Host Security Service

Best Practices

Issue 11

Date 2021-07-08



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Quickly Learning Your Host Security Status..... 1
2 Quickly Enhancing Server Security.....5
3 Detecting and Fixing Vulnerabilities..... 18
3.1 Git Credential Disclosure Vulnerability (CVE-2020-5260)..... 18
3.2 SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)..... 20
3.3 OpenSSL High-risk Vulnerability (CVE-2020-1967)..... 22
3.4 Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/CVE-2020-0938)..... 23
3.5 Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)..... 24
3.6 Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)..... 26
4 Best Practices for Defense Against Ransomware..... 29
5 Best Practices for Using Host Security Service Basic Edition (Free)..... 43
A Change History..... 50

 Copyright © Huawei Technologies Co., Ltd.

1 Quickly Learning Your Host Security Status

HSS helps you ensure the overall security of your servers. You can monitor risks in real time and prevent unauthorized intrusions, isolate and kill malicious programs, check for vulnerabilities and unsafe settings, and identify and manage assets on your servers with just a few clicks.

Risk Overview

On the HSS dashboard, you can check real-time server security statistics, including recent risks, protected servers, risk trend, handled risks, intrusion event statistics, and top 5 unsafe servers. For details, see **Server Risk Overview**.

 Copyright © Huawei Technologies Co., Ltd.

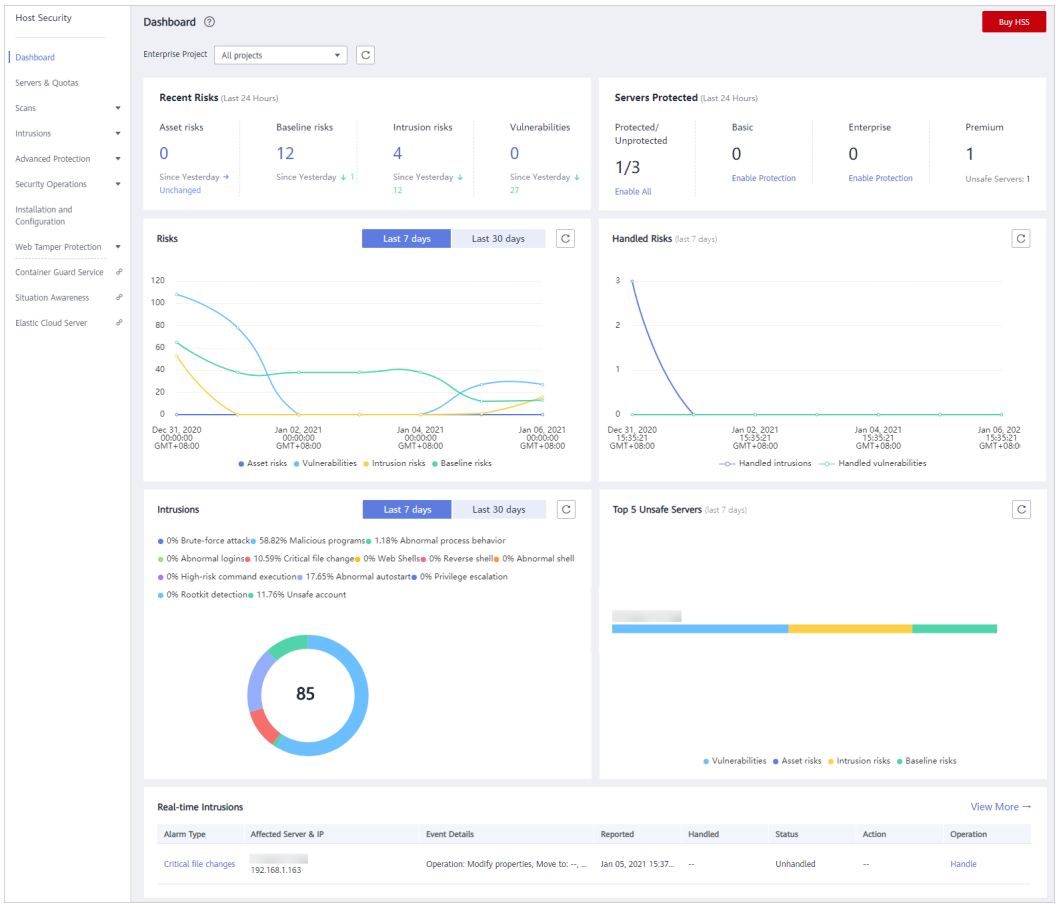


Table 1-1 Server security situation

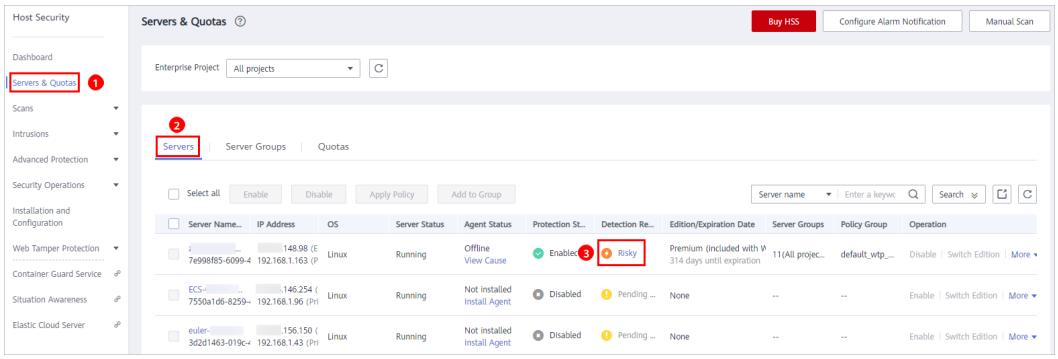
Statistics	Description
Recent risks	Number of risks (asset risks, unsafe settings, intrusions, and vulnerabilities) on protected servers You can click a number to go to the details page and handle risks. You can also check statistics changes since yesterday. • Asset risks • Baseline risks • Intrusions • Vulnerabilities
Servers protected	Numbers of servers protected with the basic, enterprise, or premium edition and the number of unprotected servers. You can check and manage server protection here.
Risks	Line chart showing the numbers of asset risks, vulnerabilities, unsafe settings, and intrusions in the last 7 days or 30 days
Handled Risks	Line chart showing the numbers of handled asset risks, vulnerabilities, unsafe settings, and intrusions in the last 7 days
Intrusions	Numbers and types of intrusions in the last 7 days or 30 days

 Copyright © Huawei Technologies Co., Ltd.

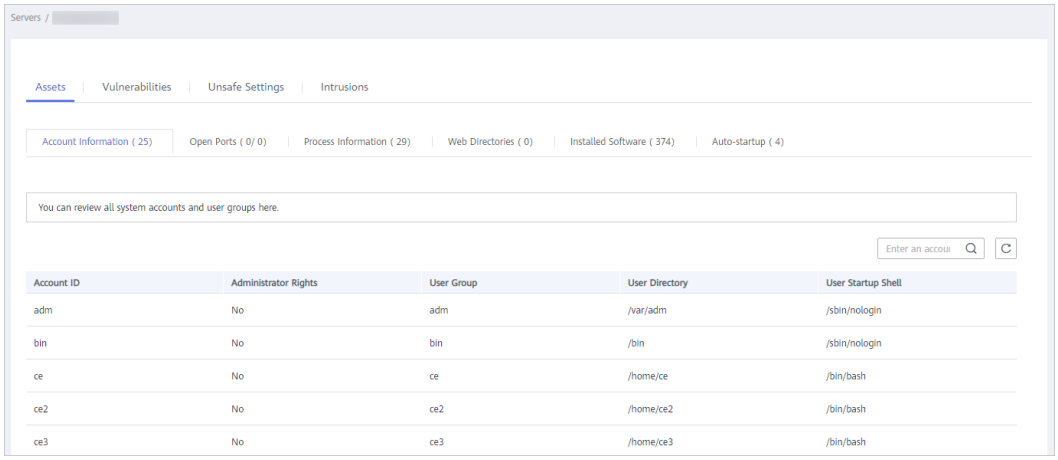
Statistics	Description
Top 5 Unsafe Servers	Top 5 unsafe servers and their asset risks, vulnerabilities, intrusions, and baseline risks
Real-time Intrusions	The latest five intrusion events that have not been handled in the last 24 hours, their alarm names, affected server names/IP addresses, description, occurrence time, and status. • To check alarm details, click an alarm name. • To handle an alarm, click **Handle** in its **Operation** column. After the alarm is handled, it will be removed from the list. The list refreshes and displays the latest five intrusion events that have not been handled in the last seven days. • To check more alarm events, click **View more** to go to the **Events** page.

Viewing the Security Check Results of a Server

To view the detailed check results of a server, choose **Servers & Quotas**, click the **Servers** tab, and click **Risky**.



Check assets, unhandled vulnerabilities, and security events on the server.



 Copyright © Huawei Technologies Co., Ltd.

Table 1-2 Server security check results

Item	Description
Assets	Asset information, including: • Accounts You can check and manage server accounts all in one place. • Open ports You can check open ports all in one place and identify high-risk and unknown ports. • Processes You can check running applications all in one place and identify malicious applications. • Web directories You can check and manage web directories all in one place. • Installed software You can check and manage all software installed on your servers, and identify insecure versions. • Auto-startup You can check automatic startup information in the current system to identify suspicious auto startups.
Vulnerabilities	OS and Web-CMS vulnerabilities, including: • Windows vulnerabilities HSS automatically subscribes to Microsoft official updates, scans servers for vulnerabilities, and pushes patches. • Linux vulnerabilities HSS scans your servers based on vulnerability libraries and identifies vulnerabilities in your system and software (such as SSH, OpenSSL, Apache, and MySQL). • Web-CMS vulnerabilities HSS scans for Web-CMS vulnerabilities in web directories and files.
Unsafe settings	You can check unsafe settings in systems, databases, and accounts. • Password risks You can check for accounts using weak passwords and remind users to change them, preventing easy guessing. • Unsafe configurations You can check for unsafe Tomcat, Nginx, and SSH login configurations found by HSS.
Intrusions	You can check alarms on 13 types of intrusion events, including brute-force attacks, abnormal process behavior, web shells, abnormal logins, and malicious processes. For details, see **Alarm Events**.

 Copyright © Huawei Technologies Co., Ltd.

2 Quickly Enhancing Server Security

Data and programs on servers without protection will probably be breached or tampered with if the servers are intruded, interrupting your business and causing great loss.

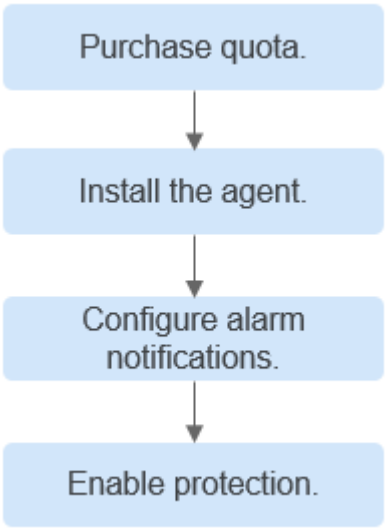
HSS provides all-round protection for servers, including pre-attack prevention, during-attack protection, and real-time or daily alarms.

This section describes how to use HSS to easily detect and eliminate security issues on your servers.

Step 1: Purchase and Enable HSS

Purchase and enable HSS, as shown in **Figure 2-1**.

Figure 2-1 Purchasing quota and enabling HSS



1. **Purchase HSS quota** as needed.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-1 Recommended editions

Requirement	Recommended Edition
APT attack detection, network protection, secure operations, and user-defined security policies	**Premium** edition HSS
Security risk prevention, virus and Trojan scan and killing, server vulnerability management, and compliance certification	**Enterprise** edition HSS
Website and file anti-tampering, hidden link scan, and server security	**Web Tamper Protection (WTP)** edition HSS

2. **Install the agent** on your servers.

   The agent runs scan tasks to scan all servers, monitors server security, and reports collected server information to the cloud protection center.

   For more information about the agent, see **What Is the HSS Agent?**
3. On the HSS console, **set alarm notifications** to yourself updated with risks in your servers and websites (if any).
4. Enable protection. For details, see **Enabling HSS**.

   When you enable HSS, a full scan is immediately performed. You can view all the detected issues on the console about 30 minutes later.

Step 2: Check Risk Overview

You can choose **Host Security Service** > **Dashboard** to check overall risk statistics, as shown in **Figure 2-2**. For details, see **Table 2-2**.

The **Dashboard** page displays server security status and risks in real time. For details, see **Dashboard**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Host security overview

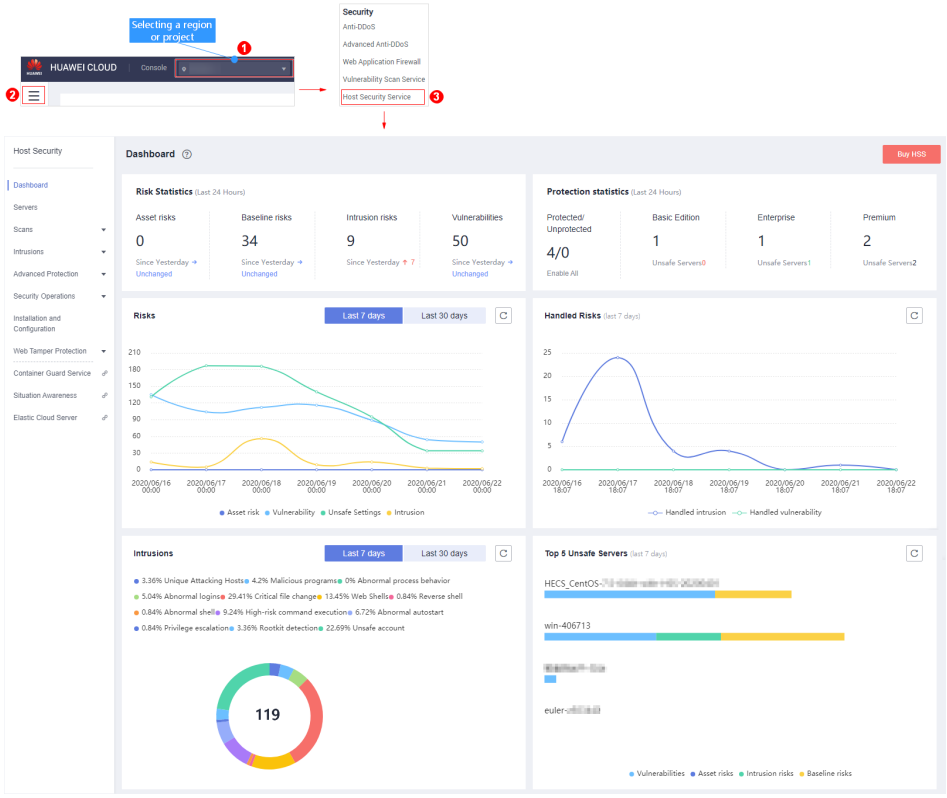


Table 2-2 Risk statistics

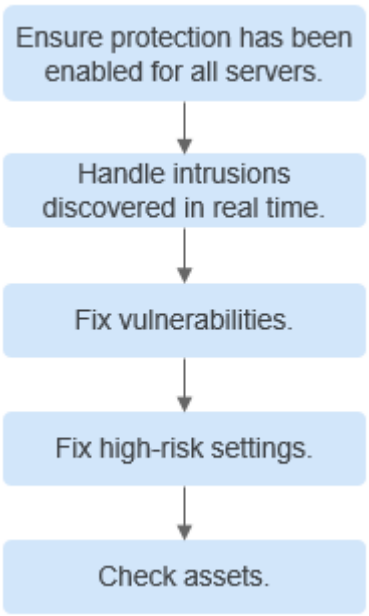
Risk Type	Description
Risk Statistics	Number of risks (unsafe settings, intrusions, and vulnerabilities) on protected servers
Protection Statistics	Numbers of servers protected with the basic, enterprise, or premium edition and the number of unprotected servers
Risks in the last 7 or 30 days	Line chart showing the numbers of asset risks, vulnerabilities, unsafe settings, and intrusions in the last 7 days or 30 days
Handled risks in the last 7 or 30 days	Line chart showing the numbers of handled asset risks, vulnerabilities, unsafe settings, and intrusions in the last 7 days or 30 days
Intrusions in the last 7 days or 30 days	Pie chart showing the number of intrusions and the percentage of each type of intrusions
Top 5 unsafe servers in the last 7 days	The five servers having the highest risks and the number of each type of risks
Real-time intrusions	The latest five unhandled risks in the last 24 hours

 Copyright © Huawei Technologies Co., Ltd.

Step 3: Handle Risks

Enable HSS and handle risks. **Figure 2-3** shows the process.

Figure 2-3 Handling risks

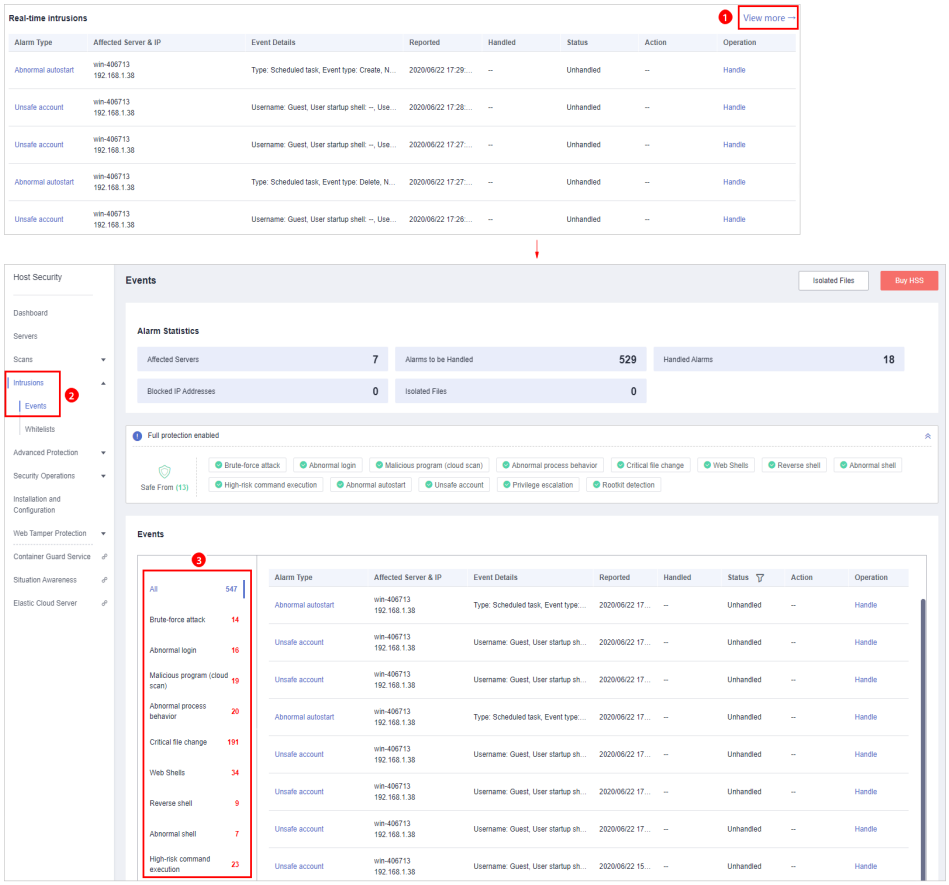


Step 1 Enable HSS for all your servers. For details, see **Enabling the Basic/Professional/Premium Edition**.

Step 2 Check and handle alarm events, as shown in **Figure 2-4**. For details, see **Checking and Handling Alarm Events**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-4 Real-time intrusions



The **Events** page displays the alarm events of the last 30 days. You can check and handle them as needed. The status of a handled event changes from **Unhandled** to **Handled**. HSS will no longer collect its statistics or display them on the **Dashboard** page.

Table 2-3 Handling alarm events

Method	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.

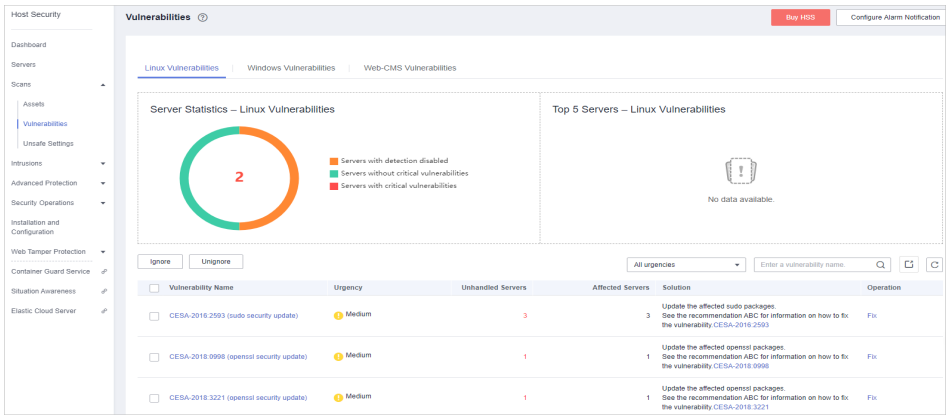
 Copyright © Huawei Technologies Co., Ltd.

Method	Description
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** to check and manage isolated files. For details, see **Managing Isolated Files**. The following types of alarm events support online isolation and killing: • Malicious program (cloud scan) • Abnormal process **NOTE** When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any) within 24 hours.
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.
Add to login whitelist	Add false alarmed items of the **Brute-force attack** and **Abnormal login** types to the login whitelist. HSS will no longer report alarm on the whitelisted items.
Add to alarm whitelist	Add false alarmed items of the following types to the login whitelist. HSS will no longer report alarm on the whitelisted items. • Reverse shell • Web shell • Abnormal process behavior • Process privilege escalation • File privilege escalation • High-risk command • Malicious program

Step 3 Manually fix the vulnerabilities based on the suggestions, as shown in **Figure 2-5**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-5 Fixing vulnerabilities



Checking vulnerabilities

HSS detects vulnerabilities and rates their urgency as **High**, **Medium**, or **Low** based on the official vulnerability scores.

- **High** indicates a vulnerability has high risks. You are advised to evaluate the impact of the vulnerability and fix it as soon as possible.
- **Medium** or **Low** indicates a vulnerability does not have direct impact on OS security. You are advised to evaluate the impact and fix the vulnerability when you upgrade your server OS or software.
- If you are sure a vulnerability does not affect your system, click **Ignore**.

  For example, if a vulnerability can be exploited only through an open port, and the port is not enabled on your servers, you can ignore this vulnerability.

Fixing vulnerabilities

Check vulnerability information, and fix or ignore it as needed.

- You can manually fix vulnerabilities one by one or fix them all in one click based on the solution provided, as shown in **Figure 2-5**.

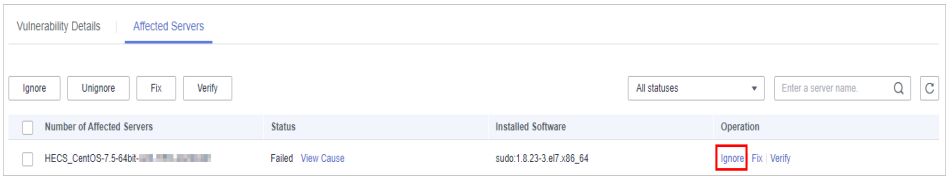
  For details, see **Fixing Vulnerabilities and Verifying the Result**.

NOTICE

Before repairing a vulnerability on a server, back up data and configurations of the server to avoid data loss.

- To ignore a vulnerability on a server, click the **Affected Servers** tab and click **Ignore** in the **Operation** column of the server, as shown in **Figure 2-6**.

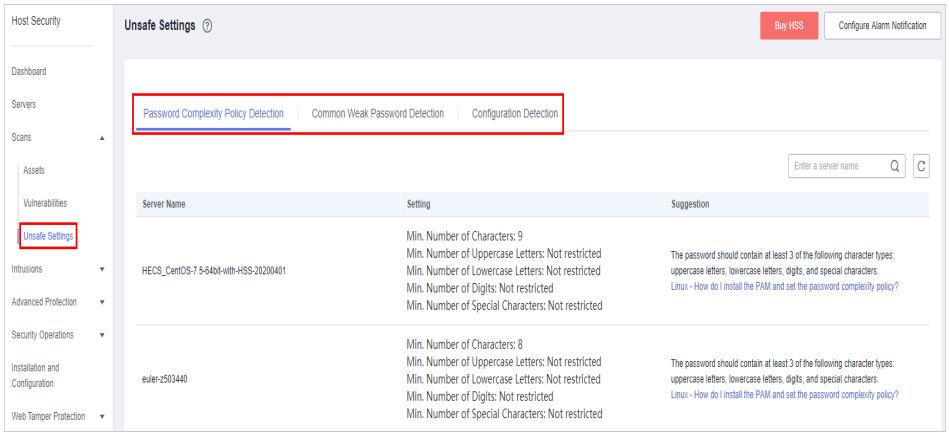
Figure 2-6 Affected servers



 Copyright © Huawei Technologies Co., Ltd.

Step 4 Go to the **Unsafe Settings** page, and fix weak password and other unsafe settings, as shown in **Figure 2-7**.

Figure 2-7 Fixing unsafe settings



Scanning for unsafe settings

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

For details about unsafe settings, see **Baseline Inspection**.

Fixing unsafe settings

Table 2-4 Unsafe settings and solutions

Issue	Description	Solution
Weak passwords	Accounts using weak passwords are exposed to cracking attacks. You can check detected weak passwords on the console. Generally, passwords that are easy to guess or be cracked in a brute-force attack are regarded weak. Weak passwords have the following characteristics: 1. Too short or simple 2. Contains any strings in a common password dictionary or other similar lists on the Internet 3. Contains personal information	You are advised to set stronger passwords for detected accounts. For details, see **How Do I Set a Secure Password?**

 Copyright © Huawei Technologies Co., Ltd.

Issue	Description	Solution
Unsafe password complexity policy	• To monitor the password complexity policy on a Linux server, install the Pluggable Authentication Modules (PAM) on the server. For details, see **How Do I Install a PAM in a Linux OS?** • For details about how to modify the password complexity policy on a Linux server, see **How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?** • For details about how to modify the password complexity policy on a Windows server, see **How Do I Set a Secure Password Complexity Policy in a Windows OS?**	You are advised to change the password complexity policy as suggested. The new policy will be used to check password complexity when users set or modify passwords.
Unsafe configuration	Insecure configurations of key applications will probably be exploited by hackers to intrude servers. Such configurations include insecure encryption algorithms used by SSH and Tomcat startup with root permissions.	Fix settings based on the suggestions provided. For details, see **Unsafe Configurations**.

Step 5 Check your assets, as shown in **Figure 2-8**.

In the early morning every day, HSS collects and displays server asset information about accounts, external port listening, process running, web directories, software, auto-started items, and file changes, helping users check and eliminate asset and security risks.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-8 Checking assets

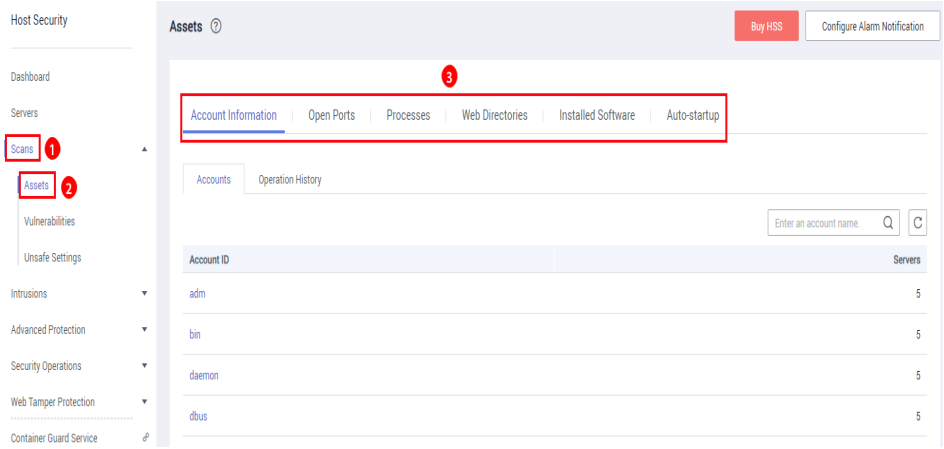


Table 2-5 Assets

Item	Solution
Account Information	You can check the information about and changes on all accounts here. If you find unnecessary or super-privileged accounts (such as **root**) that are not mandatory for services, delete them or modify their permissions to prevent exploits.
Open Ports	• Manually disabling high-risk ports If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary. It is recommended that you handle the ports with the **Dangerous** risk level promptly and handle the ports with the **Unknown** risk level based on the actual service conditions. • Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.
Processes	You can quickly check and terminate suspicious application processes on your servers.
Web Directories	You can check and delete risky web directories and terminate suspicious processes in a timely manner.
Installed Software	You can check the information about and changes on all software, upgrade software, and delete software that is unnecessary, suspicious, or in old version.
Auto-startup	You can check the servers, paths, file hashes, and last modification time of auto-started items to find and eliminate Trojans in a timely manner.

----End

 Copyright © Huawei Technologies Co., Ltd.

Step 4: Verify Server Security

Checking server risks

Verify that detected issues have been fixed, as shown in **Table 2-6**.

Table 2-6 Verification methods

Method	Scenario	Check Item	Operation
Manual scan	You need to know the rectification result as soon as possible.	The following items can be checked in one click: • Software information • Vulnerabilities • Web shells • Weak passwords • Unsafe configurations	Choose **Servers** and click **Manual Detection** in the upper right corner of the page.
		The following items can be separately checked: • Software • Vulnerabilities • Weak passwords • Unsafe configurations	Choose **Servers**. In the **Operation** column of the server list, click **View Scan Results**. • Click **Assets**. On the **Installed Software** tab, check whether there are any insecure software. • Click **Vulnerabilities**, and check its software, OS, and Web-CMS vulnerabilities. • Click **Unsafe Settings**. On the **Password Risks** tab, manually check weak passwords. • Click **Unsafe Settings**. On the **Unsafe Configurations** tab, manually check unsafe configurations.

Copyright © Huawei Technologies Co., Ltd.

Method	Scenario	Check Item	Operation
Automatic check	You are not in a hurry to know the verification result.	• A full scan is automatically performed every early morning to check the following items: – Software – Vulnerabilities – Web shells – Weak passwords – Unsafe configurations • For other items, HSS checks them in real time and you can view the verification results shortly after fixing them.	HSS automatically performs a full scan every early morning.

Checking security overview

Check risks on the **Dashboard** page.

The **Dashboard** page shows security statistics, as shown in **Figure 2-9**.

Figure 2-9 Security overview



 Copyright © Huawei Technologies Co., Ltd.

- Risk Statistics

  Check the changes in the numbers of asset risks, unsafe settings, intrusions, and vulnerabilities.
- Protection statistics

  Check whether all your servers are protected.
- Risks

  Check the changes in the numbers of risks.
- Handled Risks

  Check the changes in the numbers of handled risks.

If the risks reduced, you have made your servers more secure.

 Copyright © Huawei Technologies Co., Ltd.

3 Detecting and Fixing Vulnerabilities

3.1 Git Credential Disclosure Vulnerability (CVE-2020-5260)

Git issued a security bulletin announcing a vulnerability that could reveal Git user credentials (CVE-2020-5260). Git uses a credential helper to store and retrieve credentials.

But when a URL contains an encoded newline (%0a), it may inject unexpected values into the protocol stream of the credential helper. This vulnerability is triggered when the affected version of Git is used to execute a git clone command on a malicious URL.

Vulnerability ID

CVE-2020-5260

Vulnerability Name

Git credential disclosure vulnerability

Scope of Impact

Affected versions:

- Git 2.17.x <= 2.17.3
- Git 2.18.x <= 2.18.2
- Git 2.19.x <= 2.19.3
- Git 2.20.x <= 2.20.2
- Git 2.21.x <= 2.21.1
- Git 2.22.x <= 2.22.2
- Git 2.23.x <= 2.23.1
- Git 2.24.x <= 2.24.1

 Copyright © Huawei Technologies Co., Ltd.

- Git 2.25.x <= 2.25.2
- Git 2.26.x <= 2.26.0

Unaffected versions:

- Git 2.17.4
- Git 2.18.3
- Git 2.19.4
- Git 2.20.3
- Git 2.21.2
- Git 2.22.3
- Git 2.23.2
- Git 2.24.2
- Git 2.25.3
- Git 2.26.1

Official Solution

This vulnerability has been fixed in the latest official version. If your service version falls into the affected range, upgrade it to the latest secure version.

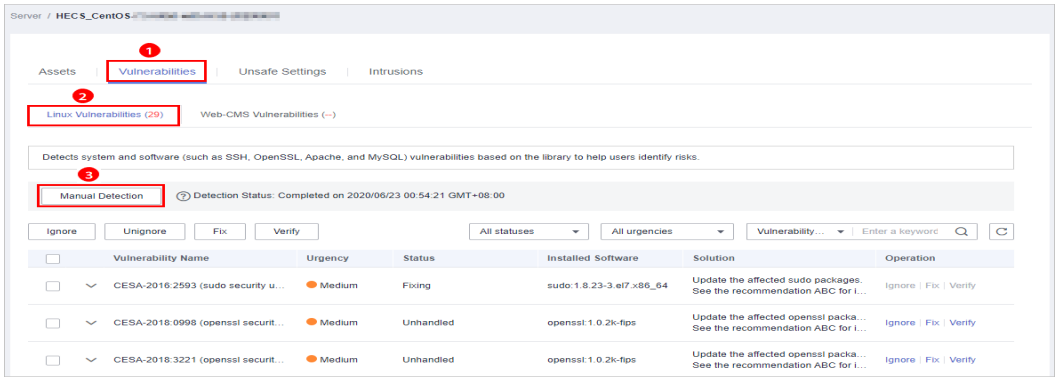
Download address: **https://github.com/git/git/releases**

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Scan and view details of a vulnerability, as shown in **Figure 3-1**. For details, see **Viewing Details of a Vulnerability**.

Figure 3-1 Manually starting a vulnerability scan



Step 2 Fix vulnerabilities and verify the result. For details, see **Fixing Vulnerabilities and Verifying the Result**.

----End

Other Protection Measures

If you cannot perform upgrade for the moment, you can take the following measures:

 Copyright © Huawei Technologies Co., Ltd.

- Disable credential helper by running the following commands:

  git config --unset credential.helper

  git config --global --unset credential.helper

  git config --system --unset credential.helper

- Be vigilant about malicious URLs.

  a. Examine the server name and username portion of URLs fed to **git clone** for the presence of encoded newlines (%0a) or evidence of credential-protocol injections (example: **host=github.com**).

  b. Avoid using submodules with untrusted repositories (do not use **clone –recurse-submodules**; use **git submodule update** only after examining the URLs found in .gitmodules).

  c. Avoid tools which may run git clone.

3.2 SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)

Security researchers discovered two serious vulnerabilities in SaltStack's products. SaltStack provides a set of product offerings written in Python for automatic C/S O&M. One of the two discovered vulnerabilities is authentication bypass vulnerabilities (CVE-2020-11651), and the other is directory traversal vulnerability (CVE-2020-11652). Attackers can exploit the vulnerabilities to remotely execute commands, read any files on the server, and obtain sensitive information.

If you are a SaltStack user, check your system and implement timely security hardening.

Vulnerability ID

- CVE-2020-11651
- CVE-2020-11652

Vulnerability Name

SaltStack remote command execution vulnerability

Scope of Impact

Affected versions:

- Versions earlier than SaltStack 2019.2.4
- Versions earlier than SaltStack 3000.2

Unaffected versions:

- SaltStack 2019.2.4
- SaltStack 3000.2

 Copyright © Huawei Technologies Co., Ltd.

Official Solution

- These vulnerabilities have been fixed in the latest official version. If your service version falls into the affected range, upgrade it to the latest secure version.

  Download address: **https://repo.saltstack.com**

- The default listening ports of Salt Master are 4505 and 4506. You can configure security group rules that prohibit opening the two ports to public networks, or only allow trusted objects to connect to the ports.

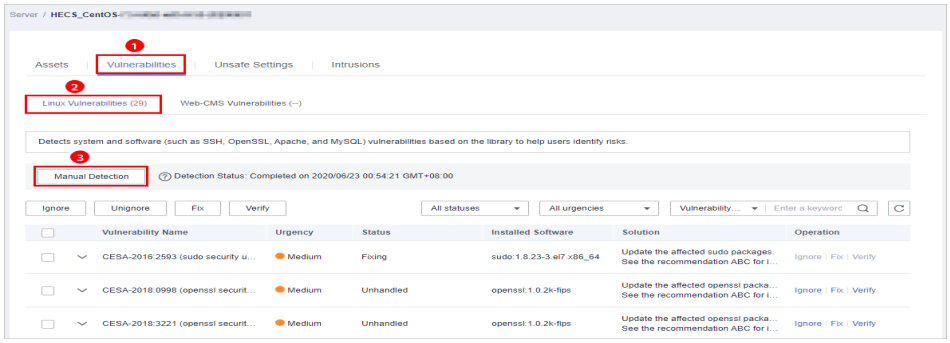
Suggestion

Perform the following steps to scan and fix a vulnerability.

- Scan for vulnerabilities and view details, as shown in **Figure 3-2**. For details, see **Viewing Details of a Vulnerability**.

  Fix vulnerabilities and verify the result. For details, see **Fixing Vulnerabilities and Verifying the Result**.

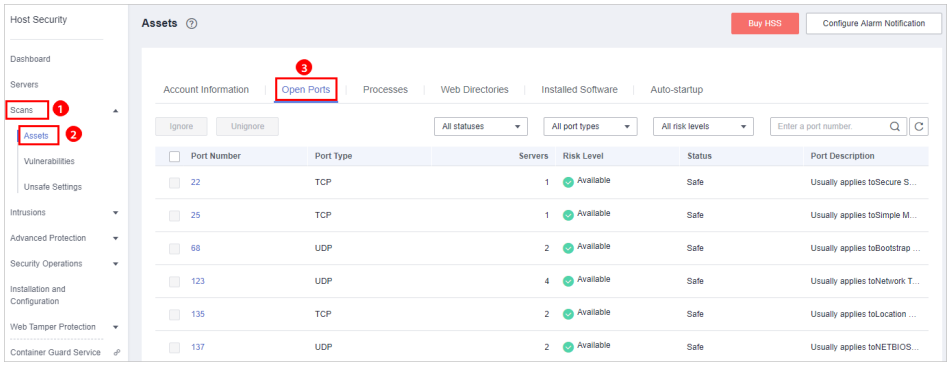
  Figure 3-2 Manually starting a vulnerability scan



- Check whether ports 4505 and 4506 are enabled on the server, as shown in **Figure 3-3**.

  If the ports are enabled, you are advised to disable them, or to enable them only for trusted objects. For details, see **Checking Open Ports**.

  Figure 3-3 Checking open ports

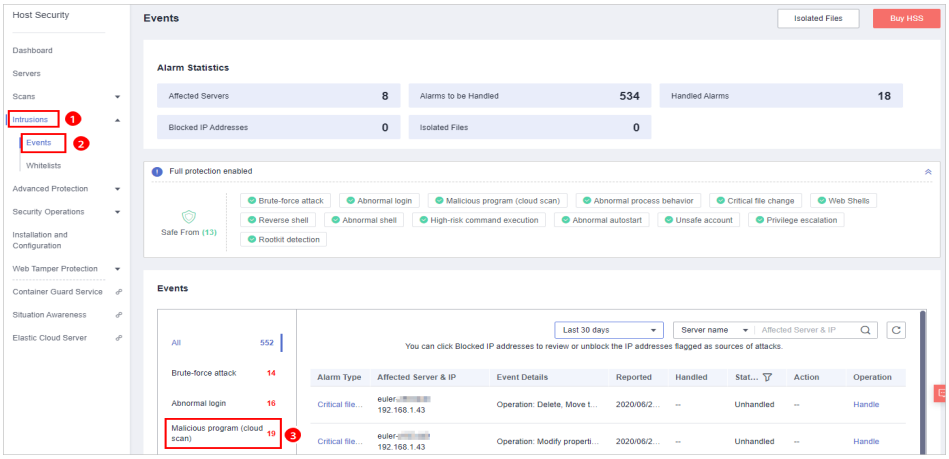


- Check for, isolate, and kill Trojans, as shown in **Figure 3-4**.

  For details about how to isolate and kill Trojans, see **Isolating and Killing Files**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Cloud scan



3.3 OpenSSL High-risk Vulnerability (CVE-2020-1967)

OpenSSL Project released update information regarding the OpenSSL vulnerability CVE-2020-1967 that affects OpenSSL 1.1.1d, OpenSSL 1.1.1e, and OpenSSL 1.1.1f. This vulnerability can be exploited to launch DDoS attacks.

Vulnerability ID

CVE-2020-1967

Vulnerability Name

OpenSSL high-risk vulnerability

Scope of Impact

- OpenSSL 1.1.1d
- OpenSSL 1.1.1e
- OpenSSL 1.1.1f

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.

- **https://www.debian.org/security/2020/dsa-4661**
- **https://security.gentoo.org/glsa/202004-10**
- **https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html**

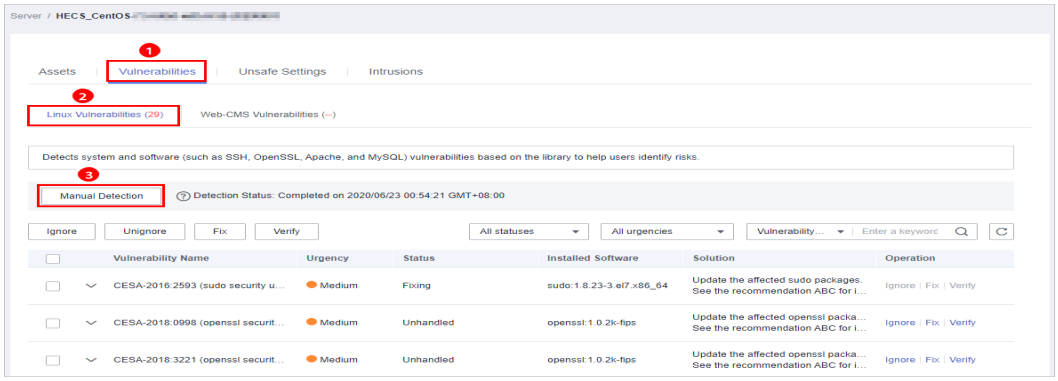
Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Scan and view details of a vulnerability, as shown in **Figure 3-5**. For details, see **Viewing Details of a Vulnerability**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Manually starting a vulnerability scan



Step 2 Fix vulnerabilities and verify the result. For details, see **Fixing Vulnerabilities and Verifying the Result**.

----End

3.4 Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/ CVE-2020-0938)

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.

For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

There are multiple ways an attacker could exploit the vulnerability, such as convincing a user to open a specially crafted document or viewing it in the Windows Preview pane.

Vulnerability ID

- CVE-2020-1020
- CVE-2020-0938

Vulnerability Name

Adobe Font Manager Library Remote Code Execution Vulnerability

Vulnerability Details

- For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely.
- For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with

 Copyright © Huawei Technologies Co., Ltd.

limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Affected Versions

All Windows OSs

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.

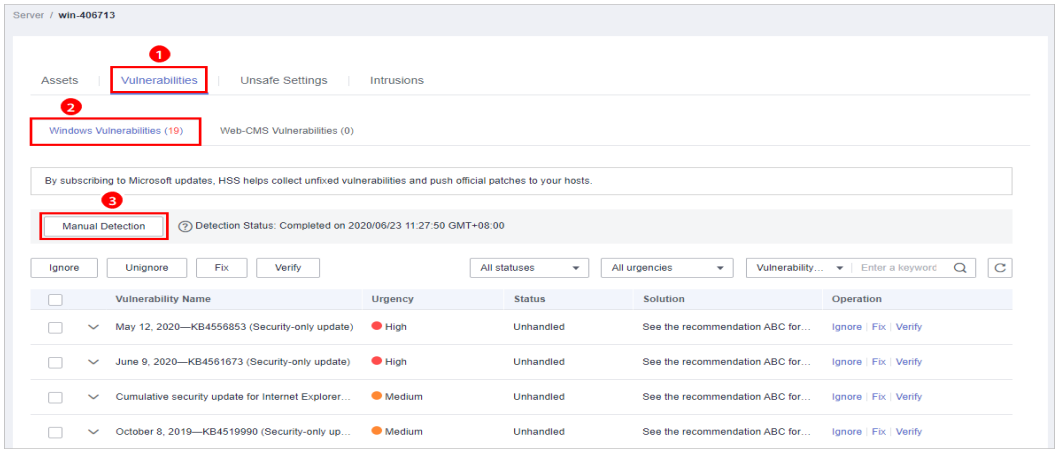
For details, see **https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020**.

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Scan and view details of a vulnerability, as shown in **Figure 3-6**. For details, see **Viewing Details of a Vulnerability**.

Figure 3-6 Manually starting a vulnerability scan



Step 2 Fix vulnerabilities and verify the result. For details, see **Fixing Vulnerabilities and Verifying the Result**.

----End

3.5 Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.

To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.

 Copyright © Huawei Technologies Co., Ltd.

Vulnerability ID

CVE-2020-1027

Vulnerability Name

Windows Kernel Elevation of Privilege Vulnerability

Vulnerability Details

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.

Affected Versions

All Windows OSs

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.

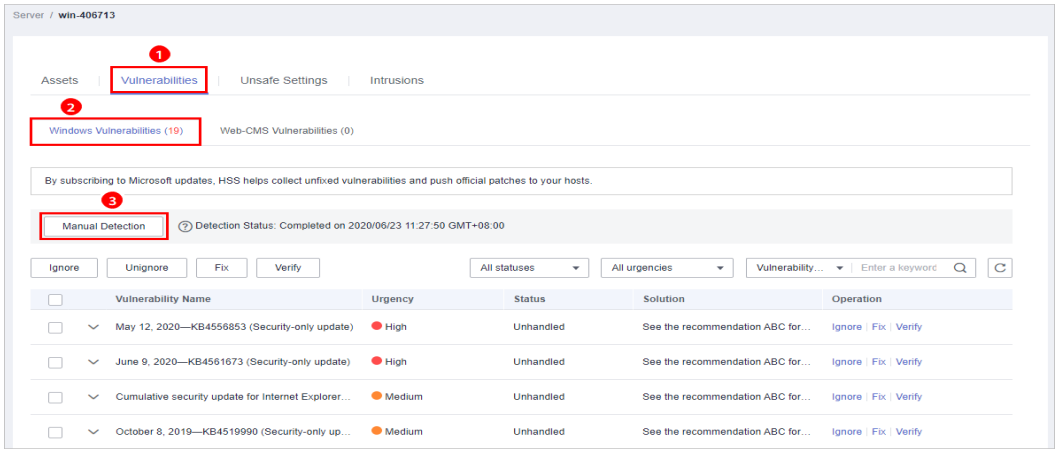
For details, see **https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1027** .

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Scan and view details of a vulnerability, as shown in **Figure 3-7**. For details, see **Viewing Details of a Vulnerability**.

Figure 3-7 Manually starting a vulnerability scan



Step 2 Fix vulnerabilities and verify the result. For details, see **Fixing Vulnerabilities and Verifying the Result**.

----End

 Copyright © Huawei Technologies Co., Ltd.

3.6 Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)

On January 15, 2020, Microsoft released a patch update list, which contains the high-risk vulnerability CVE-2020-0601 that is discovered by National Security Agency (NSA) and affects Microsoft Windows encryption. This vulnerability affects the CryptoAPI Elliptic Curve Cryptography (ECC) certificate validation mechanism. As a result, attackers can interrupt the Windows authentication and encryption trust process and remotely execute code.

Vulnerability ID

CVE-2020-0601

Vulnerability Name

Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)

Vulnerability Details

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates ECC certificates.

An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable file. The file appears to be from trusted and legitimate sources, and the user cannot know it is malicious. For example, an attacker could exploit this vulnerability to give seemingly trusted signature certificates to malware, such as ransomware, and bypass the Windows trust detection mechanism and mislead users to install the malware.

A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software. Instances that affect Windows trust relationships include common HTTPS connections, file signatures, and email signatures.

Affected Versions

- Windows 10
- Windows Server 2016 and Windows Server 2019
- Applications that depend on Windows CryptoAPI

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.

For details, see **https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601**.

Suggestion

Perform the following steps to scan and fix a vulnerability.

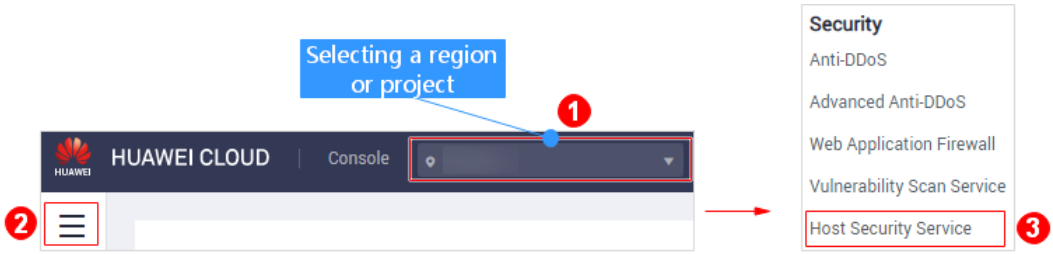
 Copyright © Huawei Technologies Co., Ltd.

Ensure you have installed the HSS agent on the server to be fixed, and has enabled protection.

Step 1 Log in to the management console.

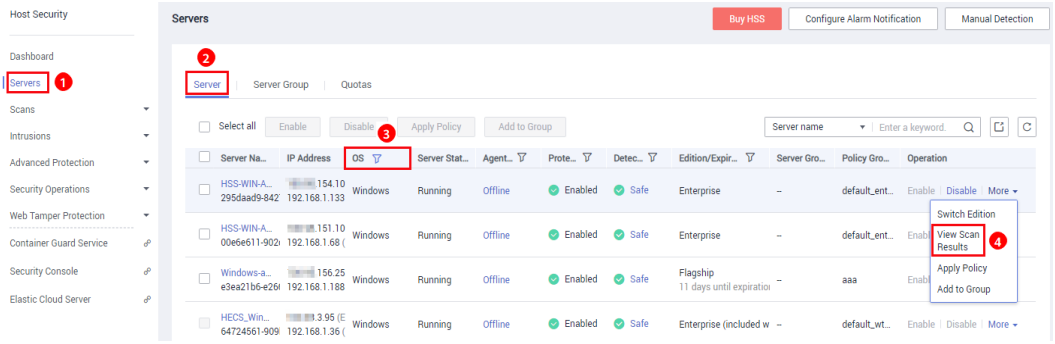
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Host Security Service**.

Figure 3-8 HSS



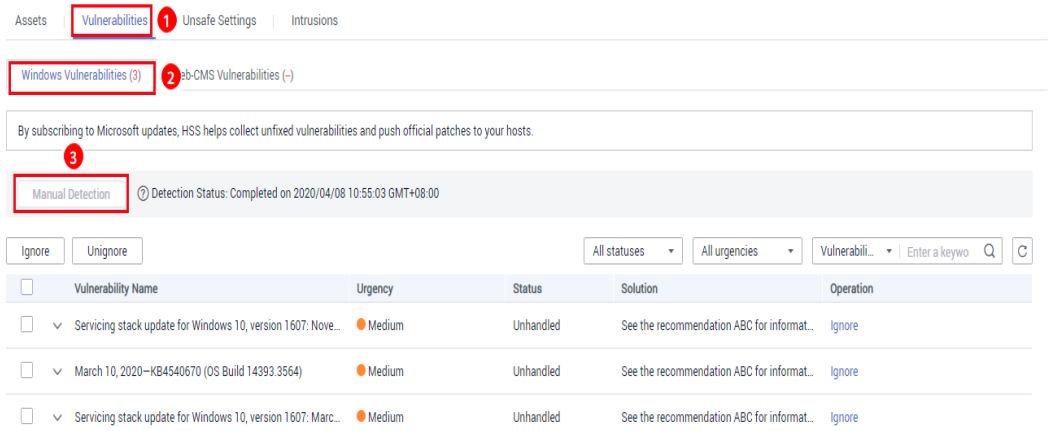
Step 3 In the navigation pane, choose **Servers**. In the server list, click **View Scan Results** in the row containing the required Windows server, as shown in **Figure 3-9**.

Figure 3-9 Viewing details



Step 4 On the details page, click **Vulnerabilities**, **Windows Vulnerabilities**, and **Manual Detection**, as shown in **Figure 3-10**.

Figure 3-10 Manually starting a vulnerability scan



 Copyright © Huawei Technologies Co., Ltd.

Step 5 Fix detected vulnerabilities according to the suggestion in the **Solution** column.

Step 6 Restart the fixed servers.

Step 7 Click **Manual Detection** again to check whether the vulnerabilities have been fixed.

NOTE

You can also click **Vulnerabilities** and then **Windows Vulnerabilities**, search for a vulnerability by its name, and then check and fix the vulnerability.

- Windows Server 2019: KB4534273
- Windows Server 2016: KB4534271

----End

 Copyright © Huawei Technologies Co., Ltd.

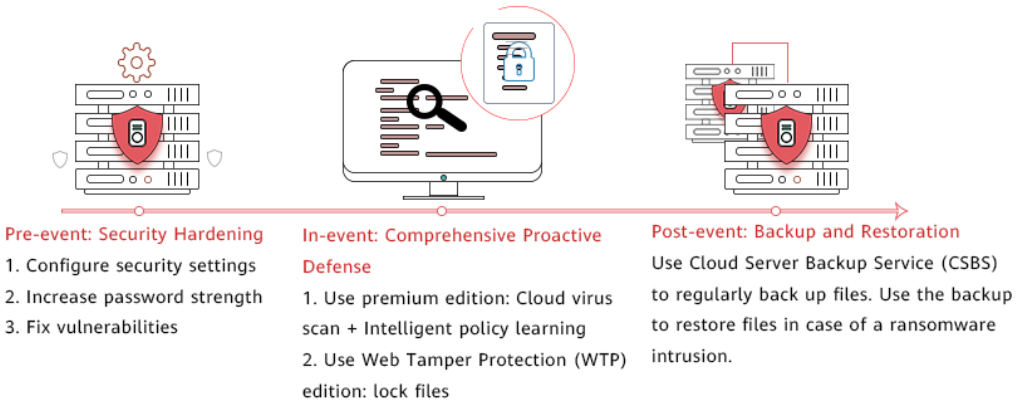
4 Best Practices for Defense Against Ransomware

Ransomware emerged with the Bitcoin economy. It is a Trojan that is disguised as a legitimate email attachment or bundled software and tricks you into opening or installing it. It can also arrive on your servers through website or server intrusion. Ransomware often uses a range of algorithms to encrypt the victim's files and demand a ransom payment to get the decryption key. Digital currencies such as Bitcoin are typically used for the ransoms, making tracing and prosecuting the attackers difficult.

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

How HSS Works

Ransomware cannot be prevented once and for all. HSS provides pre-event, in-event, and post-event protection, helping you enhance security before any attacks take place, proactively detect and fight against attacks, and restore services from backup after the attacks.



Prerequisites

- Before using HSS for ransomware prevention, ensure you have purchased and enabled HSS.

 Copyright © Huawei Technologies Co., Ltd.

- Cloud Server Backup Service (CSBS) does not back up your data by default. To use it for backup and restoration, ensure you have configured regular automatic backup.

Pre-event Security Hardening

Configuring Security Settings

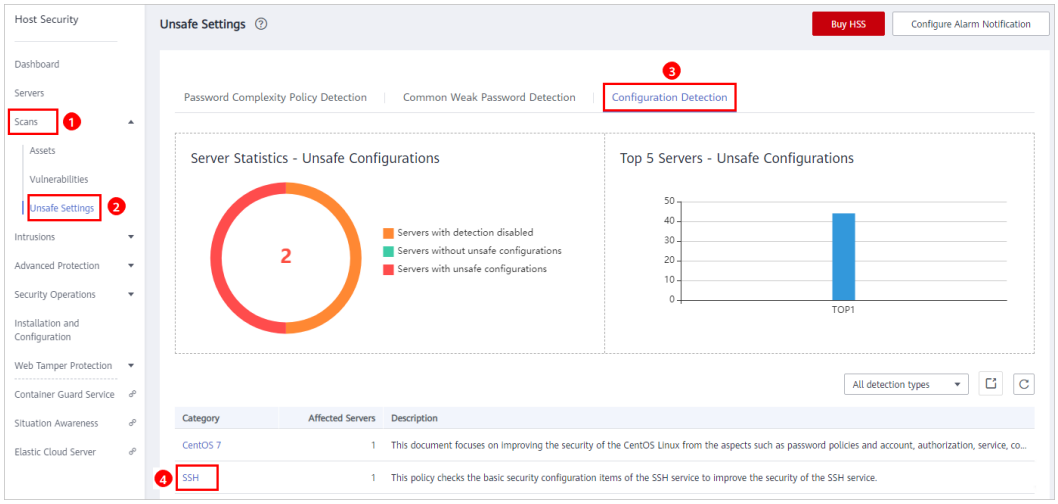
HSS scans your software for unsafe settings every early morning and provides suggestions. You can modify your settings accordingly to enhance server security.

NOTE

- The severity of a risk is rated as high, medium, or low.
- You are advised to fix the configurations with high severity immediately. You can set trusted configuration items so that they will not be reported as risks.

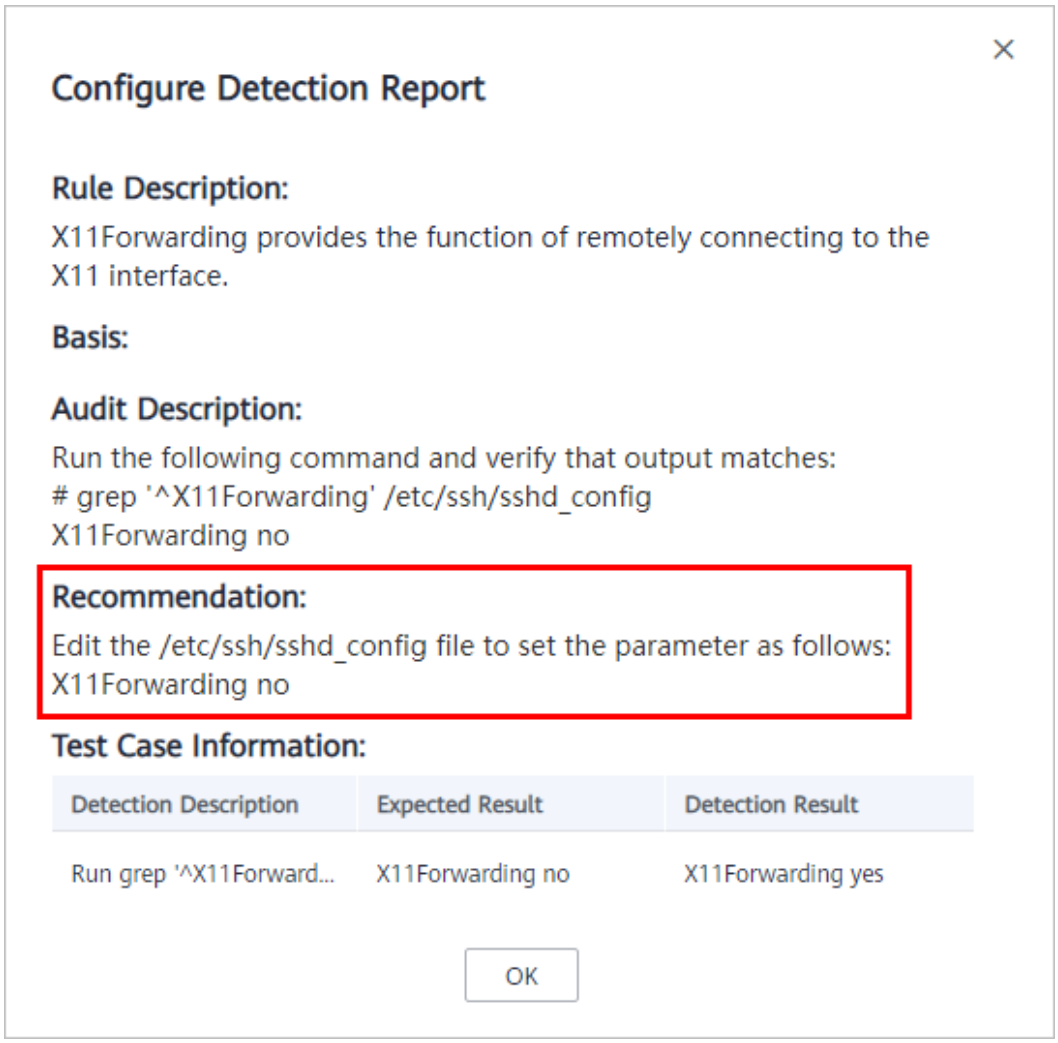
HSS can detect the following types of software: Tomcat, SSH, Nginx, Redis, Apache 2, and MySQL 5

Step 1 Choose **Scans** > **Unsafe Settings**, click the **Configuration Detection** tab, and click a check item, for example, **SSH**.



Step 2 On the detection rule details page, click **View Details**. You can verify the check result based on **Audit Description** and handle exceptions on servers based on the suggestions in **Recommendation**.

 Copyright © Huawei Technologies Co., Ltd.



Step 3 After modifying configuration items, you are advised to perform manual scan immediately to verify the result.

If you do not perform manual verification, HSS will automatically check the settings at 00:00:00 the next day. If you have no time for a manual scan, you can check the automatic scan result.

----End

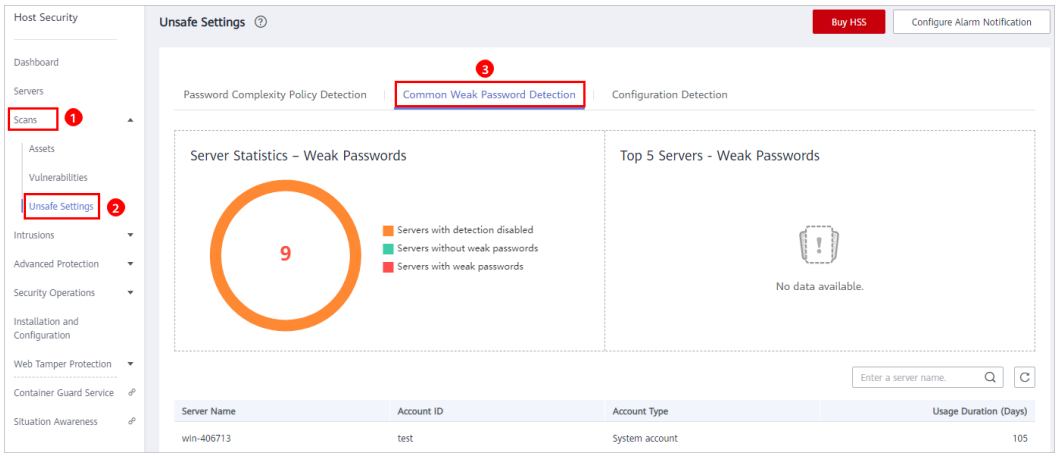
Increasing Password Strength

HSS automatically scans servers every early morning for common weak passwords and the passwords you banned, and lists the server names, account names, account types, and usage duration of the weak passwords. You can then ask the weak password users to set stronger passwords.

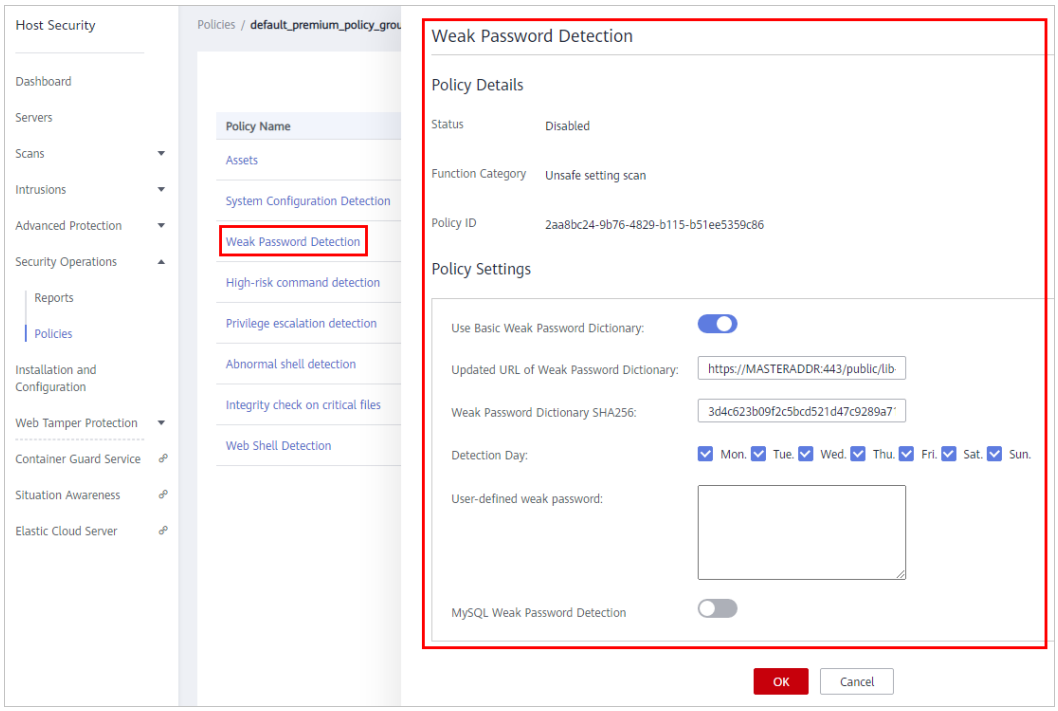
HSS can detect weak passwords in MySQL, FTP, and system accounts.

Step 1 Choose **Security** > **Host Security Service** and choose **Scans** > **Unsafe Settings**. Check and modify weak passwords.

 Copyright © Huawei Technologies Co., Ltd.



Step 2 Choose **Security Operations** > **Policies**, select a policy group, and click the **Weak Password Detection** policy to add banned passwords.

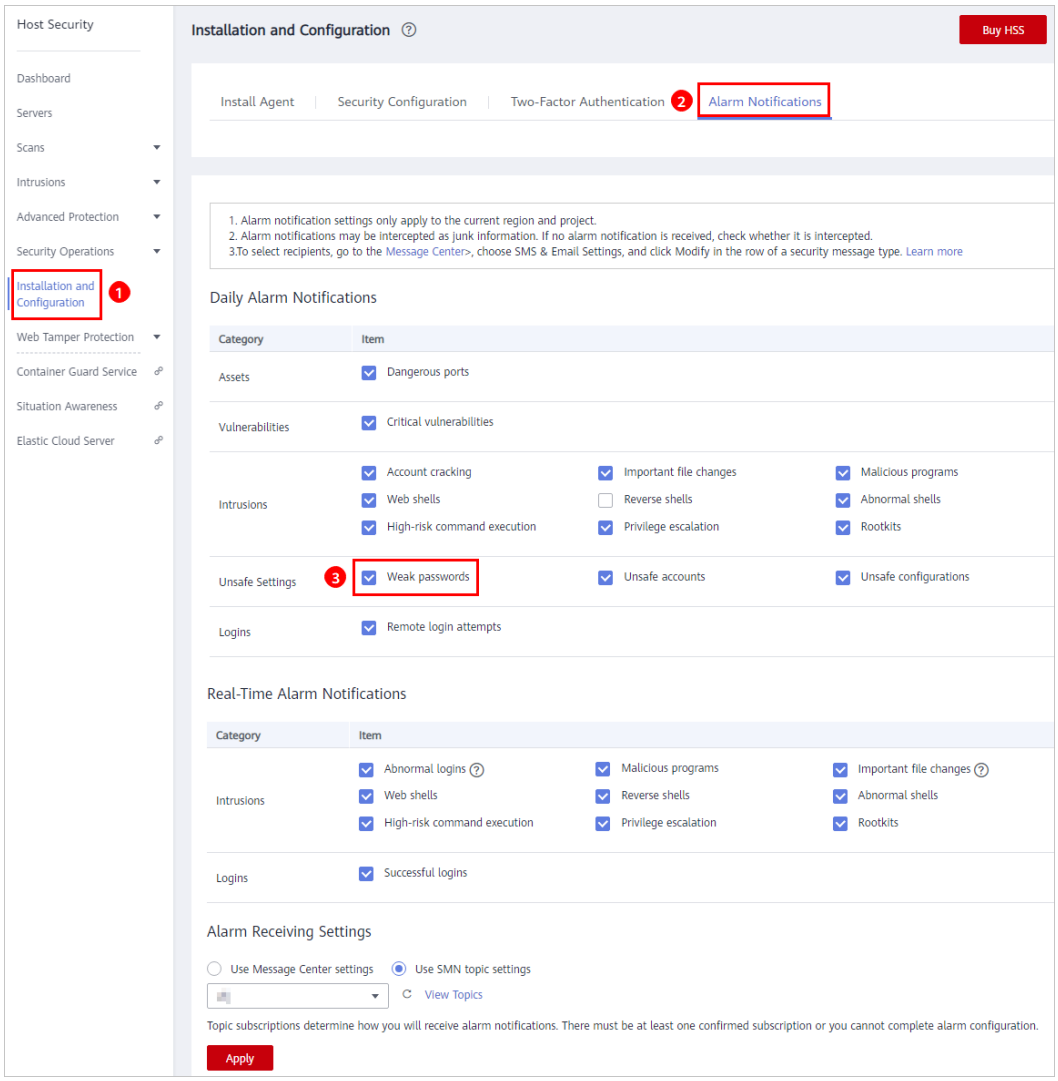


Step 3 Perform manual scan to verify password hardening.

If you do not perform manual verification, HSS will automatically check the settings at 00:00:00 the next day. If you have no time for a manual password scan, you can check the automatic scan result.

Step 4 Choose **Installation and Configuration** and click the **Alarm Notifications** tab. Select the **Weak passwords** notification item.

 Copyright © Huawei Technologies Co., Ltd.



----End

Fixing vulnerabilities

HSS automatically scans your servers for vulnerabilities in the early morning every day. The vulnerability management function subscribes to and pushes official updates, and reports system vulnerabilities and uninstalled patches. You can fix vulnerabilities and install patches without affecting services.

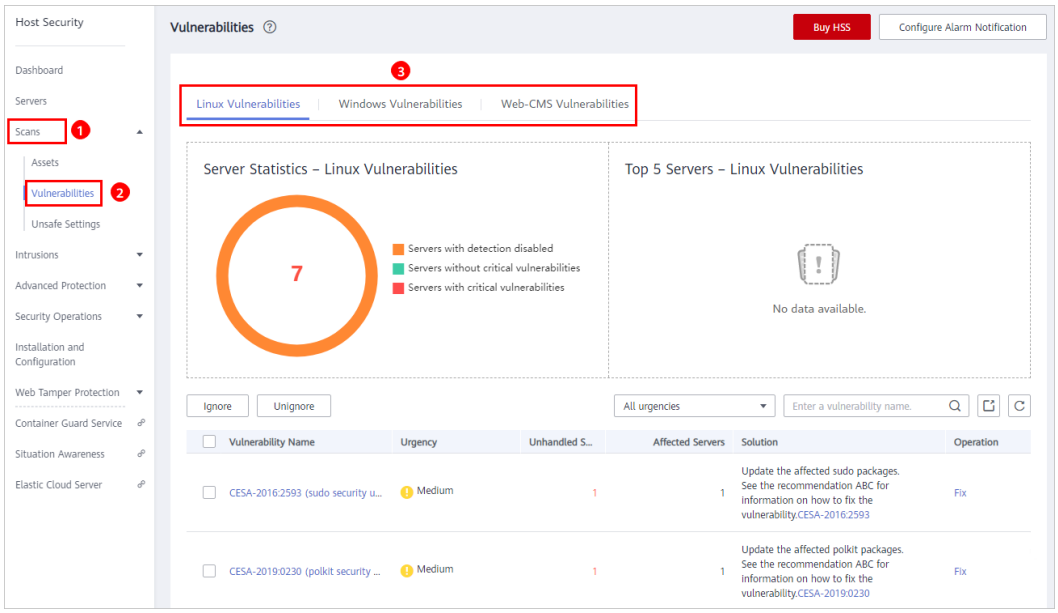
NOTE

- Vulnerability urgency is rated as high, medium, or low.
- You are advised to fix highly urgent vulnerabilities as soon as possible. You can ignore vulnerabilities that do not need to be fixed.

Step 1 Choose **Security** > **Host Security Service**. Choose **Scans** > **Vulnerabilities**.

Step 2 Click the **Linux Vulnerabilities**, **Windows Vulnerabilities**, or **Web-CMS Vulnerabilities** tab. Fix vulnerabilities in one click or manually fix them based on suggestions provided.

 Copyright © Huawei Technologies Co., Ltd.

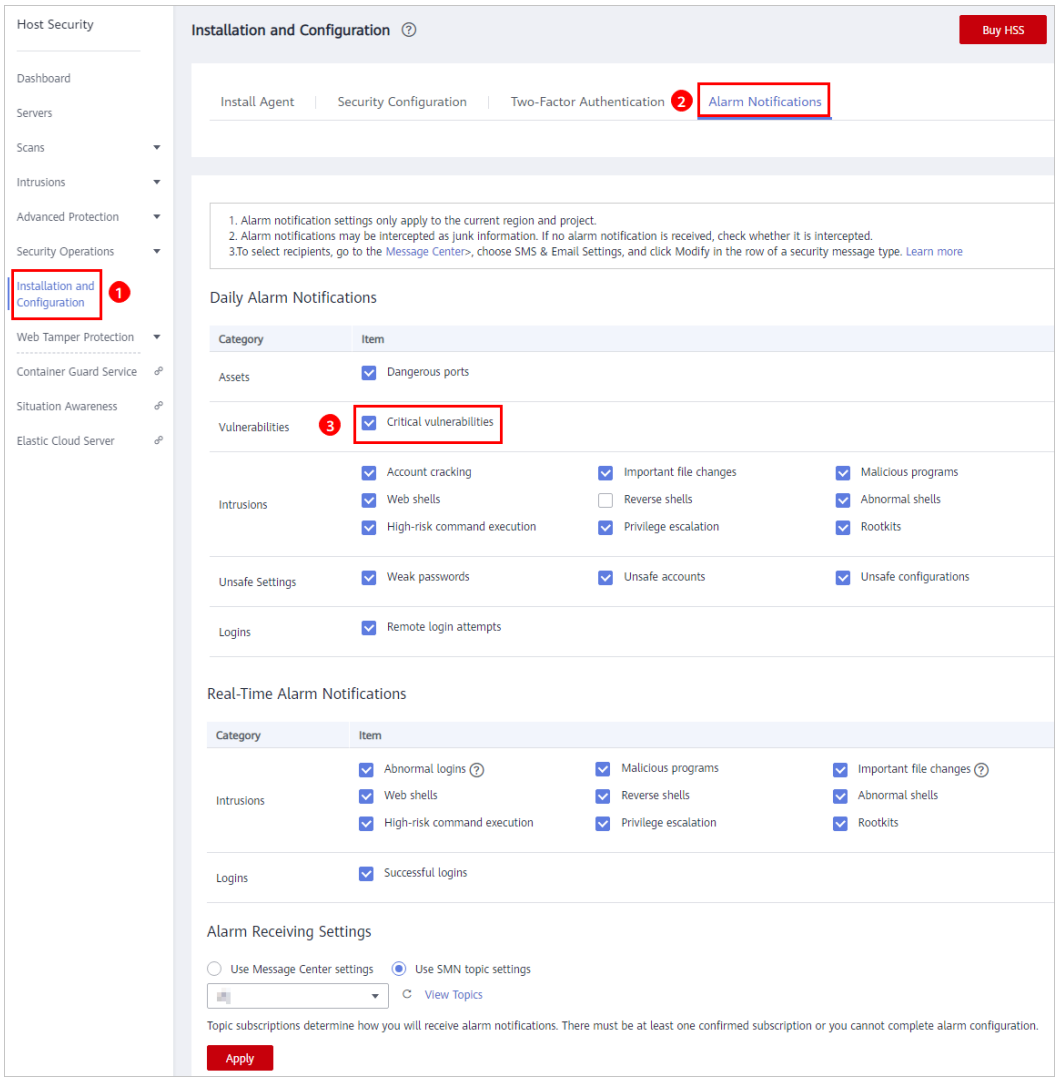


Step 3 After the vulnerability is fixed, you can click **Verify** to verify the fix.

HSS will automatically scan the settings the next day in the early morning. If you have no time for a manual scan, you can check the automatic scan result.

Step 4 Choose **Installation and Configuration**, click the **Alarm Notifications** tab, and select the **Critical vulnerabilities** notification item.

 Copyright © Huawei Technologies Co., Ltd.



----End

In-event Proactive Defense

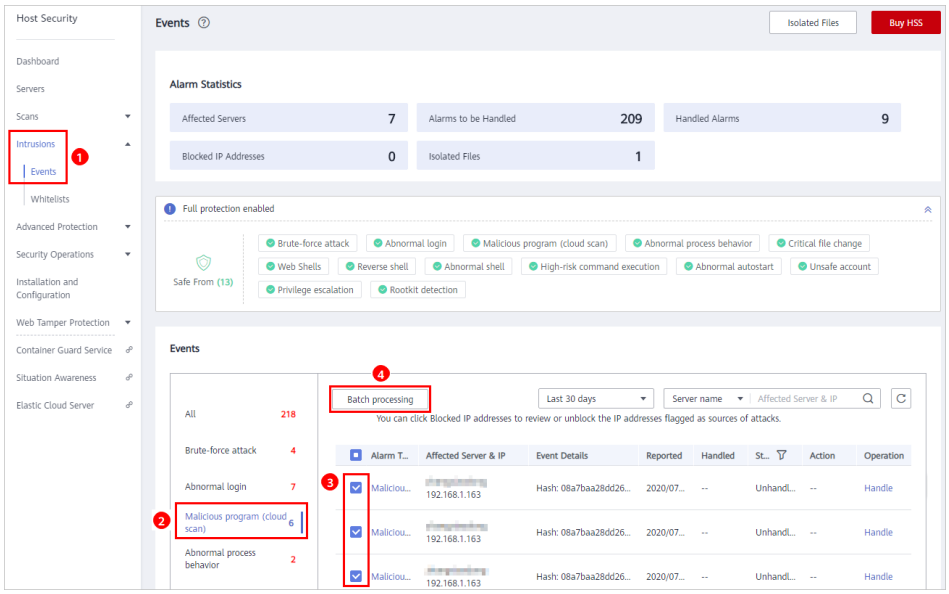
- **Using Premium Edition: Cloud Virus Scan + Intelligent Policy Learning**

Cloud Virus Scan

You can use HSS to quickly isolate and kill intruded servers to prevent the spread of viruses.

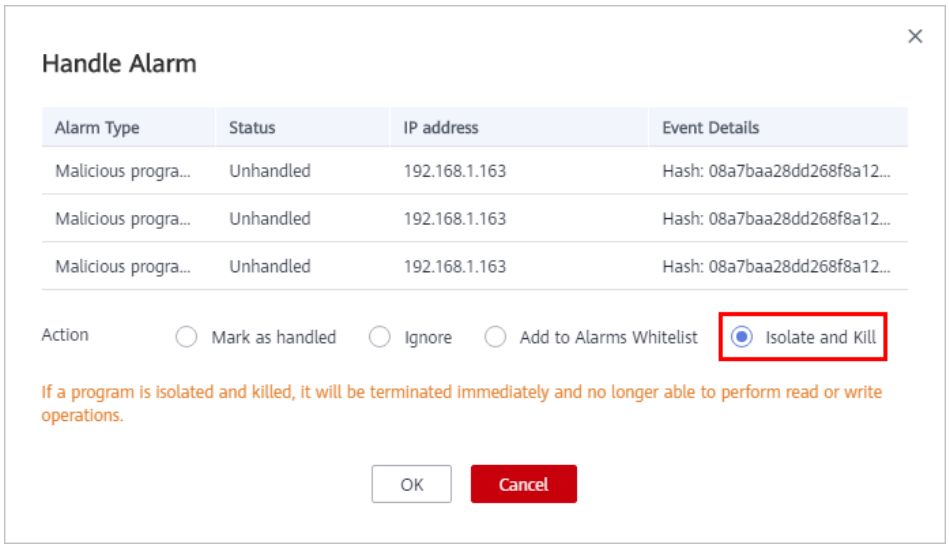
Step 1 Choose **Security** > **Host Security Service**. Choose **Intrusions** > **Events** and click **Malicious program (cloud scan)**. Select alarms and click **Batch processing**.

 Copyright © Huawei Technologies Co., Ltd.



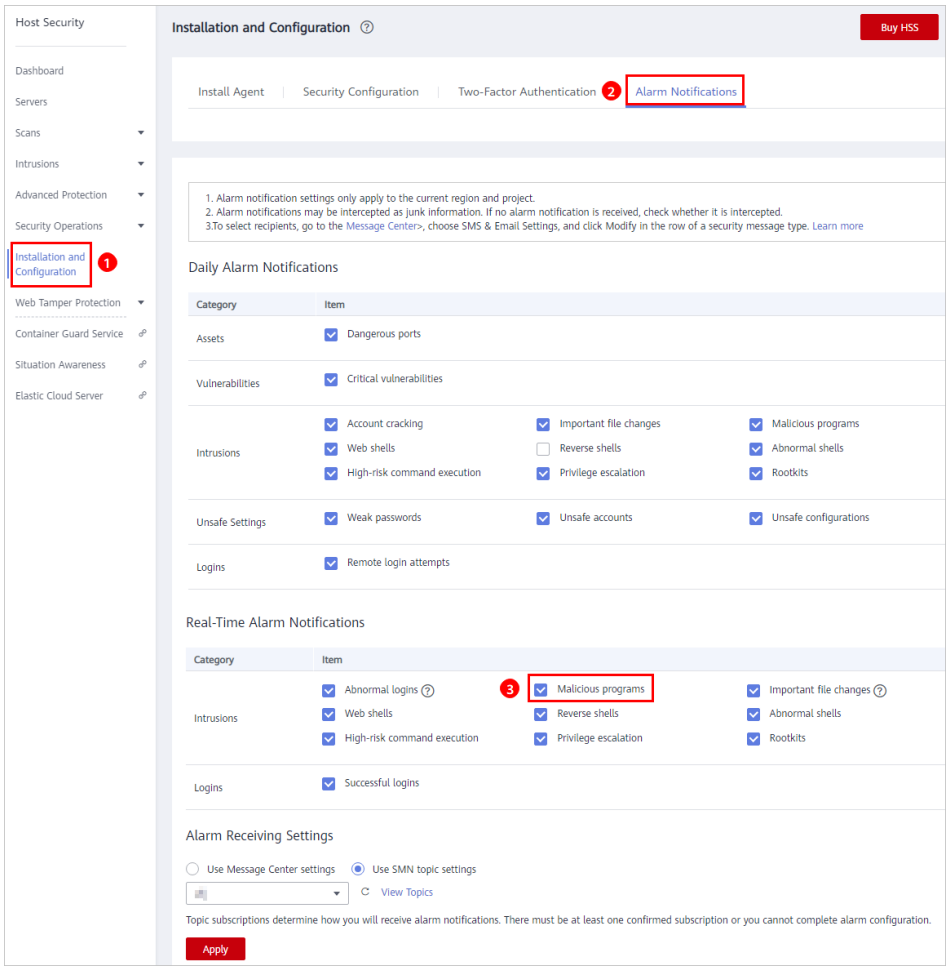
Step 2 Click **Isolate and Kill** and click **OK**.

If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers.



Step 3 Choose **Installation and Configuration**, click the **Alarm Notifications** tab, and select the **Malicious programs** notification item.

 Copyright © Huawei Technologies Co., Ltd.



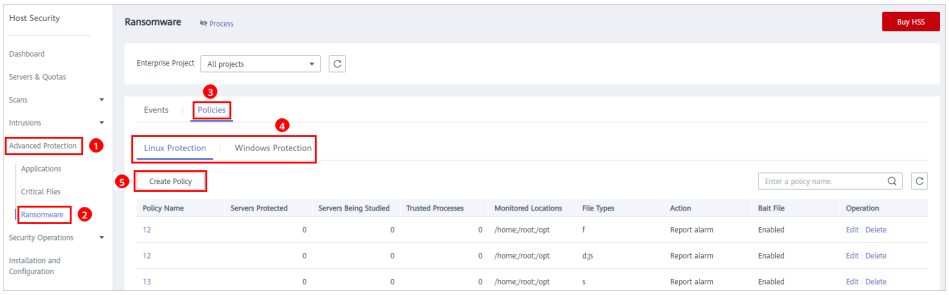
----End

Policies Against Ransomware Viruses

HSS monitors critical files stored on your servers and generates alarms on unauthorized encryption or modification, protecting your servers from ransomware.

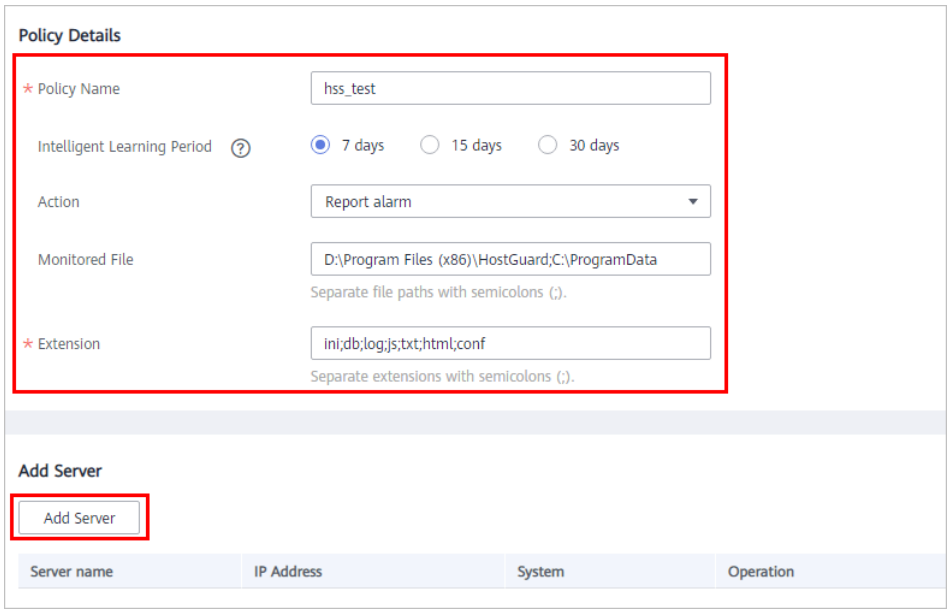
Step 1 Create an intelligent learning policy.

1. Choose **Security** > **Host Security Service**. Choose **Advanced Protection** > **Ransomware**. Click the **Policies** tab and click **Create Policy**.

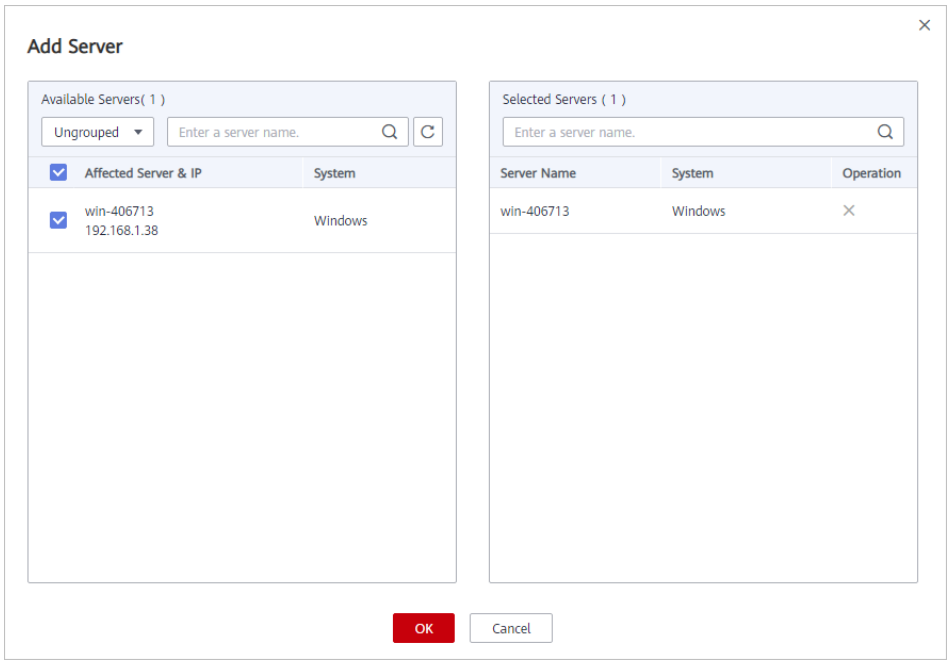


2. Configure policy details.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **Add Server** and select servers in the displayed dialog box.



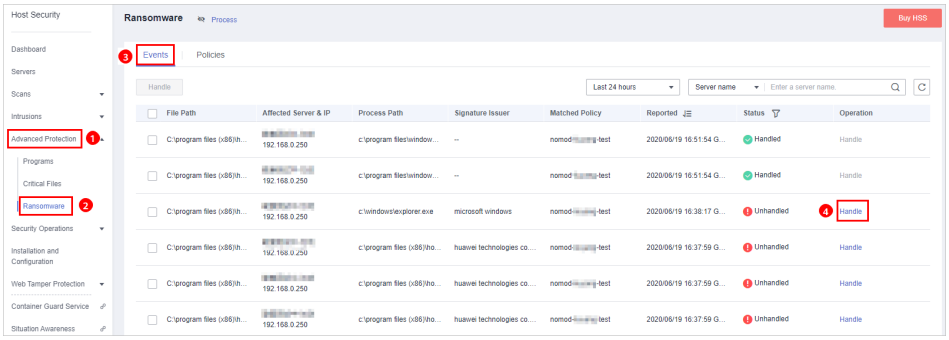
4. Click **Create and Learn**. HSS will learn the operations performed on the servers you added to the policy, collect data about normal behavior, and determine what applications are trustworthy.

   After the intelligent learning completes, HSS will monitor the files you specified in **Monitored File**, and will trigger alarms if it detects any operations performed by untrusted applications or applications that are not specified in any policies.

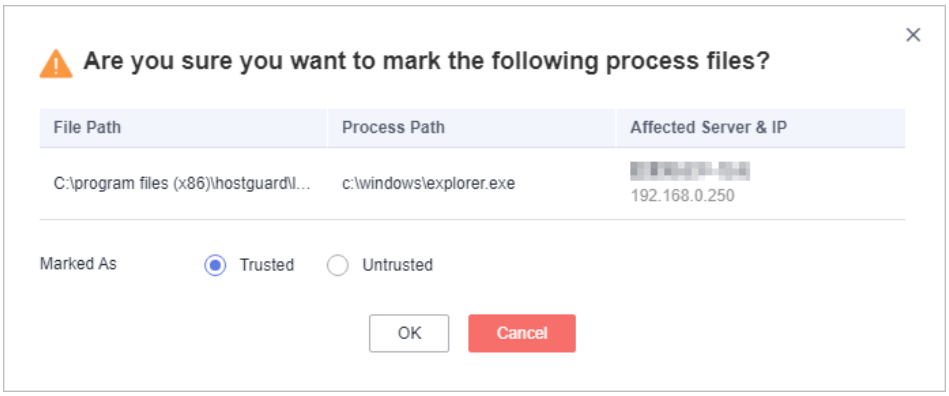
Step 2 Handling alarm events

1. Choose **Advanced Protection** > **Ransomware**. Click the **Events** tab. Click **Handle** in the **Operation** column of an event.

 Copyright © Huawei Technologies Co., Ltd.



2. Mark the event as **Trusted** or **Untrusted**.



3. You can manually block, isolate, and kill untrusted processes or processes that are not specified in any policies to prevent unauthorized encryption.

----End

- **Using Web Tamper Protection (WTP) Edition: Locking Files**

HSS can lock driver and web file directories to prevent attackers from tampering with them. If HSS detects that a file in the protected directory is tampered with, it immediately uses the backup file on your local servers to restore the file.

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

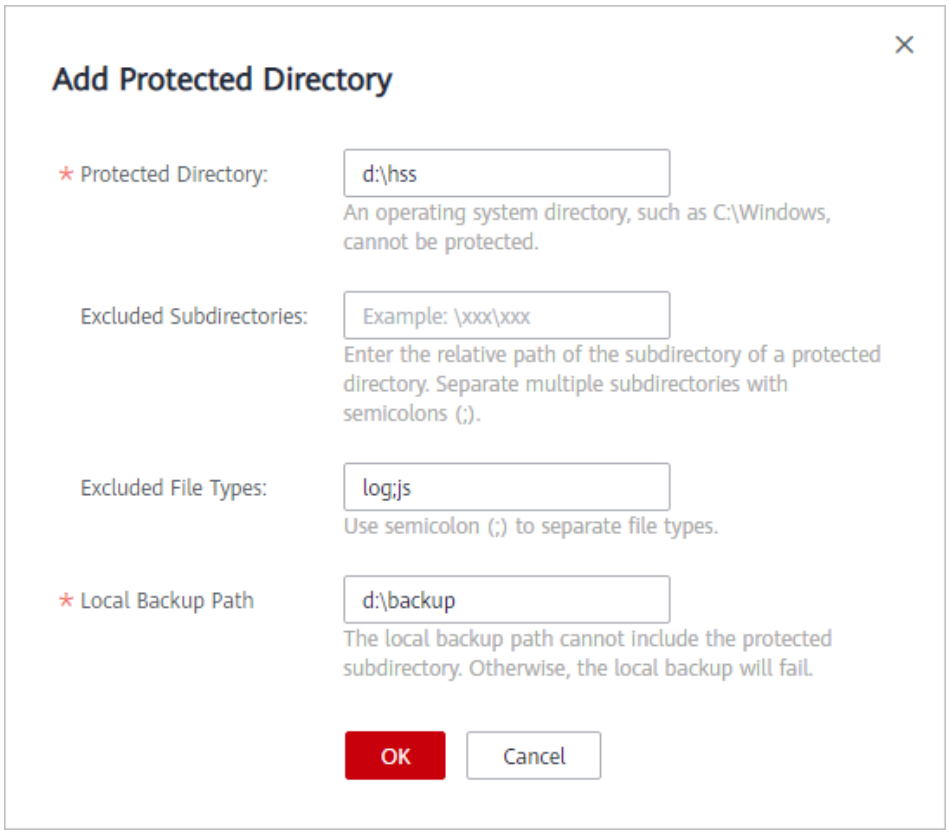
NOTE

Only the WTP edition HSS can lock file directories and use backup to restore files.

Step 1 Choose **Security** > **Host Security Service**. Choose **Web Tamper Protection** > **Server Protection**. In the **Operation** column of a server, click **Configure Protection**.

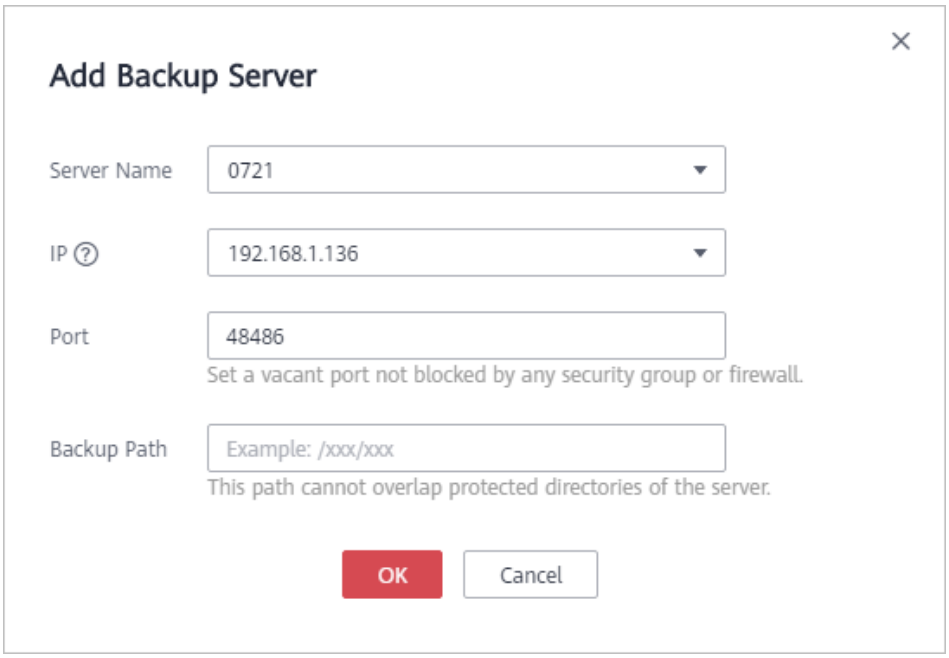
Step 2 On the **Protected Directory Settings** tab, add a protected directory and back up its files to a local path.

 Copyright © Huawei Technologies Co., Ltd.



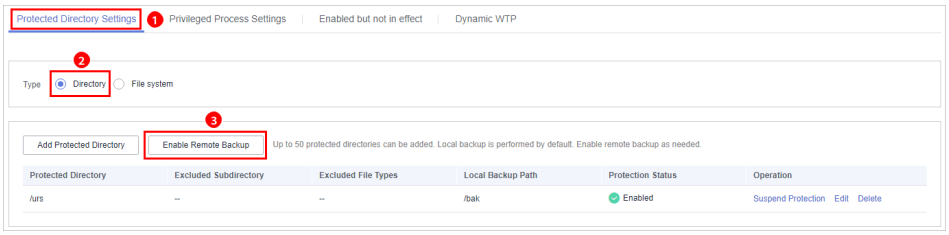
Step 3 Enable remote backup. By default, HSS backs up the files from the protected directories to the local backup directory you specified when you added protected directories. To protect the local backup files from tampering, you must enable the remote backup function.

1. Choose **Web Tamper Protection** > **Installation and Configuration**. Click the **Backup Server** tab, and click **Add Backup Server**.



 Copyright © Huawei Technologies Co., Ltd.

2. Choose **Web Tamper Protection** > **Server Protection**. In the **Operation** column of a server, click **Configure Protection**. On the **Protected Directory Settings** tab, click **Enable Remote Backup**.

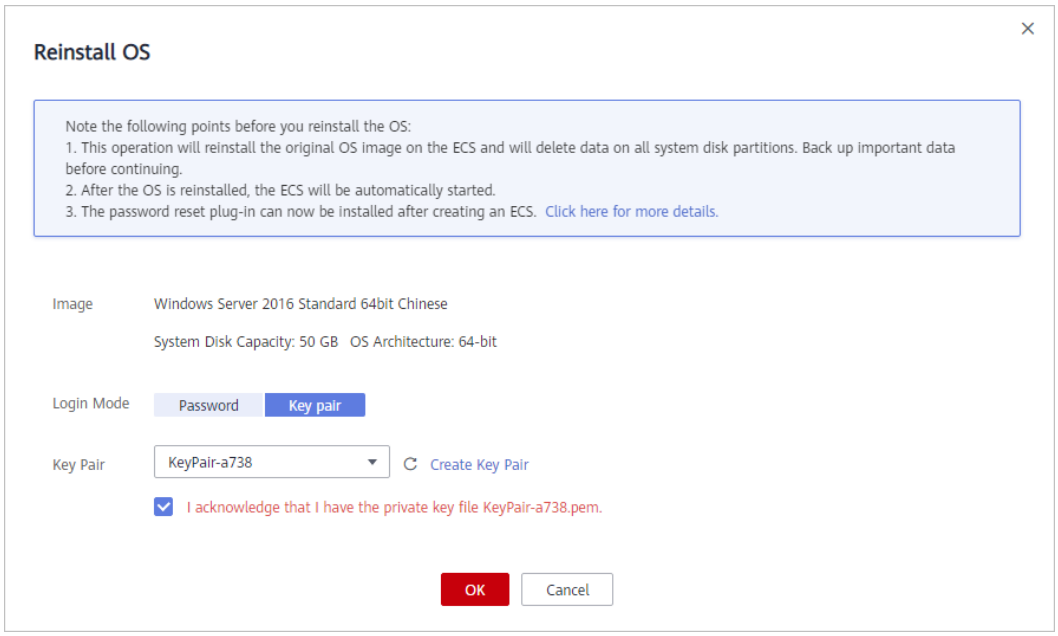


----End

Post-event Restoration

If a server has been attacked by ransomware, and your files have been encrypted or lost, you can reinstall the server OS and use the backup in CSBS to restore the server.

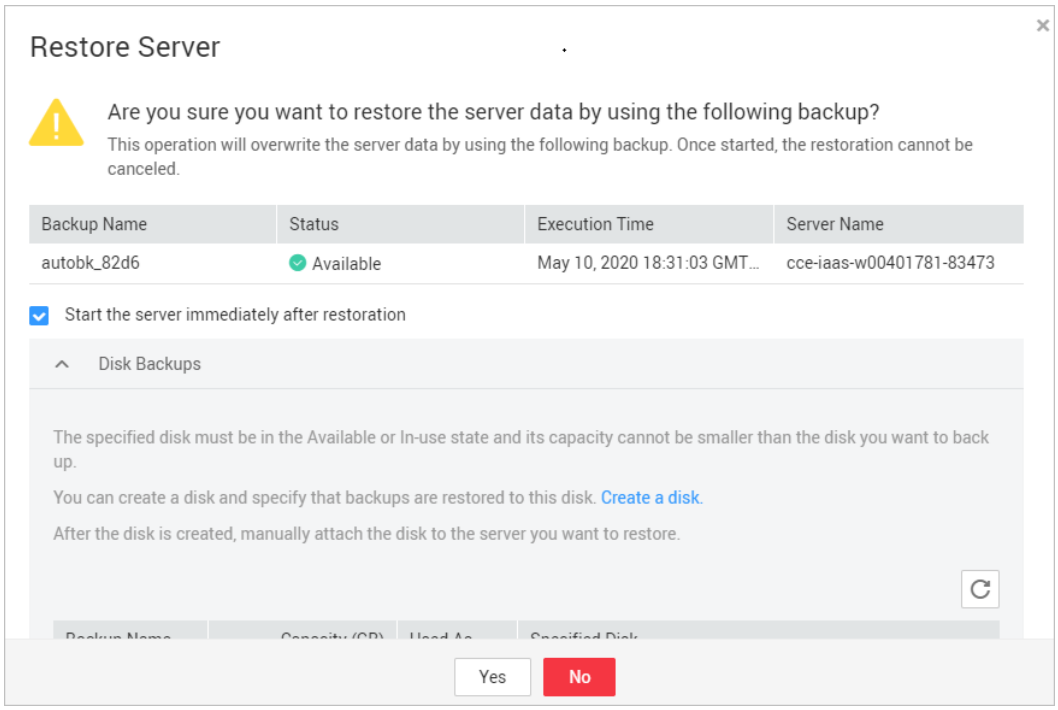
Step 1 Choose **Computing** > **Elastic Cloud Server**. In the **Operation** column of a server, click **More** and choose **Manage Image/Disk** > **Change OS**.



Step 2 Choose **Storage** > **Cloud Server Backup Service**. Locate the row of the required ECS backup and click **Restore**.

Files damaged by the ransomware will be restored.

 Copyright © Huawei Technologies Co., Ltd.



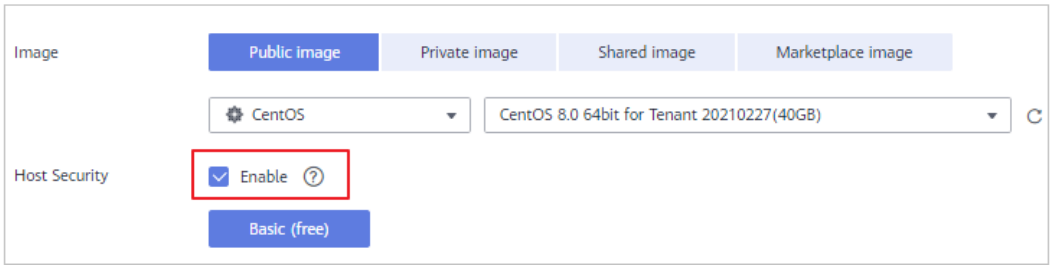
----End

 Copyright © Huawei Technologies Co., Ltd.

5 Best Practices for Using Host Security Service Basic Edition (Free)

HSS can protect your ECS against security threats, such as account cracking, abnormal login, and malicious attacks.

When you purchase an ECS, select **Enable** for **Host Security**. The HSS basic edition (pay-per-use) is free of charge. HSS can help you identify and manage the assets on your servers, eliminate risks, and defend against intrusions. There are also security operations functions available to help you easily detect and handle threats.



Billing Mode

The basic edition (pay-per-use) is free of charge and has no limit on validity period.

Overview

Table 5-1 Functions of the basic edition

Category	Feature	Description
Unsafe settings	Password complexity policy	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.

Copyright © Huawei Technologies Co., Ltd.

Category	Feature	Description
	Common weak password detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.
Intrusions	Brute-force attack	Detect password cracking attacks on accounts and block attacking IP addresses to prevent host intrusion.
	Abnormal logins	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 to the host by a brute-force attack.

Enabling Basic Edition (Pay-per-use)

Enabling mode

- When you purchase an ECS, select **Enable** for the **Host Security** parameter and select the basic edition. HSS will automatically install the agent on the ECS and enable the basic edition in pay-per-use mode.
- If you did not enable HSS when purchasing an ECS, you can install the HSS agent on the ECS and manually enable the basic edition (pay-per-use) on the HSS management console.

Procedure

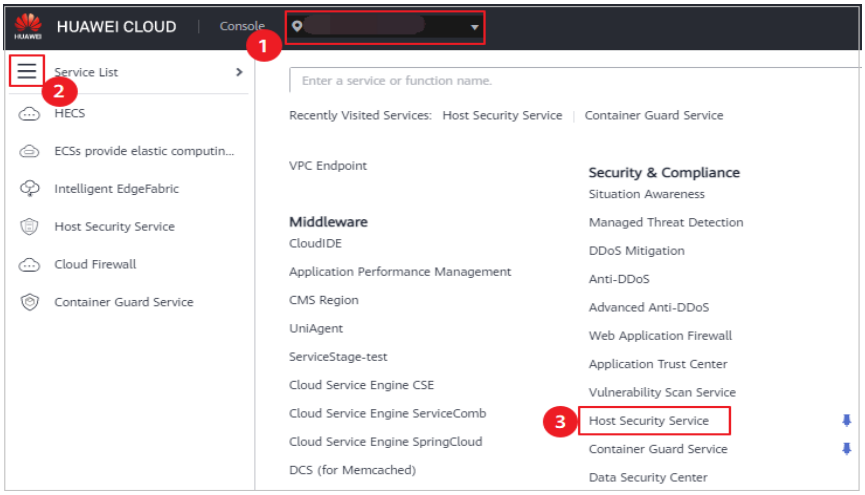
To manually enable the basic edition (pay-per-use), perform the following steps:

Step 1 Log in to the management console.

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

Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 HSS



Step 3 In the navigation pane, choose **Servers & Quotas**.

Step 4 Click the **Servers** tab. **Install the agent** for the servers to be protected.

The agent runs scan tasks to scan all servers, monitors server security, and reports collected server information to the cloud protection center.

Step 5 **Configure alarm notifications**.

After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers and web pages.

Step 6 **Enable HSS**.

When you enable HSS, a full scan is immediately performed. You can view all the detected issues on the console about 30 minutes later.

----End

Switching the HSS Edition

You can switch the HSS edition to the basic edition (yearly/monthly), enterprise edition (pay-per-use or yearly/monthly), or premium edition.

Billing Modes

 Copyright © Huawei Technologies Co., Ltd.

Table 5-2 HSS billing modes

Edition	Billing Mode	Description	Pricing
Basic	• Yearly/ Monthly • Pay-per-use	• Both modes are free of charge. • If you have purchased ECS or HECS, the basic edition in pay-per-use mode is available free of charge. • If a message indicating insufficient quota is displayed when you select **Yearly/Monthly**, switch to the pay-per-use mode.	**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		

Recommended Editions

- For test or individual users, the basic edition is recommended.
- For servers that need to meet basic security compliance requirements (such as virus and Trojan scan, one-click vulnerability fixing, and intrusion detection), the enterprise edition is recommended.
- For servers that need to meet high security requirements (for example, to protect websites or critical services), the premium or WTP edition is recommended.

  You are advised to enable the premium or WTP edition for servers that process critical services or are exposed to high risks, for example, servers that expose EIPs, application servers that store important data, and database servers.
- For servers that need to protect websites and applications from tampering, the WTP edition is recommended.
- For more information, see **Editions**.

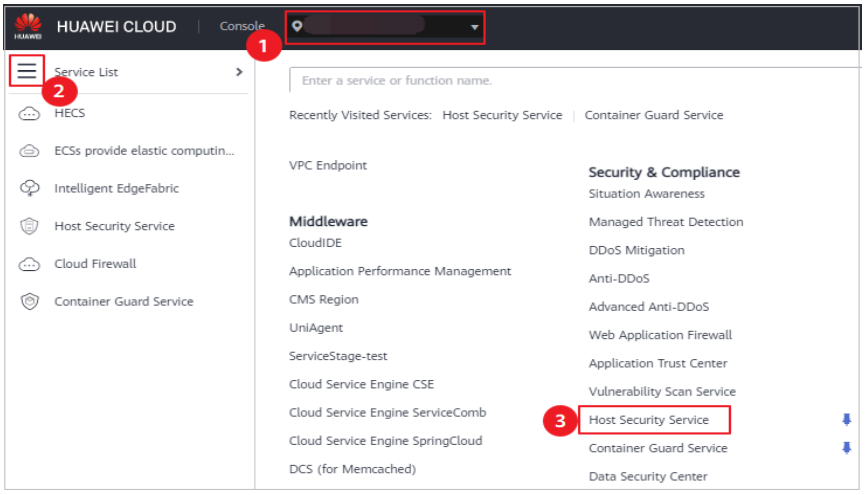
Procedure

Step 1 **Log in to the management console**.

 Copyright © Huawei Technologies Co., Ltd.

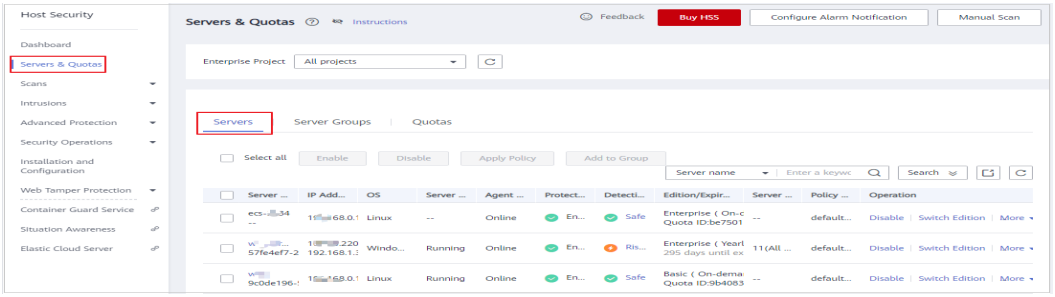
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Figure 5-2 HSS



Step 3 In the navigation tree on the left, choose **Servers & Quotas**. Click the **Servers** tab.

Figure 5-3 Server list



NOTE

You are probably in the wrong region. Only the following servers are displayed on the console:

- HUAWEI CLOUD servers purchased in the selected region
- Non-HUAWEI CLOUD hosts that have been connected to the selected region

Step 4 In the **Operation** column of a server, click **Switch Edition**.

NOTE

- To switch between billing modes in the basic or enterprise edition, disable protection, and then choose the desired billing mode when you enable protection again.
- Clicking **Enable** in the **Operation** column of a server also lets you set an HSS edition.

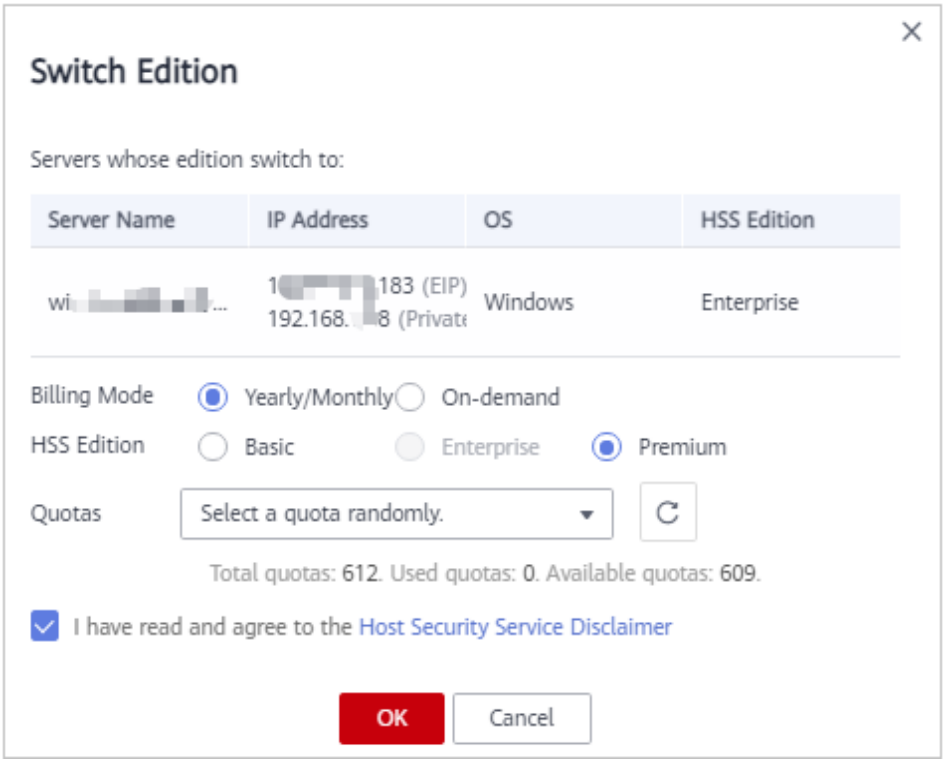
You can switch to an HSS edition in pay-per-use or yearly/monthly mode.

- Yearly/monthly

  In the displayed dialog box, select an edition, select the yearly/monthly mode, and allocate the HSS quota. Select **I have read and agree to the Host Security Service Disclaimer**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-4 Switching to a yearly/monthly edition



The quotas can be allocated in the following ways:

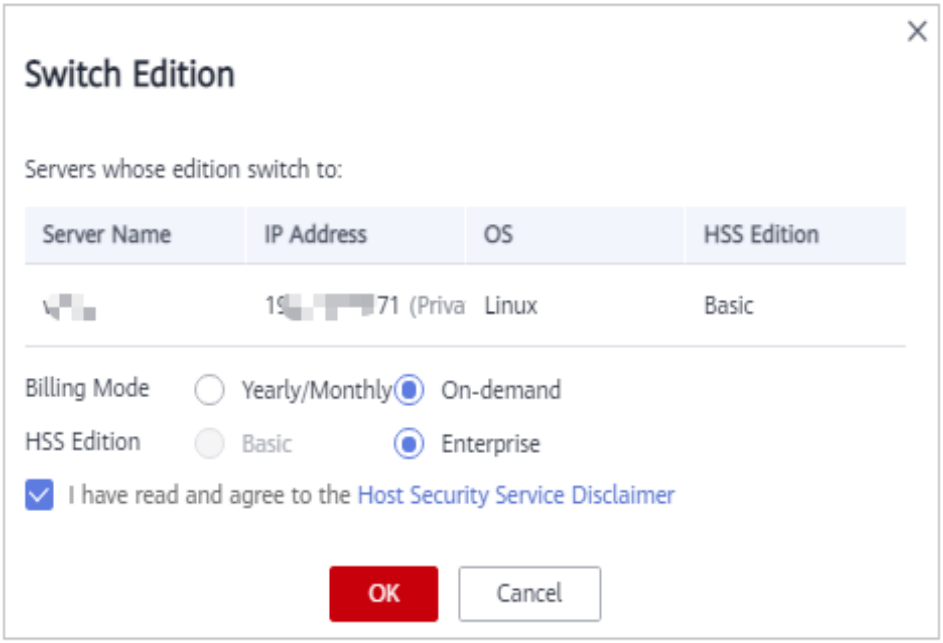
- Select **Select a quota randomly.** to let the system allocate the quota with the longest remaining validity to the server.
- Select a quota to allocate.
- Enable protection for servers in batches. The system will automatically allocate quota to them.

- Pay-per-use

  In the displayed dialog box, select **On-demand**, select an edition, and select **I have read and agree to the Host Security Service Disclaimer**, as shown in **Figure 5-5**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Switching to a pay-per-use edition



Step 5 Click **OK**. The edition information in the **Edition/Expiration Date** column will be updated.

If the edition information in the **Edition/Expiration Date** column is updated, the edition switch succeeded.

----End

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2021-07-08	This issue is the eleventh official release. The service entry is updated.
2021-05-17	This is the tenth official release. Added **Best Practices for Using Host Security Service Basic Edition (Free)**.
2020-12-30	This is the ninth official release. Added Linux ransomware protection in **Best Practices for Defense Against Ransomware**.
2020-10-15	This issue is the eighth official release. Added **Git Credential Disclosure Vulnerability (CVE-2020-5260)**. Added **Best Practices for Defense Against Ransomware**.
2020-06-19	This issue is the seventh official release. • Modified **Quickly Enhancing Server Security**. • Deleted "Precisely Locating a Malicious Process" and modified function description.
2020-05-08	This is the sixth official release. Added **SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)**.

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2020-04-26	This issue is the fifth official release, • Added **OpenSSL High-risk Vulnerability (CVE-2020-1967)**. • Added **Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/ CVE-2020-0938)**. • Added **Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)**.
2020-04-09	This is the fourth official release. Added "Precisely Locating a Malicious Process".
2020-02-12	This issue is the third official release. Added **Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)**.
2020-01-22	This issue is the second official release.
2019-11-25	This issue is the first official release.

Copyright © Huawei Technologies Co., Ltd.