servers	• Asset management • Vulnerability management • Detection & Response • Baseline inspection • Web tamper protection

Service Name	Category	Protected Object	Function
WAF	Application security	Web applications	• Basic web protection • CC attack protection • Accurate access protection

13.1.7 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.
- 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 13-4 Agent running process on a Linux server

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

Windows Agent Processes

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

The agent contains the following processes:

Table 13-5 Agent running process on a Windows server

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

13.1.8 Can HSS Automatically Detect and Remove Viruses?

Yes.

HSS supports virus scan and removal. By using a signature engine, HSS can scan for virus-infected files, including executable files, compressed files, scripts, documents, images, and audiovisual files. You can perform full scan or custom scan tasks to identify and remove viruses on servers.

For details about how to use virus scan, see **Virus Scan**.

13.2 Agent

13.2.1 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 server is identified as an attack IP address and blocked by HSS. After the IP address is unblocked, it still cannot be used for login.
- Cause: HSS and DenyHosts both block possible attack IP addresses, but HSS can not unblock the IP addresses that were blocked by DenyHosts.
- Handling method: Stop DenyHosts.
- Procedure
  a. Log in to the server as the **root** user.
  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:

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

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

chkconfig --del denyhosts;

13.2.2 How Do I Uninstall the Agent?

If you no longer need to use HSS, uninstall its agent from your servers. After the agent is uninstalled, HSS will not protect your servers or detect risks.

Uninstallation Methods

You can uninstall the agent in either of the following ways:

- One-click uninstallation: Uninstall the agent on the HSS console. For details, see **Uninstalling the Agent on the HSS Console**.
- Manual uninstallation: Uninstall the agent on the server. For details, see **Manually Uninstalling the Agent from a Server**.

You are advised to uninstall the agent in one-click mode, simple and efficient. If the agent is in **Offline** state and cannot be uninstalled on the HSS console, you can manually uninstall it.

Prerequisites

When you uninstall the agent on the management console, the **Agent Status** of the server is **Online**.

Uninstalling the Agent on the HSS Console

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. Click the **Agents** tab.

Step 5 Click the **Servers with Agents** tab and filter the servers with online agents.

Step 6 Click **Uninstall Agent** in the **Operation** column of a server. In the dialog box that is displayed, confirm the uninstallation information and click **OK**.

If you need to uninstall the agent in batches, you can select servers and click **Uninstall Agent** above the list.

----End

Manually Uninstalling the Agent from a 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 and run the following command to switch to user root:

     su - root

  b. In any directory, run the following command to uninstall the agent:

     Do not run the uninstallation command in the **/usr/local/hostguard/** directory. You can run the uninstallation command in any other directory.

     - For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **rpm -e hostguard** command.
     - For Ubuntu and Debian OSs, or other OSs that support DEB installation, run the **dpkg -P hostguard** command.

     If the information similar to the following is displayed, the agent has been uninstalled. No further action is required. Wait for about 15 minutes. The agent status of the server on the HSS console will change to **Uninstalled** or **Offline**. If the uninstallation fails, go to the **c**.

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

  c. (Optional) If the agent fails to be uninstalled in **b**, perform the following operations to uninstall the agent:

     - For OSs that support RPM installation, such as EulerOS, CentOS, and Red Hat:

       1) Run the following command to delete the installation record:

          rpm -e --justdb hostguard

       2) Run the following command to check whether there are hostguard processes:

          ps -ef | grep hostguard

          If there are residual processes, run the **kill -9 PID** command to stop all residual processes.

       3) Run the following command to check whether the **/usr/local/hostguard** directory exists:

          ll /usr/local/hostguard

          If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.

       4) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

          ll /etc/init.d/hostguard

          If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

     - For OSs that support DEB installation, such as Ubuntu and Debian:

1) Run the following command to check whether there are hostguard processes:

   ps -ef | grep hostguard

   If there are residual processes, run the **kill -9 PID** command to stop all residual processes.

2) Run the following command to check whether the **/usr/local/hostguard** directory exists:

   ll /usr/local/hostguard

   If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.

3) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

   ll /etc/init.d/hostguard

   If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

- **Uninstalling the Windows agent**

  a. 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 **C:\Program Files\HostGuard** directory and double-click **unins000.exe** to uninstall the program.
  - If you have created a folder for storing the agent shortcut under the **Start** menu when installing the agent, you can also choose **Start** > **HostGuard** > **Uninstall HostGuard** to uninstall HostGuard.

  c. In the **Uninstall HostGuard** dialog box, click **Yes**.

  d. (Optional) Restart the server.

  - If you have enabled WTP, you need to restart the server after uninstalling the agent. In the **Uninstall HostGuard** dialog box, click **Yes** to restart the server.
  - If you have not enabled WTP, you do not need to restart the server. In the **Uninstall HostGuard** dialog box, click **No** to skip server restart.

13.2.3 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 there is an EIP bound to the server.

- If yes, go to the next step.
- If there is not, bind an EIP to the server and reinstall the agent.

Step 3 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 4 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 5 **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

13.2.4 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 server memory is insufficient.
- The agent process is abnormal.

Solution

Step 1 The agent has been installed on the server for more than 10 minutes, but the agent status on the console is **Offline** or **Not installed**.

- If yes, go to **2**.
- If no, wait until the agent goes online. No further action is required. After the agent is 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 **Step 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 can access the network.

- If no, restore its network connection, then check its agent status on the console.

Step 4 Check whether the disk capacity of the server destined for agent installation is greater than 300 MB.

On a Linux server, the agent is installed in the **/usr/local/hostguard/** directory by default. Check whether the remaining capacity of the disk partition where the directory is located is greater than 300 MB. On a Windows server, the agent is installed in the **C:\Program Files\HostGuard** directory by default. Check whether the remaining capacity of drive C is greater than 300 MB.

- If yes, go to **Step 5**.
- If no, the agent will go offline due to insufficient server memory. After the capacity expansion is complete, the agent will go online again.

Step 5 If the agent process is abnormal, perform the following operations to restart it:

- 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.
  a. For details about the uninstallation method, see **How Do I Uninstall the Agent?**

     After the uninstallation is complete, wait for 5 to 10 minutes, ensure that the server is displayed on the **Server Install & Config** > **Agents** > **Servers Without Agents** page of the HSS console, and then install the agent.
  b. For details about how to install an agent, see **Installing the Agent on Servers**.

----End

13.2.5 What Is the Default Agent Installation Path?

The agent installation paths on servers running the Linux or Windows OS cannot be customized. **Table 13-6** describes the default paths.

Table 13-6 Default agent installation paths

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

13.2.6 How Many CPU, Memory, and Disk Resources Are Occupied When the Agent Is Running?

HSS uses lightweight agents, which occupy only a few resources and do not affect your services or containers.

This section describes the CPU, memory, and disk resources occupied by the agent on the server and container nodes when the agent performs a scan task. The agent is scheduled to scan your servers and containers from 00:00 to 04:00 every day. It does not affect your server of container performance.

Maximum CPU Usage

While the agent runs on a server or container node, the general CPU usage does not exceed 20% of **a vCPU**. While the agent performs a virus scan, it works with the virus scan program, and their total CPU usage do not exceed 30% of multiple

vCPUs. The actual CPU usage depends on your server specifications. For details, see **Table 13-7**.

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.

Table 13-7 CPU usage of the agent for different vCPU specifications

vCPUs	Max. CPU Usage	Max. CPU Usage During Virus Scan
1vCPUs	20%	50%
2vCPUs	10%	40%
4vCPUs	5%	35%
8vCPUs	2.5%	32.5%
12vCPUs	About 1.67%	About 31.67%
16vCPUs	About 1.25%	About 31.25%
24vCPUs	About 0.84%	About 30.84%
32vCPUs	About 0.63%	About 30.63%
48vCPUs	About 0.42%	About 30.42%
60vCPUs	About 0.34%	About 30.34%
64vCPUs	About 0.32%	About 30.32%

Peak Memory Usage

While the agent runs on a server, the maximum memory usage is 500 MB. While the agent runs a virus scan task, it works with the virus scan program, and their total memory usage is 800 MB on average.

While the agent runs on a container node, its memory usage varies by the agent deployment mode.

- **Single-node installation**: If you install the agent on every node by referring to **Installing the Agent on Servers**, the agent generally occupies 500 MB memory at most. While the agent performs a virus scan task, it works with the virus program, and their total memory usage is 800 MB on average.
- **Cluster Installation**: If you connect the entire cluster to HSS by referring to **Installing the Agent on Containers**, the agent will run as a DaemonSet. Generally, the agent occupies 1,100 MB memory at most. While the agent runs a virus scan task, it works with the virus scan program, and their total memory usage is 1,400 MB on average.

If the agent memory usage exceeds the maximum memory limit, the agent will be automatically restarted within 5 minutes.

Peak Disk Usage

While the agent runs on a server or container node, its disk usage is as follows:

- Linux: The installation directory is under **/usr/local/hostguard** and occupies up to 600 MB. The log directory is under **/var/log/hostguard/** and occupies up to 250 MB.
- Windows: The installation directory and log directories are under in **C:\Program Files\HostGuard** and occupies up to 700 MB.

13.2.7 Do Different HSS Editions Share the Same Agent?

Yes.

All HSS editions can use the same agent installed on a server.

13.2.8 How Do I View Servers Where No Agents Have Been Installed?

To check the servers where the agent is not installed, perform the following steps:

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. The agent management page is displayed.

Step 5 Click the value of **Servers Without Agents** area to filter the servers that have not installed agents.

Possible agent statuses are:

- **Not installed**: The agent has not been installed or successfully started.
- **Installing**: The agent is being installed.

----End

13.2.9 What Can I Do If the Agent Status Is Still "Not installed" After Installation?

Precautions

On a server, you only need to install the agent once.

After the installation, you are advised to restart the servers before enabling HSS and binding quotas.

Possible Cause

Now both the HSS (New) and HSS (Old) consoles are in use. The agent and protection statuses of a server can be properly displayed on only one of the consoles.

For example, if you have installed the agent on server A on the old console and try installing it again on the new console, a message will be displayed indicating the installation has succeeded, but the installation status on the new console will still be **Not installed**.

Solution

Use only one console. Do not switch between the old and new consoles.

If you are using the old console and the agent status is **Not installed** on the new console, you can upgrade the agent to use HSS (New). The upgrade is free of charge and does not affect services. After the upgrade, the agent is installed on the new console, and the agent status is **Not installed** on the old console.

NOTE

HSS (New) added application protection capabilities, which are not available in the old version. You are advised to use the new version.

13.2.10 What Do I Do If the Upgrade Fails?

About the Upgrade

- Servers are displayed on both the old and new console of HSS, regardless of whether their agents have been upgraded. The server statuses are properly displayed on the console that you are using.
- Agent upgrade is free of charge.
- The upgrade does not affect the workloads on your cloud servers.
- After the upgrade, the billing stops on the old console and starts on the new console.
- After the upgrade, your servers will be protected by HSS (New).

Possible Causes

NOTE

After the automatic upgrade is complete, it takes 5 to 10 minutes for the agent status to be refreshed.

Possible causes for abnormal agent statuses are as follows:

1. Access to port 10180 is restricted. The agent upgrade requires accessed to port 10180.
2. The available memory of the server is insufficient. The agent upgrade occupies certain memory. If the available memory is less than 300 MB, the upgrade will be affected.

Locating and Fixing the Problem

- **Restricted Access to Port 10180**

  Ensure the server where the agent is to be installed or upgraded can communicate with the network segment. The security group of your server must allow outbound access to port 10180 on the 100.125.X.X/16 network segment.

  - Troubleshooting Procedure

    i. In the upper left corner of the page, select a region, click ☰, and choose **Compute** > **Elastic Cloud Server**.

    ii. Click the name of the server. On the server details page that is displayed, click the **Security Groups** tab.

    iii. Click the **Outbound Rules** tab and check whether port 10180 is specified in the deny policy.

    1) If it is not specified, the problem was not caused by port access restriction.

    2) If it is specified, the problem was caused by port access restriction.

  - Solution

    Allow access to the port.

- **The available memory is insufficient.**

  - Troubleshooting Procedure

    - Linux

      1) Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.

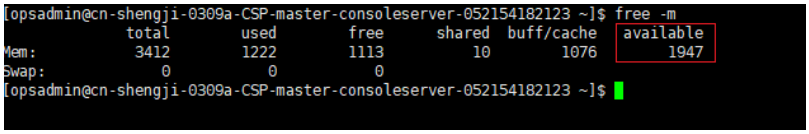
      2) Run the following command to check the memory usage of the server:

         free -m

      3) Check the value of **free** in the command output, as shown in Figure 13-1.

         If the value of **available** is smaller than 300, the memory is insufficient.

         Figure 13-1 Querying the memory

    - Windows

      1) Use a remote management tool, such as mstsc and RDP, to log in to the server.

      2) Open the Task Manager.

      3) Choose **Performance** > **Memory**, and view the available memory on the **Memory** page.

If the available memory is less than 300 MB, the memory is insufficient.

- Solution
  - Close the applications with high memory usage.

13.2.11 What If I Do Not Upgrade to the New Version?

The HSS (Old) can still work properly, until it is completely replaced by the HSS (New) version.

Why You Need to Upgrade to HSS (New)

- In the future, the HSS (New) version will replace the HSS (Old) version, which will be brought offline after the replacement.
- The HSS (New) version provides new features and enhances existing features, as described in the following table.

Table 13-8 Main changes in the HSS (New) version

Feature	Description	Type
Asset fingerprint management	HSS deeply scans assets on servers and classifies the assets into different types, such as accounts, ports, processes, web directories, and software information; and display statistics about these types.	New
Asset importance	You can configure asset importance for your servers and perform operations on them in batches, including but not limited to deploying policies, enabling or disabling protection, assigning groups, and installing agents.	New
Application vulnerabilities	HSS scans for vulnerabilities in web services, web frameworks, websites, middleware, and kernel modules.	New
Baseline report export	You can filter and export the check results of baseline configurations and common weak passwords.	New
Application protection	To protect running applications, you simply need to add probes to these applications, without having to modify application files. Detectable risks include but are not limited to SQL injections, command injections, deserialization input, file traversal, and JSP execution of OS commands.	New
Agent installation	You can install agents in batches in a few clicks.	New

Feature	Description	Type
Baseline check	You can select baseline check items to assess whether your system meets compliance requirements.	New
Alarm management	Ransomware and reverse shells can be isolated and killed. Alarms can be generated for the exploits of common vulnerabilities and Redis, Hadoop, and MySQL vulnerabilities.	New
Security report	You can customize the report period, content, and sending time.	Upgrade
Ransomware detection	HSS monitors new files and running processes in real time, dynamically generates honeypot files to lure and remove ransomware, and periodically backs up servers based on user-defined policies.	Upgrade
Container protection	The original container security function has been integrated into the HSS (New) version to manage server workloads in a unified manner.	Integration

13.2.12 What Do I Do If I Cannot Access the Download Link of the Windows Or Linux Agent?

Possible Causes

The link for downloading the agent is a Cloud private address. Before downloading the agent, you need to configure a Cloud private DNS address for your server. Otherwise, the server cannot access the link.

Solution

Contact the delivery or O&M personnel to configure the correct private DNS server address. After the configuration is complete, access the agent download link of the corresponding system version and download the agent.

13.2.13 What Do I Do If Agent Upgrade Fails and the Message "File replacement failed" Is Displayed?

Symptom

On the HSS console, choose **Installation & Configuration** > **Server Install & Config** and click the **Agents** tab. After the agent is upgraded, the agent upgrade status is **Upgrade failed**. When you hover your cursor over the status, the message "File replacement failed" is displayed.

Solution

HSS agent 3.2.4 or earlier cannot be directly upgraded to the latest version. You need to manually uninstall the old agent and install the latest HSS agent. For details, see:

1. **Uninstalling the Agent**
2. **Installing the Agent on Servers**

13.3 Vulnerability Management

13.3.1 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

13.3.2 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 "Handling Vulnerabilities".

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 yum 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 13-9 Verification commands

OS	Verification Command
CentOS/Fedora /Euler/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*

- **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.

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

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.

13.3.4 Do I Need to Restart a Server After Its Vulnerabilities Are Fixed?

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.

13.3.5 What Do I Do If Vulnerability Fix Failed?

If Linux or Windows vulnerabilities failed to be fixed on the HSS console, rectify the fault by following the instructions provided in this section.

Viewing the Cause of a Vulnerability Fixing Failure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 In the upper right corner of the **Vulnerabilities** page, click **Manage Task**.

Step 7 Click the **Fix Tasks** tab to view the vulnerability fixing results.

----End

Linux Vulnerability Fixing Failure Causes and Solutions

CAUTION

- The kernel vulnerabilities on CCE, MRS, and BMS servers cannot be fixed. Fixing them may make some functions unavailable.
- After the kernel vulnerability is fixed, you need to restart the server. If you do not restart the server, the vulnerability alarm still exists.
- The following failure causes only contain some key fields. For details, see the information displayed on the HSS console.

Failure Cause	Description	Solution
timeout	Repair timed out.	Wait for 1 hour and try fixing the vulnerability again.
This agent version does not support vulnerability verification	The agent version is too early.	Upgrade the agent and try fixing the vulnerability again.
Agent status is not normal	The agent status is abnormal.	The agent is offline and the vulnerability cannot be fixed. Recover the agent status by referring to **How Do I Fix an Abnormal Agent?** and fix the vulnerability.

Failure Cause	Description	Solution

Error: software has multiple versions	A software version with vulnerabilities is not deleted.	• If this problem occurs in common software, delete the packages of the earlier versions and check whether the problem persists.
		Run the following command to check whether an error is reported when an early version package is deleted:
		`rpm -e --test XXX`
		NOTE
		XXX indicates the full software component name, which contains the version number. You can run the **rpm -qa** command to query the full component name.
		– If an error is reported during the deletion, there are dependencies on the software package, and the package cannot be deleted. You are advised to ignore this vulnerability.
		– If no error is reported during the deletion, run the following command to delete the early version package:
		`rpm -e XXX`
		• If this problem occurs on kernel-related components such as Kernel and Glibc, deleting the early version package may cause OS problems. In this case, you are advised to ignore this vulnerability.

Failure Cause	Description	Solution
No package marked for update Error: software info not update Error: kernel is not update is already the newest version Dependencies resolved. Nothing to do. Complete!	The upgrade package of a later version is not found.	The failure cause indicates that the software has been upgraded to the latest version supported by the current image source, but the vulnerability still exists. **NOTE** • CentOS 8 has officially reached EOL and is no longer maintained. HSS checks them for vulnerabilities based on Red Hat patch notices, but cannot fix them due to the lack of official patches. You are advised to change to the OSs in active support. • Ubuntu 16.04, 18.04, and 22.04 do not support free patch updates. You need to purchase and configure Ubuntu Pro to install upgrade packages. • Debian 9 and 10 have officially reached EOL. No official patches are available. You are advised to change to the OSs in active support. • Possible cause 1: The image source is incorrectly configured. Update the image source and fix the vulnerability again. For more information, see "Image Source Management". • Possible cause 2: Kernel vulnerabilities cannot be fixed on the server. Fixing kernel vulnerabilities may make some functions unavailable. Do not fix kernel vulnerabilities. The kernel vulnerabilities on CCE, MRS, and BMS servers cannot be fixed. Fixing them may make some functions unavailable. Do not upgrade kernel components.
Error: Failed to download metadata for repo One of the configured repositories failed Errors during downloading metadata for repository Error: Cannot retrieve repository metadata	Failed to connect to the yum source.	The server cannot connect to the image source. Check whether the server can properly connect to the external network.

Failure Cause	Description	Solution
Failed connect to		
E: Failed to fetch		
Error: kernel is not update	Kernel not updated.	• Possible cause 1: The server is not restarted after the vulnerability is fixed. Solution: Restart the server. After a kernel vulnerability is fixed, you need to restart the server for the fix to take effect. Otherwise, the system will still report the vulnerability in the next scan. • Possible cause 2: Kernel vulnerabilities cannot be fixed on the server. Fixing kernel vulnerabilities may make some functions unavailable. Do not fix kernel vulnerabilities.
Error: kernel info not update		
Please install a package which provides this module, or verify that the module is installed correctly	The yum command is unavailable.	Rectify the command unavailability issue based on the suggestions provided in the failure cause.
command not found		
Error downloading packages	The upgrade package fails to be downloaded.	Check whether the server can properly connect to the Internet. • If yes, the image source is incorrectly configured. Update the image source and fix the vulnerability again. For more information, see Configuring the Image Source. • If no, ensure that your server can connect to the Internet and fix the vulnerability again.
There are no enabled repositories	No available sources are configured.	This fault occurs because the image source is incorrectly configured. Update the image source and fix the vulnerability again. For more information, see Configuring the Image Source.
Error: Cannot find a valid baseurl for repo		
There are no enabled repos		

Failure Cause	Description	Solution
dpkg was interrupted	The dpkg command is unavailable.	Rectify the command unavailability issue based on the suggestions provided in the failure cause.
Error: grub.conf still use old version.	The OS does not have GRUB. As a result, the grub.conf file does not contain the latest kernel.	Check whether the grub2-pc-modules, grub2-tools-extra and grub2-pc software is installed on the server. If not, perform the following steps: 1. Run the following commands to install the preceding software on the server: **yum install grub2-pc-modules grub2-tools-extra grub2-pc -y** 2. Run the following command to check the current kernel version: **uname -r** 3. Check the versions of all kernels. **rpm -qa | grep kernel-[0-9]** 4. Run the following command to uninstall the kernels whose versions are later than the current kernel version. **yum remove** *[Complete software name with the version number]* 5. Fix the vulnerability again.

Windows Vulnerability Fixing Failure Causes and Solutions

CAUTION

- After a Windows patch is installed, you need to restart the server, or the following problems may occur:
  - The patch does not take effect.
  - When you install other system patches or software, the blue screen of death (BSOD) or startup failure may occur.
- The following failure causes only contain some key fields. For details, see the information displayed on the HSS console.

Failure Cause	Description	Solution
timeout	Repair timed out.	Wait for 1 hour and try fixing the vulnerability again.

Failure Cause	Description	Solution
Agent status is not normal	The agent status is abnormal.	The agent is offline and the vulnerability cannot be fixed. Recover the agent status by referring to **How Do I Fix an Abnormal Agent?** and fix the vulnerability.
This agent version does not support vulnerability verification	The agent version is too early.	Upgrade the agent and try fixing the vulnerability again.

Search patch failed: Search failed, errmsg(Unknown error 0x8024401C)	Failed to find the patch.	The fault occurs because the Windows Update component on the server is faulty. Perform the following operations to recover the Windows Update component and fix the vulnerability again:
		1. Open the command-line interface (CLI).
		2. Run the following commands one by one:
		`net stop wuauserv`
		`reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
		`net start wuauserv`

Failure Cause	Description	Solution

Search patch failed: Search failed, errmsg(Unknown error 0x8024402C)	Failed to find the patch.	The fault occurs because the Windows Update client cannot connect to the Windows Update server. Perform the following operations to recover the Windows Update component and fix the vulnerability again:
		1. Check whether the network connection of the server is normal.
		Ensure your server can connect to the Internet.
		2. Clear the Windows Update cache.
		a. Open **Control Panel**.
		b. Click **System and Security**. Under **Administrative Tools**, click **Services**.
		c. Right-click **Windows Update** and choose **Stop**.
		d. Open the **C:\Windows** folder. Delete the **SoftwareDistribution** file.
		e. Right-click the **Windows Update** service and choose **Start**.
		3. Run the following commands to reset the Windows Update component:
		`net stop wuauserv`
		`net stop cryptSvc`
		`net stop bits`
		`net stop msiserver`
		`ren C:\Windows\SoftwareDistribution SoftwareDistribution.old`
		`ren C:\Windows\System32\catroot2 catroot2.old`
		`net start wuauserv`
		`net start cryptSvc`
		`net start bits`
		`net start msiserver`

Search patch failed: Search failed, errmsg(Unknown error 0x80070422)	Failed to find the patch.	The fault occurs because Windows Update is disabled on the server. Perform the following operations to start the service and fix the vulnerability again: 1. Open **Control Panel**. 2. Click **System and Security**. Under **Administrative Tools**, click **Services**. 3. Double-click the **Windows Update** service. 4. In the **Windows Update Properties** window, set **Startup type** to **Automatic**. 5. Click **OK**.

Failure Cause	Description	Solution
Search patch failed: Get updates count is 0	Failed to find the patch.	The fault occurs because the Windows Update of the server is faulty. Perform the following steps to locate the fault: 1. Check whether the network connection of the server is normal. • If yes, go to 2. • If no, fix the vulnerability again after the server network connection becomes normal. 2. Open Windows Update and check whether the patch to be installed is available. • If yes, install the patch and restart the server. • If no, check whether the failure cause contains an error code. If it contains an error code, search for the corresponding solution on the Microsoft official website based on the error code. If it does not contain any error code, reset Windows Update
Search patch failed: Search failed,errmsg	Failed to find the patch.	
Not install security patch	Failed to find the patch.	
Add patch to update collection failed: Update collection count is 0	Failed to find the patch.	
Not find patch	No patches found.	
Add patch to update collection failed	Failed to install the patch.	
Com init failed	Failed to call Windows Update.	

Failure Cause	Description	Solution
Download patch failed	Failed to download the patch.	• Possible cause 1: The Windows Update configuration is incorrect. This problem may occur only in Windows 2008 and 2012. Open **Control Panel**. Click **Windows Update** and click **Change settings**. Configure the following parameters: – **Important updates**: Select **Download updates but let me choose when to install them**. – **Recommended update**: Select this check box. – **Microsoft Update**: Deselect this check box. After the configuration is complete, open Windows Update and click **Check for Update**. After the patches to be installed are found, install them and restart the server. • Possible cause 2: The server has not been patched for a long time. As a result, Windows Update is abnormal. 1. Log in to the server and open Windows Update. 2. Click **Check for Update**. 3. After the patches to be installed are found, install them and restart the server. **NOTE** Some patches probably cannot be installed at a time. Check for updates after every patch installation until all patches are installed.
Some vulnerabilities have been fixed. You need to restart the server for the patch to take effect before fixing the remaining vulnerabilities.	The system is not updated to the latest version.	This vulnerability cannot be completely fixed at a time. Restart the server and try again until the vulnerability is fixed.

13.3.6 Why Can't I Select a Server During Manual Vulnerability Scanning or Batch Vulnerability Fixing?

Possible Causes

During manual vulnerability scanning or batch vulnerability fixing, the following servers cannot be selected:

- Servers are protected by basic edition HSS.
- Servers that are not in the **Running** state
- Servers whose agent status is **Offline**

Solution

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**. The server management page is displayed.

Step 5 On the **Servers** tab, view the server running status, agent status, and HSS version.

Confirm related information and perform the following operations to rectify the fault:

- Servers are protected by basic edition HSS.

  The HSS basic edition does not support manual vulnerability scan and batch vulnerability fixing. To use these features, upgrade the HSS edition.
- Servers that are not in the **Running** state

  Check the server and ensure the server status is **Running**.
- Servers whose agent status is **Offline**

  An offline agent cannot receive instructions delivered from the console. To put the agent back online, perform the operations described in **How Do I Fix an Abnormal Agent?**

Step 6 In the navigation pane, choose **Prediction** > **Vulnerabilities**. Select the servers you want to manually scan or fix in batches again. If the target server can be selected, the problem has been fixed.

----End

13.4 Detection & Response

13.4.1 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Check **Abnormal process behavior** events.

Choose **Detection & Response** > **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 5 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** > **Server 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 the 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**

Measure	Description	Procedure
Ensure default account security.	• Disable user **Guest**. • Disable and delete unnecessary accounts. (You are advised to disable inactive accounts for three months before deleting them.)	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.	Create users and user groups of specific types. Example: administrators, database users, audit users	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.	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.	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?**	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.	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.	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.	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.
Local shutdown	Assign the permission **Shut down the system** only to the **Administrators** group.	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.

Authorization	Description	Procedure
User rights assignment	Assign the permission **Take ownership of files or other objects** only to the **Administrators** group.	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.	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.	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.

13.4.2 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. If your process is isolated, you need to manually restore it.

Isolating and Killing a Malicious Program

- Choose **Installation & Configuration > Server Install & Config** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable this function.
- Choose **Detection & Response** > **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

1. Choose **Detection & Response** > **Alarms**. Click the value above **Isolated Files** to view the isolated files.
2. In the row containing the target server, click **Restore** in the **Operation** column. The dialog box is displayed.
3. Click **OK** to restore the isolated file.

   After you cancel isolation, the read/write permissions of files will be restored, but terminated processes will not be automatically started.

13.4.3 Why an Attack Is Not Detected by HSS?

- 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).

13.4.4 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.

Brute-force Attack IP Address

- If a brute force attack is detected, HSS blocks the attack source IP address for 12 hours by default. 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 & Response** > **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.

13.4.5 Why a Blocked IP Address Is Automatically Unblocked?

If a blocked IP address does not perform brute-force attacks in the next 12 hours, the IP address will be automatically unblocked.

13.4.6 How Often Is Malware Scan and Removal?

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.

NOTE

1. HSS can detect malicious programs (through cloud-based antivirus) and abnormal process behaviors in real time, report alarms, and isolate and kill them. For details about the detection capabilities, see Features.
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".

13.4.7 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.

13.4.8 How Do I Defend Against Ransomware Attacks?

Ransomware is developing rapidly. It can spread through Trojans, emails, files, vulnerabilities, software, and storage media. So far, no tools can eliminate ransomware attacks.

You are advised to properly use ransomware prevention tools (such as HSS) to enhance defense and mitigate damage caused by ransomware attacks.

For details, see **Ransomware Prevention Overview**.

13.4.9 How Do I Add High-risk Command Execution Alarms to the Whitelist?

If you run commands related to normal services on the server, HSS generates high-risk command execution alarms. You can add a whitelist to prevent the alarm.

To add a command alarm whitelist, perform the following steps:

1. Log in to the management console.
2. Click in the upper left corner and select a region or project.
3. In the upper left corner of the page, click and choose **Security** > **Host Security Service**.
4. In the navigation pane, choose **Security Operations** > **Policies**.
5. Locate the policy group of the protected edition corresponding to the server and click the policy group name.
6. Click **Real-time Process**.
7. Add a command whitelist. The parameters are as follows:

- Full path or program name of a process: Enter the full path or program name of the process, for example, **/usr/bin/sleep** or **sleep**.
- Regular expression in CLI: Enter the regular expression of the command to be added to the whitelist, for example, **^[A-Za-z0-9[:space:]*\\.\\ \":_'\\(>=-]+$**.

8. Click **OK** to save the change.

13.5 Abnormal Logins

13.5.1 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 13-10**.

Table 13-10 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. 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 the Login Whitelist.	Choose **Detection & Response** > **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 > Server Install & Config** 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.

13.5.2 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Detection & Response** > **Alarms**, and click **Server Alarms**.

Step 5 In the **Event Types** area, Choose **Abnormal User Behavior** > **Abnormal logins**, and click **Remote Login**.

----End

Locally Viewing Remote Login Records

- Linux

  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.

- Windows

  To view server login logs, perform the following steps:

  a. Open **Control Panel**.

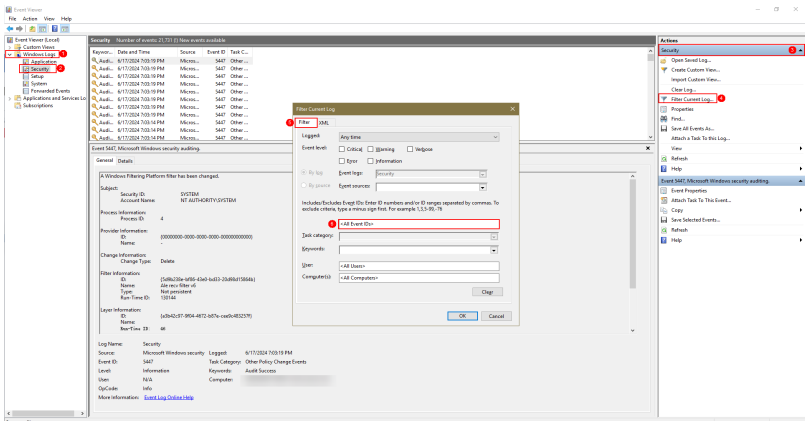
  b. Choose **Administrative Tools** > **Event Viewer**. The **Event Viewer** page is displayed.

  c. In the navigation tree on the left, choose **Windows Logs** > **Security**. The **Security** page is displayed.

  d. In the navigation tree on the right, choose **Security** > **Filter Current Log**. The **Filter Current Log** dialog box is displayed.

  e. On the **Filter** tab, locate the **<All Event IDs>**.

Figure 13-2 Filter



f. Enter the login event ID and click **OK** to filter the target login events.

- 4624: ID of successful login events
- 4625: ID of failed login events

13.5.3 How Do I Cancel the Alarm Notifications of Successful Server Logins?

- If you select **Successful Logins** in the **Real-Time Alarm Notifications** area, HSS will send alarms when detecting any successful logins.
- If all the accounts on your ECSs are managed by a single administrator, such alarms help them conveniently monitor system accounts.
- If the system accounts are managed by multiple administrators, or different servers are managed by different administrators, too many alarms will interrupt O&M personnel. In this case, you are advised to disable the alarm item.
- Alarms on this event do not necessarily indicate attacks. Logins from valid IP addresses are not attacks.

13.5.4 Can I Disable Remote Login Detection?

No.

If you do not want to receive remote login alarm notifications, add alarmed locations as common login locations, or deselect the remote login attempt item in alarm notification settings.

- On the **Common Login Locations** tab, click **Add Common Login Location**, and add common login locations. HSS does not trigger remote login alarms on logins from common login locations.
- Choose **Installation & Configuration** and click **Alarm Notifications**. In the **Masked Events** box, select **Abnormal logins**.

  Exercise caution when you deselect the **Abnormal Logins** notification item. Abnormal logins include remote logins and successful hacks. If you deselect this item, you will not receive alarms on brute-force attacks in real time.

13.5.5 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 & Response** page.
- To further determine the details, perform the following steps:
  - Linux

    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.
  - Windows

    To view server login logs, perform the following steps:

    i. Open **Control Panel**.

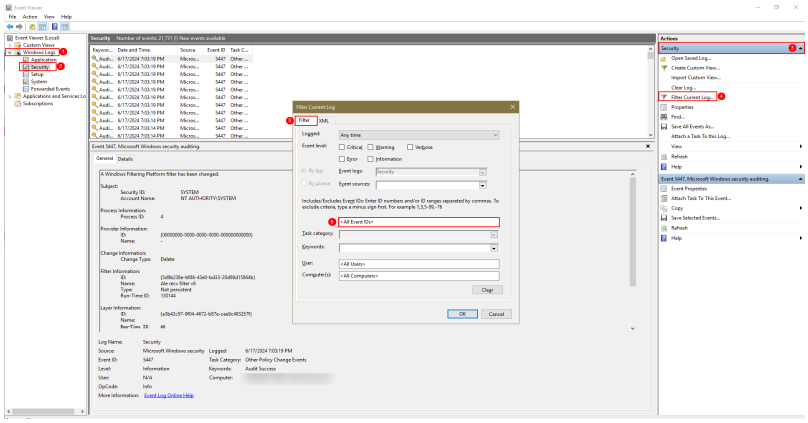
    ii. Choose **Administrative Tools** > **Event Viewer**. The **Event Viewer** page is displayed.

    iii. In the navigation tree on the left, choose **Windows Logs** > **Security**. The **Security** page is displayed.

    iv. In the navigation tree on the right, choose **Security** > **Filter Current Log**. The **Filter Current Log** dialog box is displayed.

    v. On the **Filter** tab, locate the **<All Event IDs>**.

    Figure 13-3 Filter

    vi. Enter the login event ID and click **OK** to filter the target login events.
    - 4624: ID of successful login events
    - 4625: ID of failed login events

13.6 Brute-force Attack Defense

13.6.1 How Does HSS Intercept Brute Force Attacks?

Types of Detectable Brute Force Attacks

HSS can detect the following types of brute force attacks:

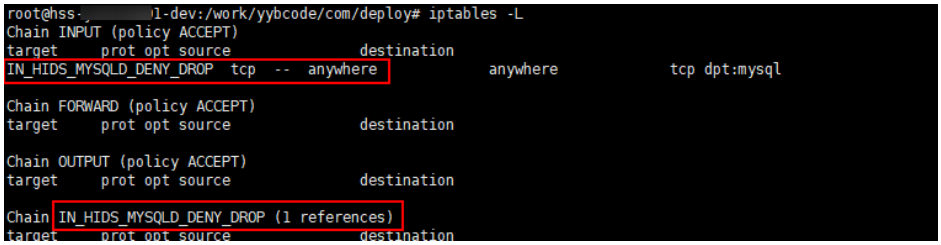
- Windows: SQL Server (automated blocking is not supported) and RDP
- Linux: MySQL, vfstpd, and SSH

If MySQL, vfstpd, or SSH is installed on your server, after HSS is enabled, the agent will add rules to iptables to prevent brute force attacks. If a brute-force attack is detected, its source IP address will be added to the blocking list.

- Added MySQL rule: IN_HIDS_MYSQLD_DENY_DROP
- Added vfstpd rule: IN_HIDS_VSFTPD_DENY_DROP
- Added SSH rule: If SSH on the server does not support the TCP Wrapper interception mode, the SSH uses iptables for interception. Therefore, the IN_HIDS_SSHD_DENY_DROP rule will be added to iptables. If you have configured an SSH login whitelist, the IN_HIDS_SSHD_DENY_DROP and IN_HIDS_SSHD_WHITE_LIST will be added to iptables.

Take the MySQL database as an example. **Figure 13-4** shows the new rule.

Figure 13-4 Added MySQL rule



NOTE

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, vfstpd, or SSH from brute-force attacks.

How Brute-force Attacks Are Blocked

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

HSS uses brute-force detection algorithms and an IP address blacklist to effectively prevent brute-force attacks and block attacking IP addresses. The blocking duration is 12 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

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 **Detection & Response** > **Alarms** page of the HSS console.

Viewing Brute-force Attack Detection Results

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Detection & Response** > **Alarms**.

Step 5 View the brute force cracking detection result of the server or container.

- View the brute force cracking detection result of the server.
  a. Click the **Server Alarms** tab.
  b. In the **Alarm Types** area, select **Abnormal User Behavior** > **Brute-force attacks** to view alarm event records on the protected server.
  c. Click the value in the **Blocked IP Addresses** area to view the blocked attack source IP address, attack type, blocking status, blocking times, blocking start time, and latest blocking time.
     - **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

       The default blocking duration is 12 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.
- View the brute force cracking detection result of a container.
  a. Click the **Container Alarms** tab.
  b. In the **Alarm Types** area, select **Abnormal User Behavior** > **Brute-force attacks** to view alarm event records on the protected container.

----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**.

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.

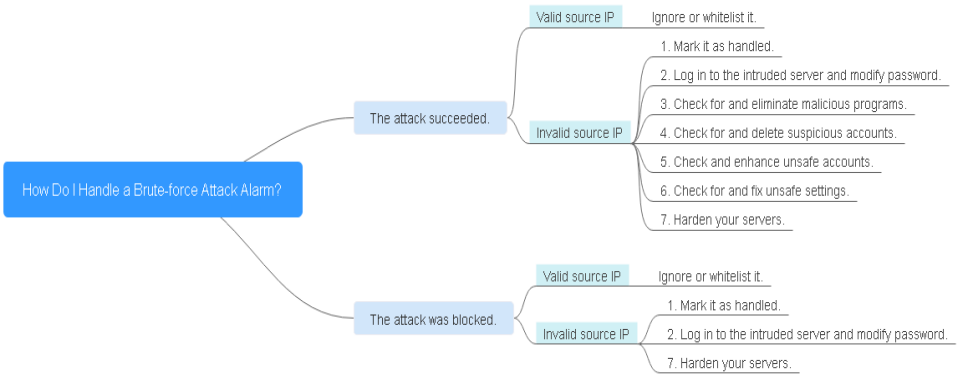
13.6.2 How Do I Handle a Brute-force Attack Alarm?

- 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 13-5 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Check whether the IP address that triggered the alarm is valid.

1. In the navigation pane, choose **Detection & Response** > **Alarms**.
2. In the **Alarm Types** area, select **Abnormal User Behavior** > **Abnormal logins** to view abnormal login alarm events.
3. Click the alarm event name. On the details page that is displayed, 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 5 Check for and eliminate malicious programs.

1. In the navigation pane, choose **Detection & Response** > **Alarms**.
2. In the **Alarm Types** area, select **Malware** > **Unclassified malware** to filter the unclassified malware.
3. In the **Alarm Type** column, select **Malicious program** and check alarm events.

   You can click an alarm name to view alarm event details.

   - 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 **Operation** column of an alarm and select **Isolate and kill**.
   - If you have confirmed that all the malicious program alarms are false, go to **Step 6**.

Step 6 Check for suspicious account change records.

1. In the navigation pane on the left, choose **Asset Management** > **Server Fingerprints**.
2. 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).

Step 7 **Check and handle invalid accounts.**

1. In the navigation pane, choose **Detection & Response** > **Alarms**.
2. In the **Alarm Types** area, select **Abnormal User Behavior** > **Invalid accounts**. View and handle the invalid account alarms.

Step 8 **Check for and fix unsafe settings.**

Check for and fix weak password complexity policies and unsafe software settings on your servers.

----End

Handling the Alarm of a Blocked Brute-force Attack

If you have enabled the HSS basic edition or higher, HSS will protect your servers against brute-force attacks.

In the basic edition and higher, you can configure a login security policy to specify the brute force cracking determination mode and blocking duration.

If you have not configured any login security check policies, the default policy is as follows: If five or more consecutive incorrect passwords are entered from the same IP address within 30 seconds, or the total number of incorrect passwords entered from the same IP address reaches 15 within 1 hour, HSS will generate an alarm for the latest user who entered an incorrect password from the IP address, and will

block the IP address (for 12 hours by default) to prevent server intrusions caused by brute-force attacks.

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

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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Detection & Response** > **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.

Step 5 Check whether the login IP address triggering the alarm is valid.

- If the source IP address is valid,
  - To handle a false alarm, click **Handle** in the row of the alarm event. Mark this event as **Ignore** or **Add to Login Whitelist**.

    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. The default blocking duration is 12 hours.
- If the source IP address is invalid or unknown,

  Click **Handle** in the **Operation** column of the brute-force attack event and select **Mark 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?

13.6.3 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.

- 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**.

- 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 13-11 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.

13.6.4 How Do I Unblock an IP Address?

If five or more consecutive incorrect passwords are entered from the same IP address within 30 seconds, or the total number of incorrect passwords entered from the same IP address reaches 15 within 1 hour, HSS will generate an alarm for the latest user who entered an incorrect password from the IP address, and will block the IP address (for 12 hours by default) to prevent server intrusions caused by brute-force attacks. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

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.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Step 5 In the **Alarm Statistics** area, click **View Details** under **Blocked IP Addresses**.

Step 6 In the blocked IP address list, select an IP address and click **Cancel Interception**.

Step 7 Wait for 1 to 2 minutes and check whether **Status** of the target attack source IP address is **Unblocked**. If yes, the blocking has been canceled.

----End

13.6.5 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.

- 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**.

- 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 13-12 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 RDP, SQL Server, MySQL, vsftpd, and SSH accounts.

By default, if five or more consecutive incorrect passwords are entered from the same IP address within 30 seconds, or the total number of incorrect passwords entered from the same IP address reaches 15 within 1 hour, HSS will generate an alarm for the latest user who entered an incorrect password from the IP address, and will block the IP address (for 12 hours by default) to prevent server intrusions caused by brute-force attacks.

If you have enabled an edition higher than HSS basic, you can configure a login security policy to specify the brute force cracking determination mode and blocking duration.

To view the IP addresses blocked by HSS, choose **Detection & Response** > **Alarms** and click the value above **Blocked IP Addresses**.

13.6.6 What Do I Do If the Port in Brute-force Attack Records Is Not Updated?

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 user **Administrator**. Open Task Manager, right-click **HostGuard** and choose **Restart** from the shortcut menu.
- Linux: Run the **service hostguard restart** command as the **root** user.

13.7 Baseline Inspection

13.7.1 Why Are Weak Password Alarms Generated After the Weak Password Detection 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.

13.7.2 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 on your servers. If PAM is not installed on a server, HSS will prompt you to install it on the **Password Complexity Policy Detection** tab of the **Prediction** > **Baseline Checks** page.

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 13-13**.

  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 13-13 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

Parameter	Description	Example
dcredit	Number of digits A negative value (for example, **-N**) indicates the number (for example, N) of digits required in a password. A positive value indicates that there is no limit.	dcredit=-1
ucredit	Number of uppercase letters A negative value (for example, **-N**) indicates the number (for example, N) of uppercase letters required in a password. A positive value indicates that there is no limit.	ucredit=-1
lcredit	Number of lowercase letters A negative value (for example, **-N**) indicates the number (for example, N) of lowercase letters required in a password. A positive value indicates that there is no limit.	lcredit=-1
ocredit	Number of special characters A negative value (for example, **-N**) indicates the number (for example, N) of special characters required in a password. A positive value indicates that there is no limit.	ocredit=-1

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

     vi /etc/pam.d/common-password
  b. Find the following information in the file:

     password requisite pam_cracklib.so retry=3 minlen=8 difok=3
  c. Add the following parameters and their values: **minlen**, **dcredit**, **ucredit**, **lcredit**, and **ocredit**. If the file already has these parameters, change their values. For details, see **Table 13-13**.

     Example:

     password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

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

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

Perform the following steps to set a local security policy:

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

NOTE

- Alternatively, click **Start** and type **secpol.msc** in the **Search programs and files** box.
- When a policy is applied to a server, the domain policy takes precedence over the locally defined policy on the server.

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 Press **Windows**+**R** to open the **Run** window.

Step 4 Enter **cmd** and click **OK**. The command prompt window is displayed.

Step 5 Run the following command to refresh policies:

gpupdate/force

After the refreshing, the settings will be applied.

----End

13.7.4 How Do I Handle Unsafe Settings?

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. Log in to the management console.

  b. Click in the upper left corner and select a region or project.

  c. In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

  d. In the navigation pane on the left, choose **Asset Management** > **Servers**. The server management page is displayed.

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

f. On the **Servers** tab, click the name of a server to view its details. Choose **Baseline Checks** > **Unsafe Configurations**.

g. Locate a baseline item, click ⌄ in front of its name to expand the check items, and click **Ignore** in the **Operation** column of an item. 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 a configuration item is fixed, you are advised to click **Verify** in the **Operation** column. After the verification, check the fix result.

13.7.5 How Do I View Configuration Check Reports?

You can view the configuration check details online.

Viewing the Configuration Check Report

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

Step 5 On the **Unsafe Configurations** tab, click a baseline name. The details page is displayed.

Step 6 In the row containing the target check item, click **View Details** in the **Operation** column to view the check item details and affected servers.

Step 7 You can rectify unsafe configuration items and ignore trusted configuration items based on the suggestions provided.

----End

13.7.6 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 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 Choose **Prediction** > **Baseline Checks** and click the **Prediction** tab.

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

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

13.7.7 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.

13.8 Web Tamper Protection

13.8.1 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.

13.8.2 How Do I Modify a Protected Directory?

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click ☰ and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

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

Step 6 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 7 In the **Edit Protected Directory** dialog box, modify the settings and click **OK**.

----End

13.8.3 What Should I Do If WTP Cannot Be Enabled?

The causes of this problem vary by scenarios.

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**.

Basic/Enterprise/Premium 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 basic, enterprise, premium, and WTP editions. Before enabling WTP for a server, ensure that basic, enterprise, or premium edition HSS has been disabled for the server.

Protection Was Enabled on the Wrong Page

To enable WTP, choose **Web Tamper Protection** > **Servers**.

13.8.4 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.

13.8.5 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.

13.8.6 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 13-14 Differences between the web tamper protection functions of HSS and WAF

Item	HSS	WAF
Static web page protection	• 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.	• 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	• 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 is 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

How Do I Select WTP?

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

13.9 Container Security

13.9.1 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.

Disabling the Container Edition

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Asset Management** > **Containers**. Click the **Container Nodes** tab.

Step 5 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 6 In the **Operation** column of a server, click **Disable Protection**.

To disable protection in batches, select multiple target servers and click **Disable Protection**.

Step 7 In the dialog box that is displayed, confirm the information and click **OK**.

Step 8 After the function is disabled, choose **Asset Management** > **Containers**. On the **Container Nodes** tab, if the **Protection Status** of the server is **Unprotected**, it indicates protection has been disabled.

----End

13.9.2 How Do I Enable Node Protection?

When you enable node protection, the system automatically installs the container security plug-in on the node.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Containers**. The container management page is displayed.

Step 5 In the **Operation** column of a node, click **Enable Protection**.

Step 6 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

13.9.3 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, save it to the YAML file, and name the file **audit-policy.yaml**.

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 **audit-policy.yaml** file to the **/etc/kubernetes/** directory.

Step 3 Go to the **/etc/kubernetes/manifests** 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.
- Add the preceding parameters to the **kube-apiserver.yaml** file, ensure that the format of the parameters is the same as that in the **kube-apiserver.yaml** file and cannot contain tab characters.

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
   ```

Step 5 Restart kube-apiserver to apply the configuration.

The method of restarting kube-apiserver varies depending on the environment.

If kube-apiserver is managed by systemd, run the following command to restart the service:

```
systemctl restart kube-apiserver.service
```

----End

13.9.4 What Do I Do If the Container Cluster Protection Plug-in Fails to Be Uninstalled?

Possible Causes

If the cluster network is abnormal or the plug-in is running, uninstalling the plug-in on the HSS console may fail.

Solution

On a cluster node where you can use **kubectl** to access the API Server, perform the following operations to uninstall the cluster protection plug-in:

Step 1 Log in to a cluster node where you can use **kubectl** to access the API Server.

Step 2 Create the file **plugin.yaml** in the **/tmp** directory and copy the following script content to the file:

```
apiVersion: v1
kind: Namespace
metadata:
  labels:
    admission.gatekeeper.sh/ignore: no-self-managing
    control-plane: controller-manager
    gatekeeper.sh/system: "yes"
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/audit-version: latest
    pod-security.kubernetes.io/enforce: restricted
    pod-security.kubernetes.io/enforce-version: v1.24
    pod-security.kubernetes.io/warn: restricted
    pod-security.kubernetes.io/warn-version: latest
  name: gatekeeper-system
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assign.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignimage.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
```

```
  name: assignmetadata.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: configs.config.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constraintpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplates.templates.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplate.expansion.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: modifyset.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
```

```
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: mutatorpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: providers.externaldata.gatekeeper.sh
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
  namespace: gatekeeper-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-mutating-webhook-configuration
---
```

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-validating-webhook-configuration
```

Step 3 Create the file **uninstall.sh** in the **/tmp** directory and copy the following script content to the file:

```
#!/bin/bash
kubectl delete -f /tmp/plugin.yaml
kubectl delete ns cgs-provider
```

Step 4 Run the following command to uninstall the container cluster protection plug-in:

```
bash /tmp/uninstall.sh
```

If information similar to the following is displayed, the plug-in has been uninstalled.

```
namespace "gatekeeper-system" deleted
resourcequota "gatekeeper-critical-pods" deleted
customresourcedefinition.apiextensions.k8s.io "assign.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignimage.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignmetadata.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "configs.config.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constraintpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplates.templates.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplate.expansion.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "modifyset.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "mutatorpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "providers.externaldata.gatekeeper.sh" deleted
serviceaccount "gatekeeper-admin" deleted
role.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
clusterrole.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
rolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
secret "gatekeeper-webhook-server-cert" deleted
service "gatekeeper-webhook-service" deleted
deployment.apps "gatekeeper-audit" deleted
deployment.apps "gatekeeper-controller-manager" deleted
poddisruptionbudget.policy "gatekeeper-controller-manager" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-mutating-webhook-configuration" deleted
validatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-validating-webhook-configuration" deleted
```

----End

13.10 Security Configurations

13.10.1 What Can I Do If I Cannot Remotely Log In to a Server via SSH?

Symptom

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 yes, perform the following steps:
  a. Log in to the console.
  b. In the navigation pane, choose **Detection & Response** > **Alarms**.
  c. Select the **Server Alarms** tab. Click the value in the **Blocked IP Addresses** area. The **Blocked IP Addresses** page is displayed.
  d. Select the target attack source IP address and click **Unblock** above the list to unblock the 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

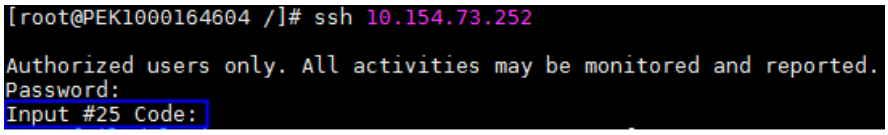
13.10.2 How Do I Use 2FA?

This FAQ shows you how to use 2FA.

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 13-6 Entering a verification 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.

13.10.3 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.

13.10.4 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

NOTE

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?**

13.10.5 How Do I Add a Mobile Number or Email Address for 2FA?

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.

13.10.6 Can I Disable HSS Alarm Notifications?

Yes.

If you do not enable alarm notifications, HSS cannot send alarm notifications to you in a timely manner. To view host security risks, you can only log in to the management console.

Setting Alarm Notifications

After you enable HSS, perform the following operations to configure alarm notifications:

1. Log in to the HSS console.
2. Choose **Installation & Configuration** > **Alarm Notifications**. Configure alarm notifications.

Disabling Alarm Notifications

If you do not want to receive HSS alarm notifications after HSS is enabled, you can disable the notification. After it is disabled, you have to log in to the management console to view alarms.

Use one of the following methods to disable the HSS alarm notification:

- Delete the SMN topic.

  After you delete the topic, your alarm notification settings will not take effect.
- Delete the subscription from the SMN topic.

  After you delete the subscription, you will no longer receive alarm notifications.
- Cancel or disable the subscription from the SMN topic.

  After you cancel the subscription, you will no longer receive alarm notifications.

13.10.7 How Do I Modify Alarm Notification Items?

If you do not want to receive certain HSS alarm notifications after HSS is enabled, you can disable the notification items. After it is disabled, you have to log in to the management console to view alarms.

Modifying Alarm Notification Items

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane, choose **Installation & Configuration**.

Step 5 Choose **Alarm Configuration**.

Step 6 Select the events whose alarm notifications are to be masked.

Step 7 Select a message topic.

Step 8 Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

To modify multiple notification topics, repeat steps **Step 6** to **Step 8**.

----End

13.10.8 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.

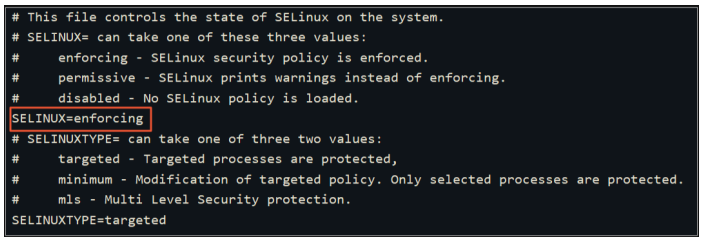
- **Permanently disable SELinux**

  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 13-7 Editing the SELinux status



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

13.11 Others

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

To use the Windows remote connection tool to connect to a Windows server, perform the following steps:

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

13.11.2 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/	• hostwatch.log • hostguard.log • upgrade.log • hostguard-service.log • config_tool.log • engine.log
Windows	C:\Program Files\HostGuard\log	• 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.	10 MB	Latest eight files	Until the HSS agent is uninstalled
hostguard.log	Records logs generated during the running of working processes.	10 MB	Latest eight files	
upgrade.log	Records logs generated during version upgrading.	10 MB	Latest eight files	
hostguard-service.log	Records logs (scripts) generated when the service starts.	100 KB	Latest two logs	
config_tool.log	Records logs (programs) generated when the service starts.	10 KB	Latest two logs	
engine.log	Records logs generated when the service exits.	10 KB	Latest two logs	

13.11.3 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

vsftp

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

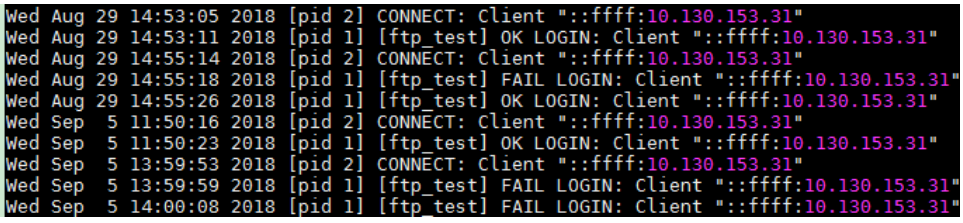
Step 1 Modify the configuration file (for example, **/etc/vsftpd.conf**) and set the following parameters:

vsftpd_log_file=log/file/path

dual_log_enable=YES

Step 2 Restart the vsftp service. If the setting is successful, log records shown in the logs shown in **Figure 13-8** will be returned when you log in to vsftp.

Figure 13-8 Log Records



----End

13.11.4 How Do I Enable or Disable the Agent Self-protection Policy?

Constraints

- Agent self-protection is supported only if the Linux agent version is 3.2.12 or later, or the Windows agent version is 4.0.18 or later.

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

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 5 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, select the default policy group **tenant_XXX_XXX_default_policy_group**.
- If you have created a policy group, select the policy group of your server. Perform the following operations:
  a. In the navigation pane on the left, choose .
  b. Click the **Servers** tab to view the policy groups of servers.

Step 6 In the row containing the target self-protection policy, click **Enable** or **Disable** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

----End

13.11.5 What Do I Do If HSS Self-Protection Cannot Be Disabled?

Root Causes

Generally, you can disable the self-protection function in the policy group. For details, see **How Do I Enable or Disable the Agent Self-protection Policy?**.

If the server network is disconnected, agents cannot receive the command for disabling self-protection delivered by the HSS console. As a result, self-protection in Windows cannot be disabled.

Solution

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 In the upper left corner of the page, click and choose **Security** > **Host Security Service**.

Step 4 In the navigation pane on the left, choose **Asset Management** > **Servers**.

Step 5 Click the **Servers** tab, click in the upper right corner of the server list and select **Agent ID**.

Step 6 Above the server list, enter a server name or ID, and press **Enter** to search for the Windows server for which you want to disable the HSS self-protection.

Step 7 In the row of the target Windows server, copy the first eight characters from the **Agent ID** column.

Step 8 Run **cmd** as the administrator.

Step 9 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 10 If **Disable self protect succeed.** is displayed, HSS self-protection is disabled successfully.

----End

A Change History

Released On	Description
2025-01-30	This issue is the first official release.