Host Security Service

Descripción general del servicio

Edición	01
Fecha	2022-12-30

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Índice

1 ¿Qué es HSS?....1
2 Ventajas....5
3 Editions and Features....7
4 Escenarios....26
5 Restricciones....28
6 Detalles de precios....31
7 Mecanismo de protección de datos personales....34
8 Gestión de permisos HSS....36
9 Servicios relacionados....38
10 Acceso y uso....40
11 Conceptos....41

1 ¿Qué es HSS?

Host Security Service (HSS) está diseñado para proteger las cargas de trabajo de servidores en nubes híbridas y centros de datos multinube. Proporciona funciones de seguridad del host, Container Guard Service (CGS) y Web Tamper Protection (WTP).

HSS puede ayudarle a comprobar y gestionar sus servidores y contenedores de manera unificada, sin importar dónde se implementen.

HSS protege la integridad de su sistema, gestiona la seguridad de las aplicaciones, supervisa las operaciones de los usuarios y detecta intrusiones.

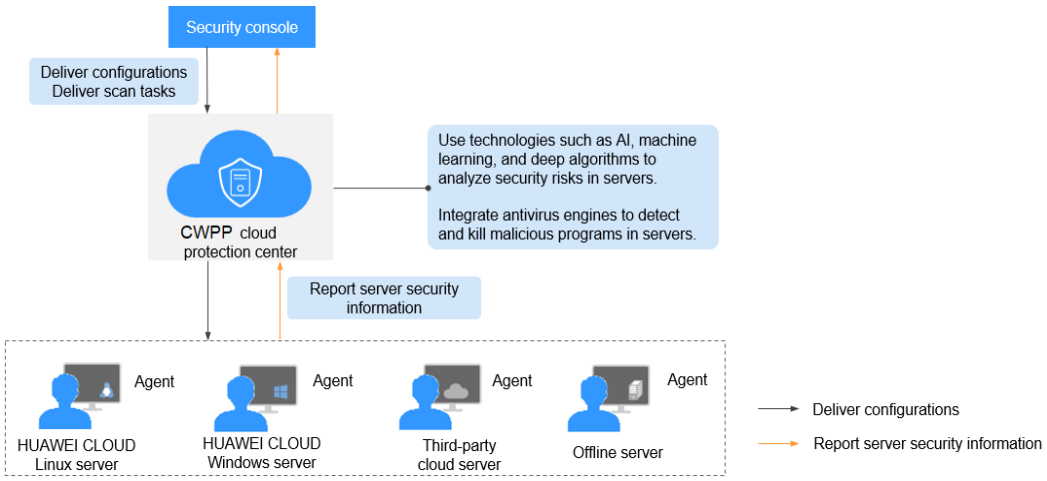
Seguridad de los hosts

Host Security Service (HSS) le ayuda a identificar y gestionar los activos de sus servidores, eliminar riesgos y defenderse de intrusiones y manipulación de páginas web. También hay funciones avanzadas de protección y operaciones de seguridad disponibles para ayudarle a detectar y manejar fácilmente las amenazas.

Instale el agente HSS en sus servidores y podrá comprobar el estado de seguridad del servidor y los riesgos en una región en la consola HSS.

Figura 1-1 ilustra cómo funciona HSS.

Figura 1-1 Principios de funcionamiento



En la siguiente tabla se describen los componentes HSS.

Tabla 1-1 Componentes

Componente	Descripción
Management console	Una plataforma de gestión visualizada, donde puede aplicar configuraciones de manera centralizada y ver el estado de defensa y los resultados de análisis de los servidores en una región.
HSS cloud protection center	● Utiliza tecnologías como IA, aprendizaje automático y algoritmos profundos para analizar los riesgos de seguridad en los servidores. ● Integra múltiples motores antivirus para detectar y eliminar programas maliciosos en servidores. ● Recibe configuraciones y tareas de análisis enviadas desde la consola y las reenvía a los agentes de los servidores. ● Recibe la información del servidor reportada por los agentes, analiza los riesgos de seguridad y las excepciones en los servidores y muestra los resultados del análisis en la consola.
Agent	● Se comunica con el centro de protección en la nube HSS a través de HTTPS y WSS. El puerto 10180 se utiliza de forma predeterminada. ● Analiza todos los servidores a primera hora de la mañana, supervisa el estado de seguridad de los servidores e informa de la información recopilada del servidor (incluyendo configuraciones no conformes, configuraciones inseguras, trazas de intrusión, lista de software, lista de puertos y lista de procesos) al centro de protección de la nube. ● Bloquea los ataques al servidor en función de las políticas de seguridad que haya configurado. **NOTA** ● Si el agente no está instalado o es anormal, HSS no está disponible. ● Se puede instalar un agente en Huawei Cloud Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), servidores fuera de línea y servidores en la nube de terceros. ● Seleccione el agente y el comando de instalación adecuados para su sistema operativo. ● Web Tamper Protection (WTP) y HSS pueden utilizar el mismo agente en un servidor.

Container Guard Service

Container Guard Service (CGS) analiza las vulnerabilidades y la información de configuración en las imágenes, ayudando a las empresas a detectar el entorno de contenedores, que no puede ser detectado por el software de seguridad tradicional. Además, CGS proporciona funciones como lista blanca de procesos de contenedores, supervisión de archivos de contenedores, recopilación de información de contenedores y detección de escape de contenedores para evitar riesgos de seguridad durante la ejecución del contenedor.

La siguiente imagen ilustra la arquitectura CGS.

Figura 1-2 Arquitectura CGS

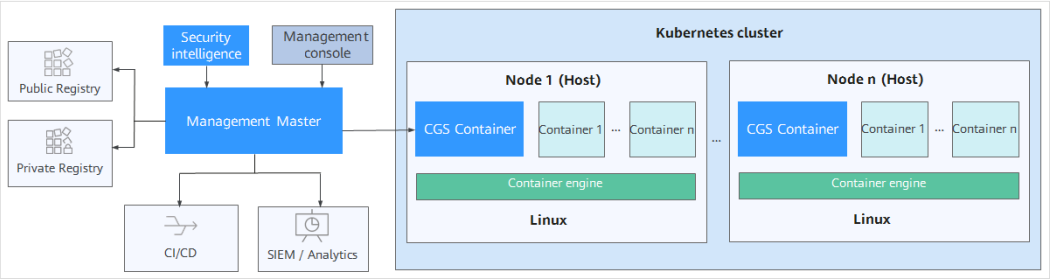


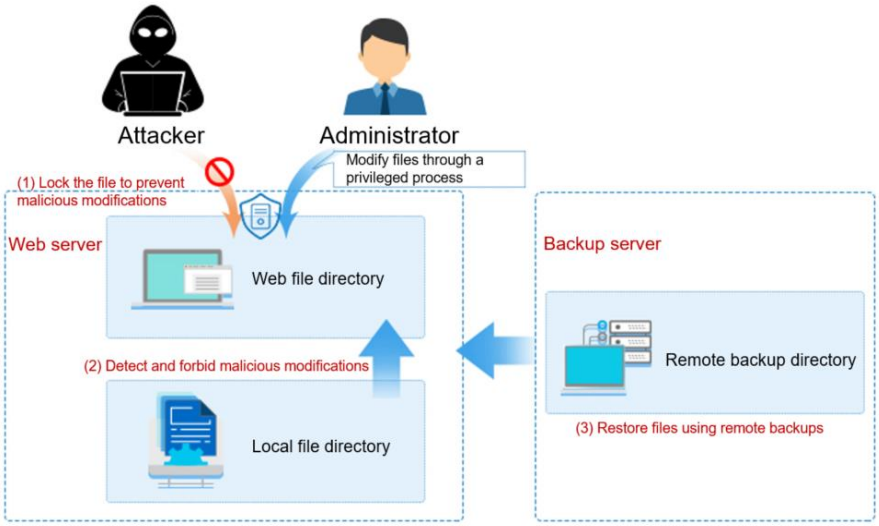
Tabla 1-2 Componentes clave de CGS

Componente	Descripción
CGS Container	Se ejecuta en cada nodo contenedor (host) para analizar todas las imágenes de contenedor en el nodo en busca de vulnerabilidades de imagen, implementar políticas de seguridad y recopilar excepciones.
Management Master	Gestiona y mantiene contenedores CGS.
Security intelligence	Proporciona una base de conocimientos de información de seguridad que contiene vulnerabilidades y bibliotecas de programas maliciosos, así como modelos de entrenamiento de IA de big data.
Management console	Proporciona una consola para que los usuarios utilicen CGS.

Web Tamper Protection

Web Tamper Protection (WTP) supervisa los directorios de sitios web en tiempo real y restaura archivos y directorios manipulados mediante sus copias de seguridad. Protege la información del sitio web, como páginas web, documentos electrónicos e imágenes, de ser manipulados o dañados por piratas informáticos.

Figura 1-3 Cómo funciona WTP



2 Ventajas

HSS le ayuda a gestionar y mantener la seguridad de todos sus servidores y a reducir los riesgos comunes.

Gestión centralizada

Puede comprobar y solucionar una serie de problemas de seguridad en una sola consola, administrando fácilmente sus servidores.

- Puede instalar el agente en ECS, BMS, servidores sin conexión y servidores en la nube de terceros de Huawei en la misma región para gestionarlos todos en una sola consola.
- En la consola de seguridad, puede ver los orígenes de los riesgos de servidor en una región, manejarlos de acuerdo con las sugerencias mostradas y usar las funciones de filtro, búsqueda y procesamiento por lotes para analizar rápidamente los riesgos de todos los servidores en la región.

Defensa precisa

HSS bloquea los ataques con precisión milimétrica mediante el uso de tecnologías de detección avanzadas y diversas bibliotecas.

Protección integral

HSS protege los servidores contra intrusiones mediante la prevención, la defensa y el análisis posterior a la intrusión.

Agente ligero

El agente ocupa solo unos pocos recursos, sin afectar al rendimiento del sistema del servidor.

WTP

- Se utilizan la tecnología antimanipulación web de tercera generación y la tecnología de activación de eventos a nivel del núcleo. Los archivos de los directorios de usuario se pueden bloquear para evitar manipulaciones no autorizadas.
- Se utilizan las tecnologías de detección y recuperación de manipulación. Los archivos modificados solo por usuarios autorizados son respaldados en servidores locales y

remotos en tiempo real, y se usarán para recuperar sitios web manipulados (si los hay) detectados por HSS.

3 Editions and Features

HSS comes in the basic, enterprise, premium, Web Tamper Protection (WTP), and Container Guard Security (CGS) editions, providing asset management, vulnerability management, baseline check, intrusion detection, ransomware protection, web tamper protection, and container image security functions. For details about the features of the editions, see **Edition Details**.

AVISO

- HSS comes in the basic, enterprise, premium, Web Tamper Protection (WTP), and container security editions. You can purchase or upgrade your edition as needed.

  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.

Features

HSS provides asset management, baseline check, ransomware prevention, and intrusion detection features, enhancing server security in all aspects. For details about the features of different editions, see **Edition Details**.

Tabla 3-1 HSS features

Feature	Description
Asset management	Perform a deep scan of the accounts, ports, processes, web directories, software, and auto-started tasks on your servers. You can manage all of your digital assets on the **Asset Management** page.

Feature	Description
Vulnerability management	Detect vulnerabilities and risks in Linux, Windows, Web content management systems (Web-CMS), and applications.
Baseline check	Scan for unsafe settings, weak passwords, and password complexity policies in server OS and key software. A security practice baseline and a compliance standard baseline can be used for scans.
Container image security	Scan the images that are running or displayed in your image list, and provide suggestions on how to fix vulnerabilities and malicious files.
Application protection	Protect running applications. You simply need to add probes to applications, without having to modify application files. So far, only Java applications can be protected.
Web page tampering prevention	Detect and prevent tampering of files in specified directories, including web pages, documents, and images, and quickly restore them using valid backup files.
Ransomware prevention	Monitor new files and running processes in real time, control risks in new files, dynamically generate bait files for proactive defense, accurately identify ransomware, and periodically back up servers based on user-defined policies.
File integrity monitoring	Check the files in the Linux OS, applications, and other components to detect tampering.
Intrusion detection	Identify and prevent intrusion to servers, discover risks in real time, detect and kill malicious programs, and identify web shells and other threats.
Container intrusion detection	Scan running containers for malicious programs including miners and ransomware; detect non-compliant security policies, file tampering, and container escape; and provide suggestions.
Whitelist management	To reduce false alarms, import events to and export events from the whitelist. Whitelisted events will not trigger alarms.
Policy management	You can group policies and servers to batch apply policies to servers, easily adapting to your business scenarios.
Security configuration	You can configure common login locations, common login IP addresses, the SSH login IP address whitelist, and automatic isolation and killing of malicious programs.

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. The pay-per-use basic 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, 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 containers that need to enhance image security, container runtime security, and to comply with security regulations, CGS is recommended.

AVISO

- 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, the HSS enterprise edition stops charging if the servers it protects are stopped.

Edition Details

Tabla 3-2 Editions

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Asset management	Server management	Manages all server assets, including their protection statuses, quotas, and policies. You can install agents on all the Linux servers in batches.	√	√	√	√	√	-
	Container management	Manage container nodes and images (private image repositories and local images).	×	×	×	×	√	-

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Asset fingerprint	Account management	Check and manage server accounts all in one place.	×	√	√	√	√	Real-time check
	Open port check	Check open ports all in one place and identify high-risk and unknown ports.	×	√	√	√	√	Real-time check
	Process management	Check running applications all in one place and identify malicious applications.	×	√	√	√	√	Real-time check
	Software management	Check and manage server software all in one place and identify insecure versions.	×	√	√	√	√	Automatic check in the early morning every day
	Auto-startup	Check auto-started entries and collect statistics on entry changes in a timely manner.	×	√	√	√	√	Real-time check
	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.	×	√	√	√	√	Once a week (05:00 a.m. every Monday)
	Web framework	Check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	×	√	√	√	√	Once a week (05:00 a.m. every Monday)

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Middleware	Check information about servers, versions, paths, and processes associated with middleware.	×	√	√	√	√	Once a week (05:00 a.m. every Monday)
	Kernel module	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.	×	√	√	√	√	Once a week (05:00 a.m. every Monday)
Vulnerability management	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 morning every day ● Manual scan
	Web-CMS vulnerability detection	HSS scans for Web-CMS vulnerabilities in web directories and files.	×	√	√	√	√	● Automatic check in the early morning every day ● Manual scan

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Application vulnerabilities	Detect vulnerabilities in assets, such as web services, web frameworks, websites, middleware, and kernel modules.	×	√	√	√	√	● Automatic check in the early morning every day ● Manual scan
Unsafe settings check	Password policy check	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.	√	√	√	√	√	● Automatic check in the early morning every day ● Manual scan
	Weak password check	Change weak passwords to stronger ones based on HSS scan results and suggestions.	√	√	√	√	√	● Automatic check in the early morning every day ● Manual scan
	Unsafe configurations	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	×	√	√	√	√	● Automatic check in the early morning every day ● Manual scan

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Container image security	Container image vulnerability management	Detect and manage vulnerabilities in local images and private image repositories based on a vulnerability database, and handle critical vulnerabilities in a timely manner.	×	×	×	×	√	● Automatic check in the early morning every day ● Manual scan
	Malicious image file detection	Scan images for malicious files (such as Trojans, worms, viruses, and adware) and identify risks.	×	×	×	×	√	Real-time check
	Image baseline check	Check for insecure configurations based on 18 types of container baselines.	×	×	×	×	√	Real-time check
Application protection	SQL injection	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities.	×	×	√	√	√	Real-time check
	OS command injection	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities.	×	×	√	√	√	Real-time check
	XSS	Detect and defend against stored cross-site scripting (XSS) injection attacks.	×	×	√	√	√	Real-time check
	Log4jRCE vulnerability	Detect and defend against remote code execution.	×	×	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Web shell upload	Detect and defend against attacks that upload dangerous files, change file names, or change file name extension types; and check web applications for related vulnerabilities.	×	×	√	√	√	Real-time check
	XML External Entity Injection	Detect and defend against XML External Entity Injection (XXE) attacks, and check web applications for related vulnerabilities.	×	×	√	√	√	Real-time check
	Deserialization input	Detect deserialization attacks that exploit unsafe classes.	×	×	√	√	√	Real-time check
	File directory traversal	Check whether sensitive directories or files are accessed.	×	×	√	√	√	Real-time check
	Struts2 OGNL	Detect OGNL code execution.	×	×	√	√	√	Real-time check
	Command execution using JSP	Detect command execution using JSP.	×	×	√	√	√	Real-time checks
	File deletion using JSP	Detects file deletion using JSP.	×	×	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Database connection exception	Detect authentication and communication exceptions thrown by database connections.	×	×	√	√	√	Real-time check
	0-day vulnerability	Check whether the stack hash of a command is in the whitelist of the web application.	×	×	√	√	√	Real-time check
	SecurityManager permission exception	Detect exceptions thrown by SecurityManager.	×	×	√	√	√	Real-time check
Web page tampering prevention	Static WTP	Protect the static web page files on your website servers from malicious modification.	×	×	×	√	×	Real-time check
	Dynamic WTP	Protect the dynamic web page files in your website databases from malicious modification.	×	×	×	√	×	Real-time check
Ransomware prevention	Ransomware prevention	Analyze operations on servers, identify trusted applications, and report alarms on or block untrusted applications, depending on your settings.	×	×	√	√	√	Real-time checks

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Monitor file integrity	File Integrity	Check the files in the Linux OS, applications, and other components to detect tampering.	×	×	√	√	√	Real-time check
Intrusion detection	Malicious program	Check and handle detected malicious programs all in one place, including web shells, Trojan horses, mining software, worms, and viruses.	×	√	√	√	√	Real-time check
	Ransomware	Check ransomware embedded in media such as web pages, software, emails, and storage media. Ransomware is used to encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.	×	×	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	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 scan for web shells on servers.	×	√	√	√	√	Real-time check
	Reverse shell	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.	×	×	√	√	√	Real-time check
	Vulnerability exploit	Detect server intrusions by exploiting vulnerabilities in real time and report alarms.	×	√	√	√	√	Real-time check
	File privilege escalation	Check the file privilege escalations in your system.	×	×	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Process privilege escalation	The following process privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities	×	×	√	√	√	Real-time check
	Change in critical file	Receive alarms when critical system files are modified.	×	√	√	√	√	Real-time check
	File/Directory changes	System files and directories are monitored. When a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.	×	√	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	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	×	√	√	√	√	Real-time check
	High-risk command execution	Receive real-time alarms on high-risk commands.	×	×	√	√	√	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

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Suspicious crontab task	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.	×	×	√	√	√	Real-time check
	Brute-force attack defense	Check for brute-force attack attempts and successful brute-force attacks. ● Your accounts are protected from brute-force attacks. HSS will block the attacking hosts when detecting such attacks. ● Trigger an alarm if a user logs in to the host by a brute-force attack.	√	√	√	√	√	Real-time check
	Abnormal login	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered.	√	√	√	√	√	Real-time check
	Invalid account	Scan accounts on servers and list suspicious accounts in a timely manner.	×	√	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Container intrusion detection	Vulnerability escape	An escape alarm is reported if a container process behavior that matches the behavior of known vulnerabilities is detected.	×	×	×	×	√	Real-time checks
	File escape	An alarm is reported if a container process is found accessing a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.	×	×	×	×	√	Real-time check
	Abnormal container process	● Malicious container program Monitor container process behavior and process file fingerprints. An alarm is reported if it detects a process whose behavior characteristics match those of a predefined malicious program. ● Abnormal process An alarm is reported if a process not in the whitelist is running in the container.	×	×	×	×	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
	Abnormal container startup	The service monitors container startups and reports an alarm if it detects that a container with too many permissions is started. Container check items include: ● Privileged container startup (**privileged:true**) ● Too many container capabilities (**capability:[xxx]**) ● Seccomp not enabled (**seccomp=unconfined**) ● Container privilege escalation (**no-new-privileges:false**) ● High-risk directory mapping (**mounts:[...]**)	×	×	×	×	√	Real-time check
	High-risk system call	You can run tasks in kernels by Linux system calls. CGS monitors container processes. This alarm is generated when CGS detects that a process uses high-risk system calls.	×	×	×	×	√	Real-time check
	Sensitive file access	The service monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.	×	×	×	×	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Whitelist management	Alarm whitelist	You can add an alarm to the whitelist when handling it. The following types of events can be added to the alarm whitelist: ● Reverse shell ● Web shells ● Abnormal process behaviors ● Process privilege escalation ● File privilege escalation ● High-risk commands ● Malicious programs	×	×	√	√	√	Real-time check
Policy management	Querying and editing rule configurations	You can define and issue different detection policies for different servers or server groups, implementing refined security operations. ● View the policy list. ● Create a policy group based on default and existing policy groups. ● Define a policy. ● Edit or delete a policy. ● Modify or disable policies in a group. ● Apply policies to servers in batches on the **Servers & Quota** page.	×	√ (Only the default enterprise policy group is supported.)	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	Check Frequency
Security report	Server security report	Check weekly or monthly server security trend, key security events, and risks.	×	√	√	√	√	-
Security configuration	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.	√	√	√	√	√	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.	√	√	√	√	√	Real-time check

Function	Item	Description	Basic (pay-per-use, yearly/monthly)	Enterprise	Premium	WTP	CGS	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. **NOTA** The SSH IP address whitelist does not take effect for servers running Kunpeng EulerOS (EulerOS with Arm).	√	√	√	√	√	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.	×	√	√	√	√	Real-time check
	2FA	Prevent brute-force attacks by using password and SMS/email authentication.	×	√	√	√	√	-
	Alarm configuration	After alarm notification is enabled, you can receive alarm notifications to learn about security risks facing your servers, containers, and web pages.	√	√	√	√	√	-

4 Escenarios

HSS

- Cumplimiento del Esquema de Protección Multinivel (MLPS) de DJCP

  La función de detección de intrusos de HSS protege cuentas y sistemas en servidores en la nube, ayudando a las empresas a cumplir con los estándares de cumplimiento.

  Para solicitar la certificación DJCP MLPS, compre la edición empresarial o una edición superior (edición premium o edición de Web Tamper Protection).

- Gestión de seguridad centralizada

  Con HSS, puede gestionar las configuraciones de seguridad y los eventos de todos sus servidores en la nube en la consola, reduciendo los riesgos y los costos de gestión.

- Evaluación de riesgos de seguridad

  Usted puede comprobar y eliminar todos los riesgos (como cuentas riesgosas, puertos abiertos, vulnerabilidades de software y contraseñas débiles) en sus servidores.

- Protección de cuentas

  Aproveche las capacidades integrales de seguridad de la cuenta, que incluyen prevención, antiataque y análisis posterior al ataque. Puede usar 2FA para bloquear ataques de fuerza bruta a las cuentas, mejorando la seguridad de sus servidores en la nube.

- Seguridad proactiva

  Cuente y analice sus activos de servidor, compruebe y corrija vulnerabilidades y configuraciones inseguras, y proteja de forma proactiva su red, aplicaciones y archivos de ataques.

- Detección de intrusiones

  Escanee todos los posibles vectores de ataque para detectar y combatir las amenazas persistentes avanzadas (APT) y otras amenazas en tiempo real, protegiendo su sistema de su impacto.

CGS

- Seguridad de las imágenes de contenedores

  Las vulnerabilidades probablemente se introducirán en su sistema a través de las imágenes descargadas desde Docker Hub o a través de marcos de código abierto.

Puede usar CGS para analizar imágenes en busca de riesgos, como vulnerabilidades de imágenes, cuentas inseguras y archivos maliciosos. Recibir recordatorios y sugerencias y eliminar los riesgos en consecuencia.

- Seguridad del entorno de ejecución de contenedores

  Desarrolle una lista blanca de comportamientos de contenedores para garantizar que los contenedores funcionen con los permisos mínimos requeridos, asegurando los contenedores contra amenazas potenciales.

- Cumplimiento con DJCP MLPS

  Evite intrusiones y código malicioso, asegurándose de que la seguridad de su contenedor y sistema cumpla con los requisitos de cumplimiento.

5 Restricciones

Tipos de servidor admitidos

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

Regiones admitidas

Tabla 5-1 Regiones soportadas por HSS en el sitio web internacional de Huawei Cloud

Código de región	Nombre de la región
cn-south-1	CN South-Guangzhou
ap-southeast-1	CN-Hong Kong
ap-southeast-2	AP-Bangkok
ap-southeast-3	AP-Singapore

Sistemas operativos compatibles

HSS puede ejecutarse en servidores Linux (como CentOS y EulerOS) y servidores Windows (como Windows 2012 y Windows 2016).

AVISO

- El agente es probablemente incompatible con las versiones de Linux o Windows que han llegado al final de su vida útil. Para obtener una mejor experiencia de servicio HSS, se recomienda instalar o actualizar a una versión del sistema operativo compatible con el agente.
  - Las versiones de CentOS 6.x ya no son actualizadas o mantenidas por Linux, por lo tanto, ya no son compatibles con HSS. Si necesita estas versiones, puede **enviar una orden de trabajo** para obtener ayuda.

- Tabla 5-2 y Tabla 5-3 describir las versiones de Linux que son utilizadas por los servidores en la nube y compatibles con HSS.

  NOTA

  Algunas distribuciones de sistema operativo no son compatibles por ahora. Se admitirán en versiones posteriores.

Tabla 5-2 Distribuciones Linux (arquitectura x86)

No.	Versión del sistema operativo
1	CentOS: 7 and 8 (64-bit)
2	Debian 7, 8, 9, 10, and 11 (32 or 64 bit)
3	EulerOS: v2r7 and v2r9 (64-bit)
4	Fedora: 24, 25, 28, and 30 (64 bit)
5	OpenSUSE: 13, 15, and 42 (64 bit)
6	Ubuntu: 16, 18, and 20 (32 or 64 bit)
7	RedHat: 8 (64-bit)
8	HCE: 2 (64-bit)
9	kylin: V7 (64-bit)
10	NeoKylin: V10 (64-bit)
11	OpenEuler: 20 and 22 (64-bit)
12	AlmaLinux: 9 (64-bit)

Tabla 5-3 Distribuciones Linux (arquitectura de Arm)

No.	Versión del sistema operativo
1	CentOS: 7and8 64bit with ARM(40GB)
2	EulerOS: 2 64bit with ARM(40GB)
3	Fedora: 29 64bit with ARM (40 GB)
4	OpenSUSE: 15 64bit with ARM(40GB)
5	Ubuntu: 18and20 64bit with ARM(40GB)
6	kylin: V10 (aarch64bit)
7	HCE: 2 (aarch64bit)
8	UOS: 20 (aarch64bit)

- Tabla 5-4 enumera las versiones de Windows que utilizan los servidores Huawei Cloud y que son compatibles con HSS.

Tabla 5-4 Versiones de Windows

No.	Versión del sistema operativo	Restricciones
1	Windows Server 2019 Datacenter 64-bit English (40 GB)	Si se ha instalado un software de seguridad de terceros, como McAfee en el servidor, detenga la función de protección del software antes de instalar un agente HSS. Después de instalar el agente, puede volver a activar la función de protección en el software.
2	Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	
3	Windows Server 2018 Datacenter 64-bit English (40 GB)	
4	Windows Server 2018 Datacenter 64-bit Chinese (40 GB)	
5	Windows Server 2016 Standard 64-bit English (40 GB)	
6	Windows Server 2016 Standard 64-bit Chinese (40 GB)	
7	Windows Server 2016 Datacenter 64-bit English (40 GB)	
8	Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	
9	Windows Server 2012 R2 Standard 64-bit English (40 GB)	
10	Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	
11	Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	
12	Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	

6 Detalles de precios

Esta sección describe los precios y la información de renovación sobre HSS. Para obtener más información, consulte **Detalles de precios**.

Artículos de facturación

Se le cobrará en función de su edición de HSS y la duración del uso.

Tabla 6-1 Artículos de facturación

Artículo	Descripción
Edition (mandatory)	Edición (básica, empresarial, premium o WTP) **NOTA** Al comprar un ECS, puede habilitar la edición básica de HSS de forma gratuita. La prueba gratuita dura 30 días.
Required Duration	El HSS anual/mensual se factura anualmente o mensualmente.

Modos de facturación

Puede comprar HSS en modo de pago por uso o anual/mensual.

Tabla 6-2 Modos de facturación HSS

Edición	Modo de facturación	Descripción	Precios
Basic	● Anual/Mensual La edición básica en modo anual/mensual no tiene un período de prueba gratuito. ● Pago por uso Puede utilizar la edición básica para cada uno de sus servidores durante 30 días naturales gratis o con cargo. Al comprar un ECS, puede habilitar la edición básica de HSS de forma gratuita. La prueba gratuita dura 30 días.	● Pago por uso: Usted paga por los recursos usados en función de la duración real del servicio (en horas), sin una tarifa mínima. ● Los recursos anuales/mensuales ofrecen un mayor descuento. Este modo se recomienda para usuarios a largo plazo. Se factura un VSS anual/mensual basado en el período de compra especificado en el pedido.	**Detalles de precios**
Enterprise	● Anual/Mensual ● Pago por uso		
Premium	Anual/Mensual		
WTP	Anual/Mensual		

Cambio de configuraciones

- Cambio del modo de facturación
  - De pago por uso a anual/mensual

    Se generará un pedido de paquete anual/mensual para usted. La cuota anual/mensual estará disponible inmediatamente cuando complete el pago. Para habilitar la cuota anual/mensual, elija **Servers & Quotas** y haga clic en la pestaña **Servers**. En la columna **Operation** del servidor requerido, haga clic en **Enable** y seleccione la cuota anual/mensual.
  - De anual/mensual a pago por uso

    Elija **Servers & Quotas** y haga clic en la pestaña **Servers**. En la columna **Operation** del servidor requerido, haga clic en **Enable** y seleccione la cuota bajo demanda.

- Cancelación de suscripción

  Si ya no necesita usar HSS, puede **darse de baja** de él en el Centro de facturación.

Renovación

Si la cuota de HSS adquirida expira, puede renovar la cuota para ampliar su período de validez. También puede configurar la renovación automática. Para obtener más información sobre HSS, consulte **Reglas de renovación**.

Vencimiento y pago atrasado

Si no renueva su suscripción anual/mensual al expirar, hay un período de retención para usted. Para obtener más información, consulte **Período de retención**.

Si su cuenta está en mora, podrá visualizar los detalles de los pagos en mora en el Centro de facturación. Para evitar que los recursos se desactiven o se liberen, debe recargar su cuenta dentro del período especificado. Para obtener más información, consulte **Reembolso de atrasos**.

Preguntas frecuentes

Para obtener más preguntas frecuentes sobre la carga, consulte **Preguntas frecuentes sobre HSS**.

7 Mecanismo de protección de datos personales

Para garantizar que sus datos personales, como su nombre de usuario, contraseña y número de teléfono móvil, no serán violados por entidades o personas no autorizadas o no autenticadas, HSS cifra sus datos personales antes de almacenarlos para controlar el acceso a los datos.

Datos personales

Tabla 7-1 describe los datos personales generados o recopilados por HSS.

Tabla 7-1 Datos personales

Tipo	Método de colección	Puede ser modificado	Obligatorio
Correo electrónico	Si 2FA está habilitado, HSS obtiene periódicamente de SMN las direcciones de correo electrónico que se suscriben a temas de notificación.	No	Sí
Número de teléfono móvil	Si se habilita la 2FA, el HSS obtiene periódicamente de SMN los números de teléfono móvil que se suscriben a temas de notificación.	No	Sí
Ubicación de inicio de sesión	Si HSS está habilitado, registra las ubicaciones de inicio de sesión del usuario.	No	Sí

Modo de almacenamiento

HSS utiliza algoritmos de encriptación para cifrar los datos confidenciales de los usuarios y almacena datos encriptacións.

- El número de teléfono móvil se cifra antes del almacenamiento.
- Las ubicaciones de inicio de sesión no son datos confidenciales y se almacenan en texto plano.

Control de acceso

Los datos personales del usuario se cifran antes de ser almacenados en la base de datos HSS. El mecanismo de lista blanca se utiliza para controlar el acceso a la base de datos.

8 Gestión de permisos HSS

Si necesita asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos de HSS, IAM es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos en la nube.

Con IAM, puede usar su cuenta de Huawei Cloud para crear usuarios de IAM para sus empleados y asignar permisos a los usuarios para controlar su acceso a tipos de recursos específicos. Por ejemplo, algunos desarrolladores de software de su empresa necesitan usar recursos HSS pero no deben eliminarlos ni realizar operaciones de alto riesgo. Para lograr este resultado, puede crear usuarios de IAM para los desarrolladores de software y concederles solo los permisos necesarios para usar los recursos HSS.

Si su cuenta de Huawei Cloud no necesita usuarios individuales de IAM para la gestión de permisos, puede omitir este capítulo.

IAM se puede utilizar de forma gratuita. Solo paga por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte **¿Qué es IAM?**

Permisos de HSS

De forma predeterminada, los nuevos usuarios de IAM no tienen permisos asignados. Debe agregar un usuario a uno o más grupos y adjuntar políticas o roles de permisos a estos grupos. Los usuarios heredan permisos de sus grupos y pueden realizar operaciones específicas en servicios en la nube.

HSS es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Para asignar permisos HSS a un grupo de usuarios, especifique el ámbito como proyectos específicos de la región y seleccione proyectos para que los permisos surtan efecto. Si se selecciona **All projects**, los permisos surtirán efecto para el grupo de usuarios en todos los proyectos específicos de la región. Al acceder a HSS, los usuarios deben cambiar a una región en la que se les haya autorizado a usar servicios en la nube.

Puede conceder permisos mediante roles o políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades del usuario. Este mecanismo proporciona solo un número limitado de roles de nivel de servicio para la autorización. Algunos roles dependen de otros roles para que surtan efecto. Cuando asigne dichos roles a los usuarios, recuerde asignar los roles de los que dependen. Sin embargo, los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.

- Políticas: Un tipo de autorización detallada que define los permisos necesarios para realizar operaciones en recursos específicos de la nube bajo ciertas condiciones. Este tipo de autorización es más flexible e ideal para un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de HSS únicamente los permisos para administrar un determinado tipo de recursos. La mayoría de las políticas definen permisos basados en API.

En la siguiente tabla se describen todos los permisos del sistema de APM.

Tabla 8-1 Permisos definidos por el sistema admitidos por HSS

Nombre de rol/política	Descripción	Tipo	Dependencia
HSS Administrator	Administrador de HSS, que tiene todos los permisos de HSS.	System-defined role	• Depende del rol de **Tenant Guest**. Tenant Guest: Un rol global, que debe asignarse en el proyecto global. • Para adquirir cuotas de protección HSS, debe tener los roles de **ECS ReadOnlyAccess** y **BSS Administrator**. – **ECS ReadOnlyAccess**: permiso de acceso de solo lectura para el ECS. Esta es una política del sistema. – **BSS Administrator**: un rol de sistema, que es el administrador del centro de facturación (BSS) y tiene permisos completos para el servicio.
HSSFullAccess	Todos los permisos de HSS	Policy	Para adquirir cuotas de protección HSS, debe tener la función de **BSS Administrator**. **BSS Administrator**: un rol de sistema, que es el administrador del centro de facturación (BSS) y tiene permisos completos para el servicio.
HSSReadOnlyAccess	Permisos de sólo lectura para HSS	Policy	Ninguno

Referencia

- **¿Qué es IAM?**
- **Creación de un usuario y concesión de permisos**

9 Servicios relacionados

Puede usar SMN para recibir notificaciones de alarma, el servicio IAM para gestionar los permisos de usuario y Cloud Trace Service (CTS) para auditar los comportamientos de los usuarios.

Elastic Cloud Server (ECS)/Bare Metal Server (BMS)

Los agentes HSS se pueden instalar en ECS, BMS, o servidores de terceros de Huawei Cloud. Se recomienda utilizar los servidores Cloud de Huawei para una experiencia de servicio mejor y más confiable.

- Para obtener más información sobre ECS, consulte la *Guía del usuario de Elastic Cloud Server*.
- Para obtener más información sobre BMS, consulte la *Guía del usuario de Bare Metal Server*.

CCE

Cloud Container Engine (CCE) crea rápidamente un clúster de contenedores altamente confiable basado en el servidor en la nube y agrega nodos en el clúster. HSS instala escudos en un clúster para proteger las aplicaciones de contenedores en los nodos de un clúster.

NOTA

CCE es un servicio de alto rendimiento y alta confiabilidad a través del cual las empresas pueden gestionar aplicaciones en contenedores. CCE es compatible con aplicaciones y herramientas nativas de Kubernetes que permiten establecer fácilmente un entorno de ejecución de contenedores en la nube. Para obtener más información, consulte la *Guía del usuario de Container Service*.

SWR

Software Repository for Container (SWR) proporciona una gestión simple, segura y confiable de las imágenes en contenedores durante todo sus ciclos de vida, lo que facilita el despliegue de servicios en contenedores. Para obtener más información, consulte la *Guía del usuario del repositorio de software para contenedores*. HSS analiza vulnerabilidades y configuraciones en las imágenes de contenedores para ayudar a las empresas a detectar el entorno de contenedores que no se puede lograr con el software de seguridad tradicional.

Simple Message Notification (SMN)

SMN es un servicio de procesamiento de mensajes extensible y de alto rendimiento.

- Para habilitar las notificaciones de alarma, primero debe configurar SMN.
- Una vez habilitado el SMN, recibirá notificaciones de alarma enviadas desde HSS si su servidor es atacado o si se detectan altos riesgos.
- En la pestaña **Alarm Notification**, puede configurar la **Daily Alarm Notification** y la **Real-Time Alarm Notification** según sea necesario.

Para obtener más información acerca de SMN, consulte la *Simple Message Notification User Guide*.

Gestión de identidades y acceso

IAM es un servicio gratuito de gestión de identidades que puede implementar un aislamiento y control de permisos de usuario refinados basados en identidades de usuario. Es el servicio básico de gestión de permisos y se puede utilizar de forma gratuita.

Para obtener más información sobre IAM, consulte *Guía del usuario de Identity and Access Management*.

Cloud Trace Service (CTS)

CTS es un servicio de auditoría de registro profesional que registra las operaciones de los usuarios en HSS. Puede utilizar los registros para el análisis de seguridad, la auditoría de cumplimiento, el seguimiento de recursos y la localización de fallos. Es el servicio básico de gestión de registros y se puede utilizar de forma gratuita.

Para obtener más información sobre CTS, consulte *Guía del usuario del servicio Cloud Trace*.

10 Acceso y uso

Inicie sesión en el portal de operación de ManageOne. Haga clic  en la esquina superior izquierda, seleccione una región y seleccione el servicio CBH.

Entrada de inicio de sesión

Paso 1 Inicie sesión en ManageOne como administrador u operador de VDC mediante un navegador.

URL: https://*Domain name of ManageOne Operation Portal*, Ejemplo: **https://console.demo.com**

Paso 2 Haga clic  en la esquina superior izquierda de la página, seleccione una región y elija **Host Security Service**.

Paso 3 En la esquina superior derecha de la página Host Security Service, haga clic en **Buy HSS**.

----Fin

11 Conceptos

Vulneración de una cuenta

Vulneración de una cuenta se refiere al comportamiento intruso de adivinar o descifrar la contraseña de una cuenta.

Ver información sobre contraseñas débiles

Una contraseña débil se puede descifrar fácilmente.

Consulta de información sobre programas maliciosos

Un programa malicioso, como una puerta trasera, un caballo de Troya, un gusano o un virus, se desarrolla con ataques o intentos de control remoto ilegales.

El malware incrusta código en otro programa para ejecutar programas intrusivos o disruptivos y dañar la seguridad e integridad de los datos en un servidor infectado. El malware incluye virus, caballos de Troya y gusanos, clasificados por sus formas de transmisión.

HSS informa de malware identificado y sospechoso.

Ransomware

El ransomware surgió con la economía Bitcoin. Es un troyano que se disfraza como un archivo adjunto de correo electrónico legítimo o software incluido y te engaña para abrirlo o instalarlo. También puede llegar a sus servidores a través de la intrusión del sitio web o servidor.

Ransomware a menudo utiliza una gama de algoritmos para cifrar los archivos de la víctima y exigir un pago de rescate para obtener la clave de descifrado. Las monedas digitales como Bitcoin se usan típicamente para los rescates, lo que dificulta el rastreo y procesamiento de los atacantes.

El ransomware interrumpe las empresas y puede causar graves pérdidas económicas. Necesitamos saber cómo funciona y cómo podemos prevenirlo.

Web Tamper Protection

Web Tamper Protection (WTP) es una edición HSS que protege sus archivos, como páginas web, documentos e imágenes, en directorios específicos contra la manipulación y el sabotaje de hackers y virus.

Clúster

Un clúster consta de uno o más ECS (también conocidos como nodos) en la misma subred. Proporciona un grupo de recursos informáticos para ejecutar contenedores.

Nodo

En CGS, cada nodo corresponde a un ECS. Los contenedores se ejecutan en nodos.

Imágenes

Una imagen es un sistema especial de archivos. Además de proporcionar programas, bibliotecas, recursos y archivos de configuración, proporciona algunos parámetros de configuración necesarios para un contenedor en funcionamiento. Una imagen Docker no contiene ningún dato dinámico y su contenido permanece sin cambios después de ser construido.

Contenedor

Un contenedor es la instancia de una imagen y se puede crear, iniciar, detener, eliminar y suspender.

Cuotas de protección

Para proteger un servidor, envíelo a una cuota HSS.

Las cuotas de las diferentes ediciones de HSS que compró se muestran en la consola.

Ejemplo:

- Si ha adquirido una cuota de edición empresarial HSS, puede vincularla a un servidor.
- Si ha adquirido 10 cuotas de edición empresarial de HSS, puede vincularlas a 10 servidores.

