Host Security Service

What's New

Issue 01

Date 2023-07-10

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 What's New

This topic describes the features of each Host Security Service (HSS) version and the corresponding documentation updates.

March 2023

No.	Feature	Description	Phase	Related Documents
1	Honeypot file protection for Windows	Honeypot files can be deployed in protected directories and important directories (except for the excluded directories specified by users) to trap possible ransomware. If an unknown ransomware attempts to encrypt a honeypot file, HSS immediately generates an alarm.	Commercial use	**Enabling Ransomware Prevention**
2	The Windows policy group supports antivirus and host intrusion prevention system (HIPS) detection policies.	You can set antivirus detection policies for Windows servers to report, isolate, and kill viruses. You can also set HIPS detection policies to detect registries, files, and processes; and to report alarms for suspicious operations such as abnormal changes.	Commercial use	**Policy Group**

No.	Feature	Description	Phase	Related Documents
3	Trojans, viruses, and worms can trigger HID alarms.	HSS can detect, generate alarms on, and remove Trojans, viruses, and worms that intrude servers.	Commercial use	Server Alarms
4	The Docker plug-in is added to enhance container security.	To improve container security capabilities, the Docker plug-in must be installed for Docker containers (Linux).	Commercial use	Installing a Plug-in

January 2023

No.	Feature	Description	Phase	Related Documents
1	Batch agent installation	The agent can be installed on multiple servers in batches.	Commercial use	Installing Agents in Batches
2	Privileged processes can be configured in the WTP edition.	If WTP is enabled, the content in the protected directories is read-only. To allow certain processes to modify files in the directories, add them to the privileged process list. Only the modification made by privileged processes can take effect. Modifications made by other processes will be automatically rolled back.	Commercial use	Adding a Privileged Process

June 2022

No.	Feature	Description	Phase	Document
1	Agent upgrade	You can upgrade agent 1.0 to agent 2.0. After the upgrade, you can view and manage the server protection status on HSS (New). HSS (Old) will stop detection.	Commercial use	-

December 2021

No.	Feature	Description	Phase	Document
1	Detection of remote code execution vulnerabilities	Apache Log4j2 remote code execution vulnerabilities (CVE-2021-44228 and CVE-2021-45046) can be detected.	Commercial use	-

