

Host Security Service

User Guide

Date 2022-12-31

Contents

1 Introduction	1
1.1 HSS	1
1.2 Functions and Features	2
1.3 Advantages	8
1.4 Editions	9
1.5 Scenarios	16
1.6 Constraints	16
1.7 HSS Permissions Management	18
1.8 Related Services	20
1.9 Concepts	21
2 Enabling HSS	23
2.1 Installing an Agent	23
2.1.1 Installing an Agent on a Linux Server	23
2.1.2 Installing an Agent on a Windows Server	
2.2 Configuring Alarm Notifications	28
2.2.1 Enabling Alarm Notification for the Basic/Enterprise/Premium Edition	
2.2.2 Enabling Alarm Notification for the WTP Edition	33
2.3 Enabling HSS	35
2.3.1 Enabling the Basic/Enterprise/Premium Edition	35
2.3.2 Enabling the WTP Edition	40
3 Viewing the Server List	
4 Dashboard	47
5 Security Configuration	52
6 Server Management	58
6.1 Creating a Server Group	
6.2 Applying a Policy	60
7 Risk Prevention	64
7.1 Asset Management	64
7.2 Vulnerability Management	66
7.2.1 Viewing Details of a Vulnerability	66
7.2.2 Fixing Vulnerabilities and Verifying the Result	70

7.3 Baseline Inspection	73
7.3.1 Checking for Unsafe Settings	
7.3.2 Suggestions on Fixing Unsafe Settings	75
8 Intrusion Detection	
8.1 Alarm Events	
8.2 Checking and Handling Intrusion Events	
8.3 Managing Isolated Files	
8.4 Configuring the Alarm Whitelist	95
8.5 Configuring the Login Whitelist	
9 Advanced Protection	
9.1 Application Recognition Service	
9.1.1 Checking the Whitelist Policy List	
9.1.2 Applying a Whitelist Policy	
9.1.3 Checking and Handling Application Events	
9.2 File Integrity Monitoring	
9.2.1 Adding a Monitored File	
9.2.2 Checking Change Statistics	
9.3 Ransomware Prevention	115
9.3.1 Checking Protection Policies	115
9.3.2 Creating a Protection Policy	119
9.3.3 Checking and Handling Protection Events	
10 Security Operations	
10.1 Checking or Creating a Policy Group	127
10.2 Modifying a Policy	
11 WTP	
11.1 Adding a Protected Directory or File System	
11.2 Adding a Remote Backup Server	
11.3 Adding a Privileged Process That Can Modify Protected Files	
11.4 Setting Scheduled WTP Protection	159
11.5 Enabling Dynamic WTP	
11.6 Viewing WTP Reports	
12 Audit	
12.1 HSS Operations Supported by CTS	
12.2 Viewing Audit Logs	
13 Permissions Management	
13.1 HSS Custom Policies	
13.2 Actions	170
14 FAQs	175
14.1 About HSS	175
14.1.1 What Is Host Security Service?	175

14.1.2 Can HSS Ouota Be Shared Between Accounts?	
14.1.3 What Is the HSS Agent?	178
14.1.4 Can HSS Automatically Detect and Remove Viruses?	179
14.1.5 Can I Add an IP Blacklist in HSS?	
14.1.6 How Often Are the HSS Virus Database and Vulnerability Database Updated?	180
14.1.7 How Does HSS Transfer Data?	
14.2 Deployment and Configuration	180
14.2.1 Alarm Notifications	180
14.2.1.1 Why No Topics Are Available for Me to Choose When I Configure Alarm Notifications?	180
14.2.1.2 Can I Disable HSS Alarm Notifications?	181
14.3 Alarm and Event Management	182
14.3.1 Brute-force Attack Defense	182
14.3.1.1 How Does HSS Block Brute-Force Attacks?	182
14.3.1.2 How Do I Handle a Brute-force Attack Alarm?	184
14.3.1.3 How Do I Defend Against Brute-force Attacks?	188
14.3.1.4 What Do I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Accounts for Linux Servers?	189
14.3.1.5 How Do I Unblock an IP Address?	190
14.3.1.6 What Do I Do If HSS Frequently Reports Brute-force Alarms?	190
14.3.2 Weak Passwords and Unsafe Accounts	191
14.3.2.1 How Do I Handle a Weak Password Alarm?	191
14.3.2.2 How Do I Set a Secure Password?	193
14.3.2.3 Why Are the Weak Password Alarms Still Reported After the Weak Password Policy Is Disa	bled?
14.3.3 Intrusions	194
14.3.3.1 Why a Process Is Still Isolated After It Was Whitelisted?	
14.3.3.2 What Should I Do If a Mining Process Is Detected on a Server?	195
14.3.3.3 What Should I Do If I Find My Servers Attacking Others?	195
14.3.3.4 Can I Unblock an IP Address Blocked by HSS, and How?	
14.3.3.5 Why a Blocked IP Address Is Automatically Unblocked?	196
14.3.3.6 How Do I Defend Against Ransomware Attacks?	
14.3.4 Abnormal Logins	196
14.3.4.1 What Can I Do If an Alarm Indicating Successful Login Is Reported?	
14.3.4.2 How Do I Know Whether an Intrusion Succeeded?	196
14.3.5 Unsafe Settings	197
14.3.5.1 How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?	197
14.3.5.2 How Do I Set a Proper Password Complexity Policy in a Windows OS?	199
14.4 Vulnerability Management	201
14.4.1 How Do I Fix Vulnerabilities?	201
14.4.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?	201
14.4.3 Why a Server Displayed in Vulnerability Information Does Not Exist?	203
14.4.4 Do I Need to Restart a Server After Fixing its Vulnerabilities?	204
14.4.5 Can I Restore the Server Data That Was Cleared During Vulnerability Fixing?	204

14 E Mich Teneren Duchastien	204
14.5 Web Tamper Protection	
14.5.1 Why Do I Need to Add a Protected Directory?	
14.5.2 How Do I Modify a Protected Directory?	
14.5.3 How Do I Modify a File After WTP Is Enabled?	
14.5.4 What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect?	
14.6 Others	206
14.6.1 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Server?	206
14.6.2 How Do I Check HSS Log Files?	208
14.6.3 How Do I Enable Logging for Login Failures?	209
14.6.4 How Do I Scan My Servers?	211
14.6.5 Why Does Manual Detection Fail?	215
14.6.6 Can HSS Alarm Logs Be Stored in OBS?	215
A Change History	216

Introduction

1.1 HSS

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

Working Principles

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

Figure 1-1 illustrates how HSS works.



Figure 1-1 Working principles

The following table describes HSS components.

Table 1-1 Components

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

1.2 Functions and Features

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

Asset Management

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

Table	1-2	Asset	management
-------	-----	-------	------------

Function	Description	Check Mode
Account informati on manage ment	 Check and manage all accounts on your servers to keep them secure. You can check real-time and historical account information to find suspicious accounts. Real-time account information includes account ID, number of servers, server names, permissions, user group, user directory, and user startup shell. Historical account change records include the change status, ECS name, account name, permissions, user group, user directory, user startup shell, and the change time. 	Real-time check
Open port check	Check open ports on your servers, including risky and unknown ports. You can check Port Type , Servers , Risk Level , Status , Port Description , and the specific Server , Bound IP Address , Status , PID , and Program File of a port.	Real-time check
Process check	Check processes on your servers and find abnormal processes. You can check Process Name , Servers , Total Number of Processes , Total Number of File Names , and the specific Server , Process Path , File Permission , User , PID , and startup time of a process.	Real-time check
Web directory manage ment	Check and manage directories used by web services on your servers. You can check the File Path , Application Type , Local Port , URL , PID , and Program File .	Real-time check
Software informati on manage ment	 Check and manage all software installed on your servers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. Real-time software information includes the Software Name, server quantity and names, and Software Version. The software operation history includes Action, Software Name, Software Version, and Time. You can use the manual detection function to check software information. 	 Autom atic check in the early mornin g every day Manua l check

Function	Description	Check Mode
Auto- startup	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	Real-time check
	You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.	

Vulnerability Management

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

 Table 1-3 Vulnerability management

Function	Description	Check Mode
Software vulnerabi lity detection	Check vulnerabilities in Linux and Windows. Check and handle vulnerabilities in your system and the software (such as SSH, OpenSSL, Apache, and MySQL) you obtained from official sources and have not compiled.	 Autom atic check in the early mornin
Web- CMS vulnerabi lity detection	Check and handle vulnerabilities found by scanning web directories and files in your Web-CMS.	g every day • Manua l check

Baseline Inspection

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

Table 1-4 Baseline	e inspection
--------------------	--------------

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

Intrusion Detection

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

on

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

Intrusion	How HSS Detects It	Check Mode	
Changes made to critical files	 Check alarms about modifications on key files (such as ls, ps, login, and top). Key file change information includes the paths of modified files, the last modification time, and names of the servers storing configuration files. 	Real- time check	
Web shells	 Check whether the files (often PHP and JSP files) in your web directories are web shells. Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. You can use the manual detection function to detect web shells on servers. 	 Real- time check Man ual check 	
Reverse shell	 Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. 		
Abnorma l shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Real- time check	
High-risk comman d execution	Check executed commands in real time and generate alarms on high-risk commands.		
Auto- startup check	Check and list auto-started services, scheduled tasks, pre- loaded dynamic libraries, run registry keys, and startup folders.	Real- time check	
Unsafe account	Scan accounts on servers and list suspicious accounts in a timely manner. You can check the name, user group, UID/SID, user directory, and startup shell of an account.	Real- time check	
Privilege escalatio n	 Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: Root privilege escalation by exploiting SUID program vulnerabilities Root privilege escalation by exploiting kernel vulnerabilities File privilege escalation 	Real- time check	

Advanced Protection

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

WTP

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

Table	1-6	WTP
-------	-----	-----

Function	Description	Check Mode
Static WTP	Prevents static web page files on website servers from being tampered with.	Real- time
Net disk tamperin g preventio n	Prevents web page files in shared net disks from being tampered with.	check
Dynamic WTP	Prevents dynamic web page content in website databases from being tampered with.	

1.3 Advantages

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

Centralized Management

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

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

Accurate Defense

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

All-Round Protection

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

Lightweight Agent

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

1.4 Editions

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

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
Asse t Man age men t	Manage account informa tion	Check and manage server accounts all in one place.	×	\checkmark	\checkmark	\checkmark
	Check open ports	Check open ports all in one place and identify high-risk and unknown ports.	×	~	~	~
	Manage applicat ions	Check running applications all in one place and identify malicious applications.	×	\checkmark	\checkmark	\checkmark

Table 1-7 Edition details

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Web director y manage ment	Check and manage web directories all in one place.	×	√	√	\checkmark
	Manage softwar e	Check and manage server software all in one place and identify insecure versions.	×	√	√	~
	Manage auto- startup	Check auto-startup entries and collect statistics on entry changes in a timely manner.	×	×	√	V
Vuln erab ility man age men t	Window s vulnera bilities	Scan Windows and software for vulnerabilities based on vulnerability databases, receive alarms generated on critical vulnerabilities, and manage them all in one place.	×	\checkmark	\checkmark	~
	Linux vulnera bilities	Scan Linux and software for vulnerabilities based on vulnerability databases, receive alarms generated on critical vulnerabilities, and manage them all in one place.	×	\checkmark	V	√
	Web- CMS vulnera bilities	Check and handle Web- CMS vulnerabilities found in web directory and file scans.	×	V	√	~
Uns afe setti ngs chec k	Passwor d policy check	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.	\checkmark	~	~	√
	Weak passwor d check	Change weak passwords to stronger ones based on HSS scan results and suggestions.	\checkmark	\checkmark	\checkmark	~

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Unsafe configur ation item check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	×	~	√	\checkmark
Intru sion dete ctio n	Brute- force attack	Your accounts are protected from brute- force attacks. HSS will block the attacking hosts when detecting such attacks.	\checkmark	~	\checkmark	\checkmark
	Abnorm al login	 Detect abnormal login behavior, such as remote login and brute-force attacks. Check and handle remote logins. HSS can check the blocked login IP addresses, and who used them to log in to which servers at what time. If a user's login location is not any common login location you set, an alarm will be triggered. Trigger an alarm if a user logs in by a brute-force attack. 	~	~	~	~
	Malicio us progra m (cloud scan)	Check and handle detected malicious programs all in one place, including web shells, Trojan horses, mining software, worms, and viruses.	×	√	√	√

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Abnorm al process behavio r	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: • Abnormal CPU usage • Processes accessing malicious IP addresses • Abnormal increase in concurrent process connections	×	~	~	~
	Change in critical file	Receive alarms when critical system files are modified.	×	~	√	\checkmark
	Web shell	 Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. You can use the manual detection function to scan for web shells on servers. 	×	√	√	√

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Reverse shell	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.	×	×	√	√
	Abnorm al shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	×	×	√	\checkmark
	High- risk comma nd executio n	Receive real-time alarms on high-risk commands.	×	×	~	~
	Auto- startup check	Check and list auto- started services, scheduled tasks, pre- loaded dynamic libraries, run registry keys, and startup folders.	×	×	√	~
	Unsafe account	Scan accounts on servers and list suspicious accounts in a timely manner.	×	\checkmark	\checkmark	

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Privilege escalati on	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities • File privilege escalation	×	×	√	√
	Rootkit	 Detect suspicious rootkit installation in a timely manner by checking: Check rootkits based on file signatures. Hidden files, ports, processes, and kernel modules 	×	×	\checkmark	\checkmark
Adv ance d prot ectio n	Progra m manage ment	Set whitelist policies, and determine whether applications are Trusted , Untrusted , or Unknown . The applications that are not whitelisted are not allowed to run. This function protects your servers from untrusted or malicious applications, reducing unnecessary resource usage.	×	×	~	~
	Monitor file integrity	Check the files in Linux, applications, and other components to detect tampering.	×	×	√	~

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Ransom ware preventi on	Analyze operations on servers, identify trusted applications, and report alarms on or block untrusted applications, depending on your settings.	×	×	V	\checkmark
Secu rity oper atio ns	Policy manage ment	 You can define and issue different detection policies for different servers or server groups, implementing refined security operation. View the policy list. Create a policy group based on default and existing policy groups. Define a policy. Edit or delete a policy. Modify or disable policies in a group. Apply policies to servers in batches on the Servers page. 	×	√ (Only the defau lt enter prise polic y grou p is supp orted .)	√	\checkmark
	Security report	Check weekly or monthly server security trend, key security events, and risks.	×	\checkmark	\checkmark	\checkmark
Secu rity confi gura tion	2FA	Prevent brute-force attacks by using password and SMS/email authentication.	\checkmark	\checkmark	\checkmark	\checkmark
Web Tam per Prot ectio n	Static WTP	Static web page files on your website servers are protected from tampering.	×	×	×	\checkmark
	Net disk tamperi ng preventi on	Files in your net disks are protected from tampering.	×	×	×	√

Fun ctio n	ltem	Description	Basic	Enter prise	Prem ium	WTP
	Dynami c WTP	Dynamic web page files in your website databases are protected from tampering.	×	×	×	\checkmark

1.5 Scenarios

Centralized Security Management

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

Security Risk Evaluation

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

Account Protection

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

Proactive Security

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

Intrusion Detection

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

1.6 Constraints

Supported Server Types

ECS

Supported OSs

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

NOTICE

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

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

No.	OS Version
1	CentOS 6, 7, and 8 (64 bit)
2	Debian 7, 8, 9, and 10 (32 bit or 64 bit)
3	EulerOS 2.2, 2.3, and 2.5 (64 bit)
4	Fedora: 24, 25, and 30 (64 bit)
5	OpenSUSE 13.2, 15.0, and 42.2 (64 bit)
6	Ubuntu 14.04, 16.0, and 18.04 (32 bit or 64 bit)
7	SUSE: 11 and 12 (64 bit) and SAP HANA
8	Gentoo: 13.0 and 17.0 (64 bit)
9	Oracle Linux 6.9 or 7.4 (64 bit)

Table 1-8 Linux versions (x86 computing)

Table 1-9 Linux versions (Kunpeng computing)

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

• Table 1-10 lists Windows versions supported by HSS.

Table 1-10 Windows versions

No.	OS Version	Constraint
1	Windows Server 2019 Datacenter 64-bit English (40 GB)	If a piece of third- party security software has been

No.	OS Version	Constraint	
2	Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	installed on your server, stop the	
3	Windows Server 2016 Standard 64-bit English (40 GB)	before installing an HSS agent. After you install the	
4	Windows Server 2016 Standard 64-bit Chinese (40 GB)		
5	Windows Server 2016 Datacenter 64-bit English (40 GB)	enable the protection function	
6	Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	on the software.	
7	Windows Server 2012 R2 Standard 64-bit English (40 GB)		
8	Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)		
9	Windows Server 2012 R2 Datacenter 64-bit English (40 GB)		
10	Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)		
11	Windows Server 2008 R2 Standard 64-bit English (40 GB)		
12	Windows Server 2008 R2 Standard 64-bit Chinese (40 GB)		
13	Windows Server 2008 R2 Datacenter 64-bit Chinese (40 GB)		
14	Windows Server 2008 R2 Enterprise 64-bit English (40 GB)		
15	Windows Server 2008 R2 Enterprise 64-bit Chinese (40 GB)		
16	Windows Server 2008 Web R2 64-bit Chinese (40 GB)		

1.7 HSS Permissions Management

If you need to assign different permissions to different employees in your enterprise to access HSS resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources. With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use HSS resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using HSS resources.

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

HSS Permissions

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

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

You can grant users permissions by using roles and policies.

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

Table 1-11 lists more details.

Role/Policy Name	Description	Role/ Policy Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS.	System- defined role	 This role depends on the Tenant Guest role. Tenant Guest: a global role, which must be assigned in the Global project

Table 1-11 System-defined permissions supported by HSS

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

1.8 Related Services

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

Elastic Cloud Server (ECS)

HSS agents can be installed on ECSs.

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

Simple Message Notification (SMN)

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

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

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

Identity and Access Management

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

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

Cloud Trace Service (CTS)

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

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

1.9 Concepts

Account Cracking

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

Viewing Information About Weak Passwords

A weak password can be easily cracked.

Viewing Information About Malicious Programs

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

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

HSS reports both identified and suspicious malware.

Ransomware

Ransomware emerged with the Bitcoin economy. It is a Trojan that is disguised as a legitimate email attachment or bundled software and tricks you into opening or installing it. It can also arrive on your servers through website or server intrusion.

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

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

Two-Factor Authentication

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

Web Tamper Protection

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

Project

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

Multiple projects can be created for one account.

2 Enabling HSS

2.1 Installing an Agent

2.1.1 Installing an Agent on a Linux Server

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

NOTE

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

Default Installation Path

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

/usr/local/hostguard/

Prerequisites

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

Installing an Agent Using Commands

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

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, copy the required installation command.



Figure 2-1 Copying the command for installing the agent

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

- You can log in to the ECS management console and click **Remote Login** in the ECS list.
- If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, or WinSCP, to log in to the server and install the agent on the server as user **root**.
- **Step 5** Paste the copied installation command and press **Enter** to install the agent on the server.

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

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

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

Hostguard is running

----End

Installing an Agent Using an Installation Package

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

- **Step 1** Log in to the management console.
- **Step 2** In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, download the agent package.



Dashboard	<u>0</u>			
Servers	Install Agent Security Configuration Two-Factor Authentication Alarm Notifications			
Scans 👻				
Intrusions 👻				
Advanced Protection 🔹				
Security Operations	3 Procedure Supported OSs:			
Installation and Configuration	1. Use a remote management tool, such as Xshell and PuTTY, to connect to your server using its EIP. 2. Copy the correct command to the server and execute the command as user root. Debian: 7, 8, and 9 (32/64-bit)			
web faitper Protection	Linux Wgetno-check-certificate 'http:///// Wgentinstall_32.sh' && chmod *x bit: WwAgentinstall_32.sh && /HwAgentinstall_32.sh Fedora: 24 and 25 (64-bit) Gropy Fedora: 24 and 25 (64-bit) UlauCS: 22 (64-bi			
	wgetno-check-certificate 'http:/// - Oracle Linux: 6.9 and 7.4(64-bit) 64 //Inux/HwAgentinstall_64.sh && chmod +x □ Copy OpenSUSE: 13.2 and 42.2(64-bit) bit: +wAgentinstall_64.sh && /HwAgentinstall_64.sh bit: bit:			
	Windows Note Overlap Agent Installation Package Use a software terminal emulator, such as PuTP, to log in to the Server using its EIP and use a file transfer tool, such as windows Windows			

- **Step 3** Download the agent to be installed based on the server OS version.
- **Step 4** Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the agent installation package to the server.
- **Step 5** Remotely log in to the server where the agent is to be installed.
 - You can log in to the ECS management console and click **Remote Login** in the ECS list.
 - If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, or WinSCP, to log in to the server and install the agent on the server as user **root**.
- **Step 6** Run **cd** *Installation_package_directory* to access the directory.
- **Step 7** Run the following command to install the agent on the server:
 - For an .rpm package, run **rpm -ivh** *Package_name*.

NOTE

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

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

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

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

Hostguard is running. Hostguard installed.

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

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

Hostguard is running

----End

2.1.2 Installing an Agent on a Windows Server

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

NOTE

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

Default Installation Path

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

C:\Program Files (x86)\HostGuard

Prerequisites

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

Procedure

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

- Method 1: Download the agent installation package, upload it to the server where the agent is to be installed, and run the installation command on the server to install the agent.
- Method 2: Log in to the server where the agent is to be installed, log in to the management console using the server, and download and install the agent.
- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 In the navigation pane on the left, choose Security Operations > Installation and Configuration. On the Install Agent tab, copy the link of the agent installation package.

Host Security Installation and Configuration ② Dashboard Security Configuration Two-Factor Authentication Alarm Notification Servers Scans Intrusions Advanced Protecti Method 1 4 Supported OSs: Security Operations 1 <u>Download Agent Installation Package</u> to a local PC. 2. Open Windows Remote Desktop Connection and choose Option > Local Resources > Local Devices and Resources and select the Clipboard check box. Connect to the server by its EIP. Upon successful connection, copy the agent installation file and paste it to the server. Then, run the agent installation program as the administrator. Windows 2016 Windows 2012 Windows 2008 tallation and nfiguration 0 Web Tamper Protection Method 2 Log in the server on the server console. Open Internet Explorer and add this website to the list of trusted sites. Access this page and download the agent installation package. Then, run the agent installation program as the administrator. Windows

Figure 2-3 Installing a Windows agent

- **Step 4** Remotely log in to the server where the agent is to be installed.
- **Step 5** Upload the agent installation package to the server where the agent is to be installed.
- Step 6 Run the agent installation program as a system administrator.

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

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

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



> 📧 Antimalware Service Executa	0%	96.1 MB
> 💽 COM Surrogate	0%	3.0 MB
> 📧 COM Surrogate	0%	1.2 MB
> 📑 HostGuard.exe 📰 🖏	0%	3.0 MB
> 💽 hostwatch.exe (0%	1.8 MB
> 📧 Intel® PROSet Monitoring S	0%	1.5 MB
👌 🐗 Java Service Wrapper Comm	0%	2.0 MB
🕌 Java(TM) Platform SE binary	0%	24.7 MB
@ Microsoft IME	0%	1.1 MB
Hicrosoft Malware Protectio	0%	2.1 MB
End		

2.2 Configuring Alarm Notifications

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

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

- Alarm notification settings are effective only for the current region. To receive notifications from another region, switch to that region and configure alarm notification.
- Alarm notifications may be mistakenly intercepted. If you do not receive any alarm notifications, view them in the message interception area.

Prerequisites

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

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

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** Choose **Installation and Configuration** and click the **Alarm Notifications** tab, as shown in **Figure 2-5**.

Host Security	Installation and Cor	figuration ⑦		Uninstall Age
Dashboard Servers	Install Agent	Security Configuration Two-Factor Aut	2 hentication Alarm Notifications	
icans	•			
ntrusions	*			
dvanced Protection	 1. Alarm notification 2. Alarm notifications 	settings only apply to the current region and project. a may be intercepted as junk information. If no alarm n	otification is received, check whether it is intercepted	ed.
ecurity Operations	•			
onfiguration	Daily Alarm Notific	ations		
eb Tamper Protection		Item		
	Assets	Dangerous ports		
	Vulnerabilities	Critical vulnerabilities		
		Account cracking	Important file changes	Malicious programs
	Intrusions	Web shells	Reverse shells	Abnormal shells
		High-risk command execution	Privilege escalation	Rootkits
	Unsafe Settings	Veak passwords	Unsafe accounts	Unsafe configurations
	Logins	Remote login attempts		
	Real-Time Alarm N	lotifications		
	Category	Item		
		Abnormal logins ?	Malicious programs	Important file changes 🕜
	Intrusions	Web shells	Reverse shells	Abnormal shells
		High-risk command execution	Privilege escalation	Rootkits
	Logins	Successful logins		
	SMN Topic			
	v	✓ C View Topics		
	Topic subscriptions dete	rmine how you will receive alarm notifications. There	e must be at least one confirmed subscription or	you cannot complete alarm configuration.
	Aunte			
	Apply			

Figure 2-5 Basic/Enterprise/Premium edition

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

Table 2-1	Notification	types
-----------	--------------	-------

Notification Type	Description	Suggestion on Selecting a Notification Item
Daily alarm notification	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 added in the SMN topic.	 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	If an attacker intrudes the server, HSS will send alarms based on the SMN topic you set.	 It is recommended that you receive all the content in the real-time alarm notification and view them in time. The HSS system monitors the security of servers in real time, detects the attacker's intrusion, and sends real-time alarm notifications for you to quickly handle the problem. Real-time alarm notifications are about urgent issues. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to SMS.

Step 5 Select a message notification topic.

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

- Multiple subscriptions can be added to a topic. Before selecting a topic, ensure that subscriptions added to it are in **Confirmed** status. Otherwise, notifications may fail to be received.
- The confirmation message about topic subscription may be regarded as spam. If you do not receive the message, check whether it is intercepted as spam.
- For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 6 Click Apply.

----End

Alarm Notifications

Notificatio n Type	ltem	Description			
Daily Alarm Notifications HSS checks risks in your servers in the early morning every day, summarizes and collects detection results, and sends the results to your mobile phone or email box at 10:00 every day.					
Assets	Dangerous port	Check for high-risk open ports and unnecessary ports.			
Vulnerabilit ies	Critical vulnerabilities	Detect critical vulnerabilities and fix them in a timely manner.			
Intrusions	Account cracking	Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts.			
		 If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. 			
		• You can check whether the IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.			
	Important file changes	HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.			
	Malicious programs	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.			
	Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells.			
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections.			
Notificatio n Type	Item	Description			
-----------------------------------	-----------------------------------	--	--	--	--
	Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.			
	High-risk command execution	HSS checks executed commands in real time and generates alarms if high-risk commands are detected.			
	Privilege escalation	HSS detects privilege escalation for processes and files in the current system.			
	Rootkits	HSS detects suspicious rootkit installation in a timely manner by checking:			
Unsafe Settings	Weak passwords	Detect weak passwords in MySQL, FTP, and system accounts.			
	Unsafe accounts	Check for suspicious and unnecessary accounts on the servers to prevent unauthorized access and operations.			
	Unsafe configuration s	Detect unsafe settings of key applications that will probably be exploited by hackers to intrude servers.			
Logins	Remote login	Check and handle remote logins.			
	attempts	If a user's login location is not any common login location you set, an alarm will be triggered.			
Real-Time A When an eve	larm Notification	ons arm notification is immediately sent.			
Intrusions	Abnormal logins	Detect abnormal login behavior, such as remote login and brute-force attacks. If abnormal logins are reported, your servers may have been intruded by hackers.			
	Malicious programs	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.			
	Important file changes	HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.			
	Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells.			

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

2.2.2 Enabling Alarm Notification for the WTP Edition

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

- Alarm notification settings are effective only for the current region. To receive notifications from another region, switch to that region and configure alarm notification.
- Alarm notifications may be mistakenly intercepted. If you do not receive any alarm notifications, view them in the message interception area.

Prerequisites

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

Enabling WTP Alarm Notifications

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Installation and Configuration** and click the **Alarm Notification** tab. Configure alarms, as shown in **Figure 2-6**.

Host Security	Installation and Configuration ⑦	
Dashboard Servers	Install Agent Alarm Notification Backup Server	
Scans 🔻		
Intrusions 🔻		
Advanced Protection Security Operations	 Alarm notification settings only apply to the current region and project. Alarm notifications are sent by SMN free of charge at the beginning of every m Alarm notifications may be intercepted as junk information. If no alarm notifi For more information on alarm notification, view video tutorials. 	onth, and you will be charged since the sent messages exceed a certain number. ication is received, check whether it is intercepted.
Installation and Configuration	Daily Alarms	U
Web Tamper Protection	Item	Time
Server Protection	Dynamic WTP	10:00
Installation and Configuration	Real-Time Alarm Notification	
	Item	Time
	Dynamic WTP	24 hours 08:00 - 20:00
	SMN Topic	
	v C View Topic	
	Only SMN topics whose status is confirmed are available.	
	Apply	

Figure 2-6 Configuring alarm notifications

Step 4 Select a message notification topic.

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

- Multiple subscriptions can be added to a topic. Before selecting a topic, ensure that subscriptions added to it are in **Confirmed** status. Otherwise, notifications may fail to be received.
- The confirmation message about topic subscription may be regarded as spam. If you do not receive the message, check whether it is intercepted as spam.
- For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 5 Click Apply.

----End

2.3 Enabling HSS

2.3.1 Enabling the Basic/Enterprise/Premium Edition

Check Mode

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

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

Prerequisites

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

Constraints

Linux

On servers running the EulerOS with ARM, HSS does not block the IP addresses suspected of SSH brute-force attacks, but only generates alarms.

- Windows
 - Authorize the Windows firewall when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS inservice period. If the Windows firewall is disabled, HSS cannot block brute-force attack IP addresses.
 - If the Windows firewall is manually enabled, HSS may also fail to block brute-force attack IP addresses.

Enabling Protection

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** In the navigation tree on the left, choose **Servers**.

Figure 2-7 Server list

Host Security	Servers ①	
Dashboard Servers	2 Server Group	
Intrusions Advanced Protection	Select all Enable Disable Apply Policy Add to Group Server name + Enter a keyw Q Search * C	3 C
Security Operations Installation and Configuration	Server Na_ IIP Address US Server SL Agencista_ Protection_ Detection_ Edition Server Gr_ Policy_ Operation ecc-ead7 69.141 Unux Running Online EnabL Image: Risky Premium hss_test	Aore ▼
Web Tamper Protection		

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

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

Figure 2-8 Enabling HSS

Enable Protection						
Servers that require	HSS protection:					
Server Name	IP Address	OS	HSS Edition			
ecs-a883	.69.141 (EIP) 192.168.0.167 (Priva	Linux	None			
HSS Edition 🧕	Basic O En	terprise 🔿 Prem	nium			
	ОК	Cancel				

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

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

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

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



Figure 2-9 Automatic security check items

----End

Viewing Detection Details

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

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

Figure 2-10 Viewing details

Host Security	Servers ①
Dashboard Servers 1 Scans • Intrusions •	Server Server Group Select all Enable Disable Apply Policy Add to Group Server name Select all Enable
Advanced Protection Security Operations installation and Configuration Web Tamper Protection	Server Na. IP Address OS Server SL. Agent Sta Protectio Detection Edition Server Gr Policy Gr Operation

The details page shows detection results and detected risks.

Figure 2-11 Viewing the detection result

Host Security		Servers & Quotas / Test				
Dashboard Servers		Assets Vulnerabilities Unsa	fe Settings Intrusions			
Scans	Ŧ	Account Information (27) Open Po	orts (0/ 0) Process Information (28)	Web Directories (1) Installed Softwa	are (375) Auto-startup (4)	
Intrusions	•					
Advanced Protection	•	You can review all system accounts and us	er groups here.			
Security Operations						Enter an acco Q C
web ramper Protection		Account ID	Administrator Rights	User Group	User Directory	User Startup Shell
Container Guard Service	ď	adm	No	adm	/var/adm	/sbin/nologin
Security Console	8	bin	No	bin	/bin	/sbin/nologin
Elastic Cloud Server	ď	daemon	No	daemon	/sbin	/sbin/nologin
		dbus	No	dbus	1	/sbin/nologin
		ftp	No	ftp	/var/ftp	/sbin/nologin
		games	No	users	/usr/games	/sbin/nologin
		halt	No	root	/sbin	/sbin/halt
		lp	No	lp	/var/spool/lpd	/sbin/nologin
		mail	No	mail	/var/spool/mail	/sbin/nologin
		nobody	No	nobody	1	/sbin/nologin

Switching Editions

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

NOTICE

- If the HSS service is switched from a higher edition to a lower edition, protected servers will be more vulnerable to attacks.
- You can only switch the HSS edition to the **basic** , **enterprise**, or **ultimate** edition.
- Preparations
 - Before switching to a lower edition, check the server, handle known risks, and record operation information to prevent O&M errors and attacks.
- Operations after the edition change
 - After switching to a lower edition, clear important data on the server, stop important applications on the server, and disconnect the server from the external network to avoid unnecessary loss caused by attacks.

- After switching to a higher edition, perform a security detection on the server, handle security risks on the server, and configure necessary functions in a timely manner.

Follow-up Operation

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

For details about the differences between editions, see Edition details.



Figure 2-12 Manual check items

Table 2-2 Manual check items

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

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

Follow-Up Procedure

Disabling HSS

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

NOTICE

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

2.3.2 Enabling the WTP Edition

The premium edition will be enabled when you enable WTP.

How WTP Prevents Web Page Tampering

Table 2	-3 Prote	ection me	echanisms
---------	----------	-----------	-----------

Туре	Mechanism
Static web page protection	 Local directory lock WTP locks files in a web file directory in a drive to prevent attackers from modifying them. Website administrators can update the website content by using privileged processes.
	2. Active backup and restoration If WTP detects that a file in a protected directory is tampered with, it immediately uses the backup file on the local server to restore the file.
	3. Remote backup and restoration If a file directory or backup directory on the local server is invalid, you can use the remote backup service to restore the tampered web page.
Dynamic web page protection	 Malicious behavior filtering based on RASP The runtime application self-protection (RASP) technologies detect program behaviors, preventing attackers from tampering with web pages through application programs.
	2. Network disk file access control WTP implements fine-grained management to control permissions for adding, modifying, and querying file content in network disks, preventing tampering without affecting website content release.

Restrictions

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

Prerequisites

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

Setting Protected Directories

You can set:

Directories

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

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

• File systems

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

OS partitions are not allowed.

Enabling WTP

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click \equiv , and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Web Tamper Protection** > **Server Protection**. Click **Enable** in the **Operation** column of a server.

Figure 2-13 Web Tamper Protection

Host Security		Ser	rver Pro	otection ⑦								
Dashboard Servers			Bloc	ked Attacks C) Protect	ed Servers 1	Protect	ed Directories	1			
Scans	• •		Enabl	e Disab	le						Server name 👻	Enter a keyword. Q
Advanced Protection	-			Server Nam	IP Address	os 🏹	Server St	Agent 🍞	w ア	Dynamic WTP	Edition/Expiration Date	Operation
Security Operations	•			ecs-a883 1c4cc66e-28e5-4	.69.141 (192.168.0.167 (E Linux	Running	Online	🕑 Ena	Disabled	Web Tamper Protection	Disable Configure Protection View F
Installation and Configuration				windows e9e40ddf-c4d3	.73.76 (E	Windows	Running	Online	O Disa	Disabled	None 2	Enable Configure Protection View R
Server Protection				test-40314 12ef6caf-1ef8-4	.68.202 (192.168.0.48 (P	E Linux	Running	Not installed	O Disa	Disabled	None	Enable Configure Protection View R
Installation and Configuration												

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

Figure 2-14 Enabling WTP

Enable WTP				2
Servers for which y	ou want to enable WTP			
Server Name	IP Address	OS	Protection Status	
windows	.73.76 (EIP) 192.168.0.99 (Private	Windows	Disabled	
	ОК	Cancel		

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

----End

NOTICE

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

Follow-Up Procedure

Disabling WTP

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

NOTICE

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

3 Viewing the Server List

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

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** On the **Server** tab, check the protection status of servers.

Figure 3-1 Server list

Host Security		Servers	0											
Dashboard		6	2											
Servers 1		Ser	ver Se	rver Group										
Scans	*	_												
Intrusions	-		Select all	Enable	Disabl	e Ap	ply Policy	Add to G	roup	s	erver name	• Enter a k	eyw Q Search ≽	C C
Advanced Protection	-		Server	IP Addr	OS	Server S	Agent S	Protecti	Detecti	Edition	Server	Policy G	Operation	
Security Operations	*		ecs-ead7	.69.1	Linux	Running	Online	🔿 Ena	Risky	Premium	hss test		Disable Switch Edition	More 🔻
Installation and Configuration			4352b5b3	-е 192.168.0.1					- · ·					
Web Tamper Protection	-													

NOTE

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

```
• To export the server list, click
```

Paramete r	Description
Agent Status	 Not installed: The agent has not been installed or successfully started. In this case, click Installed and install the agent as prompted. Online: The agent is running properly. Offline: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. Click Offline and view servers whose agents are offline and the recent the agent and the the server is abnormal.
Protection	Enabled: The server is fully protected by HSS.
Status	• Disabled : The server is not protected. If a server does not need protection, you can disable HSS for it to reduce its resource consumption.
Detection Result	 Risky: The host has risks. Safe: No risks are found. Pending risk detection: HSS is not enabled for the server.

Table 3-1 Statuses

----End

Viewing the WTP List

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Server Protection**. Check the protection status of servers.

Host Security		Server F	rotection (
Dashboard												
Servers		0	Dynamic WTP is now available. Click Configure Protection for a free trial. X									
Scans	*		Diselyed Attack	0 0-	lasted Can		Instant Directories	1				
Intrusions	*		DIOCKED ATTACK		lected Serve	315 I P	TOLECLEU DIFECTORIES	·				
Advanced Protection	•	Ena	ble Disa	ble				•		Server name	 Enter a keyword 	0 0
Security Operations	*		Server Name/II	D IP Address	05 7	Server Status	Agent Status 😽	WTP Status 🕎	Dynamic WTP	Edition/Expiration Date	Operation	
Installation and Configuration	_		ac97b007-3c98	146.89 (El 44. 192.168.1.24 (Pri	IF Linux	Running	Online	S Enabled	Disabled	Web Tamper Protection	Disable Configure Protection	View Report
Web Tamper Protection Server Protection		1	a3567c92-be6f	44' 192.168.1.10 (Pri	IF Linux	Running	Online	Disabled	Disabled	None	Enable Configure Protection	View Report
Installation and Configuration			42bff3d9-23dd-	155.92 (E 41d 192.168.0.250 (P	IF Windows	Running	Online	Disabled	Disabled	None	Enable Configure Protection	View Report

Figure 3-2 Server protection

Table 3-2 Statuses

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

----End

4 Dashboard

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

Risk Statistics on Protected Servers (Last 24 Hours)



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

Server Protection Status (Last 24 Hours)

Figure 4-2 Server protection status

Protection statistics (Last 24 Hours)					
Protected/Unprotected	Basic Edition	Enterprise	Flagship		
10/22	1	8	1		
Enable All	Unsafe Servers0	Unsafe Servers3	Unsafe Servers1		

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

To enable protection for required servers, click Enable All.

Risks





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

Table 4-1 Risks

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

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

Handled Risks (Last 7 Days)

Figure 4-4 Handled risks



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

Intrusions

Figure 4-5 Intrusions



You can check the numbers and types of intrusions in the last seven or 30 days. These intrusion statistics are updated at 00:00 a.m. every day.

Top 5 Unsafe Servers (Last 7 Days)

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

Top 5 Unsafe Ser	vers (last 7 days)	С
ecs	eulr	
ecs-		
ecs-76ef		
ecs-8285-windo	ws	
	 Vulnerabilities Asset risks Intrusion risks Baseline risks 	

If you have enabled the basic, enterprise, or premium edition HSS, you can check the top 5 unsafe servers, which have the most risks detected in the past week, and the numbers of each type of risks. At 00:00 every morning, server risks and the five servers with highest risks in the past seven days are updated.

Real-time Intrusions

Figure 4-7 Real-time intrusions

Real-ti	ime intrusio	ns							View more \rightarrow
Alarm	п Туре	Affected Server & IP	Event Details	Reported	Handled	Status	Action	Operation	
Abnor	rmal autos	HSS-WIN- 192.168.1.68	Type: Run registry key, Event type: Cr	2020/05/19 16:1	-	Unhandled	-	Handle	
Abnor	rmal autos	Windows- 192.168.1.188	Type: Run registry key, Event type: Cr	2020/05/19 16:1		Unhandled		Handle	
Abnor	rmal autos	HSS-\ 192.168.1.68	Type: Run registry key, Event type: Cr	2020/05/19 13:1	-	Unhandled	-	Handle	

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

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

5 Security Configuration

After protection is enabled, you can set security configurations, including common login locations, common login IP addresses, SSH login IP address whitelist, and the automatic isolation and killing of malicious programs.

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.

----End

Configuring Common Login Locations

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

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

Host Security	Installation and Configuration 🕜
Dashboard Servers	Install Agent Security Configuration Two-Factor Authentication Alarm Notifications
Scans •	
Advanced Protection 🔹	3 Common Login Locations Common Login IP Addresses SSH IP Whitelist Isolation and Killing of Malicious Programs
Security Operations 🔹	
Installation and Configuration	Alarms will not be generated for login attempts from common login locations.
Web Tamper 🔹	Add Common Login Location You can add 9 more IP addresses.
	Common Login Locations Server Quantity Operation
	1 Edit Delete

Figure 5-1 Adding a common login location

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

----End

Configuring Common Login IP Addresses

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

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

Host Security		Installation and Configuration ⑦
Dashboard Servers		Install Agent Security Configuration Two-Factor Authentication Alarm Notifications
Scans	•	
Intrusions	•	3
Advanced Protection	•	Common Login Locations Common Login IP Addresses SSH IP Whitelist Isolation and Killing of Malicious Programs
Security Operations	•	
Installation and Configuration		Alarms will not be generated for login attempts from common login IP addresses.
Web Tamper Protection	•	Add Common Login IP Address You can add 9 more common login IP addresses.
		Common Login IP Addresses Server Quantity Operation
		192.168.1.1 1 Edit Delete

Figure 5-2 Adding a common login IP address

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

NOTE

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

----End

Configuring an SSH Login IP Address Whitelist

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

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

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

If your service needs to access a server, but not necessarily via SSH, you do not need to add its IP address to the whitelist.

• Exercise caution when adding an IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your servers.

NOTE

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

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

Host Security Installation and Configuration ⑦ 2 Dashboard Security Configuration Install Agent Two-Factor Authentication Alarm Notification Servers Scans Intrusions Advanced Protection SSH IP Whitelist Common Login Locations Common Login IP Addresses Isolation and Killing of Malicious Programs Security Operations nstallation and Logins will be allowed only from whitelisted IP addresses. Configuration 4 Web Tamper You can add 9 more IP addresses Add IP Address Protectio Whitelisted IP Address/Range Server Quantity Status Operation 10.1.1.1 1 💿 Enabled Edit | Disable | Delete

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

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

NOTE

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

----End

Isolating and Killing Malicious Programs

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

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



Host Security		Installation and Configuration ③
Dashboard		Install Agent Security Configuration Two-Factor Authentication Alarm Notifications
Scans		
Jahreisee	÷	
intrusions	Ť	3
Advanced Protection	Ť	Common Login Locations Common Login IP Addresses SSH IP Whitelist Isolation and Killing of Malicious Programs
Security Operations	*	
Installation and Configuration		Isolate and Kill Malicious Programs
Web Tamper Protection	•	Automatically isolates and kills identified shells, Trojans, and viruses. Enabling this function may result in positives. If this happens, navigate to the Isolated Files slide-out panel on the Intrusions page and cancel isolation for or ignore the program or process that was falsely identified as malicious.

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

NOTICE

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

To isolate and kill the malicious programs that triggered alarms, choose **Intrusions** > **Events** and click **Malicious program (cloud scan)**.

Enabling 2FA

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

Prerequisites

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

- To enable two-factor authentication, you need to disable the SELinux firewall.
- On a Windows server, 2FA may conflict with G01 and 360 Guard (server edition). You are advised to stop them.

Constraints and Limitations

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

Procedure

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

Figure 5-5 2FA

Host Security		Installation and Configuration ③					
Dashboard Servers		Install Agent Security Configuration Tw	2 vo-Factor Authentication	Alarm Notification	ons		
Scans	*	•					
Intrusions	*	Enable 2FA Disable 2FA Change Topic		Serve	r name 💌 🛛 Ente	er a keyword.	QC
Advanced Protection	*	Protected Server OS Type	2FA Status	Method	SMN Topic	Operation	
Security Operations	*	ecs-Linux	Disabled			Enable 2FA	Change Topic
Configuration		3 Zih_ Linux	Disabled	-		Enable 2FA	Change Topic
Web Tamper Protection	*	vss-openvas Linux	Disabled	-	-	Enable 2FA	Change Topic

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

• SMS/Email

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

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

Figure 5-6 SMS/Email

Enable 2FA	×
Method 💽 SMS/Email 🔿 Verification code	
SMN Topic	
C View Topics	
Note: 1. There must be at least one confirmed subscription of ar 2. SMS/Email is recommended when you add subscription: 3. Enabling 2FA will modify the system login file.	I SMN topic, or you cannot complete alarm configuration. s to a topic.
Servers to Use 2FA	
Server Name	2FA Status
ecs-a883	Disabled
ОК	Cancel

• Verification code

In the Enable 2FA dialog box, set Method to Verification code, and click OK.

Figure 5-7 Setting Method to Verification code

Enable 2FA		×
Method 🔵 SMS/Email 💿 Verification	n code	
Enter the verification code when you log in to the Servers to Use 2FA	e server for secondary verification.	
Server Name	2FA Status	
ecs-a883	Disabled	
	OK Cancel	

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

NOTICE

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

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

----End

6 Server Management

6.1 Creating a Server Group

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

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- Step 3 In the navigation pane, choose Servers, and click the Server Group tab. Click Create Server Group, as shown in Figure 6-1.



Host Security		Servers ⑦				
Dashboard Servers	Ţ	Server Server Gr	oup			
Intrusions	-	Create Server Group]			Enter a server group na Q C
Advanced Protection	-	Server Group	Servers	Unsate Servers	Unprotected Servers	Operation
Security Operations	•	hss_test	1	1	0	Edit Delete
Installation and Configuration						
Web Tamper Protection	•					

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

D NOTE

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

Figure 6-2 Creating a server group

Create Server Group			×
* Server Group hss_test			
Available Servers		Selected Servers	
Ungrouped Server name E	nter a keyworc Q		
Server Name/Elastic IP Address	OS	Server Name/Elastic IP Address	OS
windows	Windows	windows .73.76	Windows
ecs-a883	Linux		
	ОК	Cancel	

Step 5 Click OK.

----End

Adding Servers to Groups

You can add servers to an existing server group.

- **Step 1** Click the **Server** tab.
- **Step 2** Select one or more servers and click **Add to Group**, as shown in **Figure 6-3**.

Figure 6-3 Adding servers to a group

Host Security		Servers ⑦ Configure Alarm Notification Manual Detection
Dashboard		0
Servers 1		Server Group
Scans	-	0
Intrusions	-	Select all Enable Disable Apply Policy Add to Group Server name 👻 Enter a keyw Q Search 😸 🖆 C
Advanced Protection	-	Server Na IP Address OS Server Sta Agent Sta Protectio Edition Server Gr Policy Gr Operation
Security Operations	*	C es-ead7
Installation and		4352b5b3-e0. 192.168.0.162
comguradon		
Web Tamper Protection	-	

NOTE

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

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

D NOTE

A server can be added to only one server group.

----End

Follow-Up Procedure

Editing a server group

- **Step 1** Locate the row where a server group resides and click **Edit** in the **Operation** column.
- **Step 2** In the displayed dialog box, add or remove servers in the group.
- Step 3 Click OK.

----End

Viewing a server group

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

Deleting a server group

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

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

6.2 Applying a Policy

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

Precautions

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

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

Accessing the Policies Page

Step 1 Log in to the management console.

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

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

----End

Creating a Policy Group

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

Figure 6-4 Copying a policy group

Host Security	Policies	
Dashboard	Delete	Enter a policy group name. Q
Servers	Policy Group Name ID Description Supported Version Set	rvers Operation
Scans 🔻	default_enterprise_policy_gr 7d142628-01d0-493b-991b Enterprise 5	
Advanced Protection	default_premium_policy_gr 9c99173c-8316-481d-8bc1 Flagship 1	Сору
Security Operations	4e018df2-2732-4fb7-bf61-9 Flagship 0	Copy Delete
Reports	console_test1 a81c376b-9a3c-4088-ae0b Flagship 0	Copy Delete
Policies 2	console_test2 ff719896-7339-467b-aa49-1 Flagship 0	Copy Delete
Installation and Configuration	cosole_test3 ed20e844-faa2-4380-ad51-c Flagship 0	Copy Delete
Web Tamper Protection 👻	console_test5 8651f270-d71e-4446-b8aa-0 Flagship 0	Copy Delete
	cosole_test4 08ccbf0e-b292-4cf8-a1f6-7 Flagship 0	Copy Delete
	aaa leSfcd60-c53b-4272-8ddb-3 aaa Flagship 0	Copy Delete
	qq 77412672-3774-41f3-b81a www Flagship 0	Copy Delete
	10 • Total Records: 19 < 1 2 >	

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

NOTE

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

Figure 6-5 Creating a policy group

Copy Policy Grou	р	×
* Policy Group Name		
Description	Æ	
	OK Cancel	

Step 3 Click OK.

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

Figure 6-6 Policies in a group

Po	licies / default_premium_policy_group					
						C
	Policy Name	Status 🏹	Function Category	OS Type	Operation	
	Assets	Enabled	Asset management	Linux, Windows	Disabled	
	System Configuration Detection	Enabled	Unsafe setting scan	Linux, Windows	Disabled	
	Weak Password Detection	Enabled	Unsafe setting scan	Linux, Windows	Disabled	
	High-risk command detection	Enabled	Data collection	Linux	Disabled	
	Privilege escalation detection	Enabled	Intrusion detection	Linux	Disabled	
	Abnormal shell detection	Enabled	Intrusion detection	Linux	Disabled	
	Integrity check on critical files	Enabled	Intrusion detection	Linux	Disabled	
	Web Shell Detection	Enabled	Intrusion detection	Linux, Windows	Disabled	

- **Step 5** Click a policy name and modify its settings as required. For details, see **Modifying a Policy**.
- **Step 6** Enable or disable the policy by clicking the corresponding button in the **Operation** column.

----End

Applying a Policy Group

- **Step 1** In the navigation pane, choose **Servers**. Click the **Server** tab.
- Step 2 Select one or more servers and click Apply Policy, as shown in Figure 6-7.

Figure 6-7 Applying policies

Host Security		Servers ⑦ Configure Alarm Notification Manual Detection
Dashboard Servers		Server Group
Scans	۳	<u>0</u>
Intrusions	*	□ Select all Enable Disable Apply Policy Add to Group Server name ▼ Enter a keyw Q Search ⇒ C C C
Advanced Protection	*	Server Na IP Address OS Server Sta Agent Sta Protectio Detection Edition Server Gr Policy Gr Operation
Security Operations	۳	3 😰 ecs-ead7 69.141 Linux Running Online 📀 Enabl 📀 Risky Premium (Yearly/Mo hss_test Disable Switch Edition
Installation and Configuration		4552/305/EW 152/100.0102
Web Tamper Protection	٣	

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

Figure 6-8 Selecting a policy group

		×
Are yo deploy	u sure you want to enable the premium server ment policy?	
Policy Group	default_premium_policy_gr 💌	
	OK Cancel	

NOTE

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

----End

7 Risk Prevention

7.1 Asset Management

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

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

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

Check Interval

Account information and open ports are checked in real time.

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

Viewing Asset Information

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** Go to the **Assets** page. Click tabs on the page to view assets detected by HSS on your servers.

Host Security	A	Assets ⑦	Configure Alarm Notification
Dashboard Servers	•	Account Information Open Ports Processes Web Directories Installed Software Auto-startup	
Assets 2 Vulnerabilities Unsafe Settings		Accounts Operation History	Enter an account name. Q C
Intrusions	-	Account ID	Servers
Advanced Protection	•	bin	1
Security Operations	-	chrony	1
Installation and Configuration		daemon	1
Web Tamper Protection	-	dbus	1
		halt	1
		lp	1
		nobody	1
		ntp	1
		polkitd	1
		postfix	1

----End

Managing Account Information

Operations made to accounts are recorded.

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

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

Checking Open Ports

You can manage all the open ports on your servers.

• Manually disabling high-risk ports

If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.

It is recommended that you handle the ports with the **Dangerous** risk level promptly and handle the ports with the **Unknown** risk level based on the actual service conditions.

 Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.

Managing Processes

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

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

Managing Web Directories

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

Managing Software

Operations made to software are recorded.

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

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

Managing Auto-start Entries

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

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

7.2 Vulnerability Management

7.2.1 Viewing Details of a Vulnerability

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

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

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

Detection Mechanisms

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

Table 7-1 Vulnerability detection mechanisms

NOTE

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

Check Interval

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

Fixing Linux or Windows Vulnerabilities

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- Step 3 Open the Linux Vulnerabilities or Windows Vulnerabilities tab.

Host Security	Vulnerabilities 💿		
Dashboard	0		
Servers	Linux Vulnerabilities Windows Vulnerabilities Web-CMS Vulnerabilities		
Scans 1 *			
Assets	Server Statistics – Linux Vulnerabilities Top 5 Servers – Linux Vulnerabilities		
Vulnerabilities 2			
Unsafe Settings	Servers with detection disabled		
Advanced Protection •	1 Servers without critical vulnerabilities		
Security Operations 🔹	No data available.		
Installation and Configuration			
Web Tamper Protection	Ignore Unignore All urgencies Enter a vulnerability name. Q [] C		
	Vulnerability Name Urgency Unhandled S Affected Servers Solution Operation		

Figure 7-2 Viewing Linux or Windows vulnerability scan results
Step 4 Click a vulnerability name to view its basic information, solution, and CVE description.

Figure 7-3 Checking vulnerability details

inux Vulnerabilities / CESA-2016.2593 (sudo security update)							
Vulnerability Details	Affected Servers						
Basic Details							
Vulnerability name	CESA-2016:2593 (sudo s	security update)	Status		🕛 Medium		
Unhandled Servers	2		Affected Servers		3		
Remediation Update the affected sudo pa Recommended fixes can be	ckages. found here: https://lists.centos	.org/pipermail/centos-cr-annour	nce/2016-Novemb	er/003522.html			
CVE Vulnerabilities	;					Enter a CVE ID.	2 C
CVE ID	CVSS Value	Disclosed		Vulnerability Descr	iption		
CVE-2016-7091	4.9	2016/12/22 00:00:00 GMT+0	8:00	sudo: It was discov Enterprise Linux ar of INPUTRC which access to a restrict content from speci sudo.	ered that the d id possibly othe could lead to in red program the ally formatted f	efault sudo configuration on Red Ha er Linux implementations preserves formation disclosure. A local user v at uses readine could use this flaw it uses readine could use this flaw	at the value with sudo to read ed by

Step 5 Check the servers affected by the vulnerability.

Figure 7-4 Checking affected servers

Linux Vulnerabilities / CESA-2016:2593 (sudo security update)			
Vulnerability Details Affected Servers			
Ignore Unignore Fix Verify		All statuses	Enter a server name. Q C
Number of Affected Servers	Status	Installed Software	Operation
EcsBindle	Unhandled	sudo:1.8.23-3.el7.x86_64	Ignore Fix Verify
HECS_CentOS-	Unhandled	sudo:1.8.23-3.el7.x86_64	Ignore Fix Verify
_ Bengresseng	Failed View Cause	sudo:1.8.23-3.el7.x86_64	Ignore Fix Verify

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

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

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

----End

Fixing Web-CMS Vulnerabilities

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- Step 3 Open the Web-CMS Vulnerabilities tab.

Dashboard Servers Sans Asets Vulnerabilities Vulnerabilities Server Statistics - Web-CMS Vulnerabilities Unsafe Settings Intrusions Vanced Protection Security Operations Installation and Configuration Web Tamper Web Tamper Ignore Unignore Alt urgencies	Host Security	Vulnerabilities ⑦			
Scans Assets Assets Server Statistics - Web-CMS Vulnerabilities Unsafe Settings Image: Server Swith detection disabled Intrusions Server Swithout critical vulnerabilities Advanced Protection Servers with detection disabled Security Operations Servers with critical vulnerabilities Installation and Configuration Servers with critical vulnerabilities Web Tamper Protection Ignore Unignore All urgencies	Dashboard Servers	Linux Vulnerabilities Windows Vulnera	2 abilities Web-CMS Vulnerabiliti	25	
Unsafe Settings Intrusions • Advanced Protection • Security Operations • Installation and Configuration Web Tamper Protection • Ignore Unignore Unignore Unignore I Enter a vulnerability name. Q C	Scans Assets	Server Statistics - Web-CMS Vulne	erabilities	Top 5 Servers - Web-CMS Vu	Inerabilities
Web Tamper Protection Ignore Unignore All urgencies Ignore Compared and Compa	Unsafe Settings Intrusions • Advanced Protection • Security Operations • Installation and	1 = 5e 5e	rvers with detection disabled rvers without critical vulnerabilities rvers with critical vulnerabilities	No dat	1) ia available.
	Web Tamper Protection	Ignore Unignore		All urgencies	nter a vulnerability name. Q

Figure 7-5 Viewing Web-CMS vulnerability detection results

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

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

Figure 7-6 Vulnerability details

rabilities / wor

Vulnerability Details	Affected Servers			
Basic Details				
Vulnerability name	wordpress		Status	1) Medium
Unhandled Servers	1		Affected Servers	2
Remediation				
undefined undefined				
Vulnerability Details				
Disclosed		Vulnerability Descrip	otion	
2020/04/13 03:09:20 GMT+08:00)	In WordPress throug using the large list o every file many time	h 4.9.2, unauthenticated attackers ca f registered .js files (from wp-includes s.	in cause a denial of service (resource consumption) by s/script-loader.php) to construct a series of requests to load
2020/04/13 02:46:07 GMT+08:00	In WordPress through 4.9.2, unauthenticated attackers can cause a denial of service (resource consumption) by using the large list of registered _is files (from wp-includes/script-loader.php) to construct a series of requests to loa every life many times.			

Figure 7-7 Affected servers

Web-CMS Vulnera	bilities / wordpress			
Vulnerabili	ity Details Affected Servers	1		
Ignore	Unignore		All statuses 💌	Enter a server name. Q
Num	ber of Affected Servers	Status	Path	Operation
	_ West	Ignored	-	Unignore
	lest	Unhandled	-	Ignore

----End

Exporting a Vulnerability Report

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

7.2.2 Fixing Vulnerabilities and Verifying the Result

Linux or Windows vulnerabilities

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

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

NOTICE

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

• Web-CMS vulnerabilities Manually fix them based on the suggestions provided on the page.

Precautions

- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper layer applications. To avoid unrecoverable errors, you are advised to use Cloud Server Backup Service (CSBS) to back up your 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.

Urgency

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

Vulnerability Display

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

Fixing Vulnerabilities in One Click

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

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** On the **Vulnerabilities** page, click **Fix**. The **Affected Servers** tab is displayed, as shown in **Figure 7-8**.

Host Security	Vulnerabilities ⑦		
Dashboard	8		
Servers	Linux Vulnerabilities Windows Vulnerabi	ilities Web-CMS Vulnerabilities	
Scans 1			
Assets	Server Statistics – Linux Vulnerabili	ities	Top 5 Servers – Linux Vulnerabilities
Unsafe Settings			
Intrusions 👻		Servers with detection disabled	
Advanced Protection 🔻	2	Servers with critical vulnerabilities	
Security Operations 👻			No data available.
Installation and Configuration			
Web Tamper Protection 👻	Ignore Unignore		All urgencies
	Vulnerability Name	Urgency Unhandled Servers A	ffected Serv Solution Operation
	CESA-2016:2593 (sudo security update)	O Medium 3	Update the afflected study packages: 3 See the recommendation ABC for information on how to fix the vulnerability.CESA-2010.2593
	CESA-2018:0998 (openssl security upda	O Medium 0	Update the affected opensil packages. 1 See the recommendation ABC for information on how to fix the Fix vulnerability.CESA-2018:0998

Figure 7-8 Fixing vulnerabilities

Step 4 Select the affected servers and click Fix.

Figure 7-9 One-click vulnerability fix

Linux Vulnerabilities / CESA-2016:2593 (sudo security update)				
Vulnerability Details Affected Servers				
Ignore Unignore Fix Verify		All	statuses	Enter a server name. Q C
Number of Affected Servers	Status	Installed Software	(Dperation
HECS_CentOS-7.5-64bit-with-HSS-20200401 Failed View Cause		sudo:1.8.23-3.el7.x86_64		gnore Fix Verify

- Step 5 In the dialog box that is displayed, select I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.
- **Step 6** Click **OK** to fix the vulnerability in one-click mode. The vulnerability status will change to **Fixing**.

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

NOTE

Restart the system after you fixed a Windows or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

----End

Manually Fixing Software Vulnerabilities

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

- Fix the vulnerabilities in sequence based on the suggestions.
- If multiple software packages on the same server have the same vulnerability, you only need to fix the vulnerability once.

NOTE

Restart the system after you fixed a Windows or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

Table 7-2	Vulneral	oility fix	commands
-----------	----------	------------	----------

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

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

Method 1: Create a VM to fix the vulnerability.

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

Method 2: Fix the vulnerability on the target server.

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

NOTE

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

Ignoring Vulnerabilities

Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. Such vulnerabilities can be ignored.

HSS will not generate alarms for ignored vulnerabilities.

Verifying Vulnerability Fix

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

Manual verification

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

Table	7-3	Verification	commands
-------	-----	--------------	----------

OS	Verification Command
CentOS/Fedora/ EulerOS/Red Hat/Oracle	rpm -qa grep <i>Software_name</i>
Debian/Ubuntu	dpkg -l grep <i>Software_name</i>
Gentoo	emergesearch Software_name
SUSE	zypper search -dCmatch-words Software_name

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

Automatic verification

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

7.3 Baseline Inspection

7.3.1 Checking for Unsafe Settings

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

Check Interval

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

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

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

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

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

Alarm Policies

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

NOTE

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

Check Items

ltem	Description
Password complexity policies	Password complexity policies on system accounts
Common weak passwords	Weak passwords defined in the common weak password library
	Common weak passwords of MySQL, FTP, and system accounts
Unsafe settings	Unsafe settings on:
	Tomcat, SSH, Nginx, Redis, Apache2, MySQL5, MongoDB, Windows, vsftp, and CentOS

Table 7-4 Check items

Procedure

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 Choose Scans > Unsafe Settings and check detected unsafe settings.

Figure 7-10 Unsafe settings

Host Security		Unsafe Settings ⑦		
Dashboard			8	
Servers		Password Complexity Po	licy Detection Common Weak Password Detection Co	nfiguration Detection
Scans 1	*			
Assets				Enter a server name. Q
Vulnerabilities		Server Name	Setting	Suggestion
Unsafe Settings Intrusions	2	ecs-ead7	Min. Number of Characters: 8 Min. Number of Uppercase Letters: Not restricted Min. Number of Lowercase Letters: Not restricted	The password should contain at least 3 of the following character types: uppercase letters, lowercase letters, digits, and special characters.
Advanced Protection	Ŧ		Min. Number of Digits: Not restricted Min. Number of Special Characters: Not restricted	Linux - How do I install the PAM and set the password complexity policy?
Security Operations	•			
Installation and Configuration				
Web Tamper Protection	•			

----End

Exporting a Check Report

On the upper right corner of the table on the Configuration Detection tab, click

to download reports.

NOTE

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

7.3.2 Suggestions on Fixing Unsafe Settings

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

Modifying the Password Complexity Policy

- To monitor the password complexity policy on a Linux server, install the Pluggable Authentication Modules (PAM) on the server. For details, see How Do I Install a PAM in Linux?
- 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 Linux?
- 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 Windows?

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

Weak Passwords

• To enhance server security, you are advised to modify the accounts with weak passwords for logging in to the system in a timely manner, such as SSH accounts.

• To protect internal data of your server, you are advised to modify software accounts that use weak passwords, such as MySQL accounts and FTP accounts.

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

Unsafe Configurations

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

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

• Modifying unsafe configuration items

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

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

Figure 7-11 Detection report

s the function of remo	otely connecting to the				
Audit Description: Run the following command and verify that output matches: # grep '^X11Forwarding' /etc/ssh/sshd_config X11Forwarding no					
Recommendation: Edit the /etc/ssh/sshd_config file to set the parameter as follows: X11Forwarding no					
Detection Description Expected Result Detection Result					
X11Forwarding no	X11Forwarding yes				
	nand and verify that o g' /etc/ssh/sshd_config config file to set the pa config file to set the pa	nand and verify that output matches: g' /etc/ssh/sshd_config config file to set the parameter as follows: config file to set the parameter as follows: confi			

• Ignoring trusted configuration items

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

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

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

8 Intrusion Detection

8.1 Alarm Events

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

Alarm Events

Alarm Name	Description	Bas ic	Ent erp ris e	Pre mi um	WT P
Brute-force attack	If hackers log in to your servers through brute-force attacks, they can obtain the control permissions of the servers and perform malicious operations, such as steal user data; implant ransomware, miners, or Trojans; encrypt data; or use your servers as zombies to perform DDoS attacks.	V	V	V	~
	Detect brute-force attacks on SSH, RDP, FTP, SOL Server, and MySOL accounts.				
	 If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. 				
	• You can check whether the IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.				
Abnormal login	Detect abnormal login behavior, such as remote login and brute-force attacks. If abnormal logins are reported, your servers may have been intruded by hackers.	V	V	V	√
	 Check and handle remote logins. You can check the blocked login IP addresses, and who used them to log in to which server at what time. 				
	If a user's login location is not any common login location you set, an alarm will be triggered.				
	• Trigger an alarm if a user logs in by a brute-force attack.				

Alarm Name	Description	Bas ic	Ent erp ris e	Pre mi um	WT P
Malicious program (cloud scan)	Malicious programs include Trojans and web shells implanted by hackers to steal your data or control your servers. For example, hackers will probably use your servers as miners or DDoS zombies. This occupies a large number of CPU and network resources, affecting service stability. Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one click. The malware is found and removed by analysis on program characteristics and behaviors, Al image fingerprint algorithms, and cloud scanning and killing.	×	√ (Is ola te an d kill)	√ (Is ola te an d kill)	√ (Isol ate and kill)
Abnormal process behavior	 Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: Abnormal CPU usage Processes accessing malicious IP addresses Abnormal increase in concurrent process connections 	×	√	√	~

Alarm Name	Description	Bas ic	Ent erp ris e	Pre mi um	WT P
Critical file change	 If hackers intrude into your system, they will probably tamper with important system files to forge identities or prepare for further attacks. Check alarms about modifications on key files (such as ls, ps, login, and top). For details about the monitored paths, see Monitored Important File Paths. Key file change information includes the paths of modified files, the last modification time, and names of the servers storing configuration files. You can add fingerprint libraries of critical files, so that HSS can better collect critical file information and detect exceptions. HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process. 	×	~	~	~
Web shell	 A web shell is a command execution environment in the form of web page files, such as PHP and JSP files. After hacking a website, a hacker usually puts a web shell among normal web page files in the web directory of a website server, and then accesses the web shell through a browser to control the server. Check whether the files (often PHP and JSP files) in your web directories are web shells. Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. You can use the manual detection function to detect web shells on servers. 	×	√	V	√

Alarm Name	Description	Bas ic	Ent erp ris e	Pre mi um	WT P
Reverse shell	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. You can configure the reverse shell detection rule on the Policies page. HSS will check for suspicious or remotely executed commands.	×	×	√	~
Abnormal shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You can configure the reverse shell detection rule on the Policies page. HSS will check for suspicious or remotely executed commands.	×	×	~	~
High-risk command execution	You can configure what commands will trigger alarms in the High-risk command detection rule on the Policies page. HSS checks executed commands in real time and generates alarms if high-risk commands are detected.	×	×	V	~
Auto-startup check	Trojans usually intrude servers by creating auto-started services, scheduled tasks, or preloaded dynamic libraries. The auto-startup check function collects information about all auto-started items, including their names, types, and number of affected servers. HSS checks and lists auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	×	×	~	~
Unsafe account	Hackers can probably crack unsafe accounts on your servers and control the servers. HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them.	×	\checkmark	\checkmark	\checkmark

Alarm Name	Description	Bas ic	Ent erp ris e	Pre mi um	WT P
Privilege escalation	After hackers intrude servers, they will try exploiting vulnerabilities to grant themselves the root permissions or add permissions for files. In this way, they can illegally create system accounts, modify account permissions, and tamper with files. HSS detects privilege escalation for processes and files in the current system. The following abnormal privilege	×	×	V	√
	 escalation operations can be detected: Root privilege escalation by exploiting SUID program vulnerabilities 				
	 Root privilege escalation by exploiting kernel vulnerabilities 				
	File privilege escalation				
Rootkit	HSS detects suspicious rootkit installation in a timely manner by checking:	×	×	√	\checkmark
	Rootkits based on file signatures				
	Hidden files, ports, and processes				

Monitored Important File Paths

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

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

8.2 Checking and Handling Intrusion Events

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of servers with alarms, handled alarms, unhandled alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarm events generated in the last 30 days.

The status of a handled event changes from **Unhandled** to **Handled**.

Constraints and Limitations

- To skip the checks on high-risk command execution, privilege escalation, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. Then HSS will not check the servers associated with disabled policies.
- Other detection items cannot be manually disabled.

Checking Alarm Events

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Intrusions** > **Events**, as shown in **Figure 8-1**.

Figure 8-1 Events page

Host Security	Events
Dashboard Servers	Alarm Statistics
Scans 💌	Affacted Servers 16 Alarms to be Handled 773 Handled Alarms 78
Intrusions 1 .	Blocked IP Addresses 1 Isolated Files 0
Whitelists	Full protection enabled
Advanced Protection Security Operations Installation and Configuration	Image: Safe From (13) Image: Brute-force attack Image: Abnormal login Image: Malicious program (cloud scan) Image: Abnormal process behavior Image: Critical file change Image: Web Shells Image: Reverse shell Safe From (13) Image: Abnormal shell Image: High-risk command execution Image: Abnormal autostant Image: Umage: Uma
Web Tamper Protection 🔹	Events
	Last 30 days Server name Alledad Server & IP Q C All 851 You can click Blocked IP addresses to review or unblock the IP addresses flagged as sources of attacks. C
	Brute-force attack 7 Alarm Type Affected Server & IP Event Details Reported Handled Status 🖓 Action Operation
	Abnormal login 8 Abnormal a HSS Type: Run registry key, Even 2020/05/19 Unhandled Handle

Table 8-1 Alarm events

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

Alarm Event	Description
Handled Alarms	Number of handled alarms.
Blocked IP Addresses	Number of blocked IP addresses. You can click the number to check blocked IP address list.
	If a valid IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can manually unblock it. If a server is frequently attacked, you are advised to fix its vulnerabilities in a timely manner and eliminate risks.
	NOTICE After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the Events page. You can click Isolated Files on the upper right corner to check them.
	You can recover isolated files. For details, see Managing Isolated Files.

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

Figure 8-2 Alarm event statistics

Events

All	3202		You can clici	La k Blocked IP addresses to review o	st 30 days runblock the IP add	 Server dresses flagged a 	name 🔻 Af	fected Server & IP ks.	QC
Brute-force attac	12	Alarm Type	Affected Server & IP	Event Details	Reported	Handled	Status 🏹	Action	Operation
Abnormal login	85	Unsafe acco	test 192.168.1.169	Username: 📕 User startup s	2020/04/14	-	Unhandled		Handle
Malicious progra (cloud scan)	m 15	Unsafe acco	test 192.168.1.169	Username: ttt, User startup sh	2020/04/14		Unhandled		Handle
Abnormal proces behavior Critical file chan	s 18 ne 39	Unsafe acco	EPS_Test 192.168.1.98	Username: 34,	2020/04/14		Unhandled		Handle
Web Shells	2183	Unsafe acco	EPS_Test 192.168.1.98	Username: U	2020/04/14		Unhandled	-	Handle
Reverse shell	3	Unsafe acco	EPS_Test 192.168.1.98	Username:	2020/04/14	-	Unhandled		Handle
Abnormal shell	12	Unsafe acco	EPS_Test 192.168.1.98	Username 📕, User startup s	2020/04/14		Unhandled		Handle

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



Figure 8-3 Alarm details

----End

Handling Alarm Events

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

NOTE

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

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Intrusions** > **Events**.

Figure 8-4 Events page

Host Security	Events		
Dashboard Servers	Alarm Statistics		
Scans 🔻	Affected Servers	16 Alarms to be Handled	773 Handled Alarms 78
Intrusions 1 .	Blocked IP Addresses	1 Isolated Files	0
Whitelists	Full protection enabled		
Advanced Protection Security Operations Installation and Configuration	Safe From (13)	k Abnormal login Malicious program (cloud scan) High-risk command execution Abnormal autostart	Abnormal process behavior Critical file change Web Shells Reverse shell Unsafe account Privilege escalation Rootkit detection
Web Tamper Protection 🔹	Events		
	All 851	You can click Blocked IP addresses	Last 30 days • Affected Server & IP Q C to review or unblock the IP addresses flagged as sources of attacks.
	Brute-force attack 7	Alarm Type Affected Server & IP Event Details	Reported Handled Status 🏹 Action Operation
	Abnormal login 8 A	Kbnormal a HSS-V 192.168.1.68 Type: Run registry	r key, Even 2020/05/19 Unhandled Handle

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

NOTE

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

Events								
All 054	Batch processing		Last	30 days 👻	Server nar	me 🔻 🛛 Affec	ted Server & IP	QC
All 851		You can click Block	ked IP addresses to review or	unblock the IP addres	ses flagged as s	ources of attacks		
Brute-force attack 7	Alarm Type	Affected Server & IP	Event Details	Reported	Handled	Status 🏹	Action	Operation
Abnormal login 8	Abnormal	HSS-11111111111111111111111111111111111	Type: Run registry key, Ev	e 2020/05/1	-	Unhandled		Handle
Malicious program (cloud 6 scan)	Abnormal	2 Windows-a 192.168.1.188	Type: Run registry key, Ev	e 2020/05/1		Unhandled		Handle
Abnormal process behavior3	Abnormal	HSS-WIN-	Type: Run registry key, Ev	e 2020/05/1	-	Unhandled	-	Handle
Web Shells 396	Abnormal	Windows- 192.168.1.188	Type: Run registry key, Ev	e 2020/05/1	-	Unhandled	-	Handle
Reverse shell 2	Abnormal	Windows-	Type: Run registry key, Ev	e 2020/05/1	-	Unhandled		Handle
Abnormal shell 7	Abnormal	HSS- 192.168.1.68	Type: Run registry key, Ev	e 2020/05/1		Unhandled		Handle
High-risk command execution 26	Abnormal	ecs-	Type: Autostarted service,	2020/05/1	2020/05/1	Handled	Mark as h	Handle
Abnormal autostart 164 Unsafe account 127	Abnormal	ecs-	Type: Autostarted service,	2020/05/1	-	Unhandled		Handle
Privilege escalation 2	Abnormal	ecs-	Type: Autostarted service,	2020/05/1	-	Unhandled		Handle
Rootkit detection 20	Abnormal	Windows-	Type: Run registry key, Ev	e 2020/05/1	-	Unhandled	-	Handle

Figure 8-5 Handling alarm events

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

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

Method	Description						
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.						
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the Isolated Files slide-out panel and cannot harm your servers.						
	You can click Isolated Files on the upper right corner to check the files. For details, see Managing Isolated Files .						
	The following types of alarm events support online isolation and killing:						
	Malicious program (cloud scan)						
	Abnormal process behavior						
	NOTE When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any).						
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.						
Add to whitelist	Add false alarmed items of the Brute-force attack and Abnormal login types to the login whitelist.						
	HSS will no longer report alarm on the whitelisted items.						
Add to alarm	Add false alarmed items of the following types to the login whitelist.						
whitelist	HSS will no longer report alarm on the whitelisted items.						
	Reverse shell						
	Web shell						
	Abnormal process behavior						
	Process privilege escalation						
	File privilege escalation						
	High-risk command						
	Malicious program						

Table 8-2 Event handling methods

----End

Handling Suggestion

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

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

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

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

8.3 Managing Isolated Files

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

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

- Malicious program (cloud scan)
- Abnormal process behavior

Isolating and Killing Files

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Intrusions** > **Events**.

Figure 8-6 Events page

Host Security	Events
Dashboard Servers	Alarm Statistics
Scans 👻	Affected Servers 16 Alarms to be Handled 773 Handled Alarms 78
Itrusions 1	Blocked IP Addresses 1 Isolated Files 0
Whitelists	Full protection enabled
Ivanced Protection	Image: Safe From (13) Image: Safe From (13)
nfiguration eb Tamper Protection 🛛 👻	Events
	Last 30 days Server name Affected Server & IP Q C All 851 You can click Blocked IP addresses to review or unblock the IP addresses flagged as sources of attacks. C
	Brute-force attack 7 Alarm Type Affected Server & IP Event Details Reported Handled Status 🖓 Action Operation
	Abnormal login 8 Abnormal a HSN Type: Run registry key, Even 2020/05/19 Unhandled Handle

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

Figure 8-7	Isolating	and killing	malicious	programs
------------	-----------	-------------	-----------	----------

		Batch	processing				Last 30 days	•	Server nam	e 🔻 Affecte	d Server & IP	Q (
All	86			You ca	n click Blocked IF	addresses to re	view or unblock th	e IP addresses	flagged as so	urces of attacks.		
Brute-force attack	0		Alarm Type	Affected	Server & IP	Event Deta	ils	Reported	Handled	Stat 7	Action	Operation
Abnormal login	0		Abnormal	 192.168.	0.162	Hash: 484	5dbb7c2e3e064	Aug 26, 2		Unhandled	2	Handle
Malicious program (c scan)	loud 1									×		
Abnormal process	3		Handle	Alarm								
behavlor		·	Alarm Type	е	Status	IP addr	ess	Event	t Details			
Critical file change	9		Abnormal	process	Unhandled	192.16	3.0.162	Hash	: 4845dbb7c2e	e3e064d88		
Web Shells	0		Action		Mark as handled	I O Ignore	Add to Al	arms Whitelist	 Isolat 	te and Kill 3		
Reverse shell	0		If you mark	this alarm	as handled, it wi	ll no longer be r	eported.					
Abnormal shell	33		Remarks									
High-risk command execution	2									1		
						OK	Cancel					

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

----End

Checking Isolated Files

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

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

Figure 8-8 Checking isolated files

Isolated Files									
Server Name	Path	Modify Time	Operation						
test	/root/inotify_x64	2020/04/14 09:54:11 GMT+08	Restore						

----End

Recovering Isolated Files

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

Step 2 Click OK.

NOTE

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

----End

8.4 Configuring the Alarm Whitelist

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

Whitelisted events will not trigger alarms.

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

Adding Events to the Alarm Whitelist

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

Table 8-3 Configuring the alarm whitelist

Checking the Alarm Whitelist

Perform the following steps to check the alarm whitelist:

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- Step 3 On the Whitelists page, click Alarm Whitelist.

-								
Host Security	v	Vhitelists						
Dashboard		3						
Servers		Alarm Whitelist	Login Whitelist					
Scans	•	Import Export A	II Delete		All tunes	Hach - Entar a keyward	0	C
Intrusions 1	*	Export	Delete		- All types +		4	<u> </u>
Events		Alarm Type	SHA256	CmdLine	Data Source	Mark Time	Operation	
Whitelists 2		Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
Advanced Protection	*	Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
Security Operations	•	Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
Installation and Configuration		Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
Web Tamper Protection	•	Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
		Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
		Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	
		Web Shells	66baecfe7208c00e139b898509626e	-	Import	2020/05/19 18:10:57 GMT+08:00	Delete	

Figure 8-9 Alarm whitelist

----End

Importing and Exporting the Alarm Whitelist

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

NOTICE

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

Format:

"Alarm_type","SHA256',"Command_line","Data_source","Marking_time"
"webshell","66baecfe7208c00e139b898509626ee4d2ea81382ef15a4283b95d50f669b121",""," <i>File</i>
<i>imported</i> ',"2020/02/28 07:32:44 GMT+08:00"

- The alarm whitelist supports incremental import. If the same record is imported again, only one entry will be displayed for it.
- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- Step 3 On the Whitelists page, click the Alarm Whitelist tab, as shown in Figure 8-10.

5		5			
Host Security		Whitelists			
Dashboard		8			
Servers		Alarm Whitelist			
Scans	•	Import Export All Delete		All types	Enter a keyword. Q
Events		Alarm Type SHA256 CmdLi	ne Data S	ource Mark Time	Operation
Whitelists 2		Web Shells 66baec(e7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
Advanced Protection	•	Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
Security Operations	•	Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
Installation and Configuration		Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
Web Tamper Protection	•	Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
		Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
		Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete
		Web Shells 66baecfe7208c00e139b898509626e	Import	2020/05/19 18	:10:57 GMT+08:00 Delete

Figure 8-10 Clicking the Alarm Whitelist tab

- Click **Export All** to export the current alarm whitelist as a .csv file.
- Click **Import** and select the exported Excel file to import the alarm whitelist. In the displayed dialog box, click **Upload** and select a file. After the import is complete, you can check the imported alarms in the whitelist.

NOTE

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

----End

Follow-Up Procedure

Removing alarms from the whitelist

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

NOTE

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

8.5 Configuring the Login Whitelist

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

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

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

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

Adding Login Information to the Login Whitelist

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** On the **Whitelists** page, click the **Login Whitelist** tab and click **Add**, as shown in **Figure 8-11**.

Figure 8-11 Login whitelist

Host Security	Whitelists				
Dashboard	3				
Servers	Alarm Whitelist Login White	elist			
Scans					
Intrusions 1	Add Delete			Server IP address 🔹	QC
Events	Server IP Address	Logged IP Address	Login Username	Created Time	Operation
Whitelists 2	192.168.1.1	192.168.1.2	hss	2020/04/14 09:13:39 GMT+08:00	Delete
Advanced Protection					
Security Operations					
Web Tamper Protection	,				

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

NOTE

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

 Add to Login Whitelist

 * Server IP address
 192.168.1.1

 * Logged IP address
 192.168.1.2

 * Login username
 http://test

 DK
 Cancel



Step 5 Click OK.

----End

Other Operations

Removing login information from login whitelist

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

NOTE

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

9 Advanced Protection

9.1 Application Recognition Service

9.1.1 Checking the Whitelist Policy List

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

Function Description

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

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

NOTE

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

Checking the Whitelist Policy List

Step 1 Log in to the management console.

- Step 2 In the upper left corner of the page, select a region, click =, and choose Security > Host Security Service.
- **Step 3** On the **Programs** page, click the **Whitelist Policies** tab, as shown in **Figure 9-1**.

Host Security	Programs 💩 Process				
Dashboard		8			
Servers	Events Servers Protected	Whitelist Policies			
Scans 💌	Crosta Ballov				
Intrusions •	Create Policy				
Advanced Protection	Policy Name Servers Prote	cted Status	Applications	Status	Operation
Programs 2	qqqqq	0 🌐 Learning	Trusted 25		Edit Delete
Critical Files	qin01	0 the Learning	Trusted 29		Edit Delete
Ransomware Security Operations •	qin01	0 🚓 Learning	Trusted 59		Edit Delete
Installation and	99999	0 🔅 Learning			Edit Delete
Web Tamper Protection •	eewwwwwwwwww	0 🔅 Learning	Trusted 30 Untrusted 1		Edit Delete
	test	0 🔅 Learning complete. Policy not i	Trusted 66		Edit Delete

Figure 9-1 Checking the whitelist policy list

Table 9-1 Policy list parameters

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

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

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

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

Figure	9-2	App	lication	list
--------	-----	-----	----------	------

Whitelist Policies / xiang1			
Applications Servers Protected			
Mark Total 29 Trusted 27 Untrusted 2 Unknown 0			С
File SHA256	Marked As 🛛	Operation	
03d1316407796b32c03f17f819cca5bede2b0504ecdb7ba3b845c1ed618ae934	Trusted	Mark	
1128499ac255bb11f25cd617f766b15f65f9eab1e0a531200c3878e80c96e41e	Trusted	Mark	
132db6b472cc7d90b67a05cd8216964ec46305053555d2a9433c12eb894cd7c4	Trusted	Mark	
25dfb8168246e5d04dd6f124c95e4c4c4e8273503569acd5452205558d099871	Trusted	Mark	
38d1695f08ec655945ca7a40e7d9485696ffa0bfb7dc809e4cbdba09ea160bc9	Trusted	Mark	

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

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

- **Suspicious Operations** include startup of processes that are not in the whitelist policy or marked as **Untrusted** or **Unknown**.
- Action in the following figure indicates that HSS will report an alarm when detecting suspicious operations.
Figure 9-3 Checking protected servers

Whi	telist Policies / xiang1						
	Applications Servers Protected						
	Add Server			Server name	▼	Q	С
	Affected Server	Suspicious Operations	Action		Operation		
	win-4447 14	0	Alarm		Delete		

NOTE

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

```
----End
```

9.1.2 Applying a Whitelist Policy

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

Prerequisites

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

Creating a Whitelist Policy

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** On the **Programs** page, click the **Whitelist Policies** tab, and click **Create Policy**, as shown in **Figure 9-4**.

Host Security	Programs & Process				
Dashboard		8			
Servers	Events Servers Protected	Whitelist Policies			
Scans • Intrusions •	Create Policy				Enter a policy name. Q
Advanced Protection 1 .	Policy Name Servers Prot	acted Status	Applications	Status	Operation
Programs 2	qqqqq	0 🔅 Learning	Trusted 25		Edit Delete
Critical Files	qin01	0 🔅 Learning	Trusted 29		Edit Delete
Ransomware Security Operations •	qin01	0 🔅 Learning	Trusted 59		Edit Delete
Installation and	qqqqq	0 the Learning	-		Edit Delete
Web Tamper Protection •	eewwwwwwwwww	0 🍀 Learning	Trusted 30 Untrusted 1		Edit Delete
	test	0 Cearning complete. Policy not i	Trusted 66		Edit Delete

Figure 9-4 Creating a whitelist policy

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

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

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

Figure 9-5 Configuring a policy

olicies / Create Policy			
Policy Details			
* Policy Name	hss_test		
Intelligent Learning Period 👩	● 7 days ○ 15 days ○ 30 days		
Add Server			
Add Server			
Server name	IP Address	System	Operation
windows	.73.76	Windows	Delete
Create and Learn Cancel			

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

NOTICE

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

vailable Servers(1)		Selected Servers (1)	1	
Ungrouped Enter a server	r name. Q C	Enter a server nam	e.	Q
Affected Server & IP	System	Server Name	System	Operation
windows 192.168.0.99	Windows	windows	Windows	×
ecs-a883 192.168.0.167	Linux			

Figure 9-6 Adding servers for policy learning

Step 6 Click OK.

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

Step 7 Click Create and Learn.

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

Step 8 Wait until the whitelist policy learning is complete and the policy status becomes

Learning complete. Policy not in effect, and click **O** to enable the whitelist policy.

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

----End

Associating Servers

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

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

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

Figure 9-7 Associating servers

Host Security	Programs & Process				
Dashboard		3			
Scans v	Events Servers Pr	btected Whitelist Policies			
Intrusions 👻	Create Policy				Enter a policy name. Q C
Advanced Protection	Policy Name Servers	Prote Status	Applications	Status	Operation
Programs 2	eewwwwww	0 CE Learning	Trusted 30 Untrusted 1		Edit Delete
Critical Files	test	0 🚯 Learning complete. P	Trusted 66		Edit Delete
Security Operations	% () 8*——d	0 CE Learning	Trusted 27		Edit Delete
Installation and	test2	0 🛛 🎲 Learning complete. P	Trusted 27 Untrusted 1		Edit Delete
Web Tamper Protection 🔻	xiang1	0 SLearning complete. P	Trusted 27 Untrusted 2		4 Applications Edit Delete
	sdf	0 Elearning	Trusted 63		Edit Delete

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

Vhitelist policy xiang1		Action	Alarm	•	
Available Servers(1) Ungrouped	me. Q C	Select	ted Servers (1)		
Affected Server & IP	System	Server	r Name	System	Operation
win-	Windows	win-4	613	Windows	×
.155.92	Windows				

Figure 9-8 Associating servers

Step 3 Click OK.

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

----End

Follow-Up Procedure

Managing protected servers

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

You can check the server names and IP addresses, whitelist policy, number of suspicious operations, and the way to handle the operations.

To remove a protected server, click **Remove** in the **Operation** column. After a
whitelist policy is deleted, the applications on the servers associated to it will
no longer be protected.

Editing a whitelist policy

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

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

Deleting a whitelist policy

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

9.1.3 Checking and Handling Application Events

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

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

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

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

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

Checking Application Events

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 On the Programs page, click the Events tab, as shown in Figure 9-9.

lost Security		Pro	gram	S 🗞 Proc	ess							
ashboard			6									
ervers		1	Even	ts Servers	Protected	Whitelist Policies						
cans	*		Hane	die				Last 24 ho	urs 🔻	Server name 🔻		Q
ntrusions	*											
dvanced Protection				Program path	Marked As	Affected Serv	Matched Whit	Reported ↓Ξ	Event Details		Status 🍞	Operation
Programs 2				C:\Windows\Sy	Unknown	win-406713 192.168.1.38	88WWWWWW	2020/06/28 09:	Hash:, PID: 4	, User: SYSTEM, File permissio	I Handled (is	Handle
Critical Files Ransomware				C:\Windows\Sy	Unknown	win-406713 192.168.1.38	eewwwwww	2020/06/28 09:	Hash: a10b1b8	993ad18b6422844b67c42091a	() Unhandled	Handle
acurity Operations	•			C:\Windows\Sy	Unknown	win-406713 192.168.1.38	eewwwwww	2020/06/28 09:	Hash:, PID: 1	92, User:, File permission: 20	() Unhandled	Handle
eb Tamper Protection	Ţ			C:\Windows\Sy	Unknown	win-406713 192.168.1.38	eewwwwww	2020/06/28 09:	Hash: cbb1f47	if531b8b4c6d4376ef3a6346189	() Unhandled	Handle
				C:\Windows\Sy	Unknown	win-406713 192.168.1.38	eewwwwwww	2020/06/28 09:	Hash:, PID: 2	88, User:, File permission: 20	() Unhandled	Handle

Figure 9-9 Application event management page

 Table 9-2 Application event parameters

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

----End

Handling Application Events

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

Figure 9-10 Handling an application event

Host Security	Programs 🗞 Process								
Dashboard	3								
Servers	Events Servers Pro	otected Whitelist F	Policies						
Scans • Intrusions •	Handle					Last 24 hours v Server name v		Q	С
Advanced Protection	Program path	Marked As	Affected Server & IP	Matched Whitelist	Reported J≣	Event Details	Status 7	Operation	
Programs 2	/usr/local/hostguard	Unknown	192.168.1.10	test	2020/06/18 19:41:4	Hash: 53a078bf39745f64d60fa77ef4a5d7548ae91259b21	() Unhandled	Handle	
Critical Files Ransomware	/usr/local/hostguard	Unknown	192.168.1.10	test	2020/06/18 18:41:4	Hash: 53a078bf39745f64d60fa77ef4a5d7548ae91259b21	Handled (isolat	Handle	
Security Operations -	/usr/local/hostguard	Unknown	192.168.1.10	test	2020/06/18 17:41:3	Hash: 53a078bf39745f64d60fa77ef4a5d7548ae91259b21	Handled (marked)	Handle	
Configuration Web Tamper Protection	/usr/local/hostguard	Unknown	192.168.1.10	test	2020/06/18 16:41:3	Hash: 53a078bf39745f64d60fa77ef4a5d7548ae91259b21	Handled (marked)	Handle	
	/usr/local/hostguard	Unknown	192.168.1.10	test	2020/06/17 17:37:4	Hash: 53a078bf39745f64d60fa77ef4a5d7548ae91259b21	Handled (marked)	Handle	

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

Handle Event				×
Event Type	Matched Whitel	Reported	Status	
application_whit	test	2020/06/18 19:4	🕛 Unhandled	
Action Trusted Don't isolate or kil	◯ Untrusted ◯ Un	known 🔵 Isolate and	d Kill	
	ОК	Cancel		

Figure 9-11 Handling an application event

Table 9-3 Event handling actions

Action	Description
Trusted	Marks an application as trusted. The application startup will no longer trigger alarms.
Untrus ted	Marks an application as untrusted. The application startup will trigger alarms.
Unkno wn	Marks an application as unknown. The application startup will trigger alarms.
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the Isolated Files slide-out panel and cannot harm your servers.
	You can click Isolated Files on the upper right corner to check the files. For details, see Managing Isolated Files .
	NOTE When an application is isolated and killed, it is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious files (if any).
Don't	Cancels the isolation and killing of an application.
isolate or kill	NOTE Exercise caution when performing this operation. If you restore a malicious application, it will harm your servers.

Step 3 Click OK.

----End

9.2 File Integrity Monitoring

9.2.1 Adding a Monitored File

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

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

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

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

The registry monitoring function will be available soon.

NOTICE

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

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

Enabling FIM

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** On the **Critical Files** page, click **C** to enable FIM, as shown in **Figure 9-12**. The default setting is **C**.

Figure 9-12 Enabling FIM

Host Security		Critical Files 3				
Dashboard						
Servers			Changes	Actions		
Scans	•	Servers	Total Changes	35 0 32 Modify Create	3 Delete	
Intrusions	*		Files:35 Regis	stries:0		
Advanced Protection	0					
Programs						
Critical Files 2		Server Modified Files				
Security Operations	•				Enter a server name.	Q Search 😸 C
Installation and Configuration		Server name	Changes	Modified Files	Modified Registries	Last Modified
Web Tamper Protection	•	ecs-	35	35	0	2020/05/19 16:24:33 GMT+08:00

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

----End

Adding a Monitored File

To add a management file, ensure that:

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

Perform the following steps to add a monitored file:

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 In the navigation pane, choose Security Operations > Policies.
- Step 4 On the Policies page, click the policy group deployed on your servers. Take the default policy group of the premium edition group as an example, as shown in Figure 9-13.

Figure 9-13 Default policy group

Host Security	Policies					
Dashboard	Delete				Enter a policy group na	ame. Q C
Servers	Policy Group Name	ID	Description	Supported Version	Servers	Operation
Scans -	default_enterprise_poli	7d142628-01d0-493b-991b-731b	0.000	Enterprise	1	
Advanced Protection	default_premium_polic	9c99173c-8316-481d-8bc1-264b	Contraction in the local distribution of the	Premium	0	Сору
Security Operations	console_test1	a81c376b-9a3c-4088-ae0b-75b4		Premium	0	Copy Delete
Reports	console_test2	ff719896-7339-467b-aa49-1238a	-	Premium	0	Copy Delete
Policies 2	console_test5	86511270-d71e-4446-b8aa-0ec7		Premium	0	Copy Delete
Installation and Configuration	aaa	1e5fcd60-c53b-4272-8ddb-3830	aaa	Premium	0	Copy Delete
Web Tamper Protection 👻	PP []	77412672-3774-41f3-b81a-153a	www	Premium	0	Copy Delete
	222	260ddbcb-3f8d-45ef-8c43-b262a	222	Premium	1	Сору

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

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

		Policy Dotails		
		Policy Details		
Policy Name	Status	Status	Enabled	
Assets	Enabled	Function Category	Intrusion dete	ection
System Configuration Detection	Enabled			
Weak Password Detection	Enabled	Policy ID	aaefac24-202	23-496d-8a03-8faf1868109e
High-risk command detection	Enabled	Policy Settings		
Privilege escalation detection	Enabled	Full Detection Ir	nterval (s):	3600
Abnormal shell detection	Enabled	File Status Chec	k Interval (s):	20
Integrity check on critical files	Enabled	Detection Break	Time (ms):	50
Web Shell Detection	Enabled	File Path:		/bin/ls /usr/bin/ls /bin/ps /usr/bin/ps /usr/bin/bash /usr/bin/bash

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

Step 6 Click OK.

----End

Follow-Up Procedure

Disabling FIM

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

9.2.2 Checking Change Statistics

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

Checking Change Statistics

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Go to the **Critical Files** page to check change statistics, as shown in **Figure 9-15**.

Figure 9-15 Checking change statistics

Host Security	Critical Files 3				
Dashboard					
Servers	1	Changes	Actions		
Scans •	Servers	Total Changes	35 0 32 Modify Create	3 Delete	
Intrusions 👻		Files:35 Regi	itries:0		
Advanced Protection					
Programs					
Critical Files 2	Server Modified Files				
Security Operations 👻				Enter a server name.	Q Search ≽ C
Installation and Configuration	Server name	Changes	Modified Files	Modified Registries	Last Modified
Web Tamper Protection 🔹	ecs-	35	35	0	2020/05/19 16:24:33 GMT+08:00
Web Tamper Protection 🔹	ecs-	35	35	0	2020/05/19 16:24:33 GMT+08:00

Table 9-4 Change statistics

ltem	Description				
Servers	al number of managed servers				
Changes	 Changes: total number of modifications in monitored files Files: total number of files Registries: total number of registries 				
Actions	 Modify: total number of changes in monitored files Create: total number of created files Delete: total number of deleted files 				

----End

Checking Modified Files on a Single Server

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

Figure 9-16 Server list

Server Modified Files				
			Enter a server name.	Q Search ≽ C
Server name	Changes	Modified Files	Modified Registries	Last Modified
ec:	35	35	0	2020/05/19 16:24:33 GMT+08:00

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

NOTE

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

Figure 9-17 Server change details

Crit	ical Files / ecs						
	Changes35 Modified Files35	Modified Registries0		1	Name	▼ Enter a file name.	Q Search ⊗ C
	File	Path	Change Description	Туре		Action	Time Range
	55	/usr/sbin/ss	-	File		Delete	2020/05/19 16:24:33 GMT+0
	SS	/usr/sbin/ss	-	File		Create	2020/05/18 17:08:25 GMT+0
	SS	/usr/sbin/ss	-	File		Delete	2020/05/18 16:49:56 GMT+0
	SS	/usr/sbin/ss		File		Create	2020/05/15 19:03:07 GMT+0
	SS	/usr/sbin/ss		File		Delete	2020/05/15 18:57:36 GMT+0

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

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

D NOTE

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

----End

Checking All the Modified Files

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

Figure 9-18 Changed files

Server Modified	Files					
				Name 👻	Enter a file name.	Q Search ≽ C
Name	Path	Change Description	Server name	Туре	Action	Time Range
\$\$	/usr/sbin/ss		ecs-t 7	File	Delete	2020/05/19 16:24:33 G
55	/usr/sbin/ss		ecs-	File	Create	2020/05/18 17:08:25 G
SS	/usr/sbin/ss	-	ecs-	File	Delete	2020/05/18 16:49:56 G
SS	/usr/sbin/ss	-	ecs	File	Create	2020/05/15 19:03:07 G
\$\$	/usr/sbin/ss		ecs-(7	File	Delete	2020/05/15 18:57:36 G

NOTE

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

9.3 Ransomware Prevention

9.3.1 Checking Protection Policies

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

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

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

Prerequisites

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

Checking the Policy List

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** On the **Ransomware** page, click the **Policies** tab. The ransomware prevention policy list is displayed, as shown in **Figure 9-19**.

Figure	9-19	Policy	list
--------	------	--------	------

Host Security	Ra	nsomware 🍖 Process	5										
Dashboard		Events 3 Policies											
Servers		Create Ballay								los o polícu pomo			C
Scans 👻		create Policy								ter a policy name.		u (<u> </u>
Intrusions 👻		Policy Name	Servers Protected	Servers Being Studied	Trusted Processes		Monitored File	Extension	Action		Operation		
Advanced Protection		2	C		0	0	C:\2	23	Report alarm		Edit Delete		
Programs		4	c		0	0	c:\4	4	Report alarm		Edit Delete		
Critical Files		6	c		0	0	c:\7	7	Report alarm		Edit Delete		
Ransomware 2		aaa	c		2	0	-	log	Report alarm		Edit Delete		
Security Operations 🔹		aaw1	c		0	0	c\11x	18xss;ss	Report alarm		Edit Delete		
Installation and Configuration		aaw1	0		0	0	c.\sd2e	ddoxc	Report alarm		Edit Delete		
Web Tamper Protection 🔹		dasd	c		0	0	-	sd	Report alarm		Edit Delete		
		dddddddddddddssss	C		0	0	-	sd	Report alarm		Edit Delete		

Table 9-5 Policy parameters

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

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

- **Step 4** Click a policy name to check its details and process files, as shown in Figure 9-20.
 - You can check the policy name, intelligent learning period, protection status, monitored file path, file name extension, and update time.
 - You can check the total number of processes, number of trusted processes, number of untrusted processes, process files, signature issuer, process hash, and trust status.
 - You can mark a process file as **Trusted** or **Untrusted**. An alarm will be generated if an untrusted process is started.

Policies / nomod-test						
Policy Details 🖉						
Policy Name	nomod	Monitored File	C:\Program Files (x86)\HostGuard;C:\Pr	ogramData		
Intelligent Learning Period	7 days	Extension	ini;db;log;js;txt;html;conf			
Action	Report alarm	Updated	2020/06/19 16:49:45 GMT+08:00			
Process File A	ssociated Servers					
Mark Total Nur	nber of Processes 11 Trusted 10 Untrusted 1					C
Process File	Signature Issuer	Pro	cess Hash	Marked As 🛛	Operation	
hostguard.exe	technologies co., ltd.	-		Trusted	Mark	
hostwatch.exe	technologies co., ltd.	-		Trusted	Mark	
iexplore.exe	microsoft corporation	-		Trusted	Mark	
explorer.exe	microsoft windows	-		Trusted	Mark	
msmpeng.exe	microsoft windows publisher	-		Trusted	Mark	

Figure 9-20 Protection policy details

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

Figure 9-21 Checking associated servers

Policies / nomod-test							
Policy Name nomod-test		Monitored Fil	le C:\Program Files (x86)\HostGuard;C:\Pro	ogramData			
Intelligent Learning Period 7days		Extension	ini;db;log;js;txt;html;conf				
Action Report alarm		Updated	2020/06/19 16:49:45 GMT+08:00				
Process File Associated Servers							
Add Server Learn Again Delete					Server name 🔹	Enter a server name.	QC
Server name	IP Address	S	ystem	Status		Operation	
win-406713	192.168.1.38	W	Vindows	Learning		Learn Again Delete	

Table 9-6 Associated servers

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

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

----End

9.3.2 Creating a Protection Policy

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

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

Creating a Protection Policy

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** On the **Ransomware** page, click the **Policies** tab, and click **Create Policy**, as shown in **Figure 9-22**.

Figure 9-22 Policy management

Host Security	F	Ransomware 🗞 Proces	55									
Dashboard		Events 3 Policies										
Servers	4	Create Policy							Enter a poli	icy name.	Q	С
Intrusions v		Policy Name	Servers Protected	Servers Being Studie	ed Trusted Processes		Monitored File	Extension	Action	Operation		
Advanced Protection		2		0	0	0	C:\2	23	Report alarm	Edit Delete		
Programs		4		0	0	0	c:\4	4	Report alarm	Edit Delete		
Critical Files		6		0	0	0	c:\7	7	Report alarm	Edit Delete		
Ransomware 2		aaa		0	2	0		log	Report alarm	Edit Delete		
Security Operations 🔹		aaw1		0	0	0	c/11x	18xss;ss	Report alarm	Edit Delete		
Installation and Configuration		aaw1		0	0	0	c:\sd2e	ddixxc	Report alarm	Edit Delete		
Web Tamper Protection 🔹		dasd		0	0	0	-	sd	Report alarm	Edit Delete		
		dddddddddddddssss		0	0	0		sd	Report alarm	Edit Delete		

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

Figure 9-23 Configuring a ransomware prevention policy

Policy Details					
★ Policy Name	hss_test				
Intelligent Learning Period	● 7 days ○ 15 days ○ 30 days				
Action	Report alarm 🔻				
Monitored File	c:\hss				
	Separate file paths with semicolons (;).				
* Extension	log;ls				
	Separate extensions with semicolons (;).				

Table 9-7 Basic information parameters

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

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

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

vailable Servers(2)		Selected Servers (1))	
Ungrouped Enter a server nar	me. QC	Enter a server nam	е.	Q
Affected Server & IP	System	Server Name	System	Operation
win-406713 192.168.1.38	Windows	win-406713	Windows	×
192.168.0.250	Windows			

Figure 9-24 Associating servers

Step 6 Click OK.

NOTE

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

Step 7 Click Create and Learn.

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

Events Policies									
Create Policy							Enter a policy name	e.	QC
Policy Name	Servers Protected	Servers Being Studied	Trusted Processes	Monito	red File	Extension	Action	Operation	
2	0	0		0 C:\2		23	Report alarm	Edit Delete	
4	0	0		0 c:\4		4	Report alarm	Edit Delete	
6	0	0		0 c:\7		7	Report alarm	Edit Delete	
aaa	0	1		0		log	Report alarm	Edit Delete	
aaw1	0	0		0 c:\11x		18xss;ss	Report alarm	Edit Delete	

Figure 9-25 Ransomware prevention policy list

Table 9-8 Policy list parameters

Parameter	Description
Policy Name	Intelligent learning policy name
Servers Protected	Number of servers protected by the policy
Servers Being Studied	Number of servers where the learning is performed
Trusted Processes	Number of trusted processes. After the intelligent learning policy takes effect, HSS automatically identifies and counts trusted processes on your server.
Monitored File	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored.
	the policy are monitored.
Extension	Extension of monitored files. Multiple paths are separated by semicolons (;).
Action	Action taken when suspicious operations on monitored files are detected.
	For example, report alarms.

----End

Associating Servers

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

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

		5 1						
Host Security	Ransomware & Proces	55						
Dashboard	Events 3 Policies							
Servers Scans 🗸	Create Policy						Enter a policy name	e. Q C
Intrusions 👻	4 Name	Servers Protected	Servers Being Studied	Trusted Processes	Monitored File	Extension	Action	Operation
Advanced Protection	2	0	0	0	C:12	23	Report alarm	Edit Delete
Programs	4	0	0	0	c:\4	4	Report alarm	Edit Delete
Critical Files	6	0	0	0	c:\7	7	Report alarm	Edit Delete
Ransomware 2	888	0	1	0	**	log	Report alarm	Edit Delete
Security Operations 🔹	aaw1	0	0	0	c:\11x	18xss;ss	Report alarm	Edit Delete
Installation and Configuration	aaw1	0	0	0	c:\sd2e	ddixic	Report alarm	Edit Delete

Figure 9-26 Accessing the policy details page

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

Figure 9-27 Adding associated servers

Policies / hss-test						
Policy Details 🖉						
Policy Name hss-test		Monitored File				
Intelligent Learning Period 7days		Extension	log			
Action Report alarr	Action Report alarm		2020-12-04 16:18:09 GMT+08:00			
0						
Process File Associated Se	rvers					
Add Server Learn Again	Delete		Server name 💌 Enter a	a server name. Q C		
Server name	IP Address	System	Status	Operation		
ecs-8285-windows	192.168.1.209	Windows	t Learning	Learn Again Delete		

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

Available Servers(2)		Selected Servers (1)		
Ungrouped Enter a server name.	QC	Enter a server name).	Q
Affected Server & IP	System	Server Name	System	Operation
win-406713 192.168.1.38	Windows	win-406713	Windows	×
192.168.0.250	Windows			

Figure 9-28 Associating servers

Step 4 Click OK.

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

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

----End

Follow-Up Procedure

Editing a policy

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

Deleting a policy

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

9.3.3 Checking and Handling Protection Events

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

NOTE

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

Checking Ransomware Prevention Events

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 On the Ransomware page, click the Events tab, as shown in Figure 9-29.

Figure 9-29 Ransomware prevention events

Host Security	Ransomware & Process							
Dashboard	3 Events Policies							
Servers	Handle				Lost 24 hours	- Canvas nama	- Feler a conver nom	
Scans 💌	Harrold				Last 24 nouis	* Server name	Enter a server nam	
Intrusions 👻	File Path	Affected Server & IP	Process Path	Signature Issuer	Matched Policy	Reported J⊟	Status 🖓	Operation
Advanced Protection	C:\program files (x86)\h	192.168.0.250	c:\program files\window	-	nomod-j-test	2020/06/19 16:51:54 G	I Handled	Handle
Programs Critical Files	C:\program files (x86)\h	192.168.0.250	c:\program files\window		nomod-lest	2020/06/19 16:51:54 G	I Handled	Handle
Ransomware 2	C:\program files (x86)\h	192.168.0.250	c:\windows\explorer.exe	microsoft windows	nomodtest	2020/06/19 16:38:17 G	() Unhandled	Handle
Installation and Configuration	C:\program files (x86)\h	192.168.0.250	c:\program files (x86)\ho	huawei technologies co	nomod-test	2020/06/19 16:37:59 G	() Unhandled	Handle
Web Tamper Protection 🔹	C:\program files (x86)\h	192.168.0.250	c:\program files (x86)\ho	huawei technologies co	nomod-test	2020/06/19 16:37:59 G	() Unhandled	Handle
	C:(program files (x86))h	192.168.0.250	c:\program files (x86)\ho	huawei technologies co	nomod-li -test	2020/06/19 16:37:59 G	() Unhandled	Handle

Table 9-9 Ransomware prevention event parameters

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

Handling Ransomware Prevention Events

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

Host Security	1	Ransomware & Process							
Dashboard		3 Events Policies							
Servers									
Scans	•	Handle				Last 24 hours	Server name	 Enter a server nam 	e. Q C
Intrusions	-	File Path	Affected Server & IP	Process Path	Signature Issuer	Matched Policy	Reported JΞ	Status 🖓	Operation
Advanced Protection		C:\program files (x86)\h	192.168.0.250	c:\program files\window		nomodtest	2020/06/19 16:51:54 G	I Handled	Handle
Programs Critical Files		C:\program files (x86)\h	192.168.0.250	c:\program files\window	-	nomodlest	2020/06/19 16:51:54 G	I Handled	Handle
Ransomware 2		C:\program files (x86)\h	192.168.0.250	c:\windows\explorer.exe	microsoft windows	nomodtest	2020/06/19 16:38:17 G	() Unhandled	Handle
Installation and Configuration		C:\program files (x86)\h	192.168.0.250	c:\program files (x86)/ho	huawei technologies co	nomodtest	2020/06/19 16:37:59 G	() Unhandled	Handle
Web Tamper Protection	•	C:\program files (x86)\h	192.168.0.250	c:\program files (x86)\ho	huawei technologies co	nomodtest	2020/06/19 16:37:59 G	() Unhandled	Handle
		C:\program files (x86)\h	192.168.0.250	c:\program files (x86)\ho	huawei technologies co	nomod-	2020/06/19 16:37:59 G	() Unhandled	Handle

Figure 9-30 Checking ransomware prevention events



Figure 9-31 Handling ransomware events

🛕 Are yo	u sure you wa	nt to mark the following	g process files?	×
File Path		Process Path	Affected Server & IP	
C:\program files (x86)\hostguard\l		c:\windows\explorer.exe	192.168.0.250	
Marked As	Trusted	O Untrusted		
		OK Cancel		

Table 9-10 Event handling parameters

Marke d As	Description
Trusted	An application marked as trusted will not trigger alarms if it performs operation on files under monitored paths.
Untrus ted	An application marked as untrusted will trigger alarms if it performs operation on files under monitored paths.

Step 3 Click OK.

----End

10 Security Operations

10.1 Checking or Creating a Policy Group

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

Precautions

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

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

Policy List

Policy	Action	Supported OS	Enterpri se Edition	Premiu m Edition	WTP Edition
Weak password detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.	Linux and Windows	√ (Check only custom weak password s)	\checkmark	√

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

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

Accessing the Policies Page

- **Step 1** Log in to the management console.
- Step 2 In the upper left corner of the page, select a region, click =, and choose Security > Host Security Service.

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

----End

Checking the Policy Group List

Step 1 On the **Policies** page, check the policy group list, as shown in **Figure 10-1**. For more information, see **Table 10-1**.

NOTE

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

Figure 10-1 Policy group list

Host Security	Policies						
Dashboard	Delete					Enter a policy group name. Q	
Servers	Policy Group Name	ID	Description	Supported Version	Servers	Operation	
Scans 🔻	default_enterprise_policy	7d142628-01d0-493b-991b	0.000000	Enterprise	5		
Intrusions •	default_premium_policy_gr.		3420.0960	Flagship	0	Сору	
Security Operations		4e018df2-2732-4fb7-bf61	-	Flagship	0	Copy Delete	
Reports	console_test1	a81c376b-9a3c-4088-ae0b	-	Flagship	0	Copy Delete	
Policies 2	console_test2	ff719896-7339-467b-aa49	-	Flagship	0	Copy Delete	
Installation and Configuration	cosole_test3	ed20e844-faa2-4380-ad51	-	Flagship	0	Copy Delete	
Web Tamper Protection 👻	console_test5	8651f270-d71e-4446-b8aa	-	Flagship	0	Copy Delete	

Table 10-1 Policy group parameters

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

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

NOTE

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

Figure 10-2 Policy group details

Pol	cies / default_premium_policy_group					
					С	
	Policy Name	Status 🏹	Function Category	O\$ Type	Operation	
	Assets	Enabled	Asset management	Linux, Windows	Disabled	
	System Configuration Detection	Enabled	Unsafe setting scan	Linux, Windows	Disabled	
	Weak Password Detection	Enabled	Unsafe setting scan	Linux, Windows	Disabled	
	High-risk command detection	Enabled	Data collection	Linux	Disabled	
	Privilege escalation detection	Enabled	Intrusion detection	Linux	Disabled	
	Abnormal shell detection	Enabled	Intrusion detection	Linux	Disabled	
	Integrity check on critical files	Enabled	Intrusion detection	Linux	Disabled	
	Web Shell Detection	Enabled	Intrusion detection	Linux, Windows	Disabled	

Step 3 Click the name of a policy to check its details. The **Weak Password Detection** policy is used as an example.

NOTE

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

Figure 10-3 Policy details

Policies / default_premium_policy_group	Policies / default_premium_policy_group Weak Password Detection				
		Policy Details			
Policy Name S	Status	Status	Enabled		
Assets E	nabled	Function Category	Unsafe setting scan		
System Configuration Detection	nabled	5.7			
Weak Password Detection	Enabled	Policy ID	1ccddcbe-8005-4271-ad22-	11500a90bdb1	
High-risk command detection E	Enabled	Policy Settings			
Privilege escalation detection E	Enabled	Use Basic Weak	Password Dictionary:		
Abnormal shell detection E	Enabled	Updated URL of	Weak Password Dictionary:	https://MASTERADDR:443/public/lib-	
Integrity check on critical files	Enabled	Weak Password	Dictionary SHA256:	3d4c623b09f2c5bcd521d47c9289a71	
Web Shell Detection E	Enabled	Detection Day:		🖌 Mon. 💙 Tue. 💙 Wed. 💙 Thu. 💙 Fri. 💙 Sat. 🏹 Sun.	
		User-defined we	ak password:		
		MySQL Weak Pa	ssword Detection		
				OK Cancel	

Creating a Policy Group

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

Figure	10-4	Copying	а	policy	group
--------	------	---------	---	--------	-------

Host Security	Policies	
Dashboard	Delete	Enter a policy group name. Q
Servers	Policy Group Name ID Description Supported Version	Servers Operation
Scans •	default_enterprise_policy_gr 7d142628-01d0-493b-991b Enterprise	5
Advanced Protection	default_premium_policy_gr 9c99173c-8316-481d-8bc1 Flagship	1 3 Copy
Security Operations	4e018df2-2732-4fb7-bf61-9 Flagship	0 Copy Delete
Reports	console_test1 a81c376b-9a3c-4088-ae0b Flagship	0 Copy Delete
Policies 2	console_test2 ff719896-7339-467b-aa49-1 Flagship	0 Copy Delete
Installation and Configuration	cosole_test3 ed20e844-faa2-4380-ad51-c Flagship	0 Copy Delete
Web Tamper Protection 🔹	console_test5 8651f270-d71e-4446-b8aa-0 Flagship	0 Copy Delete
	cosole_test4 08ccbf0e-b292.4cf8-a1f6-7 Flagship	0 Copy Delete
	asa 1e5fcd60-c53b-4272-8ddb-3 aaa Flagship	0 Copy Delete
	qq 77412672-3774-41f3-b81a www Flagship	0 Copy Delete
	10 V Total Records: 19 < 1 2 >	

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

NOTE

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

Figure 10-5 Creating a policy group

Copy Policy Grou	р	×
★ Policy Group Name		
Description	OK Cancel	

Step 3 Click OK.

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

Figure 10-6 Policies in a group

Pol	icies / default_premium_policy_group					
						C
	Policy Name	Status 🖓	Function Category	OS Type	Operation	
	Assets	Enabled	Asset management	Linux, Windows	Disabled	
	System Configuration Detection	Enabled	Unsafe setting scan	Linux, Windows	Disabled	
	Weak Password Detection	Enabled	Unsafe setting scan	Linux, Windows	Disabled	
	High-risk command detection	Enabled	Data collection	Linux	Disabled	
	Privilege escalation detection	Enabled	Intrusion detection	Linux	Disabled	
	Abnormal shell detection	Enabled	Intrusion detection	Linux	Disabled	
	Integrity check on critical files	Enabled	Intrusion detection	Linux	Disabled	
	Web Shell Detection	Enabled	Intrusion detection	Linux, Windows	Disabled	

- **Step 5** Click a policy name and modify its settings as required. For details, see **Modifying a Policy**.
- **Step 6** Enable or disable the policy by clicking the corresponding button in the **Operation** column.

----End

Follow-Up Procedure

Deleting a policy group

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

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

Figure 10-7 Deleting policy groups

Host Security	Policies					
Dashboard	3 Delete					Enter a policy group name. Q
Servers	Policy Group Name	ID	Description	Supported Version	Servers	Operation
Scans 💌	default_enterprise_policy	7d142628-01d0-493b-991b	企业版策略组	Enterprise	5	
Intrusions •	default_premium_policy_gr	. 9c99173c-8316-481d-8bc1	旗舰版策略组	Flagship	0	Сору
Advanced Protection	Ihwtest	4e018df2-2732-4fb7-bf61		Flagship	0	Copy Delete
Reports	console_test1	a81c376b-9a3c-4088-ae0b	-	Flagship	0	Copy Delete
Policies 2	✓ console_test2	ff719896-7339-467b-aa49	-	Flagship	0	Copy Delete
Installation and Configuration	cosole_test3	ed20e844-faa2-4380-ad51	-	Flagship	0	Copy Delete
Web Tamper Protection 🔹	console_test5	8651f270-d71e-4446-b8aa		Flagship	0	Copy Delete

NOTE

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

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

----End

10.2 Modifying a Policy

You can modify policies in a policy group.

NOTICE

Modifications on a policy take effect only in the group it belongs to.

Accessing the Policies Page

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Security Operations** > **Policies**.

----End

Asset

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- Step 2 Click Assets.
- Step 3 In the Policy Settings area, modify the settings as required, as shown in Figure 10-8. For more information, see Table 10-2.

Figure 10-8	Assets							
Assets								
Policy Details								
Status	Enabled							
Function Category	Asset							
Policy ID	Policy ID 1019c3bb-9eac-4509-bb01-dd42b38d0e6f							
Policy Settings								
Asset Scan Set	tings							
Detection Time:		00:01						
Detection Day:		Mon. 🔽	Tue. 🔽	Wed. 🔽	Thu. 🔽	Fri. 🔽	Sat. 🔽	Sun.
Software Whose	Information to Be Collected:							

Open Ports	
Obtain UDP Port:	
Port Information Check Interval (s):	30 You can open the program running authentication policy to obtain more comprehensive process data.
	OK Cancel

/usr/local,/usr/bin,/usr/sbin,/usr/lib

Not for the Windows servers.

Software Name

openssl

Add

If this parameter is not specified, information about all installed software is obtained.

Software Main Prog...

openssl

Execute Command

version

Ор...

Del...

Table 10-2 Assets parameters

Software Search Path:

Main Applications/Components:

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

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

Step 4 Click OK.

----End

System Configuration Detection

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- Step 2 Click System Configuration Detection.
- **Step 3** In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-9**. For more information, see **Table 10-3**.

Figure 10-9 System Configuration Detection

System Configuration Detection

Policy Details		
Status	Enabled	
Function Category	Conf	
Policy ID	c591ec54-e84d-4ca7-ac43-80272971697f	
Policy Settings		
Detection Time:	00:10	
Detection Day:	💙 Mon. 💙 Tue. 💙 Wed. 💙 Thu. 💙 Fri. 💙 Sat. 💙	Sun.
Enable 0	perating System	Name
	inux	ssh
	inux	nginx
L	inux	tomcat
Z L	inux	apache2
L	inux	redis
L	inux	mysql5
L	inux	mongodb
	inux	vsftp

OK Cancel

centos7

Table 10-3 System	configuration	detection	parameters
-------------------	---------------	-----------	------------

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

Step 4 Select the OSs to be checked.

Linux

Step 5 Click OK.

----End

Weak Password Detection

Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no less security risks than any type of vulnerabilities. Data and programs will become insecure if their passwords are cracked.

HSS proactively detects the accounts using weak passwords and generates alarms for the accounts. You can also add a password that may have been leaked to the weak password list to prevent server accounts from using the password.

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- Step 2 In the policy group list, click Weak Password Detection.
- **Step 3** In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-10**. For more information, see **Table 10-4**.

Weak Password Detection			
Policy Details			
Status	Enabled		
Function Category	Unsafe setting scan		
Policy ID	1ccddcbe-8005-4271-ad22-1	11500a90bdb1	
Policy Settings			
Use Basic Weak Password Dictionary:			
Updated URL of Weak Password Dictionary:		https://MASTERADDR:443/public/lib-	
Weak Password Dictionary SHA256:		3d4c623b09f2c5bcd521d47c9289a71	
Detection Day:		💙 Mon. 🗹 Tue. 💙 Wed. 💙 Thu. 💙 Fri. 💙 Sat. 💙 Sun.	
User-defined weak password:			
MySQL Weak Pa	ssword Detection		
		OK Cancel	

Figure 10-10 Weak password detection

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

Table 10-4 Weak password detection parameters

Step 4 Click OK.

----End

High-risk Command Detection

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- Step 2 Click High-risk command detection.
- **Step 3** In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-11**. For more information, see **Table 10-5**.
Figure 10-11 High-risk command detection

Policy Settings

Reporting or Logging of Process Termination:	
Re-reporting via the Message Channel:	
Interval for Reporting Process Statistics (Minute)	600
Max. CPU Usage of Independent Process (%)	10
Max. Memory Usage of Independent Process (%)	300
Data Receiving IP & Port of Independent Process	
Max. Independent Process Data Sending Rate (kbit/s)	4
Log Compaction:	
Collecting Process Network Info	
Record Logs:	
Log File Path:	/usr/local/hostguard/log/hc
Maximum Size of a Log File (MB):	20
High-Risk Commands:	
Whitelist (Do Not Record Logs):	Process Path or Regular Expression in CLI Operation
	Add
	OK Cancel

Table 10-5 High-risk command detection parameters

Parameter	Description
Reporting or	Reports or records process termination.
Termination	• C: enable
	• Constant disable

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

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

Step 4 Click OK.

----End

Privilege Escalation Detection

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- **Step 2** Click **Privilege escalation detection**.
- **Step 3** In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-12**. For more information, see **Table 10-6**.

y Detaits		
tus	Enabled	
nction Category	Intrusion	detection
licy ID	c43d8261-c296-4d1b-8b72-b5f0e402c4ef	
olicy Settings	File Dette	/usr/lib64/hal/hald-runner
Ignored Process	File Path:	/usr/sbin/hald /opt/nfast/sbin/privconn /usr/sbin/dhclient

Figure 10-12 Privilege escalation detection

 Table 10-6 Privilege escalation detection parameters

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

Cancel

Step 4 Click OK.

----End

Abnormal or Reverse Shell Detection

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- Step 2 Click Abnormal shell detection.
- **Step 3** In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-13**. For more information, see **Table 10-7**.

Abnormal shell detection	
Policy Details	
Status Enabled	
Function Category Intrusion detection	
Policy ID 63feeddc-6c4c-4407-8	3477-7d14eb8f5639
Policy Settings	
Reverse Shell Ignored Process File Path:	/usr/bin/gnome-terminal /usr/local/spes/spesservice /usr/local/syscheck/messageservice /usr/local/hostguard/bin/hostguard /usr/bin/uvp-monitor /opt/zabbix/sbin/zabbix_acentd
Reverse Shell Scanning Period (s):	30
Abnormal Shell Detection:	
Max. open files per process:	4000
	OK Cancel

Figure 10-13 Abnormal or reverse shell detection

Table 10-7 Abnormal or reverse shell detection parameters

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

Step 4 Click OK.

----End

File Integrity Monitoring

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

Step 2 Click Integrity check on critical files.

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

FIGURE TO-14 INTEGRILY CHECK ON CHUICAL HIE	Figure	10-14	Integrity	check	on	critical	files
--	--------	-------	-----------	-------	----	----------	-------

Integrity check	k on critica	al files	
Policy Details			
Status	Enabled		
Function Category	Intrusion dete	ction	
Policy ID	aaefac24-2023	3-496d-8a03-8faf1868109e	
Policy Settings			
Full Detection Int	erval (s):	3600	
File Status Check	Interval (s):	20	
Detection Break T	lime (ms):	50	
File Path:		/bin/ls /usr/bin/ls /bin/ps /usr/bin/ps /bin/bash /usr/bin/bash	
		ок	Cancel

Table	10-8	File	integrity	monitoring	parameters
-------	------	------	-----------	------------	------------

Parameter	Description
Full Detection Interval (s)	Interval between two consecutive full scans on specified files. The value range is 3,600 to 100,000.
	For example, setting it to 3600 means the full scan is performed every hour.
File Status Check Interval (s)	Interval for checking file status. The value range is 10 to 600.
Detection Break Time (ms)	Interval between the checks of two files. The value range is 0 to 1000.
	For example, if this parameter is set to 50 , the system checks /usr/bin/ls 50 milliseconds after it checks /bin/ls .

Parameter	Description		
File Path	Path of the files to be checked		
	NOTE		
	 Exercise caution when modifying its settings. Its default values are all critical files and you are not advised to delete any of them. 		
	 HSS does not monitor changes on the files that are not specified here. 		

Step 4 Click OK.

----End

Web Shell Detection

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

- **Step 1** In the policy group list, click the name of the group that contains the required policy.
- Step 2 Click Web Shell Detection.
- **Step 3** In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-15**. For more information, see **Table 10-9**.

Web Shell De	tection
Policy Details	
Status	Enabled
Function Category	Intrusion detection
Policy ID	7fb9f09d-3090-4698-8fa8-56475491bcdb
Policy Settings Asset Discovery	Linkage:
Monitored Web	Directory Path:
Detected File Na	ime Extension: jsp.jspx,jspf,php,php5,pl
Monitor File Mo	dification:
	OK Cancel

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

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

Table 10-9 Web shell detection parameters

Step 4 Click OK.

----End

11 wtp

11.1 Adding a Protected Directory or File System

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

You can specify directories or network file systems to protect.

Constraints and Limitations

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

Setting a Protected Directory

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click \equiv , and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-1	Web	Tamper	Protection	page
-------------	-----	--------	------------	------

Host Security		Server Protection ⑦	
Dashboard			
Servers		Blocked Attacks 0 Protected Servers 1 Protected Directories 1	
Scans	•		
Intrusions	•	Enable Disable Server name	3
Advanced Protection	•	Server Name IP Address OS 🖓 Server St Agent 🖓 WT 🖓 Dynamic W Edition/Expir Operation	
Security Operations	Ŧ	est-a88369.141 (E) Linux Running Online 🥥 Enab Disabled Web Tamper Disable Configure Protection View Report	
Installation and Configuration		windows 73.76 (EIP Windows Running Online O Disa. Disabled None Enable Configure Protection View Report	
Server Protection		test-40314 68.202 (El Unux Running Not installed O Disa Disabled None Enable Configure Protection View Report	
Installation and Configuration			

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

Figure 11-2 Setting a protected directory

Protected Directory Settings 1 Privileged Process Settings Enabled but not in effect Dynamic WTP							
2	0						
Type 💿 Directory 🔿 File system							
3							
Add Protected Directory	Enable Remote Backup	Up to 50 protected directories of	can be added. Local backup is per	formed by default. Enable remot	e backup as needed.		
Protected Directory	Excluded Subdirectory	Excluded File Types	Local Backup Path	Protection Status	Operation		
/home	-	-	/home1	📀 Enabled	Suspend Protection Edit Delete		

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

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

Figure 11-3 Adding a protected directory

Protected Directory:	d:\hss\test
	An operating system directory, such as C:\Windows, cannot be protected.
Excluded Subdirectories:	Example: \xxx\xxx
	Enter the relative path of the subdirectory of a protected directory. Separate multiple subdirectories with semicolons (;).
Excluded File Types:	Example: log; js
	Use semicolon (;) to separate file types.
Local Backup Path	d:\backup
	The local backup path cannot include the protected subdirectory. Otherwise, the local backup will fail.

Table 11-1 Parameters for a protected directory

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

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

2. Click **OK**.

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

Step 6 Enable remote backup.

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

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

1. Click Enable Remote Backup.

Figure 11-4 Enabling remote backup

Protected Directory Settings	Privileged Process Setting	s Enabled but not in eff	ect Dynamic WTP		
Type 💿 Directory 🔾 Fil	e system				
Add Protected Directory	Enable Remote Backup	Up to 50 protected directories	can be added. Local backup is pe	rformed by default. Enable remot	e backup as needed.
Protected Directory	Excluded Subdirectory	Excluded File Types	Local Backup Path	Protection Status	Operation
/home		-	/home1	Senabled	Suspend Protection Edit Delete
/opt	-	-	/home1	Enabled	Suspend Protection Edit Delete

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

Figure 11-5 Setting remote backup

Enable Remote Backup				
Server address/port:	ecs-a883(192.168.0.167:48486) 🔻			
Create/Modify Remot	e Backup Server			
	OK Cancel			

3. Click OK.

----End

Setting a Protected File System

D NOTE

Only network file systems running on Linux can be protected.

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click \equiv , and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-6 Web Tamper Protection page

Host Security		Ser	ver Pr	otection ⑦									
Dashboard Servers			Blo	cked Attacks <mark>0</mark>	Protected	d Servers 1	Protecte	ed Directories 1					
Scans	÷		Enab	Disable							Server name	▼ Enter a keyword.	QC
Advanced Protection	*			Server Name	IP Address	os 🗸	Server St	Agent 🍞	WT 77	Dynamic W	Edition/Expir	Operation	
Security Operations	*			ecs-a883 1c4cc66e-28e5-4	.69.141 (E	Unux	Running	Online	🕑 Enab	Disabled	Web Tamper	Disable Configure Protection	View Report
Installation and Configuration Web Tamper Protection				windows e9e40ddf-c4d3-4	.73.76 (EI 192.168.0.99 (Pr	Windows	Running	Online	O Disa	Disabled	None	Enable Configure Protection	View Report
Server Protection				test-40314 12ef6caf-1ef8-43	.68.202 (E 192.168.0.48 (Pr	Unux	Running	Not installed	O Disa	Disabled	None	Enable Configure Protection	View Report
Installation and Configuration													

Step 4 Set Type to File system.

Figure 11-7 Setting a protected file system

Protected Directory Settings Prive	ileged Process Settings Enabled	d but not in effect Dynamic WTP		
Type O Directory 🖲 File system				
Add File System Up to five file s	ystems can be added. OS partitions are r	not allowed.		
File System Name	Unprotect Subdirectory	Unprotect File Type	Protection Status	Operation
sfs	-	-	📀 Enabled	Suspend Protection Edit Delete

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

		×
Add Protected Dire	ctory	
* Protected Directory:	sts	
	Enter a file system name.	
	System disks are not allowed.	
Excluded Subdirectories:	Example: /xxx/xxx	
	Enter the relative path of the subdirectory of a protected	
	directory. Separate multiple subdirectories with	
	semicolons (;).	
Excluded File Types:	log	
Excluded file types.		
	Use semicolon (;) to separate file types.	
	OK Cancel	
	Cancer	

Figure 11-8 Adding a file system

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

Table 11-2 Parameters for a protected directory

NOTICE

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

Step 6 Click OK.

----End

Follow-Up Procedure

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

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

NOTICE

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

11.2 Adding a Remote Backup Server

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

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

Prerequisites

The following servers can be used as remote backup servers:

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

NOTICE

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

Configuring a Remote Backup Server

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Installation and Configuration**. Click the **Backup Server** tab and click **Add Backup Server**.

Figure 11-10 Configuring a backup server

Host Security	Installation and Configu	uration ⑦					
Dashboard Servers	Install Agent A	larm Notification	3 Backup Server				
Scans 🔻							
Intrusions 👻							
Advanced Protection 🔹							
Security Operations 🔹	Configure servers here if	you have enabled remote ba	ckup for protected directorie	15.			
Installation and Configuration	Add Backup Server						С
Web Tamper Protection	Server Name	Address	Port	Backup Path	Status	Operation	
Server Protection	ecs-a883	192.168.0.167	48486	/backup	Running	Edit Delete	
Installation and Configuration							

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

Figure 11-11 Adding a remote backup server

Server Name	ecs-a883 🔹
IP ⑦	192.168.0.167 🔹
Port	48486 Set a vacant port not blocked by any security group or firewall.
Backup Path	Example: /xxx/xxx This path cannot overlap protected directories of the server.

Table 11-3 Parameters for a remote backup server

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

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

Step 5 Click OK.

----End

Enabling Remote Backup

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

	Figure	11-12	Web	Tamper	Protection	page
--	--------	-------	-----	--------	------------	------

Host Security	Server Protection ⑦
Dashboard	
Servers	Blocked Attacks O Protected Servers 7 Protected Directories 7
Scans •	Enable Disable Enter a keyword. Q C
Advanced Protection	Server Name IP Address OS 🖓 Server St Agent 🖓 WT 🖓 Dynamic W Edition/Expir Operation
Security Operations 👻	Configure Protection View Report
Installation and Configuration	windows 73.76 (EIP windows Running Online O Disa Disabled None Enable Configure Protection View Report
Server Protection	test-40314 68.202 (El Unux Running Not Installed O Disa Disabled None Enable Configure Protection View Report
Installation and Configuration	

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

Figure 11-13 Enabling remote backup

Protected Directory Settings	Privileged Process Setting	s Enabled but not in effe	ect Dynamic WTP		
Type 💿 Directory 🔾 Fi	ile system				
Add Protected Directory	Enable Remote Backup	Up to 50 protected directories	can be added. Local backup is p	erformed by default. Enable remo	te backup as needed.
Protected Directory	Excluded Subdirectory	Excluded File Types	Local Backup Path	Protection Status	Operation
/home	-	-	/home1	S Enabled	Suspend Protection Edit Delete
/opt	-	-	/home1	S Enabled	Suspend Protection Edit Delete

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

Figure 11-14 Setting remote backup

Enable Remote	e Backup
Server address/port:	ecs-a883(192.168.0.167:48486)
Create/Modify Remot	e Backup Server
	OK Cancel

Step 4 Click OK.

----End

Follow-Up Procedure

Disabling remote backup

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

11.3 Adding a Privileged Process That Can Modify Protected Files

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

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

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

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

Prerequisites

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

Adding a Privileged Process

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-15 Web Tamper Protection page

Host Security	Server Protection ⑦
Dashboard	
Servers	Blocked Attacks 0 Protected Servers 1 Protected Directories 1
Scans 👻	
Intrusions -	Enable Disable Server name + Enter a keyword. Q
Advanced Protection	Server Name IP Address OS 🖓 Server St Agent 🖓 WT 🖓 Dynamic W Edition/Expir Operation
Security Operations	ecs-a88369.141 (El Linux Running Online S Enab Disabled Web Tamper Disable Configure Protection View Report
Installation and Configuration Web Tamper Protection	e9e40ddf-cdd-4 192.168.0.99 (Pr): Windows Running Online O Disa Disabled None Enable Configure Protection View Report
Server Protection	test-40314 68.202 (El Linux Running Not installed O DIsa Disabled None Enable Configure Protection View Report
Installation and Configuration	

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

Figure 11-16 Adding a privileged process							
Protected Directory Settings Privileged Process S	Enabled but not in effect Dynamic WTP						
Add Privileged Process Privileged processes can access pr	otected directories. You can add a maximum of 10 paths of privileged process files.						
Process File Path	Operation						
/user	Edit Delete						

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

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

Step 6 Click OK.

----End

Follow-Up Procedure

Modifying or deleting existing privileged processes

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

NOTE

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

11.4 Setting Scheduled WTP Protection

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

NOTE

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

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

F igure 11-17 Web	Tamper	Protection	page
--------------------------	--------	------------	------

Host Security		Serve	r Protection ⑦									
Dashboard Servers			Blocked Attacks 0	Protected	l Servers 1	Protecte	d Directories 1					
Intrusions	-		Enable Disable	2					Se	erver name	▼ Enter a keyword.	QC
Advanced Protection	*		Server Name	IP Address	os 🔽	Server St	Agent 🔽	wт Г	Dynamic W	Edition/Expir	Operation	
Security Operations	•		ecs-a883 1c4cc66e-28e5-4	.69.141 (E 192.168.0.167 (P	Linux	Running	Online	🕑 Enab	Disabled	Web Tamper	Disable Configure Protection	View Report
Installation and Configuration Web Tamper Protection			windows e9e40ddf-c4d3-4	.73.76 (EI	Windows	Running	Online	O Disa	Disabled	None	Enable Configure Protection	View Report
Server Protection			test-40314 12ef6caf-1ef8-43	.68.202 (E 192.168.0.48 (Pr	Linux	Running	Not installed	Disa	Disabled	None	Enable Configure Protection	View Report
Installation and Configuration												

Step 4 Enable scheduled protection.



Step 5 Click OK.

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

Figure 11-19 Setting scheduled protection parameters

Protected Directory Settings Privileged Process Settings Enabled but not in effect Dynamic WTP						
Scheduled Protection Periodically stop static WTP so that you can update and release web pages during unprotected periods.						
Add Unprotected Period You can add 4 more periods.						
Unprotected Period	Description	Operation				
15:00-16:00	-	Modify Delete				
Days in a Week to Disable Protection						
Monday Tuesday Wednesday Thursday Friday Saturday OK						

----End

Rules for Setting an Unprotected Period

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

11.5 Enabling Dynamic WTP

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

Prerequisites

You are using a server running on Linux.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-20 Web Tamper Protection page

Host Security		Server Protection ⑦	
Dashboard			
Servers		Blocked Attacks 0 Protected Servers 1 Protected Directories 1	
Scans	*		
Intrusions	*	Enable Disable Server name	
Advanced Protection	*	Server Name IP Address OS 🖓 Server St Agent 🖓 WT 🖓 Dynamic W Edition/Expir Operation	
Security Operations	Ť	ecs-a883 69.141 (El Linux Running Online 🥑 Enab Disabled Web Tamper Disable Configure Protection View Report	
Configuration		windows 73.76 (EIP e9e40ddf-c4d3-4 192.168.0.99 (Pr) Windows Running Online O Disa. Disabled None Enable Configure Protection View Report	
Server Protection		test-40314 68.202 (El Unux Running Not installed O Disa. Disabled None Enable Configure Protection View Report.	
Installation and Configuration			

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

Figure 11-21 Dynamic WTP

Protected Directory Settings Privileged Process Settings Enabled but not in effect	Dynamic WTP
Protect your data while Tomcat is running, detecting dynamic data tampering in databases.	
Dynamic WTP 🚺 After you enable it, restart Tomcat to make the setting take effect.	

Step 5 Restart Tomcat for the function to take effect.

----End

11.6 Viewing WTP Reports

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

- Step 2 In the upper left corner of the page, select a region, click =, and choose Security > Host Security Service.
- **Step 3** On the WTP console, Choose **Server Protection**. Click **View Report** in the **Operation** column.

Host Security		Serv	er Prot	ection (?)									E	🍞 Wizard
Dashboard														
Servers			Bl	ocked Attacks <mark>()</mark>	Protected	Servers 3	Protected Di	rectories 1						
Scans	•													
Intrusions	•		Enable	Disable							Server name	 Enter a keyword. 	Q	С
Advanced Protection	•		S	erver Name/ID	IP Address	os 7	Server Status	Agent Status 🏼 🏹	WTP St 7	Dynamic WTP	Edition/Expiration	Operation		
Security Operations	•			ISS-QYDXMU-001 92fe418-647e-4ee7-9a	192.168.1.241 (Private)	Linux	Stopped	Offline	Enabled	Disabled	Web Tamper Prote 20 days until expiration	Disable Configure Protection	View Report	3
Web Tamper Protection	*			IECS_Windows-2012-F i4724561-909b-4dfa-81	192.168.1.36 (EIP)	Windows	Running	Offline	🕑 Enabled	Disabled	Web Tamper Prote	Disable Configure Protection	View Report	
Installation and Configuration				ISS-Agent-AutoTest 1953746-8e4f-4a0f-84	144.31 (EIP) 192.168.1.64 (Private)	Linux	Stopped	Offline	Enabled	Disabled	Web Tamper Prote 16 days until expiratio	Disable Configure Protection	View Report	

Figure 11-22 Viewing a protection record

Step 4 View details on the report page.

Figure 11-23 Static WTP records

Static WTP Dynamic WTP	
Blocked Tampering Attacks: $oldsymbol{0}$	
For the convenience of local tests, you can set privileged processes.	Aug 06, 2020 09:35:26 - Aug 13, 2020 09:36:09 X 🗎 Query
Detected	Protected File

Figure 11-24 Dynamic WTP records

Static WTP	Dynamic WTP				
Detected Tamp	ering Attacks: ${\it 0}$				
	All severities	▼ All attack res ▼	Aug 06, 2020 09:35:26 -	Aug 13, 2020 09:40:50	X 🗎 Query
Alarm Time	Threat Type	Severity	Attack Source IP Address	Attacked URL	Attack Result

----End

12 Audit

12.1 HSS Operations Supported by CTS

Cloud Trace Service (CTS) records all operations on HSS, including requests initiated from the management console or open APIs and responses to the requests, for tenants to query, audit, and trace.

Table 12-1 lists HSS operations recorded by CTS.

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

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

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

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

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

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

12.2 Viewing Audit Logs

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

Viewing an HSS Trace on the CTS Console

- **Step 1** Log in to the management console.
- **Step 2** Click on the top of the page and choose **Cloud Trace Service** under **Management & Deployment**. The CTS console is displayed.
- Step 3 Choose Trace List in the navigation pane.
- **Step 4** Click **Filter** and specify filtering criteria as needed. The following four filters are available:
 - Trace Type, Trace Source, Resource Type, and Search By.

Select the filter from the drop-down list.

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

Step 5 Click Query.

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

Figure 12-1 Expanding trace details

Т	race Name	Resource Type	Trace Source	Resource ID 💿	Resource Name 💮	Trace Status 🕐	Operator (?)	Operation Time	Operation
^ m	nanualDetection	hss	HSS	-		ormal	1.000	Dec 05, 2019 20:19:38 GMT+08:00	View Trace
code	2	00							
source	Lip 👘	-C-028							
trace_t	type C	onsoleAction							
event_t	type sy	system							
project	Lid 6:	63661f4fa990431eb79a308709b5d660							
trace_i	d 8:	8235bfe1-1759-11ea-9718-891dd39b46ec							
trace_r	name m	manualDetection							

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

Figure 12-2 Viewing a trace

View Trace

"pr	oject id": "63661f4fa990431eb79a308709b5d660",
"co	ntext": {
	"request": "{\"X-Auth-Token\":\"MIIakAYJKoZIhvcNAQcCoIIagTCCGn0CAQExDTALBglghkgBZQMEAgEwghiiBgkqhkiG9w0BBw
	"code": "200",
	"source_ip": "",
	"trace_type": "ConsoleAction",
	"event_type": "system",
	"project_id": "63661f4fa990431eb79a308709b5d660",
	"trace_id": "8235bfe1-1759-11ea-9718-891dd39b46ec",
	"trace_name": "manualDetection",
	"resource_type": "hss",
	"trace_rating": "warning",
	"api_version": "v1",
	"service_type": "HSS",
	"response": "{}",
	"tracker_name": "system",
	"time": "1575548378373",
	"record_time": "1575548379231",
	"request_id": "d1a98cd8-ff03-4d90-b283-b14e5fe9ed08",
	"user": {
	"name": "",
	"id": "06a022904380105f1fb6c010bf36c684",
	"domain": {
	"name": "',
	"id": "0c264ba0cefb48c0a9674fee0c6e144f"

----End

×

13 Permissions Management

13.1 HSS Custom Policies

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

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

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

Example Custom Policies

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

• Example 2: Denying agent uninstallation

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

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

```
"Version": "1.1",
"Statement": [
```

{

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

Multi-action policy

}

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

```
{
     "Version": "1.1",
     "Statement": [
           {
                 "Effect": "Allow",
                 "Action": [
                       "hss:hosts:list"
                 1
          },
{
                 "Effect": "Allow",
                 "Action": [
                       "hss:hosts:switchVersion",
                       "hss:hosts:manualDetect",
                       "hss:manualDetectStatus:get"
                 ]
           }
     ]
}
```

13.2 Actions

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

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

You can grant users permissions by using roles and policies. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

Supported Actions

HSS provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies and implement more refined access control. Actions supported by policies are specific to APIs. Common concepts related to policies include:

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

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

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

Actions

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

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

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

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

14_{FAQs}

14.1 About HSS

14.1.1 What Is Host Security Service?

Host Security Service (HSS) helps you identify and manage the assets on your servers; manage programs, file integrity, security operations, and vulnerabilities; check for unsafe settings; and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

Working Principles

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

Figure 14-1 illustrates how HSS works.
Figure 14-1 Working principles



The following table describes HSS components.

Tuble 14 I components	Table	14-1	Components
------------------------------	-------	------	------------

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

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

14.1.2 Can HSS Quota Be Shared Between Accounts?

No.

HSS can only be shared by multiple IAM users under the same account, or by an account and its IAM users.

HSS Shared by Multiple IAM Users Under the Same Account

For example, you have created the account **Domain** and two IAM users **user1** and **user2** under **Domain**.

If **user1** has purchased HSS and **user2** has the HSS Administrator permission, **user2** can also use HSS.

Figure 14-2 HSS shared by multiple IAM users under the same account



HSS Shared Between an Account and IAM Users Under the Account

For example, you have created the account **Domain** and the IAM user **user2** under **Domain**.

• If **Domain** has purchased HSS and **user2** has the HSS Administrator permission, **user2** can also use HSS.

Figure 14-3 HSS shared between an account and IAM users under the account (1)



• If user2 has purchased HSS, Domain can also use HSS.

Figure 14-4 HSS shared between an account and IAM users under the account (2)



14.1.3 What Is the HSS Agent?

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

Functions of the Agent

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

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

Linux Agent Processes

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

The agent contains the following processes:

Table 14-2 Linux	agent	processes
------------------	-------	-----------

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

Windows Agent Processes

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

The agent contains the following processes:

Table	14-3	Windows	agent	processes
-------	------	---------	-------	-----------

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

14.1.4 Can HSS Automatically Detect and Remove Viruses?

HSS can detect intrusion threats, such as malicious programs and ransomware, but cannot automatically remove viruses.

You can manually isolate and remove detected malicious programs and abnormal processes.

HSS helps you cope with ransomware attacks before, during, and after an intrusion.

You can also install antivirus software to further harden server security.

14.1.5 Can I Add an IP Blacklist in HSS?

HSS has a common IP blacklist to block brute-force attacks, but users cannot modify it.

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

14.1.6 How Often Are the HSS Virus Database and Vulnerability Database Updated?

The databases are updated in real time.

The HSS vulnerability database is updated immediately when Windows and Linux patches are released.

The virus database is updated immediately when new viruses are detected.

14.1.7 How Does HSS Transfer Data?

HSS servers use port 443, and HSS agents use random ports for communication. Agents can transfer data from any port to port 443 of HSS servers.

HSS transfers data via IP. Agents transmit data via DNS. No data is lost during the transmission.

14.2 Deployment and Configuration

14.2.1 Alarm Notifications

14.2.1.1 Why No Topics Are Available for Me to Choose When I Configure Alarm Notifications?

No Topics Created

On the **Alarm Notification** page, click **View Topics** in the **SMN Topic** area, and create a topic on the SMN console.

Figure 14-5 Viewing SMN topics

SMN Topic			
hss	•	С	View Topic

Only SMN topics whose statuses are Confirmed are available.

No Subscribed Topics

After creating a topic, you need to add one or more subscriptions to the topic and confirm the subscriptions as prompted.

14.2.1.2 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, you can use either of the following methods to set alarm notifications:

- Enabling Alarm Notifications for Basic, Professional, or Premium Edition
 - On the **Servers** page, click **Set Alarm Notifications** in the **Instructions** area.

Figure 14-6 Set Alarm Notifications

Host Security	Servers & Quotas 🥑 🐵 Instructions		Buy HSS	Configure Alarm Notification Manual Scan
Dashboard	Enterprise Project All projects	с		
Scans 💌	Instructions			×
Intrusions •	-1)	-2	-3	-4
Security Operations	Install Agent Install the Agent on each host you wish to protect. Hosts without Agent Installed: 12	Set Alarm Notifications After you enable alarm notifications, HSS notifies users you specified of risks in a timely manner.	Enable HSS On the Servers tab, click Enable and select a protection quota for your server.	View Scan Results On the Servers tab, locate your server and choose More > View Scan Results in the Operation column.
Installation and Configuration		Note: Alarm notifications has not been set yet. Set it on the Installation and Configuration page.		Alternatively, go to the Scans or Intrusions page, view detection results about protected servers.
Web Tamper Protection		3 Set Alarm Notifications		
Container Guard Service d				

- Choose Installation and Configuration > Alarm Notifications.
- Enabling Alarm Notifications for the WTP Edition

Choose Web Tamper Protection > Installation and Configuration > Alarm Notification.

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.

14.3 Alarm and Event Management

14.3.1 Brute-force Attack Defense

14.3.1.1 How Does HSS Block Brute-Force Attacks?

Protection Scope

HSS can block attacks on MySQL, SQL Server 2012, VSFTP, SSH, and RDP.

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

Figure 14-7 Added rules

100 10002-343504-111454 13.7 4517 1	UCal/HUSLUUATU/LUU# IDLa	DICO TIL	
Chain INPUT (policy ACCEPT)			
target prot opt source	destination		
IN HIDS MYSQLD BIP DROP tcp	0.0.0.0/0	0.0.0.0/0	tcp dpt:3306
IN_HIDS_MYSQLD_DENY_DROP tcp	0.0.0.0/0	0.0.0.0/0	tcp dpt:3306
Chain FORWARD (policy ACCEPT)			
target prot opt source	destination		
Chain OUTPUT (policy ACCEPT)			
target prot opt source	destination		
Chain IN_HIDS_MYSQLD_BIP_DROP	(1 references)		
target prot opt source	destination		
Chain IN_HIDS_MYSQLD_DENY_DROP	(1 references)		
target prot opt source	destination		

NOTICE

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

How Brute-Force Attacks Are Blocked

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

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

NOTE

If HSS detects account cracking attacks on servers using Kunpeng EulerOS (EulerOS with ARM) or CentOS 8.0 or later, it does not block the source IP addresses and only generates alarms. The SSH login IP address whitelist does not take effect for such servers.

Alarm Policies

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

Viewing Account Cracking Detection Results

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** In the table displayed after you click **Brute-force attack**, you can view blocked attacks on protected servers.

Figure 14-8 Brute-force attack

Host Security	Events	
Dashboard Servers	Alarm Statistics	
Scans 👻	Affected Servers 16 Alarms to be Handled	773 Handled Alarms 78
Intrusions 1 .	Blocked IP Addresses 1 Isolated Files	0
Whitelists	Full protection enabled	*
Advanced Protection Security Operations Installation and Configuration	Safe From (13) Brute-force attack	Can) • Abnormal process behavior • Critical file change • Web Shells • Reverse shell • Insafe account • Privilege escalation • Rootkit detection • • Rootkit detection • Rootkit • Rootkit detection • Ro
Web Tamper Protection 🔹	Events	
	All 851 Batch processing You can click Blocked IP a	Last 30 days • Affected Server & IP Q C iddresses to review or unblock the IP addresses flagged as sources of attacks.
	Brute-force attack 7 3 Alarm Type Affected Server & IP Ev	ent Details Reported Handled Status 🖓 Action Operation
	Abnormal login 8 Brute-force attack ecs- 192 168.1.46 Att	ack type: ssh, Port: 22, A 2020/05/1 Unhandled Handle

- **Step 4** Click **Blocked IP Addresses** to check the source IP addresses, attack types, number of intercepted attacks, the time of the first and last interceptions, and the interception status.
 - Blocked indicates the brute-force attack has been blocked by HSS.
 - Canceled indicates you have unblocked the source IP address of the brute force attack.

NOTE

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

----End

Managing Blocked IP Addresses

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

NOTICE

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.

14.3.1.2 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 14-9 Troubleshooting



Handling the Alarm of a Successful Brute-force Attack

If you received an alarm notification indicating that your account had been cracked, you are advised to harden your servers as soon as possible.

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 Check whether the IP address that triggered the alarm is valid.

Choose **Intrusions** > **Events**. In the **Events** area, click **Abnormal login** and check the login IP address.

- If the IP address is from a normal user (for example, who entered incorrect password for multiple times but logged in before their account is blocked), your server is not intruded. In this case, you can click **Handle** and ignore the event.
- If the IP address is invalid, your server may have been intruded.

In this case, mark this event as handled, log in to the intruded server, and change its password to a stronger one. For details, see **How Do I Set a Secure Password?**

Figure 14-10 Abnormal logins

Host Security		Events ⑦							Isolated Fi	les Buy HSS
Dashboard Servers & Quotas		Alarm Statistics								
Scans	¥	Affected Servers		8	Alarms to be Har	ndled	132	Handled Alarms		1
Intrusions 1 Events 2	•	Blocked IP Addresse	5	0	Isolated Files		0			
Whitelists		Full protection enabled	bled							*
Advanced Protection Security Operations Installation and Configuration	•	Safe From (13)	 Brute-force Abnormal 	attack O Abnormal login shell O High-risk command	Malicious prog execution S Ab	ram (cloud scan) O At	bnormal process behavio Isafe account	Critical file chan	ge 🛛 🥹 Web shell 👘	S Reverse shell
Web Tamper Protection	•	Events								
Container Guard Service Situation Awareness Elastic Cloud Server	8 8 8	All	133	Handle	You can	click Blocked IP addresses to	Last 30 days p review or unblock the I	Server name P addresses flagged as sou	 Affected Server & irces of attacks. 	IP Q C
		Brute-force attack	3 ⁰	Alarm Type Affe	cted Server & IP	Event Details	Reported	Handled S	tatus 🖓 Action	Operation
		Abnormal login	2	Remote Lo 192	-0002 168.0.143	Login IP address:	184 Dec 17, 20)2 U	inhandled	Handle
		Malicious program (cloud scan)	26	Remote Lo 192	-0002 168.0.143	Login IP address:	.184 Dec 17, 24)2 U	inhandled	Handle

Step 4 Check for and eliminate malicious programs.

Click Malicious program (cloud scan) and check alarm events.

• If you find malicious programs implanted in your servers, locate them based on their process paths, users running them, and startup time.

To kill a malicious program in an alarm event, click **Handle** in the row of this event and select **Isolate and kill**.

 If you have confirmed that all the malicious program alarms are false, go to Step 5.

Host Security	Alarm Statistics	Malicious program (cloud scan)
Dashboard	Affected Servers 5 Alarms to be Handled	
Servers & Quotas	Blocked IP Addresses 1 Isolated Files	Server Name 2
Scans 🔻		IP address 192.168.1.163
Intrusions	Full protection enabled	Program Path /root/ff/app/test/VirusShare_c070bcde668beccefb059afb422fbf10
Events 1 Whitelists	Image: Safe From (13) Image: Reverse shell Image: Abnormal login Image: Malkious program (cloud scan) Image: Abnormal shell	Hash 3e7c9be7b797a5ac139625d2729b14b9441589773ea87e70fe86162527
Advanced Protection		File Permission
Security Operations 🔹	Events	User
Installation and Configuration	Handle Last 30-	Program Started
Web Tamper Protection •	All 143 You can click Blocked IP addresses to review or unb	Status Unhandled
Container Guard Service d ^o	Brute-force attack 1 Alarm Type Affected Server & IP Event Details	
Situation Awareness d ^o Elastic Cloud Server d ^o	Abnormal login 0 (3 Malicious 192.168.1.163 Hash: 3e7c9be7b797a5ac1	
	Malicious program (cloud scan) 35 Malicious 192.168.1.163 Hash: 9211e746ea45d8531	
	Abnormal process behavior 25	

Figure 14-11 Malicious program (cloud scan)

Step 5 Check for and delete suspicious accounts.

Choose **Scans** > **Assets** and click the **Account Information** tab. Delete suspicious accounts to prevent attackers from creating accounts or escalating account permissions (for example, adding login permissions to an account).

Step 6 Check and enhance unsafe accounts.

Choose Intrusions > Events. In the Events area, click Unsafe account.

Step 7 Check for and fix unsafe settings.

Check for and fix weak password complexity policies and unsafe software settings on your servers.

- **Step 8** Harden your servers.
 - You can also enhance the defense against brute-force attacks by following the instructions provided in **How Do I Defend Against Brute-force Attacks?**

----End

Handling the Alarm of a Blocked Brute-force Attack

Check whether blocked IP addresses can be trusted. HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3600 seconds.

Constraints and Limitations

• Linux OS

On servers running the EulerOS with ARM, or Centos 8.0 or later, HSS does not block the IP addresses suspected of SSH brute-force attacks, but only generates alarms.

- Windows OS
 - Authorize the Windows firewall when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS inservice period. If the Windows firewall is disabled, HSS cannot block brute-force attack IP addresses.
 - If the Windows firewall is manually enabled, HSS may also fail to block brute-force attack IP addresses.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** Choose **Intrusions** > **Events**. In the **Events** area, click **Brute-force attack**.

Brute-force attack alarms will be generated if:

- The system uses weak passwords, is under brute-force attacks, and attacker IP addresses are blocked.
- Users fail to log in after several incorrect password attempts, and their IP addresses are blocked.

Figure 14-12 Brute-force attacks

Host Security		Alarm Statistics								
Dashboard		Affected Servers	5	Alarms to be Handled		138 ⊦	andled Alarms			5
Servers & Quotas		Blocked IP Addresses	1	Isolated Files		1				
Scans	•									
Intrusions 1	*	Full protection enabled								
Events 2		Surve-force attack	Image: Strute-force attack Image: Abnormal login Image: Malicious program (cloud scan) Image: Abnormal process behavior Image: Critical file change Image: Web shell From (13) Image: Reverse shell Image: Abnormal shell Image: High-risk command execution Image: Abnormal autostart Image: Unsafe account Image: Privilege escalation Image: Reverse shell Image: Rev							
Whitelists		Safe From (13) Safe From (13)	Abnormal shell	High-risk command exect	ution 🛛 🥹 Abnormal autostar	t 🛛 Vinsal	fe account	Privilege escalation	en 🥹 Rootkit	detection
Advanced Protection	•									
Security Operations	•	Events	From (13) Adhormal shell Adhormal shell High-Fisk command electron Adhormal aluosart. Unitare account Privilege exclasion V Robot detection							
Installation and Configuration		Har	dle		Last 30 d	ays •	r Server nar	ne 🔻 Affecter	d Server & IP	Q C
Web Tamper Protection	•	All 143		You can click Blocke	d IP addresses to review or unblo	ock the IP addre	esses flagged as s	ources of attacks.		
Container Guard Service	ø	3 Brute-force attack 1	Alarm Type Aff	ected Server & IP	Event Details	Reported	Handled	Status ∑	Action Or	peration
Situation Awareness	o ^o							P	-	
Elastic Cloud Server	ø	Abnormal login 0	Brute-force 192	2.168.1.163	Attack type: ssh, Port: 22, A	Nov 10, 20		Unhandled	Ha	andle

Step 4 Check whether the login IP address triggering the alarm is valid.

- If the IP address is valid,
 - To handle a false alarm, click **Handle** in the row of the alarm event. Ignore or whitelist the IP address.

This does not unblock the IP address.

 To unblock the IP address, click Blocked IP Address in the Alarm Statistics area, select the IP address, and unblock it. Alternatively, you can just wait for it to be automatically unblocked when its blocking duration expires.

By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours.

If the source IP address is invalid or unknown,

Mark this event as handled.

Immediately log in to your server and change your password to a stronger one. You can also enhance the defense against brute-force attacks by following the instructions provided in **How Do I Defend Against Brute-force Attacks?**

----End

Helpful Links

- How Does HSS Block Brute-Force Attacks?
- How Do I Unblock an IP Address?

14.3.1.3 How Do I Defend Against Brute-force Attacks?

Preventive Measures

Configure your applications and networks to enhance security.

• Applications

Using SSH keys for login

Enable SSH key login for server resources and application servers. A user can log in only if its private key matches the public key.

• Network

- Configuring the SSH login whitelist

The SSH login whitelist allows logins from only whitelisted IP address to prevent account cracking.

- Using 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).

HSS **prevents brute-force attacks** on server accounts in real time and blocks attack source IP addresses. 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 14-4	4 Setting IP	addresses to	remotely	connect to I	ECSs
------------	--------------	--------------	----------	--------------	------

Direct ion	Protocol/ Application	Port	Source IP Address
Inbou nd	SSH (22)	22	For example, 192.168.20.2/32

14.3.1.4 What Do I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Accounts for Linux Servers?

Possible Causes

The dependency, **libwrap.so**, which sshd in the host system depends on, is missing.

NOTE

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

Solution

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

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

Affected Image Versions

- The following are Gentoo images that have the problem:
 - Gentoo Linux 17.0 64bit (40 GB)
 - Gentoo Linux 13.0 64bit (40 GB)
- The following are OpenSUSE images that have the problem:
 - OpenSUSE 42.2 64bit (40 GB)
 - OpenSUSE 13.2 64bit (40 GB)

14.3.1.5 How Do I Unblock an IP Address?

HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3600 seconds. If a normal IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can unblock the IP address.

If you manually unblocked an IP address, but incorrect password attempts from this IP address reach the threshold again, this IP address will be blocked again.

NOTE

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

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Intrusions** > **Events**.
- Step 4 In the Alarm Statistics area, click Blocked IP Addresses.
- **Step 5** In the blocked IP address list, select an IP address and click **Unblock**.

----End

14.3.1.6 What Do I Do If HSS Frequently Reports Brute-force Alarms?

NOTE

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 cause: 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.

- 1. Configure a whitelist.
- 2. Use another port.
- 3. Configure security group rules.
- 4. Enable 2FA.
- 5. Configure a strong password.

For details, see How Do I Defend Against Brute-force Attacks?

14.3.2 Weak Passwords and Unsafe Accounts

14.3.2.1 How Do I Handle a Weak Password Alarm?

Servers using weak passwords are exposed to intrusions. If a weak password alarm is reported, change the password that triggered the alarm immediately.

Causes

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

Checking and Changing Weak Passwords

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- Step 3 Choose Scans > Unsafe Settings and click the Common Weak Password Detection tab.
- **Step 4** Check the server, account name, account type, and usage duration of the weak password. Log in to the server and change the password.

----End

Changing a Weak Password

System	Procedure	Remarks
Windows OS	 To change the password in the Windows 10, perform the following steps: 1. Log in to the Windows OS. 2. Click in the lower left corner and click . 3. In the Windows Settings window, click Accounts. 4. Choose Sign-in options from the navigation tree. 5. On the Sign-in options tab, click Change under Password. 	None
Linux OS	Log in to the Linux server and run the following command: passswd [<user>]</user>	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. NOTE Replace <i><user></user></i> with the username.
MySQL database	 Log in to the MySQL database. Run the following command to check the database user password: SELECT user, host, authentication_string From user; This command is probably invalid in certain MySQL versions. In this case, run the following command: SELECT user, host password From user; Run the following command to change the password: SET PASSWORD FOR' Username'@'Host'=PASSW ORD('New_password'); Run the following command to refresh password settings: flush privileges: 	None

System	Procedure	Remarks
Redis database	 Open the Redis database configuration file redis.conf. Run the following command to change the password: requirepass <i><password></password></i>; 	 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. NOTE Replace <i><password></password></i> with the new password.
Tomcat	1. Open the conf/tomcat-user.xml configuration file in the Tomcat root directory.	None
	2. Change the value of password under the user node to a strong password.	

14.3.2.2 How Do I Set a Secure Password?

Comply with the following rules:

• Use a password with high complexity.

The password must meet the following requirements:

- a. Contains at least eight characters.
- b. Contain at least three types of the following characters:
 - i. Uppercase letters (A-Z)
 - ii. Lowercase letters (a-z)
 - iii. Digital (0-9)
 - iv. Special characters
- 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.

14.3.2.3 Why Are the Weak Password Alarms Still Reported After the Weak Password Policy Is Disabled?

If you have enhanced passwords before disabling the weak password policy, the weak password alarm will not be reported again.

If you do not enhance passwords before disabling the weak password policy, the reported alarm will persist and be retained for 30 days.

- To enhance server security, you are advised to enhance the passwords of the accounts used for logging in to servers, such as SSH accounts.
- To protect internal data of your servers, you are advised to enhance the passwords of software accounts, 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.

14.3.3 Intrusions

14.3.3.1 Why a Process Is Still Isolated After It Was Whitelisted?

After you add a process to the whitelist, it will no longer trigger certain alarms, but its isolation will not be automatically canceled.

Isolating and Killing a Malicious Program

- Choose **Installation and Configuration** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable this function.
- Choose Intrusions > Events. In the Events area, manually isolate and kill malicious programs.

If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers.

Canceling the Isolation of Files

- Choose Intrusions > Events. Click Isolated Files in the upper right corner. Cancel the isolation of the whitelisted file.
- Choose Intrusions > Events. In the Events area, manually cancel the isolation and killing of the whitelisted file.

After you cancel isolation, the read/write permissions of files will be restored, but terminated processes will not be automatically started.

14.3.3.2 What Should I Do If a Mining Process Is Detected on a Server?

NOTE

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.

You are advised to:

- 1. Back up data and disable unnecessary ports.
- 2. Set a stronger server password.
- 3. Enabled HSS. Your servers will be protected from mining processes by its intrusion detection functions, such as account cracking prevention, remote login detection, malicious program detection, and web shell detection; as well as malicious program killing and vulnerability fixing functions.

14.3.3.3 What Should I Do If I Find My Servers Attacking Others?

If your servers are launching attacks, they may be infected with Trojans. You are advised to reinstall the OS and set strong passwords to harden the servers and applications such as phpStudy and Redis. Countermeasures include:

- Set strong passwords for all accounts. Do not use default passwords or other passwords that are easy to guess.
- Configure security group policies. Set fixed access IP addresses for non-public service ports to avoid its exposure to the Internet.
- Update the system and applications, installing the latest patches in a timely manner.
- Regularly back up data.
- Delete or rename the **phpmyadmin** folder.

14.3.3.4 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

 HSS block attacking IP addresses to prevent intrusions. The blocking duration for suspicious SSH attacks is 12 hours and that for other suspicious attacks is 24 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked. If you are sure that a source IP address can be trusted, you can manually unblock it. Choose Intrusions > Events, click 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.

14.3.3.5 Why a Blocked IP Address Is Automatically Unblocked?

If a blocked IP address does not perform brute-force attacks in the next 24 hours, the IP address will be automatically unblocked.

14.3.3.6 How Do I Defend Against Ransomware Attacks?

Generally, ransomware is spread through Trojan implantation, emails, files, vulnerabilities, bundles, and storage media.

You can defend against ransomware by handling alarms on the HSS console in a timely manner.

14.3.4 Abnormal Logins

14.3.4.1 What Can I Do If an Alarm Indicating Successful Login Is Reported?

- This alarm does not necessarily indicate a security issue. If you have selected **Successful Logins** in the **Real-Time Alarm Notifications** area, HSS will send alarms when detecting any successful logins.
- If all the accounts on your 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.

14.3.4.2 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 Intrusion **Detection** page.
- For more details, view logs in the **/var/log/secure and /var/log/message** on the Linux server, or run the **last** command to check for abnormal login records.

14.3.5 Unsafe Settings

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

Installing a PAM

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

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

NOTE

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

Setting a Password Complexity Policy

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

NOTE

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

• For CentOS, Fedora, and EulerOS based on Red Hat 7.0, run:

man pam_pwquality

• For other Linux OSs, run:

man pam_cracklib

- CentOS, Fedora, and EulerOS
 - Run the following command to edit the /etc/pam.d/system-auth file:
 vi /etc/pam.d/system-auth
 - b. Find the following information in the file:
 - For CentOS, Fedora, and EulerOS based on Red Hat 7.0: password requisite pam_pwquality.so try_first_pass retry=3 type=
 - For other CentOS, Fedora, and EulerOS systems:

password requisite pam_cracklib.so try_first_pass retry=3 type=

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

Example:

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

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

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

Table 14-5 Parameter description

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

vi /etc/pam.d/common-password

b. Find the following information in the file:

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

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

Example:

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

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

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

Perform the following steps to set a local security policy:

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

NOTE

Alternatively, click **Start** and type **secpol.msc** in the **Search programs and files** box, as shown in **Figure 14-13**.

Figure 14-13 Using the search box

Programs (1)
🖥 secpol
secpol.msc Log off

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

- Double-click **Password must meet complexity requirements**, select **Enable**, and click **OK** to enable the policy.
- Double-click **Minimum password length**, enter the length (greater than or equal to **8**), and click **OK** to set the policy.

Figure 14-14 Configuring local security policies



Step 3 Run the **gpupdate** command to refresh your system settings. Figure 14-15 shows that the refresh is successful and the settings are applied in the system.

Figure 14-15 Execution result



----End

14.4 Vulnerability Management

14.4.1 How Do I Fix Vulnerabilities?

Procedure

- **Step 1** Check the vulnerability detection results.
- **Step 2** Based on provided solutions, fix vulnerabilities one by one in descending order by severity.
 - Restart the Windows OS after you fix its vulnerabilities.
 - For a Linux server, you need to restart it if you have fixed its kernel vulnerabilities.
- Step 3 HSS scans all Linux, Windows, and Web-CMS servers for vulnerabilities every early morning. After you fix the vulnerabilities, you are advised to perform a check immediately to verify the result. For details, see Starting a Software Vulnerability Detection.

----End

14.4.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?

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.

Vulnerability Cause

After the vulnerability is fixed, it will still be displayed on the console. You can on the **Vulnerabilities** page. The status may be **Fixed** or **Failed**.

- If a vulnerability is fixed, its status will change to Fixed.
 Fixed vulnerabilities will remain in the list within 30 days after it was fixed.
- If it fails to be fixed, its status will change to Failed.

D NOTE

For more information, see **Fixing Vulnerabilities and Verifying the Result**. Perform the following operations to locate the cause and fix the problems on Windows or Linux servers.

Possible Causes and Solutions on a Windows Server

• The patch package failed to be downloaded.

Your server may not have the permission to access the Internet. In this case, connect to the Internet and fix the vulnerability again.

• The patch package does not match your OS.

In this case, select the vulnerability and click **Ignore** on the **Vulnerabilities** page.

• Another patch is being installed.

In this case, wait until the current patch is installed, and then fix the vulnerability.

- Server settings hinder vulnerability fix or alarm clearance.
 - If automatic patch update is enabled on the server, and you have confirmed that a patch has been installed to fix the vulnerability, you can ignore the vulnerability on the console.
 - If the latest patch has overwritten old patches (in Windows Server 2016 and later), and you have confirmed that a patch has been installed to fix the vulnerability, you can ignore the vulnerability on the console.
 - If a piece of security software (such as the Server Edition of 360 Guard) blocks the vulnerability patch, stop the software, fix the vulnerability, and then start the software again.

NOTICE

• Microsoft has stopped updating and maintaining Windows Server 2008 R2 since January 14, 2020. To continue to use the system, you need to purchase Extended Security Update (ESU) keys and activate or replace the Windows OS.

Possible Causes and Solutions on a Linux Server

• No yum sources have been configured.

In this case, configure a yum source suitable for your Linux OS, and fix the vulnerability again.

• The yum source does not have the latest upgrade package of the corresponding software.

Switch to the yum source having the required package and fix the vulnerability again.

• The intranet environment cannot connect to Internet.

Servers need to access the Internet and use external yum sources to fix vulnerabilities. If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the provided by .

• 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	14-6	Verification	commands
abic	14 0	vermeation	communus

OS	Verification Command
CentOS/Fedora /Euler/ Redhat/Oracle	rpm -qa grep <i>Software_name</i>
Debian/Ubuntu	dpkg -l grep Software_name
Gentoo	emergesearch Software_name

Follow-up Operations

After the vulnerability is fixed, you are advised to perform a manual detection to verify the result. For details, see **How Do I Scan My Servers?**

NOTE

- HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.
- Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

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

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

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

- On a Windows server, you need to restart it after you fix its vulnerabilities.
- On a Linux server, you need to restart it after you fixed a kernel vulnerability. Restart is not required for other vulnerability fixes.

14.4.5 Can I Restore the Server Data That Was Cleared During Vulnerability Fixing?

Yes.

You can restore the server data by using its latest backup. Data not backed up cannot be restored.

14.5 Web Tamper Protection

14.5.1 Why Do I Need to Add a Protected Directory?

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

14.5.2 How Do I Modify a Protected Directory?

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click -, and choose **Security** > **Host Security Service**.
- **Step 3** In the navigation pane, choose **Web Tamper Protection** > **Server Protection**.
- Step 4 Locate the target server and click Configure Protection in the Operation column.
- **Step 5** Select the required protected directory and click **Edit** in the **Operation** column.

NOTE

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

Figure 14-16 Configuring protection

Host Security	We	b Tamper Protection / EPS_Test					
Dashboard		3 Protected Directory Settings	Privileged Process	Settings Enable	l but not in effect	Dynamic WTP	
Servers							
Scans	•	4					
Intrusions	-	Type Directory	e system				
Advanced Protection	-						
Security Operations	•	Add Protected Directory	Enable Remote Bac	Up to 50 protec	ted directories can be a	dded. Local backup is perfori	med by default. Enable remote backup as needed.
Web Tamper Protection		Protected Directory	Excluded Subdirectory	Excluded File Types	Local Backup Path	Protection Status	Operation 5
Server Protection 2		/opt	-	-	/home1	🕑 Enabled	Suspend Protection Edit Delete
Installation and Configuration							



Edit Protocted Dire	ctop	>
Eult Protected Dire		
* Protected Directory:	/opt	
	Note: Do not add a system directory, such as /bin, as a protected directory.	
Excluded Subdirectories:	Example: /xxx/xxx	
	Enter the relative path of the subdirectory of a protected directory. Separate multiple subdirectories with semicolons (;).	
Excluded File Types:	Example: log; js	
★ Local Backup Path	/backup	
	subdirectory. Otherwise, the local backup will fail.	
	OK Cancel	

Figure 14-17 Editing protected directory

----End

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

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

Specifying Privileged Processes

Privileged processes have the permission to modify files.

- Privileged processes can access protected directories. Ensure that privileged processes are secure and reliable.
- You can configure privileged processes only for Windows OSs.

Temporarily Disabling WTP

Disable WTP while you modify files in protected directories.

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

Setting Scheduled Protection

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

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

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

Dynamic WTP protects your Tomcat applications.

For this function to take effect, ensure that:

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

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

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

14.6 Others

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

Procedure

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

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

🖫 Remote D	esktop Connection			_ 🗆 🗙
N	Remote Des Connectio	ktop on		
General Dis	splay Local Resource: dio Configure remote audi <u>S</u> ettings	s Program o settings.	is Experience	Advanced
Keyboard -	Apply Windows <u>k</u> ey co Only when using the f Example: ALT+TAB	ombinations full screen	:	•
Local devic	tes and resources Choose the devices any your remote session. I✓ Prin <u>t</u> ers <u>M</u> ore	nd resource	es that you want	to use in
Options			Connect	<u>H</u> elp

Figure 14-18 Remote desktop connection

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

🖫 Remote	Desktop Conne	ction		_ 🗆 ×
	Remote Conne	Desktop ction		
General D	tisplay Local Re tings	sources Program	s Experience	Advanced
	Computer:	Administrator		
	You will be aske	d for credentials w	hen you connect	
	Allow me to s	save c <u>r</u> edentials		
	Save the current saved connectio	t connection setting	gs to an RDP file	or open a
	Save	Sa <u>v</u> e A	s	0p <u>e</u> n
Options			Connect	<u>H</u> elp

Figure 14-19 Setting general parameters

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

----End

14.6.2 How Do I Check HSS Log Files?

Log Paths

The following table describes log files and their paths.

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

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

Log Retention

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

14.6.3 How Do I Enable Logging for Login Failures?

MySQL

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

- Step 1 Log in to the host as the root user.
- **Step 2** Run the following command to query the **log_warnings** value:

show global variables like 'log_warnings'

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

set global log_warnings=2

- **Step 4** Modify the configuration file.
 - For a Windows OS, modify the **my.ini** file by adding **log_warnings=2** to **[mysqld]**.
 - For a Linux OS, modify the **my.conf** file by adding **log_warnings=2** to **[mysqld]**.
 - ----End

Filezilla

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

To enable the logging function, perform the following steps:

- Step 1 Open FileZilla.
- Step 2 Choose Edit > Settings > Logging and select Enable logging to file (see Figure 14-20).

Figure 14-20 Enabling logging in FileZilla



----End

vsftp

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

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

vsftpd_log_file=log/file/path

dual_log_enable=YES

Step 2 Restart the vsftp service. If the setting is successful, log records shown in the logs shown in Figure 14-21 will be returned when you log in to vsftp.

Figure 14-21 Log records

Wed	Aug	29	14:53:05	2018	[pid 2]	CONNECT: Client "::ffff:10.130.153.31"
Wed	Aug	29	14:53:11	2018	[pid 1]	<pre>[ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"</pre>
Wed	Aug	29	14:55:14	2018	[pid 2]	CONNECT: Client "::ffff:10.130.153.31"
Wed	Aug	29	14:55:18	2018	[pid 1]	<pre>[ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"</pre>
Wed	Aug	29	14:55:26	2018	[pid 1]	<pre>[ftp test] OK LOGIN: Client "::ffff:10.130.153.31"</pre>
Wed	Sep	5	11:50:16	2018	[pid 2]	CONNECT: Client "::ffff:10.130.153.31"
Wed	Sep	5	11:50:23	2018	[pid 1]	<pre>[ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"</pre>
Wed	Sep	5	13:59:53	2018	[pid 2]	CONNECT: Client "::ffff:10.130.153.31"
Wed	Sep	5	13:59:59	2018	[pid 1]	[ftp test] FAIL LOGIN: Client "::ffff:10.130.153.31"
Wed	Sep	5	14:00:08	2018	[pid 1]	[ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"

----End

14.6.4 How Do I Scan My Servers?

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

NOTICE

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

Prerequisites

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

Check Items

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

Scan Duration

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

Performing a Manual Scan with One Click

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

Step 1 Log in to the management console.
- **Step 2** In the upper left corner of the page, select a region, click =, and choose **Security > Host Security Service**.
- **Step 3** In the upper right corner of the **Servers** page, click **Manual Scan**.

Host Security		Server	s 🕐								Config	jure Alarm Noti	fication	Manual (Detection
Dashboard Servers Scans	Ŧ	Se	2 rver Ser	ver Group											3
Intrusions Advanced Protection	• •		Select all	Enable	Disable	App	ly Policy	Add to Gro	oup	Server nar	ne 🔻	Enter a keywc	Q	Search 😸 [C C
Security Operations	•		ecs-a883 1c4cc66e-28	IP Addre .69.14 192.168.0.16	OS Linux	Server S	Agent St Online	Protecti	Oetectio Risky	Edition Premium (included	Server G	Policy G	Disable	n Switch Edition	More 🔻
Configuration Web Tamper Protection	÷		windows e9e40ddf-c4	.73.76	Windows	Running	Online	🕑 Ena	🔗 Risky	Premium	hss_test	default	Disable	Switch Edition	More 🔻
			test-403 12ef6caf-1e	.68.20 f 192.168.0.48	Linux	Running	Not inst Install Ageni	O Disa	! Pen	None			Enable	Switch Edition	More 🔻

Figure 14-22 Performing a manual scan



Figure 14-23 Manual scan

 Manual Detection sup 2. Manual Detection per detection, web shell dete 3. After the detection is console. 	ports detection on serv forms the following de ection, password risk de complete, view the stat	ers protected l tections for the tection, and co istics of each r	by enterprise edi e selected server: onfiguration dete risk item or view	tion whose agent statuses software information dete ection. the detection results of the	are Online. ction, vulnerability e server on the HSS
elect at least one serv Enterprise Pre railable Servers Select a	ver. emium Ill (2) Server name	▼ Enter	a keyworc Q	Selected Servers	
Server Name/Elastic	IP Addr OS	WTP Status	HSS Edition	Server Name/Elastic I	OS
ecs-a883	Linux	Enabled	Premium (included with V	ecs-a883 .69.141	Linux
windows	Windows	Enabled	Premium (included with V		

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

----End

Manually Checking an Item

Step 1 Log in to the management console.

- **Step 2** In the upper left corner of the page, select a region, click —, and choose **Security > Host Security Service**.
- **Step 3** In the navigation pane, choose **Servers**. In the **Operation** column of the server list, click **View Scan Results**.

Figure 14-24 Viewing scan results

Host Security	Servers (0)
Dashboard Servers Scans	Server Group
Intrusions •	Select all Enable Dicable Apply Policy Add to Group Server name • Enter a keyv Q Search • C
Advanced Protection *	Server Name/ID IP Address OS Server Status Agent Status Protection Stat. Detection Result Edition Server Group Policy Group Operation
Security Operations Installation and Configuration	ets-ead7 59.141 (EP) Unux Running Online Stabled O Roky Premium (Ye hos_test Disable Switch Edition Nove + 4352b593-eta6-46 192.168.0.162 (Ph)
Web Tamper Protection	Apply Policy Add to Group

Checking software information
 Click Installed Software on the Assets tab, and click Scan.

Figure 14-25 Viewing software information

Assets Vulnerabilities Unsafe Settings Intrusions	
Account Information (20) Open Ports (0/ 1) Process Information (25) Web	Directories (0) Installed Software (378) Auto-startup (5)
Lists installed software to give you a clear overview of software asset and help you identify risky software	re versions.
Scan Gan status: Completed on Dec 10, 2020 15:11:36 GMT+08:00	
	Enter a software name. Q
Software Name	Software Version
acl	2.2.51-14.el7.x86_64
aic94xx-firmware	30-6.el7.noarch
alsa-firmware	1.0.28-2.el7.noarch

• Detecting vulnerabilities

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

NOTE

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

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

Figure 14-26 Detecting system vulnerabilities

Assets Vulnerabilities Unsafe Settings Intrusions					
Linux Vulnerabilities (3) Web-CMS V	ulnerabilities ()				
Detects system and software (such as SSH, C	penSSL, Apache, and MySQL) vu	Inerabilities based on	the library to help users identify risks.		
	Dec 17, 2020 15:00:12 CMT 02				
Scan (%) Scan status: Completed or	TDec 17, 2020 15:08:13 GMT+08.	00			
Ignore Unignore Fix	Verify		All statuses 👻 All un	gencies 👻 Vulnerabilit 👻	Enter a keywork Q C
Vulnerability Name	Urgency	Status	Installed Software	Solution	Operation
				Undate the affected openssl packages	
CESA-2018:0998 (openssl secu	irity upda 🗢 Medium	Unhandled	openssl:1.0.2k-fips	See the recommendation ABC for infor	Ignore Fix Verify
CESA-2018:3221 (openeol sect	rity unda 😑 Medium	Unbandled	openssi-1.0.2k-fins	Update the affected openssl packages.	Ignore Ex Verify
	wediam	onnanuteu	openssc r.o.2k-nps	See the recommendation ABC for infor	

 Click the Vulnerabilities tab. Click Web-CMS Vulnerabilities, select a vulnerability, and click Scan. HSS will detect Web-CMS vulnerabilities immediately.

Figure 14-27 Detecting Web-CMS vulnerabilities

Assets Vulnerabilities Unsafe Settings Intrusions				
Linux Vulnerabilities (3) Web-CMS Vulnera	abilities (0)			
Identifies Web-CMS vulnerabilities by inspecting web directories and files.				
Scan Scan status: Pending risk detection				
Ignore Unignore		Unhandled •	All urgencies 💌	Vulnerability name
Vulnerability Name	Urgency Status	Path	Solution	Operation

• Detecting password risks

Click the **Unsafe Settings** tab and click **Password Risks**. Click **Scan** to manually detect unsafe configurations.

Figure 14-28 Detecting weak passwords

Assets Vulnerabilities Unsafe Settings Intrusions							
Password Risks (0) Unsafe	Password Risks (0) Unsafe Configurations (0)						
Detects password complexity policie the user will be prompted to change	Detects password complexity policies and provides suggestions to help users improve password security. Detects commonly used weak passwords. If a weak password is detected, the user will be prompted to change the password to prevent password guessing attacks.						
Manual Detection Detection	Manual Detection Detection Status: Completed on 2020/04/14 00:35:05 GMT+08:00						
Accounts with Weak Passwords	Password Complexity Policy						
		C					
Account ID	Account Type	Usage Duration (Days)					

No data available

• Detecting unsafe settings

Click the **Unsafe Settings** tab and click **Unsafe Configurations**. Click **Scan** to manually detect unsafe configurations.

Figure 14-29 Detecting unsafe settings

Assets Vulnerabilities Unsafe Settings Intrusions				
Password Risks (0) Unsafe Configurations (0)				
Inspects Tomcat, SSH login, and Nginx configurations to he	lp users discover unsafe configurations.			
Scan Scan status: Pending risk detection				
			All detection types	
Category	Risky Item	Passed	Description	

Step 4 Wait until **Detection Status** changes to **Completed**, click ^C to refresh the detection results.

----End

14.6.5 Why Does Manual Detection Fail?

Manual detection will probably fail if you perform it too frequently. At least a three-minute interval is required between two manual detections for the same item.

14.6.6 Can HSS Alarm Logs Be Stored in OBS?

No. The log files are stored in the service folder. For details about the storage path and log retention period, see **How Do I Check HSS Log Files?**

A Change History

Released On	Description
2022-12-30	This is the third official release. Optimized descriptions.
2022-08-30	This is the second official release. Optimized descriptions.
2020-09-30	This is the first official release.