Host Security Service

Service Overview

Issue	15
Date	2022-08-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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.

Contents

1 HSS

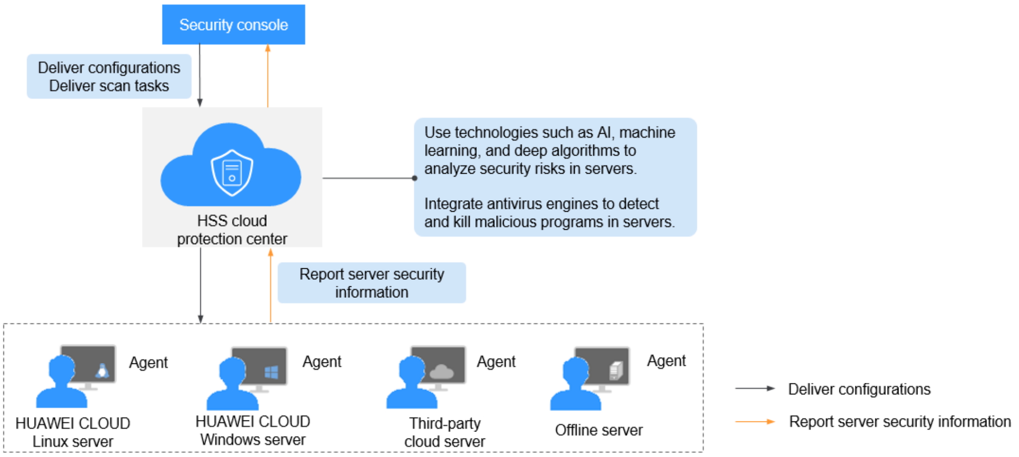
Host Security Service (HSS) helps you identify and manage the assets on your servers; manage programs, file integrity, security operations, and vulnerabilities; check for unsafe settings; and defend against intrusions and web page tampering. There are also advanced protection and security operations 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 1-1 illustrates how HSS works.

Figure 1-1 Working principles


Security console
Deliver configurations
Deliver scan tasks
HSS cloud protection center
Use technologies such as AI, machine learning, and deep algorithms to analyze security risks in servers.
Integrate antivirus engines to detect and kill malicious programs in servers.
Report server security information
Agent
Agent
Agent
Agent
HUAWEI CLOUD Linux server
HUAWEI CLOUD Windows server
Third-party cloud server
Offline server
Deliver configurations
Report server security information

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. ● An agent can be installed on HUAWEI CLOUD Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), offline servers, and third-party cloud servers. ● Select the agent and installation command suitable for your OS. ● Web Tamper Protection (WTP) and HSS can use the same agent on a server.

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 2-1 Asset management

Function	Description	Check Mode
Account information management	Check and manage all accounts on your servers to keep them secure. You can check real-time and historical account information to find suspicious accounts. ● Real-time account information includes **Account ID**, server quantity and names, **Administrator Rights**, **User Group**, **User Directory**, and **User Startup Shell**. ● The operation history of an account includes the **Action**, **Account ID**, **Administrator Rights**, **User Group**, **User Directory**, **User Startup Shell**, and **Time** of the action.	Real-time check
Open port check	Check open ports on your servers, including risky and unknown ports. You can check **Port Type**, **Servers**, **Risk Level**, **Status**, **Port Description**, and the specific **Server**, **Bound IP Address**, **Status**, **PID**, and **Program File** of a port.	Real-time check

Function	Description	Check Mode
Process check	Check processes on your servers and find abnormal processes. You can check **Process Name**, **Servers**, **Total Number of Processes**, **Total Number of File Names**, and the specific **Server**, **Process Path**, **File Permission**, **User**, **PID**, and startup time of a process.	Real-time check
Web directory management	Check and manage directories used by web services on your servers. You can check the **File Path**, **Application Type**, **Local Port**, **URL**, **PID**, and **Program File**.	Real-time check
Software information management	Check and manage all software installed on your servers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the **Software Name**, server quantity and names, and **Software Version**. ● The software operation history includes **Action**, **Software Name**, **Software Version**, and **Time**. ● You can use the manual detection function to check software information.	● Automatic check in the early morning every day ● Manual check
Auto-startup	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.	Real-time check

Vulnerability Management

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

Table 2-2 Vulnerability management

Function	Description	Check Mode
Software vulnerability detection	Check vulnerabilities in Linux and Windows OSs. Check and handle vulnerabilities in your system and the software (such as SSH, OpenSSL, Apache, and MySQL) you obtained from official sources and have not compiled.	● Automatic check in the early

Function	Description	Check Mode
Web-CMS vulnerability detection	Check and handle vulnerabilities found by scanning web directories and files in your Web-CMS.	morning every day ● Manual check

Baseline Inspection

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

Table 2-3 Baseline inspection

Function	Description	Check Mode
Password policy check	● Check whether your password complexity policy is proper and modify it based on suggestions provided by HSS, improving password security. ● You can use the manual detection function to check password complexity policies.	● Automatic check in the early morning every day ● Manual check
Common weak password detection	● Check for weak passwords and remind users to change them, preventing easy guessing. ● On the **Common Weak Password Detection** tab, you can view the account name, account type, and usage duration of a weak password. ● You can use the manual detection function to detect weak passwords on servers.	● Automatic check in the early morning every day ● Manual check

Function	Description	Check Mode
Unsafe configuration item check	Check for unsafe Tomcat, Nginx, and SSH login configurations. On the **Configure Detection** page, you can view the description, matched detection rule, threat level, and status of a configuration. ● You can handle risky configuration items and ignore trusted items based on the detection rules and detection results. ● You can use the manual detection function to check key configurations.	● Automatic check in the early morning every day ● Manual check

Intrusion Detection

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

Table 2-4 Intrusion detection

Intrusion	How HSS Detects It	Check Mode
Brute-force attack	Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. ● If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. ● You can check whether the IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.	Real-time check
Abnormal login	Detect abnormal login behavior, such as remote login and brute-force attacks. ● Check and handle remote logins. HSS can check the blocked login IP addresses, and who used them to log in to which servers at what time. If a user's login location is not any common login location you set, an alarm will be triggered. ● Trigger an alarm if a user logs in by a brute-force attack.	Real-time check

Intrusion	How HSS Detects It	Check Mode
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. HSS can detect only running malicious programs. You can manually isolate and kill identified and suspicious malicious programs, and cancel the isolation of and ignore trusted programs. **NOTE** HSS can detect only running malicious programs.	Real-time check
Abnormal process behavior	All the running processes on all your servers are monitored for you. You can create a process whitelist to ignore alarms on trusted processes, and can receive alarms on unauthorized process behavior and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	Real-time check
Changes made to critical files	● Check alarms about modifications on key files (such as **ls**, **ps**, **login**, and **top**). ● Key file change information includes the paths of modified files, the last modification time, and names of the servers storing configuration files.	Real-time check
Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells. ● Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. ● You can use the manual detection function to detect web shells on servers.	● Real-time check ● Manual check
Reverse shell	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.	Real-time check
Abnormal shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Real-time check

Intrusion	How HSS Detects It	Check Mode
High-risk command execution	Check executed commands in real time and generate alarms on high-risk commands.	Real-time check
Auto-startup check	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	Real-time check
Unsafe account	Scan accounts on servers and list suspicious accounts in a timely manner. You can check the name, user group, UID/SID, user directory, and startup shell of an account.	Real-time check
Privilege escalation	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation	Real-time check
Rootkit	Detect suspicious rootkit installation in a timely manner by checking: ● File signatures ● Hidden files, ports, processes, and kernel modules	Automatic check every day

Advanced Protection

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

Function	Description	Check Mode
Ransomware prevention	Analyze operations on servers, identify trusted applications, and report alarms on 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 2-5 WTP

Function	Description	Check Mode
Static WTP	Prevents static web page files on website servers from being tampered with.	Real-time check
Dynamic WTP	Prevents dynamic web page content in website databases from being tampered with.	

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.

- You can install the agent on HUAWEI CLOUD ECSs, BMSs, offline 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.

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.

4 Editions

HSS comes in basic, enterprise, premium, and WTP editions. **Table 4-2** describes their functions. For more details, see **Functions and Features**.

NOTICE

- HSS comes in basic, enterprise, premium, and WTP editions.

  You can upgrade your editions in the following scenarios.
  - If you have purchased the basic edition, you can upgrade it to the enterprise, premium, or WTP edition.
  - If you have purchased the enterprise edition, you can upgrade it to the premium or WTP edition.
- The premium edition is provided for free if you have purchased the WTP edition.

Recommended Editions

- 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.
- 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, purchase the Web Tamper Protection edition.
- 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 purchase the premium or Web Tamper Protection edition.
- For servers that need to protect websites and applications from tampering, the WTP edition is recommended.

  For details about the application scenarios of each version, see **Table 4-1**.

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.
- In the pay-per-use mode, HSS stops charging if the servers it protects are stopped.

Table 4-1 Recommended Editions

Edition	Billing Mode	Scenario
Basic	● Pay-per-use You can use the basic edition for each of your servers for 30 calendar days free or charge. When purchasing an ECS, you can enable the HSS basic edition for free. The free trial lasts 30 days. ● Yearly/Monthly The basic edition in yearly/monthly mode does not have a free trial period.	This edition 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 MLPS certification. You can use this edition to protect test servers or individual users' servers. The basic edition only provides part of the baseline check and intrusion detection functions, and displays the security risk overview of assets on the cloud. **NOTE** ● If the basic edition in yearly/monthly mode expires, HSS resources protecting your servers will be released. ● If you select **Yearly/Monthly** and a message indicating insufficient quota is displayed, you need to purchase HSS and then enable it.

Edition	Billing Mode	Scenario
Enterprise edition	- Purchasing HSS in Pay-per-use Mode - Yearly/Monthly	Use this edition of you need to obtain DJCP MLPS L2 certification. This edition can scan your servers for Trojans and other viruses, fix vulnerabilities in one click, and detect intrusions.
Premium	Yearly/Monthly	Use this edition if you need to obtain DJCP MLPS L3 certification. 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 this edition.
Web Tamper Protection	Yearly/Monthly	Use this edition if you need to obtain DJCP MLPS certifications for your websites. For servers that need to protect websites and applications from tampering, the WTP edition is recommended. The premium edition is available for free if you have purchased the WTP edition.

Edition Details

NOTE

The basic edition provides only part of the security scan capabilities. This edition does not provide protection capabilities, nor does it provide support for DJCP MLPS certification.

To protect your ECSs or pass the DJCP MLPS certification, purchase the enterprise edition or a higher edition (premium edition or Web Tamper Protection edition).

Table 4-2 Edition details

Function	Item	Description	Basic (Pay-per-use)	Basic (Yearly/Monthly)	Enterprise	Premium	WTP
Asset Management	Manage account information	Check and manage server accounts all in one place.	×	×	√	√	√

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

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

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

Function	Item	Description	Basic (Pay-per-use)	Basic (Yearly/Monthly)	Enterprise	Premium	WTP
	Abnormal process behavior	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	×	×	√	√	√
	Change in critical file	Receive alarms when critical system files are modified.	×	×	√	√	√

Function	Item	Description	Basic (Pay-per-use)	Basic (Yearly/Monthly)	Enterprise	Premium	WTP
	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.	×	×	√	√	√
	Reverse shell	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.	×	×	×	√	√
	Abnormal shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	×	×	×	√	√

Function	Item	Description	Basic (Pay-per-use)	Basic (Yearly/Monthly)	Enterprise	Premium	WTP
	High-risk command execution	Receive real-time alarms on high-risk commands.	×	×	×	√	√
	Auto-startup check	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	×	×	×	√	√
	Unsafe account	Scan accounts on servers and list suspicious accounts in a timely manner.	×	×	√	√	√
	Privilege escalation	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation	×	×	×	√	√

Function	Item	Description	Basic (Pay-per-use)	Basic (Yearly/Monthly)	Enterprise	Premium	WTP
	Rootkit	Detect suspicious rootkit installation in a timely manner by checking: ● Check rootkits based on file signatures. ● Hidden files, ports, processes, and kernel modules	×	×	×	√	√
Advanced protection	Program management	Set whitelist policies, and determine whether applications are **Trusted**, **Untrusted**, or **Unknown**. The applications that are not whitelisted are not allowed to run. This function protects your servers from untrusted or malicious applications, reducing unnecessary resource usage.	×	×	×	√	√
	Monitor file integrity	Check the files in the Linux OS, applications, and other components to detect tampering.	×	×	×	√	√
	Ransomware prevention	Analyze operations on servers, identify trusted applications, and report alarms on untrusted applications, depending on your settings.	×	×	×	√	√

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

Function	Item	Description	Basic (Pay-per-use)	Basic (Yearly/Monthly)	Enterprise	Premium	WTP
	Dynamic WTP	Dynamic web page files in your website databases are protected from tampering.	×	×	×	×	√

5 Scenarios

Security Compliance

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

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.

6 Constraints

Supported Server Types

- ECS
- BMS
- Third-party cloud server
- Offline server

  HSS does not allow multiple offline servers to use the same EIP. A server protected by HSS must use a unique EIP. If there are servers sharing the same EIP, contact technical support.

Supported OSs

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

NOTICE

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

- **Table 6-1** and **Table 6-2** list Linux OS versions supported by HSS.

Table 6-1 Linux OS version (x86 computing)

No.	OS Version
1	CentOS: 7, 8 (64 bit)
2	Debian: 7, 8, 9, and 10 (32/64 bit)
3	EulerOS: 2.2, 2.3, and 2.5 (64 bit)
4	Fedora: 24, 25, and 30 (64 bit)
5	OpenSUSE: 13.2, 15.0, and 42.2 (64 bit)

No.	OS Version
6	Ubuntu: 14.04, 16.04, 18.04, and 20.04 (32/64 bit)
7	Gentoo: 13.0 and 17.0 (64 bit)
8	Oracle Linux: 6.9 and 7.4 (64 bit)

Table 6-2 Linux OS version (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 64-bit with ARM (40 GB)
3	Fedora: 29 64-bit with ARM (40 GB)
4	OpenSUSE: 15.0 64-bit with ARM (40 GB)
5	Ubuntu: 18.04 64-bit with ARM (40 GB)

- The following table describes the Huawei Cloud Windows OS versions supported by HSS.

Table 6-3 Supported Windows OSs

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

No.	OS Version	Constraint
9	Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	
10	Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	

7 Project and Enterprise Project

Project

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

Enterprise Project

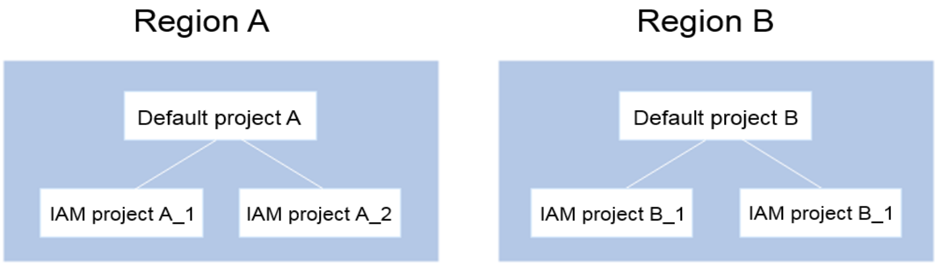
Enterprise projects are used to categorize and manage multiple resources. Resources of the same type can be put under an enterprise project. The use of enterprise projects does not affect the use of HSS.

You can classify resources by department or project group and put related resources into one enterprise project for management. Resources can be moved between enterprise projects.

Differences Between Projects and Enterprise Projects

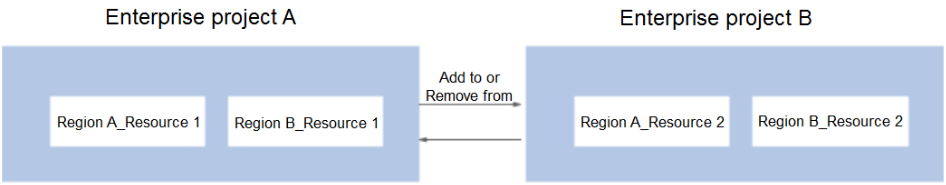
- IAM Project

  Projects are used to categorize and physically isolate resources in a region. Resources in an IAM project cannot be transferred. They can only be deleted and then rebuilt.

- Enterprise Project

  Enterprise projects are upgraded based on IAM projects and used to categorize and manage resources of different projects of an enterprise. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects. If you have enabled enterprise management, you cannot create an IAM project and can only manage existing projects. In the future, IAM projects will be replaced by enterprise projects, which are more flexible.



Both projects and enterprise projects can be managed by one or more user groups. Users who manage enterprise projects belong to user groups. After a policy is granted to a user group, users in the group can obtain the rights defined in the policy in the project or enterprise project.

For details about how to create a project, create an enterprise project, and assign permissions, see **Creating an Enterprise Project**.

8 Pricing Details

This section describes the pricing and renewal information about HSS. For details, see **Pricing Details**.

Billing Items

You will be charged based on your HSS edition and usage duration.

Table 8-1 Billing items

Item	Description
Edition (mandatory)	Edition (basic, enterprise, premium, or WTP) **NOTE** Basic edition HSS provides a free trial when you purchase an ECS.
Required Duration	Yearly/Monthly HSS is billed on a yearly or monthly basis.

Billing Modes

You can purchase HSS in pay-per-use or yearly/monthly mode.

Table 8-2 HSS billing modes

Edition	Billing Mode	Description	Pricing
Basic	● Yearly/ Monthly ● Pay-per-use	● Only part of the security scan capabilities are available. This edition does not provide protection capabilities, nor does it provide support for DJCP MLPS certification. ● If you have purchased ECS, the basic edition free trial is available in pay-per-use mode and available for 30 days. ● If you select **Yearly/ Monthly** and a message indicating insufficient quota is displayed, you need to purchase HSS and then enable it.	**Pricing Details**
Enterprise	● Yearly/ Monthly ● Pay-per-use	● In pay-per-use mode, you pay for the used resources based on the actual service duration (in hours), without a minimum fee. ● Yearly/monthly resources provide a higher discount. This mode is recommended for long-term users. In yearly/monthly mode, you are billed based on the purchase period specified in the order.	
Premium	Yearly/Monthly		
WTP	Yearly/Monthly		

Changing Configurations

- Changing the billing mode
  - From pay-per-use to yearly/monthly

    A yearly/monthly package order will be generated for you. The yearly/monthly quota will be available immediately when you complete payment. To enable the yearly/monthly quota, choose **Servers**. In the **Operation** column of the required server, click **Enable**, and select the yearly/monthly quota.
  - From yearly/monthly to pay-per-use

    Choose **Servers**. In the **Operation** column of the required server, click **Enable**, and select the on-demand quota.

- Unsubscription

  You can **unsubscribe** from HSS in the Billing Center.

Renewal

If the purchased HSS quota expires, you can renew the quota to extend its validity period. You can also set automatic renewal. For details about HSS, see **Renewal Rules**.

Expiration and Overdue Payment

If you do not renew your yearly/monthly resources, they will enter a grace period or retention period before expire. For details, see **Retention Period**.

If your account is in arrears, you can view the arrears details in the Billing Center. To prevent resources from being disabled or released, you need to top up your account within the specified period. For details, see **Repaying Arrears**.

FAQ

For more charging FAQs, see **HSS FAQs**.

9 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 to control access to the data.

Personal Data

Table 9-1 lists the personal data generated or collected by HSS.

Table 9-1 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.

10 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 access to your HUAWEI 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 the groups to which they are added and can perform specified operations on cloud services based on the permissions.

HSS is a project-level service deployed and accessed in specific physical regions. To assign 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 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 also need to assign other roles that the permissions depend on to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.

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

Table 10-1 lists more details.

Table 10-1 System-defined permissions supported by HSS

Role/Policy Name	Description	Role/ Policy Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS.	System-defined role	● This role depends on the **Tenant Guest** role. **Tenant Guest**: a global role, which must be assigned in the Global project ● To purchase HSS protection quotas, you must have the **ECS ReadOnlyAccess** and **BSS Administrator** 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 all permissions for the service.

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

Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting Permissions**

11 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)/Bare Metal Server (BMS)

HSS agents can be installed on HUAWEI CLOUD ECSs/BMSs. The agents can also be installed on 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**.

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*.

Enterprise Management

You can manage multiple projects in an enterprise, separately settle their costs, and assign different personnel for them. A project can be started or stopped independently without affecting others. You can easily manage your projects after creating an enterprise project for each of them.

For more information about enterprise management, see *Enterprise Management 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*.

12 Concepts

Account Cracking

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

HSS can detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts.

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 (Cloud Scan)

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.

Software Vulnerabilities

Vulnerabilities in Linux and Windows are included.

Web-CMS Vulnerabilities

Vulnerabilities found in web directory and file scans are included.

Configuration Check

HSS can check for unsafe Tomcat, Nginx, and SSH login configurations.

Web Shell

HSS can check whether the files (often PHP and JSP files) in your web directories are web shells.

Reverse Shells

HSS can monitor user process behaviors to detect reverse shells caused by invalid connections. TCP, UDP, and ICMP protocols are checked.

Abnormal Shells

HSS can detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.

Privilege Escalation

HSS can detect privilege escalation for processes and files in the current system.

Abnormal privilege escalation operations include:

- Root privilege escalation by exploiting SUID program vulnerabilities

- Root privilege escalation by exploiting kernel vulnerabilities
- File privilege escalation

Rootkit Programs

HSS can detect suspicious rootkit installation in a timely manner, including file signatures, hidden files, ports, and processes.

Protection Quotas

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
2022-08-30	This issue is the fifteenth official release. Added the description about protection quotas.
2022-04-25	This is the fourteenth official release. Optimized the description of the basic edition and its capabilities.
2021-12-30	This is the thirteenth official release. Added recommended editions in **Editions**. Added the description about alarms in **Concepts**.
2021-08-12	This is the twelfth official release. Deleted Windows Server 2008 R2 from Windows OS versions supported by HSS agent in **Constraints**.
2021-08-03	This is the eleventh official release. Added the description that only running malicious programs can be detected in **Functions and Features**.
2021-05-08	This is the tenth official release. Deleted the Linux versions (SUSE: 11 and 12 64-bit and SAP HANA) supported by the agent in **Constraints**.
2021-01-26	This is the ninth official release. Added recommended editions in **Editions**.
2020-12-08	This is the eighth official release. Added description about the basic edition (pay-per-use) not supporting two-factor authentication in **Editions**.
2020-06-19	This is the seventh official release. ● Added **Project and Enterprise Project**. ● Added the description of ransomware in **Concepts**.

Released On	Description
2020-05-18	This is the sixth official release. Added **Pricing Details**.
2020-04-09	This is the fifth official release. ● Added the functions of the premium edition in **Functions and Features**. ● Added the description of the premium edition in **Editions**. ● Added the description of HSS fine-grained authorization in **Permissions Management**.
2019-11-01	This is the fourth official release. Added **Personal Data Protection Mechanism**.
2019-04-08	This is the third official release. Modified **Related Services**.
2018-09-15	This is the second official release. Modified **Scenarios**.
2018-08-16	This is the first official release.