Host Security Service

Service Overview

Issue 15

Date 2024-03-25

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 What Is HSS?

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

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

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

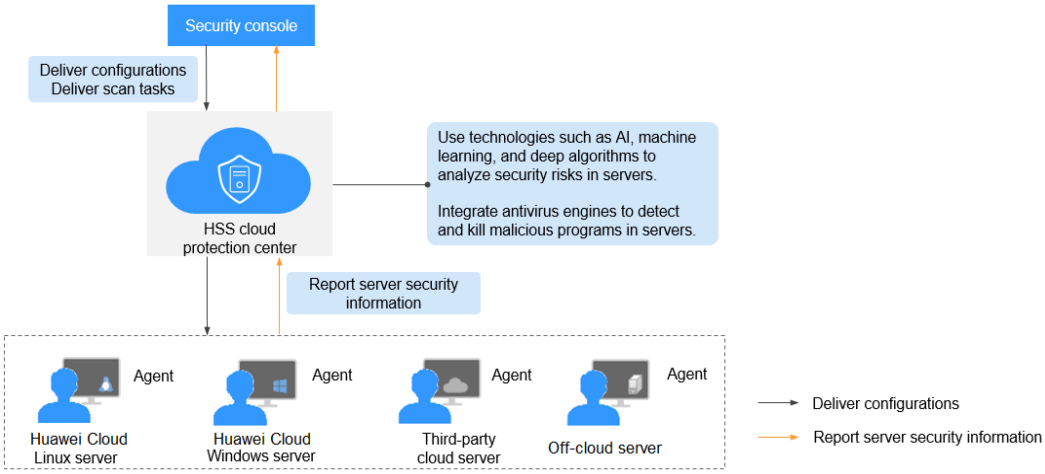
Host Security

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

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

Figure 1-1 illustrates how HSS works.

Figure 1-1 Working principles



The following table describes the HSS components.

Table 1-1 Components

Component	Description
Management console	A visualized management platform, where you can apply configurations in a centralized manner and view the protection status and scan results of servers in a region.
HSS cloud protection center	• Analyzes security risks in servers using AI, machine learning, and deep learning algorithms. • Integrates multiple antivirus engines to detect and kill malicious programs in servers. • Receives configurations and scan tasks sent from the console and forwards them to agents on the servers. • Receives server information reported by agents, analyzes security risks and exceptions on servers, and displays the analysis results on the console.
Agent	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10180 is used by default. • Scans all servers every early morning; monitors the security status of servers; and reports the collected server information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. • Blocks server attacks based on the security policies you configured. **NOTE** • If no agent is installed or the agent installed is abnormal, the HSS is unavailable. • The agent can be installed on Huawei Cloud Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), on-premises servers, and third-party cloud servers. • Select the agent and installation command suitable for your OS. • The HSS agent can be used for all editions, including container security and Web Tamper Protection (WTP). You only need to install the agent once on the same server.

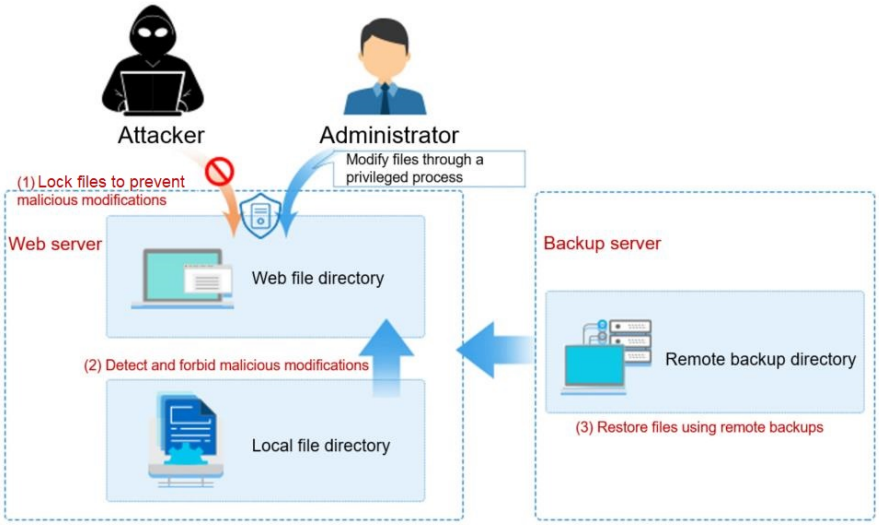
Container Security

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

Web Tamper Protection

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

Figure 1-2 How WTP works



2 Advantages

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

Centralized Management

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

- You can install the agent on Huawei Cloud ECSs, BMSs, on-premises servers, and third-party cloud servers in the same region to manage them all on a single console.
- On the security console, you can view the sources of server risks in a region, handle them according to displayed suggestions, and use filter, search, and batch processing functions to quickly analyze the risks of all servers in the region.

All-Round Protection

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

Lightweight Agent

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

WTP

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

3 Scenarios

HSS

- DJCP Multi-level Protection Scheme (MLPS) compliance

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

  To apply for the DJCP MLPS certification, purchase the enterprise edition or a higher edition (premium edition or Web Tamper Protection edition).
- Centralized security management

  With HSS, you can manage the security configurations and events of all your cloud servers on the console, reducing risks and management costs.
- Security risk evaluation

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

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

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

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

CGS

- Container image security

  Vulnerabilities will probably be introduced to your system through the images downloaded from Docker Hub or through open-source frameworks.

  You can use CGS to scan images for risks, including image vulnerabilities, unsafe accounts, and malicious files. Receive reminders and suggestions and eliminate the risks accordingly.

- Container runtime security

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

- Compliance with DJCP MLPS

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

4 Specifications of Different Editions

HSS provides Basic, Professional, Enterprise, Premium, Web Tamper Protection, and Container editions. It provides the following functions: **Overview**, **Asset Overview**, **Host Management**, **Container Management**, **Asset Fingerprint**, **Vulnerability Management**, **Baseline Check**, **Container Image Security**, **Application Protection**, **Web Tamper Protection**, **Ransomware Protection**, **File Integrity Management**, **Virus Scanning**, **Dynamic Port Honeypot**, **Container Firewall**, **Application Process Control**, **Container Cluster Protection**, **Host Intrusion Detection**, **Container Intrusion Detection**, **Whitelist Management**, **Policy Management**, **Historical Handling Records**, **Security Reports**, and **Security Configurations**. The functions supported by each edition are different. You can select a proper edition based on your service requirements.

- To protect test servers or individual users' servers, use the basic edition. It can protect any number of servers, but only part of the security scan capabilities are available. This edition does not provide protection capabilities, nor does it provide support for DJCP Multi-level Protection Scheme (MLPS) certification. For a server that uses the basic edition for the first time, this edition is free of charge for 30 days.
- If you need to obtain the **DJCP MLPS L2 certification**, purchase the **enterprise edition**.
- If you need to obtain the **DJCP MLPS L3 certification**, purchase the **premium edition**.
- If you need to obtain the **DJCP MLPS certification for a website**, you are advised to purchase the **Web Tamper Protection edition**.
- For servers that need to protect websites and key systems from tampering, the **WTP edition** is recommended.
- For containers that need to enhance image security, container runtime security**, and to comply with security regulations**, container edition is recommended.
- If your servers store important data assets, have high security risks, use publicly available EIPs, or there are databases running on your servers, you are advised to use the **premium or Web Tamper Protection edition**.

NOTICE

- You are advised to **deploy HSS on all your servers** so that if a virus infects one of them, it will not be able to spread to others and damage your entire network.
- After you purchase a protection quota edition, you can upgrade or switch the edition. For details, see **Upgrading Protection Quotas** and **Switching the HSS Quota Edition**.
- The meanings of the symbols in the table are as follows:
  - √: supported
  - ×: not supported

Dashboard

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

Table 4-1 Functions

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Dashboard	You can check the security score, risks, and protection overview of all your assets in real time, including servers and containers.	√	√	√	√	√	√	Linux and Windows	Real-time check

Assets

Asset Management displays the asset status and their statistics.

Table 4-2 Assets

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Assets	Collect statistics on asset status and usage of all servers, including the agent status, protection status, quota status, and asset fingerprint.	√	√	√	√	√	√	Linux and Windows	Real-time check

Servers & Quota

Server management allows users to view and manage target servers by server.

Table 4-3 Server management functions

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs
Servers & Quota	Manage all server assets, including their protection statuses, quotas, and policies. You can install agents on all the Linux servers in batches.	√	√	√	√	√	√	Linux and Windows Note: Only Linux agents can be installed in batches.

Containers & Quota

Container management allows you to view and manage target servers by container.

Table 4-4 Containers & Quota

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs
Containers & Quota	Manage container nodes and images (private image repositories and local images).	×	×	×	×	×	√	Linux

Asset Fingerprints

The function collects and displays statistics of **Server fingerprints** and **Container fingerprints**.

Table 4-5 Asset fingerprints

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Account	Check and manage server accounts all in one place.	×	×	√	√	√	√	Linux and Windows	Automatic check every hour
Open ports	Check open ports all in one place and identify high-risk and unknown ports.	×	×	√	√	√	√	Linux and Windows	Automated check every 30 seconds

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Process	Check running applications all in one place and identify malicious applications.	×	×	√	√	√	√	Linux and Windows	Automatic check every hour
Installed software	Check and manage server software all in one place and identify insecure versions.	×	×	√	√	√	√	Linux and Windows	Automatic check every day
Auto-started items	Check auto-startup entries and collect statistics on entry changes in a timely manner.	×	×	√	√	√	√	Linux and Windows	Automatic check every hour
Web application	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	×	×	√	√	√	√	Linux and Windows (only Tomcat is supported)	Once a week (04:10 a.m. every Monday)
Web service	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	×	×	√	√	√	√	Linux	Once a week (04:10 a.m. every Monday)

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Web frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	×	×	√	√	√	√	Linux	Once a week (04:10 a.m. every Monday)
Website	Check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, and key processes of websites.	×	×	√	√	√	√	Linux	Once a week (04:10 a.m. every Monday)
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware.	×	×	√	√	√	√	Linux and Windows	Once a week (04:10 a.m. every Monday)
Database	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	×	×	√	√	√	√	Linux and Windows (only MySQL is supported)	Once a week (04:10 a.m. every Monday)

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Kernel modules	Check information about all the program module files running in kernels, including associated servers, version numbers, module descriptions, driver file paths, file permissions, and file hashes.	×	×	√	√	√	√	Linux	Once a week (04:10 a.m. every Monday)

Vulnerability Management

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

Table 4-6 Vulnerabilities

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Linux vulnerability detection	Based on the vulnerability database, check and handle vulnerabilities in the software (such as kernel, OpenSSL, vim, glibc) you obtained from official Linux sources and have not compiled.	√	√	√	√	√	√	Linux	• Automatic scan (reporting based on the software asset collection period) • Scheduled scan (once a week by default) • Manual

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
									scan

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Windows vulnerability detection	Detect vulnerabilities in Windows OS based on the official patch releases of Microsoft.	√	√	√	√	√	×	Windows	• Automatic scan (reporting based on the software asset collection period) • Scheduled scan (once a week by default) • Manual scan

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Web-CMS vulnerability detection	Scan for Web-CMS vulnerabilities in web directories and files.	×	√	√	√	√	√	Linux and Windows	• Automatic scan (reporting based on the software asset collection period) • Scheduled scan (once a week by default) • Manual scan

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Application vulnerability detection	Detect vulnerabilities in JAR packages, ELF files, and other files of open source software, such as Log4j and spring-core.	×	×	√	√	√	√	Linux and Windows	• Automatic scan (reporting based on the middleware asset collection period) • Scheduled scan (once a week by default) • Manual scan

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Emergency vulnerability detection	Checks whether the software and any dependencies running on the server have vulnerabilities through version comparison and POC verification. Reports risky vulnerabilities to the console and provides vulnerability alarms for you.	×	√	√	√	√	√	Linux	• Scheduled scan (manual configuration is required) • Manual scan

Baseline Inspection

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

Table 4-7 Baseline checks

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Password complexity policies	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.	√	√	√	√	√	√	Linux	• Automatic check in the early morning every day • Manual scan
Common weak passwords	Change weak passwords to stronger ones based on HSS scan results and suggestions.	√	√	√	√	√	√	Linux and Windows	• Automatic check in the early morning every day • Manual scan

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Unsafe configuration	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	×	×	√	√	√	√	Linux and Windows	• Automatic check in the early morning every day • Manual scan

Container Image Security

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

Table 4-8 Container images

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
SWR image repository vulnerabilities	Detect system and application vulnerabilities in SWR image repository based on a vulnerability database and handle critical vulnerabilities in a timely manner.	×	×	×	×	×	√	Linux	• Automatic check in the early morning every day • Manual scan
Viewing Malicious File Detection Results	Scan images for malicious files (such as Trojans, worms, viruses, and adware) and identify risks.	×	×	×	×	×	√	Linux	Real-time check

Application protection

Application protection provides security defense for running applications. you simply need to add probes to them, without having to modify application files. Currently, only Linux servers are supported, and only Java applications can be connected.

Table 4-9 Application protection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
SQL injection	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities.	×	×	×	√	√	√	Linux	Real-time check
OS command injection	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities.	×	×	×	√	√	√	Linux	Real-time check
XSS	Detect and defend against stored cross-site scripting (XSS) injection attacks.	×	×	×	√	√	√	Linux	Real-time check
Log4jRCE vulnerability	Detect and defend against remote code execution.	×	×	×	√	√	√	Linux	Real-time check
Web shell upload	Detect and defend against attacks that upload dangerous files, change file names, or change file name extension types; and check web applications for related vulnerabilities.	×	×	×	√	√	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
XML External Entity Injection	Detect and defend against XML External Entity Injection (XXE) attacks, and check web applications for related vulnerabilities.	×	×	×	√	√	√	Linux	Real-time check
Deserialization input	Detect deserialization attacks that exploit unsafe classes.	×	×	×	√	√	√	Linux	Real-time check
File directory traversal	Check whether sensitive directories or files are accessed.	×	×	×	√	√	√	Linux	Real-time check
Struts2 OGNL	Detect OGNL code execution.	×	×	×	√	√	√	Linux	Real-time check
Command execution using JSP	Detect command execution using JSP.	×	×	×	√	√	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
File deletion using JSP	Detects file deletion using JSP.	×	×	×	√	√	√	Linux	Real-time check
Database connection exception	Detect authentication and communication exceptions thrown by database connections.	×	×	×	√	√	√	Linux	Real-time check
0-day vulnerability	Check whether the stack hash of a command is in the whitelist of the web application.	×	×	×	√	√	√	Linux	Real-time check
SecurityManager permission exception	Detect exceptions thrown by SecurityManager.	×	×	×	√	√	√	Linux	Real-time check

Web Tamper Protection (WTP)

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

Table 4-10 Web Tamper Protection

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

Ransomware prevention

Ransomware protection supports user-defined ransomware backup and restoration policies. Help you identify some unknown ransomware attacks by using static and dynamic honeypot files.

Table 4-11 Ransomware prevention

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Ransomware prevention	Help you identify some unknown ransomware attacks by using static and dynamic honeypot files.	×	×	×	√	√	√	Linux and Windows	Real-time check

Application Process Control

Application process control can detect malicious processes and generate alarms.

Table 4-12 Application process control

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

Monitor file integrity

File integrity management checks and records changes to key files.

Table 4-13 File integrity monitoring

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Monitor file integrity	Check the files in the Linux OS, applications, and other components to detect tampering.	×	×	×	√	√	√	Linux	Real-time check

Virus Scan

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

Table 4-14 Virus scan

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

Dynamic Port Honeypot

Dynamic Port Honeypot function uses real ports as bait ports to induce attackers to access the intranet. In the horizontal penetration scenario, the function can effectively detect attackers' scanning and identify faulty servers.

Table 4-15 Function

Service Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Dynamic Port Honeypot	The dynamic port honeypot function is a deception trap. It uses a real port as a bait port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user.	×	×	×	√	√	√	Linux and Windows	Real-time check

Container Firewalls

Container firewalls provides services for container runtime.

Table 4-16 Container firewall

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Container Firewalls	Control and intercept network traffic inside and outside a container cluster to prevent malicious access and attacks.	×	×	×	×	×	√	Linux	Real-time check

Container Cluster Protection

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

Table 4-17 Container cluster protection

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

Intrusion detection

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

Table 4-18 Server intrusion detection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojan, mining software, worms, and viruses.	×	√	√	√	√	√	Linux and Windows	Real-time check
Viruses	Check servers in real time and report alarms for viruses detected on servers.	×	√	√	√	√	√	Linux and Windows	Real-time check
Worms	Detect and kill worms on servers and report alarms.	×	√	√	√	√	√	Linux and Windows	Real-time check
Trojans	Detect programs that are hidden in normal programs and have special functions such as damaging and deleting files, sending passwords, and recording keyboards. If a program is detected, an alarm is reported immediately.	×	√	√	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Botnets	Detect whether zombie programs that have been spread exist in servers and report alarms immediately after detecting them.	×	√	√	√	√	√	Linux and Windows	Real-time check
Backdoors	Detect web shell attacks in the server system in real time and report alarms immediately after detecting them.	×	√	√	√	√	√	Linux and Windows	Real-time check
Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	×	√	√	√	√	√	Linux	Real-time check
Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.	×	×	×	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Hacker tools	Check whether non-standard tool used to control the server exist and report alarms immediately after detecting them.	×	×	√	√	√	√	Linux and Windows	Real-time check
Webshell	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. ● Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. ● You can use the manual detection function to detect web shells on servers.	×	√	√	√	√	√	Linux and Windows	Real-time check
Mining	Detect whether mining software exists on servers in real time and report alarms for the detected software.	×	√	√	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Remote code execution	Check whether the server is remotely called in real time and report an alarm immediately once remote code execution is detected.	×	×	√	√	√	√	Linux and Windows	Real-time check
Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.	×	√	√	√	√	√	Linux	Real-time check
Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.	×	√	√	√	√	√	Linux	Real-time check
MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.	×	√	√	√	√	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Reverse shells	Monitor user process behaviors in real time to detect and block reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. **NOTE** To enable automatic reverse shell blocking, perform the following operations: 1. You can enable automatic reverse shell blocking in the **Malicious File Detection** rule or configure automatic blocking in the **HIPS Detection** rule. For details, see **Configuring Policies**. 2. Enable isolation and killing of malicious programs. For details, see **Isolating and Killing Malicious Programs**.	×	√	√	√	√	√	Linux	Real-time check

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

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	×	×	√	√	√	√	Linux and Windows	Real-time check
High-risk command executions	Check executed commands in real time and generate alarms if high-risk commands are detected.	×	√	√	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
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.	×	√	√	√	√	√	Linux	Real-time check
Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.	×	×	×	√	√	√	Linux and Windows	Real-time check
System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately.	×	×	√	√	√	×	Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Backup deletion	Detect the preparations for ransomware encryption: Delete backup files or files in the **Backup** folder. Once backup deletion is detected, an alarm is reported immediately.	×	×	√	√	√	√	Windows	Real-time check
Suspicious registry operation	Detect operations such as disabling the system firewall through the registry and using the ransomware **Stop** to modify the registry and write specific strings in the registry. An alarm is reported immediately when such operations are detected.	×	×	√	√	√	√	Windows	Real-time check
System log deletion	An alarm is generated when a command or tool is used to clear system logs.	×	×	√	√	√	×	Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Suspicious command executions	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution.	×	×	√	√	√	√	Linux and Windows	Real-time check
Suspicious process execution	Detect and report alarms on unauthenticated or unauthorized application processes.	×	×	√	√	√	×	Linux and Windows	Real-time check
Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories.	×	×	√	√	√	×	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Brute-force attacks	Check for brute-force attack attempts and successful brute-force attacks. • Detect password cracking attacks on accounts and block attacking IP addresses to prevent server intrusion. • Trigger an alarm if a user logs in to the server by a brute-force attack.	√	√	√	√	√	√	Linux and Windows	Real-time check
Abnormal logins	Check and handle remote logins. If a user's login location is not any common login location, an alarm will be triggered.	√	√	√	√	√	√	Linux and Windows	Real-time check
Invalid accounts	Scan accounts on servers and list suspicious accounts in a timely manner.	×	√	√	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
User account added	Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands.	×	×	√	√	√	√	Windows	Real-time check
Password thefts	Detect the abnormal obtaining of hash value of system accounts and passwords on servers and report alarms.	×	×	√	√	√	√	Linux and Windows	Real-time check
Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections.	×	√	√	√	√	√	Linux	Real-time check
Port forwarding	Report alarms on port forwarding using suspicious tools.	×	√	√	√	√	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected.	×	×	√	√	√	×	Windows	Real-time check
Suspicious HTTP request	An alarm is generated when a suspicious HTTP request that uses a system tool or process to execute a remote hosting script is detected.	×	×	√	√	√	×	Windows	Real-time check
Port scan	Detect scanning or sniffing on specified ports and report alarms.	×	×	×	√	√	√	Linux	Real-time check
Host scan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms.	×	×	×	√	√	√	Linux	Real-time check

Container intrusion detection

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

Table 4-19 Container intrusion detection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Unclassified malware	Check and handle malicious programs in a container, including web shells, Trojan, mining software, worms, and viruses.	×	×	×	×	×	√	Linux	Real-time check
Ransomware	Check and handle alarms on ransomware in containers.	×	×	×	×	×	√	Linux	Real-time check
Webshell	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells.	×	×	×	×	×	√	Linux	Real-time check
Vulnerability escape detection	An escape alarm is reported if a container process behavior that matches the behavior of known vulnerabilities is detected.	×	×	×	×	×	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
File escape detection	An alarm is reported if a container process is found accessing a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.	×	×	×	×	×	√	Linux	Real-time check
Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.	×	×	×	×	×	√	Linux	Real-time check
File privilege escalation	Check the file privilege escalations in your system.	×	√	√	√	√	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Process privilege escalations	The following process privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities	×	×	×	×	×	√	Linux	Real-time check
Important file changes	Receive alarms when critical system files are modified.	×	√	√	√	√	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	×	×	√	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Abnormal container processes	• Malicious container program detection Monitor container process behavior and process file fingerprints. An alarm is reported if it detects a process whose behavior characteristics match those of a predefined malicious program. • Abnormal processes The service reports an alarm if it detects that a process not in the whitelist is running in the container.	×	×	×	×	×	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Abnormal container startup detection	The service monitors container startups and reports an alarm if it detects that a container with too many permissions is started. Container check items include: ● Privileged container startup (**privileged:true**) ● Too many container capabilities (**capability:[xxx]**) ● Seccomp not enabled (**seccomp=unconfined**) ● Container privilege escalation (**no-new-privileges:false**) ● High-risk directory mapping (**mounts:[...]**)	×	×	×	×	×	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
High-risk command executions	Check executed commands in containers and generate alarms if high-risk commands are detected.	×	×	×	×	×	√	Linux	Real-time check
High-risk system calls	You can run tasks in kernels by Linux system calls. The container edition reports an alarm if it detects a high-risk call.	×	×	×	×	×	√	Linux	Real-time check
Sensitive file access detection	The service monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.	×	×	×	×	×	√	Linux	Real-time check
Container image blocking	If a container contains insecure images specified in **Suspicious Image Behaviors**, an alarm will be generated and the insecure images will be blocked before a container is started in Docker. **NOTE** You need to **install the Docker plug-in**.	×	×	×	×	×	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Suspicious command executions	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution.	×	×	√	√	√	√	Linux and Windows	Real-time check
Brute-force attacks	Detect and report alarms for brute-force attack behaviors, such as brute-force attack attempts and successful brute-force attacks, on containers. Detect SSH, web, and Enumdb brute-force attacks on containers. **NOTE** Currently, brute-force attacks can be detected only in the Docker runtime.	×	×	×	×	×	√	Linux	Real-time check
Invalid accounts	Detect suspicious accounts and report alarms.	×	×	×	×	×	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Password thefts	Detect the abnormal obtaining of hash value of system accounts and passwords on servers and report alarms.	×	×	√	√	√	√	Linux and Windows	Real-time check
Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections.	×	√	√	√	√	√	Linux	Real-time check
Port forwarding	Report alarms on port forwarding using suspicious tools.	×	√	√	√	√	√	Linux	Real-time check
Kubernetes event deletions	Detect the deletion of Kubernetes events and report alarms.	×	×	×	×	×	√	Linux	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Abnormal pod behaviors	Detect abnormal operations such as creating privileged pods, static pods, and sensitive pods in a cluster and abnormal operations performed on existing pods and report alarms.	×	×	×	×	×	√	Linux	Real-time check
User information enumerations	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms.	×	×	×	×	×	√	Linux	Real-time check
Binding cluster roles	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms.	×	×	×	×	×	√	Linux	Real-time check

Whitelist Management

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

Table 4-20 Whitelists

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Alarm whitelist	You can add an alarm to the whitelist when handling it.	√	√	√	√	√	√	Linux and Windows	Real-time check
Login Whitelist	Add IP addresses and usernames to the Login Whitelist as needed. HSS will not report alarms on the access behaviors of these IP addresses and users.	√	√	√	√	√	√	Linux and Windows	Real-time check
System user whitelist	Users (non-root users) that are newly added to the root user group on a server can be added to the system user whitelist. HSS will not report risky account alarms for them.	√	√	√	√	√	√	Linux and Windows	Real-time check

Policy Management

You can configure **Policy management** and group policies and servers to batch apply policies to servers, easily adapting to your business scenarios.

Table 4-21 Policies

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

Viewing the Handling History

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

Table 4-22 Handling history

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

Security Report

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

Table 4-23 Security report

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

Security Configurations

Security configuration allows you to configure common login locations, common login IP addresses, the SSH login IP address whitelist, and automatic isolation and killing of malicious programs.

Table 4-24 Security configuration

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Agent management	You can view the agent status of all servers and upgrade, uninstall, and install agents.	√	√	√	√	√	√	Linux and Windows	Real-time check
Common login location	For each server, you can configure the locations where users usually log in from. The service will generate alarms on logins originated from locations other than the configured common login locations. A server can be added to multiple login locations.	√	√	√	√	√	√	Linux and Windows	Real-time check
Common login IP address	For each server, you can configure the IP addresses where users usually log in from. The service will generate alarms on logins originated from IP addresses other than the configured common IP addresses.	√	√	√	√	√	√	Linux and Windows	Real-time check

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Configuring an SSH Login IP Address Whitelist	The SSH login whitelist controls SSH access to servers to prevent account cracking. After you configure the whitelist, SSH logins will be allowed only from whitelisted IP addresses.	√	√	√	√	√	√	Linux	Real-time check
Malicious program isolation and removal	HSS automatically isolates and kills identified malicious programs, such as web shells, Trojans, and worms, removing security risks.	×	√	√	√	√	√	Linux and Windows	Real-time check
Two-factor Authentication (2FA)	Prevent brute-force attacks by using password and SMS/email authentication.	Pay per use: × Yearly/Monthly: √	√	√	√	√	√	Linux and Windows	-

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs	Check Frequency
Alarm configurations	After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers, containers, and web pages.	√	√	√	√	√	√	Linux and Windows	-
Plug-in management	Install, uninstall, upgrade, and manage plug-ins in a unified manner.	×	×	×	×	×	√	Linux	-

Server self-protection

Server self-protection is a self-protection function of HSS.

Table 4-25 Server self-protection

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

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition	Supported OSs
	access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).							

5 Provided Free of Charge

HSS provides the following free services:

- Free trial of HSS basic edition for 30 days

  When purchasing an ECS, you can select HSS basic edition for free for one month. HSS basic edition provides OS vulnerability detection, weak password detection, and brute force cracking detection. For details, see **Specifications of Different Editions**. For more information, see **Free trial of HSS basic edition for 30 days**.

- Free health check

  HSS provides a monthly free health check service for ECS that are not protected. HSS can detect software assets, OS vulnerabilities, and weak password risks of servers and generate security reports for you to view. For more information, see **Free health check**.

6 Personal Data Protection Mechanism

To ensure that your personal data, such as your username, password, and mobile phone number, will not be breached by unauthorized or unauthenticated entities or people, HSS encrypts your personnel data before storing it and control access to the data.

Personal Data

Table 6-1 describes the personal data generated or collected by HSS.

Table 6-1 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Email	If 2FA is enabled, HSS periodically obtains from SMN the email addresses subscribing to notification topics.	No	Yes
Mobile phone number	If 2FA is enabled, HSS periodically obtains from SMN the mobile phone numbers subscribing to notification topics.	No	Yes
Login location	If HSS is enabled, it records user login locations.	No	Yes

Storage Mode

HSS uses encryption algorithms to encrypt users' sensitive data and stores encrypted data.

- Mobile phone number are encrypted before storage.
- Login locations are not sensitive data and stored in plaintext.

Access Control

User personal data is encrypted before being stored in the HSS database. The whitelist mechanism is used to control access to the database.

7 Security

7.1 Shared Responsibilities

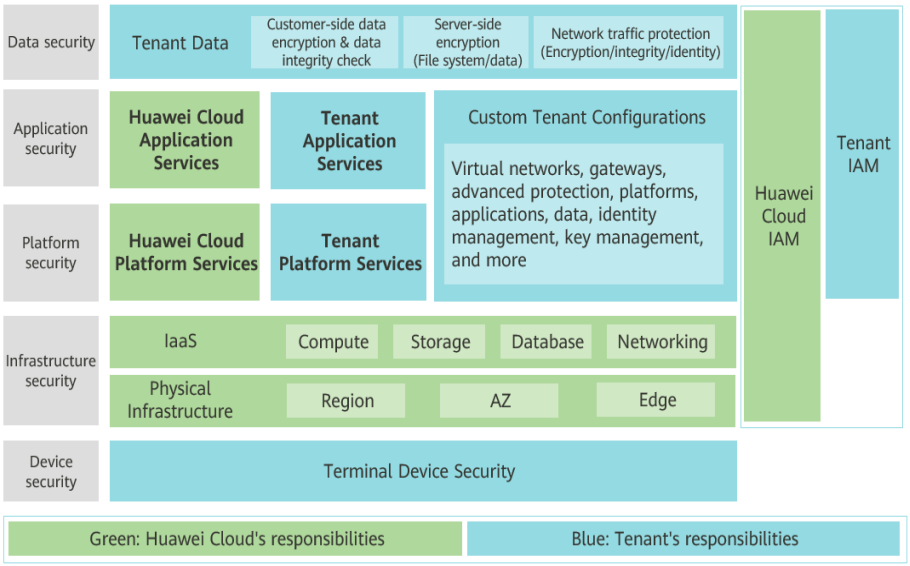
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 7-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 7-1 Huawei Cloud shared security responsibility model

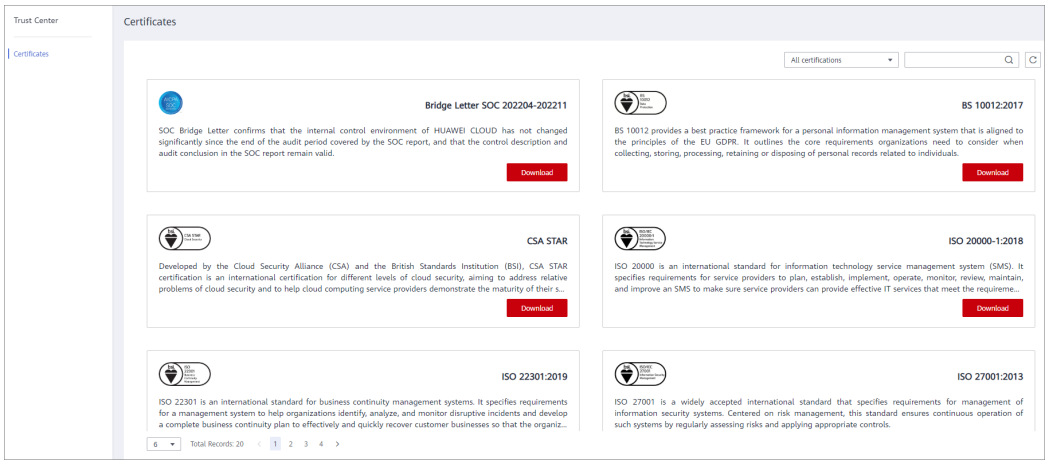


7.2 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

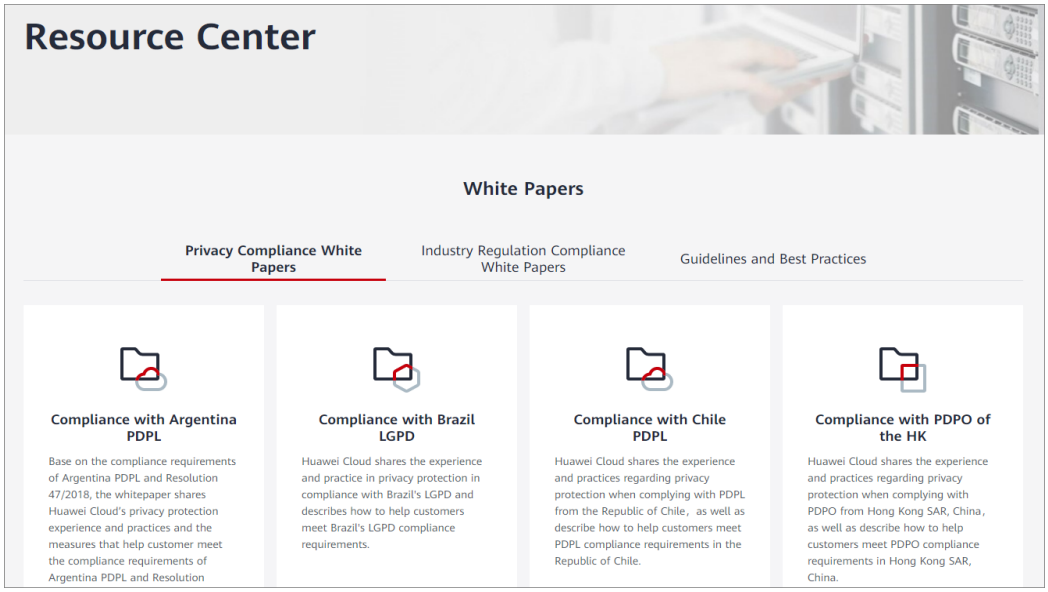
Figure 7-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 7-3 Resource center



7.3 Asset Identification and Management

Host Security Service (HSS) collects information about assets on your servers, such as accounts, processes, open ports, auto-started items, software, web frameworks, websites, middleware, and kernel modules. You can learn the overall status of your assets at a glance.

7.4 Identity Authentication and Access Control

Identity and Access Management (IAM) provides refined permissions management for HSS resources. You can:

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

  For details about HSS permission policies, see **Creating a User and Granting Permissions**.

7.5 Data Protection Technologies

HSS takes different measures to keep data stored in HSS secure and reliable.

Measure	Description

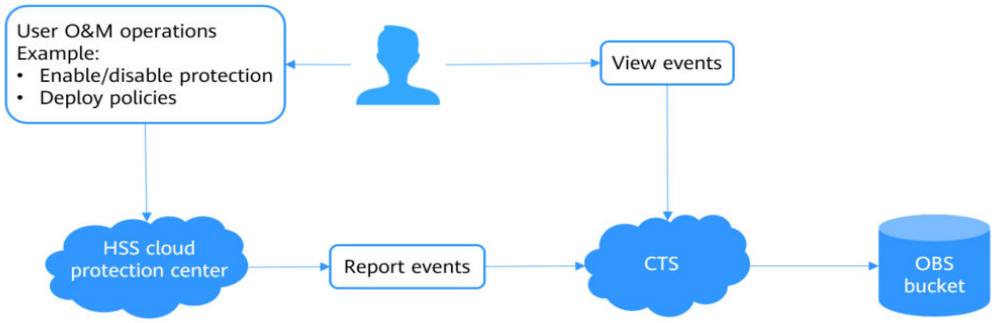
Transmission encryption (HTTPS)	Data is encrypted when it is transmitted between microservices to prevent leakage or tampering during transmission. Your configurations are kept secure when transmitted over HTTPS.
Data redundancy	Data such as asset information and alarm events can be backed up and restored using copies.
Encrypted data storage	HSS encrypts sensitive data to prevent leakage.

You can also enable the Web Tamper Protection (WTP) edition protect business data.

For more information, see **Enabling the WTP Edition**.

7.6 Audit and Logging

Cloud Trace Service (CTS) keeps track of user activities and resource changes on your cloud resources. It helps you collect, store, and query operational records for security analysis, audit and compliance, and fault location.



For details about how to enable and configure CTS, see **Enabling CTS**.

For details about the HSS operations that can be audited by CTS, see **HSS Operations Supported by CTS**.

7.7 Service Resilience

HSS uses a four-level reliability architecture. It provides inspection, resistance, and recovery capabilities to help you manually or automatically recover services, enhancing data durability and reliability.

Table 7-1 Reliability architecture

Category	Capability	Description	Type
Inspection	Situation Awareness (SA)	HSS interconnects with SA and evaluates asset risks based on alarms, vulnerabilities, and baseline check results.	System
	Cloud Eye	With Cloud Eye, you can understand the resource usage and status of HSS, receive alarm notifications in a timely manner, and react to changes to keep your services run smoothly.	System
Resistance	Attack prevention	The agent provides self-protection, anti-removal, and anti-tamper capabilities.	Security
	Data backup	All key data can be backed up. Even if the database is completely damaged, services can be restored using the backup data.	System
	Service self-protection	HSS consists of microservices, which are independently deployed, started, and stopped. The agent strictly controls its resource usage. If its resource usage exceeds the threshold, the agent is isolated or a bypassing operation is performed to avoid affecting user workloads. If system resources are insufficient, the agent performance will be degraded.	System
Restoration	System restoration	A VM or service can be manually or automatically rebuilt if it is faulty.	System
	Process protection	If a process exits, the process will be automatically started to facilitate service recovery.	System

7.8 Risk Monitoring

Cloud Eye provides multi-dimensional monitoring for your resources on the cloud. It allows you to view the resource usage and service running status, and respond to exceptions in a timely manner to ensure smooth running of services.

HSS uses Cloud Eye to perform monitoring over resources and operations, helping you monitor server security and receive alarms and notifications in real time. You can check the number of unprotected servers, the number of unsafe servers, and the number of agents that are not installed or offline in real time.

For details about HSS metrics and how to create alarm rules, see **Monitoring**.

7.9 Fault Rectification

All HSS components are deployed in primary/standby or cluster mode to support cross-AZ and cross-region DR, preventing single-node faults.

7.10 Update Management

N/A

8 HSS Permissions Management

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

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

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

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **What Is IAM?**

HSS Permissions

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

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

You can grant permissions by using roles or policies.

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

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

The following table describes more details.

Table 8-1 System-defined permissions supported by HSS

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

Reference

- What Is IAM?
- Creating a User and Granting Permissions

9 Constraints and Limitations

Supported Server Types

- Elastic Cloud Server (ECS)
- Bare Metal Server (BMS)
- Huawei Cloud Workspace
- Third-party cloud server
- On-premises server

NOTE

Currently, only some regions support access to non-Huawei Cloud servers. For details about the regions, see **Where Is HSS Available?**

Supported OSs

HSS uses the agent to monitor security risks and defend against external intrusions. To protect a server with HSS, ensure the agent is up and running on the server. For more information, see **Supported OSs**.

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.
- If a piece of third-party security software, such as McAfee, has been installed on your server, stop the protection function on the software before installing an HSS agent. After you install the agent, you can re-enable the protection function on the software.
- CentOS 6.x is no longer updated or maintained on the Linux official website, and HSS no longer supports CentOS 6.x or earlier.

Table 9-1 Supported OSs

OS Type	System Architecture	Supported OSs	Support for Vulnerability Scan (√: Supported. ×: Not supported.)
Windows	X86	Windows 10 (64-bit) **NOTE** Only Huawei Cloud Workspace can use this OS.	×
		Windows 11 (64-bit) **NOTE** Only Huawei Cloud Workspace can use this OS.	×
		Windows Server 2012 R2 Standard 64-bit English (40 GB)	√
		Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	√
		Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	√
		Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	√
		Windows Server 2016 Standard 64-bit English (40 GB)	√
		Windows Server 2016 Standard 64-bit Chinese (40 GB)	√
		Windows Server 2016 Datacenter 64-bit English (40 GB)	√
		Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	√
		Windows Server 2019 Datacenter 64-bit English (40 GB)	√
		Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	√
Linux	X86	CentOS 7.4 (64-bit)	√
		CentOS 7.5 (64-bit)	√
		CentOS 7.6 (64-bit)	√
		CentOS 7.7 (64-bit)	√
		CentOS 7.8 (64-bit)	√
		CentOS 7.9 (64-bit)	√

OS Type	System Architecture	Supported OSs	Support for Vulnerability Scan (√: Supported. ×: Not supported.)
		CentOS 8.1 (64-bit)	×
		CentOS 8.2 (64-bit)	×
		CentOS 8 (64-bit)	×
		CentOS 9 (64-bit)	×
		Debian 9 (64-bit)	√
		Debian 10 (64-bit)	√
		Debian 11.0.0 (64-bit)	√
		Debian 11.1.0 (64-bit)	√
		EulerOS 2.2 (64-bit)	√
		EulerOS 2.3 (64-bit)	√
		EulerOS 2.5 (64-bit)	√
		EulerOS 2.7 (64-bit)	×
		EulerOS 2.9 (64-bit)	√
		Fedora 28 (64-bit)	×
		Ubuntu 16.04 (64-bit)	√
		Ubuntu 18.04 (64-bit)	√
		Ubuntu 20.04 (64-bit)	√
		Ubuntu 22.04 (64-bit)	√
		Red Hat 7.4 (64-bit)	×
		Red Hat 7.6 (64-bit)	×
		Red Hat 8.0 (64-bit)	×
		Red Hat 8.7 (64-bit)	×
		OpenEuler 20.03 LTS (64-bit)	×
		OpenEuler 22.03 SP3 (64-bit)	×
		OpenEuler 22.03 (64-bit)	×
		AlmaLinux 8.4 (64-bit)	√
		AlmaLinux 9.0 (64-bit)	×
		Rocky Linux 8.4 (64-bit)	×

OS Type	System Architecture	Supported OSs	Support for Vulnerability Scan (√: Supported. ×: Not supported.)
		Rocky Linux 8.5 (64-bit)	×
		Rocky Linux 9.0 (64-bit)	×
		HCE 1.1 (64-bit)	√
		HCE 2.0 (64-bit)	√
		SUSE 12 SP5 (64-bit)	√
		SUSE 15 (64-bit)	×
		SUSE 15 SP1 (64-bit)	√
		SUSE 15 SP2 (64-bit)	√
		SUSE 15 SP3 (64-bit)	×
		SUSE 15.5 (64-bit)	√
		Kylin V10 (64-bit)	√
	ARM	CentOS 7.4 (64-bit)	√
		CentOS 7.5 (64-bit)	√
		CentOS 7.6 (64-bit)	√
		CentOS 7.7 (64-bit)	√
		CentOS 7.8 (64-bit)	√
		CentOS 7.9 (64-bit)	√
		CentOS 8.0 (64-bit)	×
		CentOS 8.1 (64-bit)	×
		CentOS 8.2 (64-bit)	×
		CentOS 9 (64-bit)	×
		EulerOS 2.8 (64-bit)	√
		EulerOS 2.9 (64-bit)	√
		Fedora 29 (64-bit)	×
		Ubuntu 18 (64-bit)	×
		Kylin V7 (64-bit)	×
		Kylin V10 (64-bit)	√
		HCE 2.0 (64-bit)	√

OS Type	System Architecture	Supported OSs	Support for Vulnerability Scan (√: Supported. ×: Not supported.)
		UnionTech OS V20 (64-bit)	√ (UOS V20 server editions E and D)

10 Related Services

You 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)/Bare Metal Server (BMS)

HSS agents can be installed on Huawei Cloud ECSs, BMSs, or third-party servers. You are advised to use Huawei Cloud servers for better and more reliable service experience.

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

Cloud Container Engine (CCE)

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

NOTE

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

Software Repository for Container (SWR)

SWR provides easy, secure, and reliable management over container images throughout their lifecycles, facilitating the deployment of containerized services. For more information, see the *Software Repository for Container User Guide*. HSS scans for vulnerabilities and configurations in container images to help you detect the container environment that cannot be achieved by traditional security software.

Simple Message Notification (SMN)

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

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

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

Identity and Access Management

IAM is a free identity management service that can implement refined 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*.

11 Basic Concepts

Account Cracking

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

Weak Password

A weak password can be easily cracked.

Malicious Program

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

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

HSS reports both identified and suspicious malware.

Ransomware

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

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

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

Two-Factor Authentication

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

Web Tamper Protection

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

Cluster

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

Node

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

Image

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

Container

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

Security Policy

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

Project

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

Multiple projects can be created for one account.

Protection Quota

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

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

Example:

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

A Change History

Released On	Description
2024-03-25	This is the fifteenth official release. Optimized: • **Specifications of Different Editions**: Added the description of the dynamic port honeypot function. • **Constraints and Limitations**: HCE 1.1 is supported by HSS.
2024-02-02	This is the fourteenth official release. Modified the detection period of the vulnerability management function in **Specifications of Different Editions**.
2023-12-21	This is the thirteenth official release. Optimized **Specifications of Different Editions**.
2023-10-27	This is the twelfth official release. Optimized: • Monitoring metrics in **Risk Monitoring** • Added container cluster protection and application process control in **Specifications of Different Editions**.
2023-07-25	This issue is the eleventh official release. Added: • 1.8-Privacy Statement Optimized: • **Specifications of Different Editions**: Added the description about intrusion detection items. • Added the description about OSs supported by the vulnerability detection and fixing in **Constraints and Limitations**.

Released On	Description
2023-06-01	This is the tenth official release. Changed the name of HSS advanced edition to professional edition.
2022-12-10	This is the ninth official release. Optimized the description of ransomware prevention in **Specifications of Different Editions**.
2022-11-15	This is the eighth official release. Added the following section: • **Security**
2022-09-20	This is the seventh official release. Added the description about purchasing the basic edition (yearly/monthly).
2022-08-31	This is the sixth official release. Modified the description about the basic edition. The basic edition can be used free of charge within a specific period.
2022-08-15	This issue is the fifth official release. The following types of alarms are added: • Malicious program • Common vulnerability exploit • Abnormal system behavior - suspicious crontab task Added the description of the two-factor authentication (2FA) feature. The enterprise edition can report alarms on unauthorized accounts.
2022-08-10	This issue is the third official release. Added the description about application protection.
2022-07-28	This issue is the second official release. Added the supported systems and versions. For details, see **Supported OSs**.
2022-06-30	This issue is the second official release. Added the description about the web framework and web service features. Added the description about the application vulnerability management feature.
2022-05-30	This issue is the first official release.

