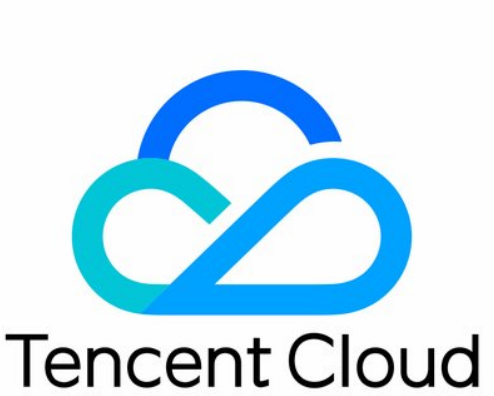
Cloud Workload Protection Platform Practical Tutorial



Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Practical Tutorial
Interpretation Of Host Security Classified Protection Assessment

Last updated: 2025-02-27 11:26:17

Interpretation Of Classified Protection Standard

Tencent Cloud Workload Protection (CWPP) product complies with the main standards of the level protection 2.0 system. According to the "Basic Requirements for Cybersecurity Level Protection" (GB/T 22239-2019), Tencent CWPP (limited to the Professional and Ultimate editions with purchased log analysis) meets the security requirements of level three and below:

No	Classified Protection Standard Section	Classified Protection Standard Serial Number	Classified Protection Standard Content	Corresponding Feature Description
1	Security area boundary—Boundary Protection	8.1.3.1 c)	It should be able to check and limit unauthorized connections from internal users to the public network.	CWPP supports detecting and intercepting unauthorized malicious outbound connections from Cloud Virtual Machines to external malicious domain names and IP addresses.
2	Security boundary – Intrusion prevention	8.1.3.3 a)	It should detect, prevent, or limit network attacks initiated from outside at key network nodes.	CWPP supports detecting and blocking brute force attacks, detecting common network attacks, and one-click vulnerability defense for some vulnerabilities.

3	Security boundary – Intrusion prevention	8.1.3.3 b)	Network attacks initiated from inside should be detected, prevented, or limited at key network nodes.	CWPP can detect outbound connections and attack behaviors at the system layer and application layer of CVM, and send alarms for abnormal process and command behaviors.
4	Security boundary – Intrusion prevention	8.1.3.3 c)	Technical measures should be taken to analyze network behaviors, achieving analysis of network attacks, especially new types of network attacks.	CWPP supports analysis based on security data from hosts, networks, and cloud platforms, enabling detection and alarms for new attacks such as mining, ransomware, Trojans, and worms.
5	Security boundary – Intrusion prevention	8.1.3.3 d)	When an attack is detected, record the source IP, attack type, attack purpose, and attack time. An alarm should be provided in the event of a serious intrusion event.	When CWPP detects a brute force attack, it records the source IP, source location, attacked server IP/name, port, protocol, username, time, cracking status, blocking status, and sends an alarm.
6	Security boundary – Security audit	8.1.3.5 b)	Audit records should include the date and time of the event, user, event type, whether the event was successful, and other audit–related information.	CWPP supports server login audit, recording information including source IP, source location, server IP/name, login username, login time, status, and risk level.
7	Secure computing environment –	8.1.4.1 a)	Users logging in should be identified and authenticated. Identifiers should be	CWPP baseline check capability supports regular security checks on cloud

	Identity authentication		unique, and authentication information should meet complexity requirements and be periodically replaced.	service customer login configurations and password complexity, provides warnings for risk items, and offers security advice.
8	Secure computing environment – Identity authentication	8.1.4.1 b)	The login failure processing feature should be enabled, and measures such as ending session, limiting the number of unauthorized login attempts, and automatically exiting when the login connection times out should be configured and enabled.	CWPP supports host login failure defense configuration, allowing flexible configuration of rules to lock users after multiple login failures within a certain time period.
9	Secure computing environment – Identity authentication	8.1.4.1 c)	Necessary measures should be taken to prevent authentication info from being eavesdropped during network transmission when performing remote management.	CWPP supports checks for improper remote management configurations, such as a baseline check prohibiting the use of telnet.
10	Secure computing environment – Access control	8.1.4.2 b)	The default account should be renamed or deleted, and the default password of the default account should be modified.	CWPP supports account permission configuration checks. Asset management supports displaying all login accounts, supports default weak password security checks, and provides alarms and remediation suggestions when risks are detected.

11	Secure computing environment – Access control	8.1.4.2 c)	Redundant or expired accounts should be deleted or disabled in a timely manner to avoid the existence of shared accounts.	CWPP supports security configuration checks for CVM accounts. Asset management supports displaying all login accounts, provides alarms for abnormal account login IPs, and supports alerts to avoid the existence of shared accounts.
12	Secure computing environment – Security audit	8.1.4.3 a)	Security audit should be enabled, covering each user, auditing important user behaviors and significant security events.	CWPP supports recording cloud server account login operations, as well as auditing high-risk commands and high-risk operations.
13	Secure computing environment – Security audit	8.1.4.3 b)	Audit records should include the date and time of the event, user, event type, whether the event was successful, and other audit-related information.	CWPP log records include host IP, host instance ID, account, source IP, destination IP, process ID, port, event type, occurrence time, action policy, etc.
14	Secure computing environment – Security audit	8.1.4.3 c)	Audit records should be protected, regularly backed up, and prevented from unexpected deletion, modification, or overwrite.	The host security product supports a log audit storage feature, which can store log data for at least 6 months. Different tenants use completely independent log spaces, and log data has a multi-replica backup mechanism.

15	Secure computing environment – Intrusion prevention	8.1.4.4 b)	Unnecessary system services, Default Sharing, and high-risk ports should be closed.	CWPP asset management supports unified control of services, processes, and open ports running on cloud servers.
16	Secure computing environment – Intrusion prevention	8.1.4.4 c)	Management terminals accessed via the network should be restricted by setting terminal access methods or network address ranges.	CWPP supports adding allowlists for host login IP addresses. Logins from non-allowlisted users will be blocked. Combined with security groups, it enables cloud network management and restriction.
17	Secure computing environment – Intrusion prevention	8.1.4.4 e)	It should be able to detect potential known vulnerabilities and fix them promptly after thorough testing and evaluation.	CWPP supports detecting Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities, assessing risk levels, and providing remediation suggestions.
18	Secure computing environment – Intrusion prevention	8.1.4.4 f)	It should be able to detect intrusions on critical nodes and provide alarms when serious intrusion events occur.	CWPP supports detecting intrusions on critical nodes, including malicious files, abnormal logins, password cracking, malicious requests, high-risk commands, rebound shell, local privilege escalation,

				file tampering, and other threats, providing alarms and some proactive blocking capabilities.
19	Secure computing environment – Malicious code prevention	8.1.4.5	Technical measures to prevent malicious code attacks or proactive immune verify trustworthiness mechanisms should be used to promptly identify and effectively block intrusions and viruses.	CWPP supports malicious file scanning and killing, real-time monitoring of Trojans, viruses, and automatic isolation.
20	Security Management Center – Security Management	8.1.5.3 a)	Security administrators should undergo identity authentication, be allowed to perform security management operations only through specific commands or operation interfaces, and these operations should be audited.	CWPP supports security management operations on cloud resources through the console, and can audit login behaviors and high-risk commands.
21	Security Management Center – Security Management	8.1.5.3 b)	Security policies in the system should be configured by security administrators, including setting security parameters, uniformly marking Subjects and objects, authorizing Subjects, and configuring trusted verification policies.	CWPP supports configuring security policies in the host system through the console.
22	Security Management Center –	8.1.5.3 e)	Centralized management should be conducted for	CWPP supports centralized management of

	Centralized Control		security policies, malicious code, patch upgrades, and other security-related matters.	vulnerabilities, malicious code detection, and isolation for host security.

Cybersecurity Classified Protection Compliance Service Baseline Policy

Tencent Cloud CWPP by default provides the Cybersecurity Classified Protection Compliance Baseline Policy, supporting periodic detection and one-click detection of baseline detection items. It helps understand the baseline pass rate and risk situation, provides risk levels and remediation suggestions for baselines and detection items, aiding in quick rectification to meet compliance requirements. The following are the supported detection items for Cybersecurity Classified Protection Compliance:

Baseline Categorization	Baseline Name	Number Of Included Check Items
Classified Protection Level 2	Level-2 Cybersecurity Classified Protection - CentOS 6 Security Baseline Check	16
	Level-2 Cybersecurity Classified Protection - CentOS 7 Security Baseline Check	18
	Level-2 Cybersecurity Classified Protection - CentOS 8 Security Baseline Check	16
	Level-2 Cybersecurity Classified Protection - Ubuntu 14 Security Baseline Check	19
	Level-2 Cybersecurity Classified Protection - Ubuntu 16 Security Baseline Check	19
	Level-2 Cybersecurity Classified Protection - Ubuntu 18 Security Baseline Check	21
	Level-2 Cybersecurity Classified Protection - Ubuntu 20 Security Baseline Check	29
Classified Protection Level 3	Level-3 Cybersecurity Classified Protection - CentOS 6 Security Baseline Check	27
	Level-3 Cybersecurity Classified Protection -	31

	CentOS 7 Security Baseline Check	
	Level-3 Cybersecurity Classified Protection - CentOS 8 Security Baseline Check	36
	Level-3 Cybersecurity Classified Protection - Ubuntu 14 Security Baseline Check	35
	Level-3 Cybersecurity Classified Protection - Ubuntu 16 Security Baseline Check	33
	Level-3 Cybersecurity Classified Protection - Ubuntu 18 Security Baseline Check	40
	Level-3 Cybersecurity Classified Protection - Ubuntu 20 Security Baseline Check	48
	Level-3 Cybersecurity Classified Protection - Windows 2008 Security Baseline Check	19
	Level-3 Cybersecurity Classified Protection - Windows 2012 Security Baseline Check	19
	Level-3 Cybersecurity Classified Protection - Windows 2016 Security Baseline Check	19

Auto Fix Of Vulnerabilities

Last updated: 2025-02-27 11:28:48

This topic describes the tutorial for automatically fixing vulnerabilities.

> **Note:**
> Auto-fixing of vulnerabilities may involve executing commands on your servers, which may affect running applications or core system components, and may impact your business continuity. For servers used for your core business, we recommend that you take the impact into full consideration when deciding which vulnerabilities to fix and in what order.

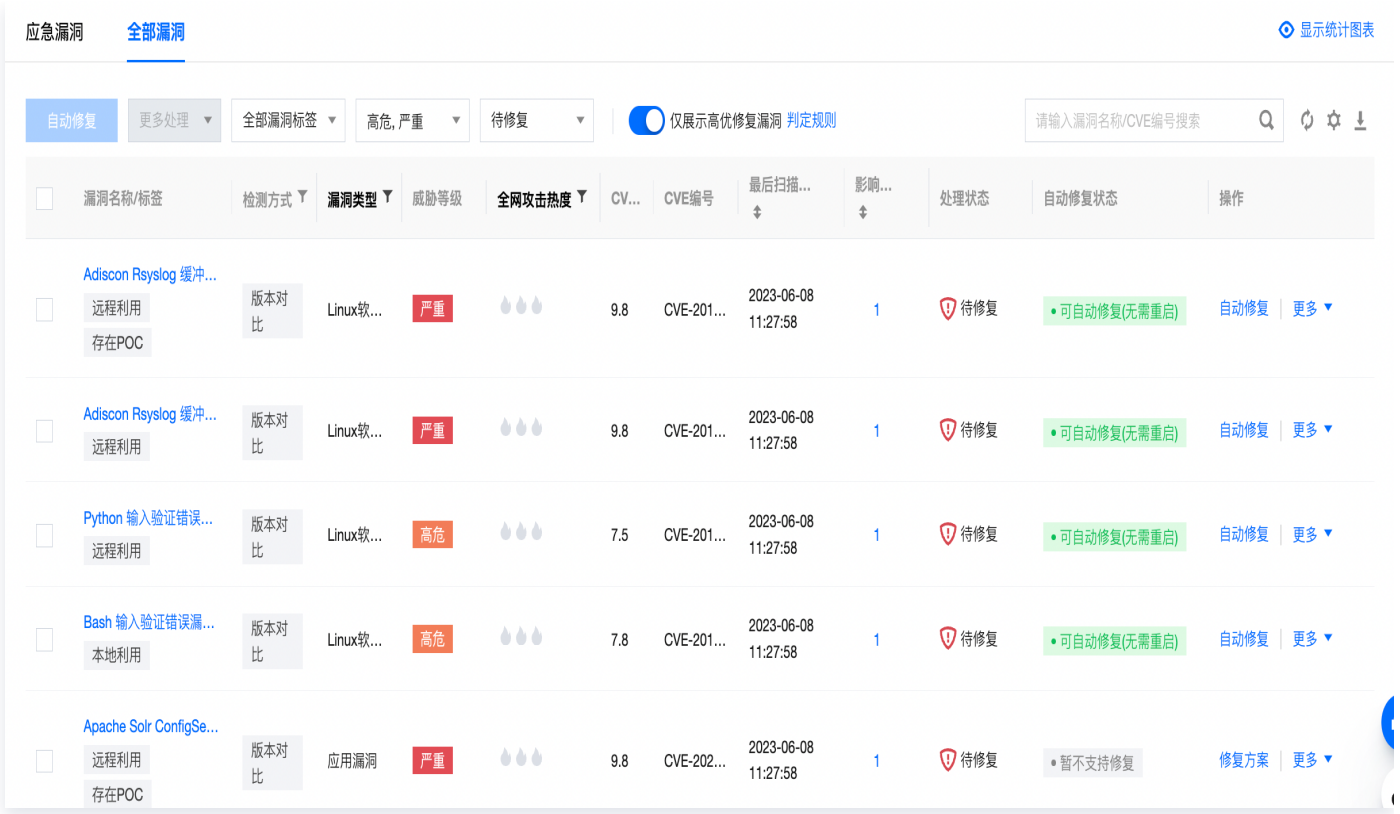
Explanation

- Supported servers: Only CVM servers on Tencent Cloud (host security client online and bound with CWPP Ultimate license).
- Vulnerabilities that can be fixed automatically: Linux software vulnerabilities (some) and Web-CMS vulnerabilities (some).

Operation Guide

1. Log in to the CWPP Console and click **Vulnerability Management** in the left navigation pane. Then the list of detected vulnerabilities is shown at the bottom.
2. The **Vulnerability List** is categorized into Emergency Vulnerabilities and All Vulnerabilities. Since both are displayed from the detection dimension, there is not much difference in functionality. The steps for fixing vulnerabilities automatically are described below using **All Vulnerabilities** as an example.

   > **Note:**
   > - Vulnerability Fix Priorities: Urgent vulnerabilities > High-priority vulnerabilities > All vulnerabilities.
   > - For vulnerabilities that can be automatically fixed, **Auto Fix** is shown in the operation column; for vulnerabilities that cannot be automatically fixed, **Fix Scheme** is shown in the column.



Step 1: View Vulnerability Details

Click **Auto Fix** to open the vulnerability details pop-up window.

Step 2: Select the Host To Fix

1. In the list of affected servers, select the host you want to fix and click **Fix**.

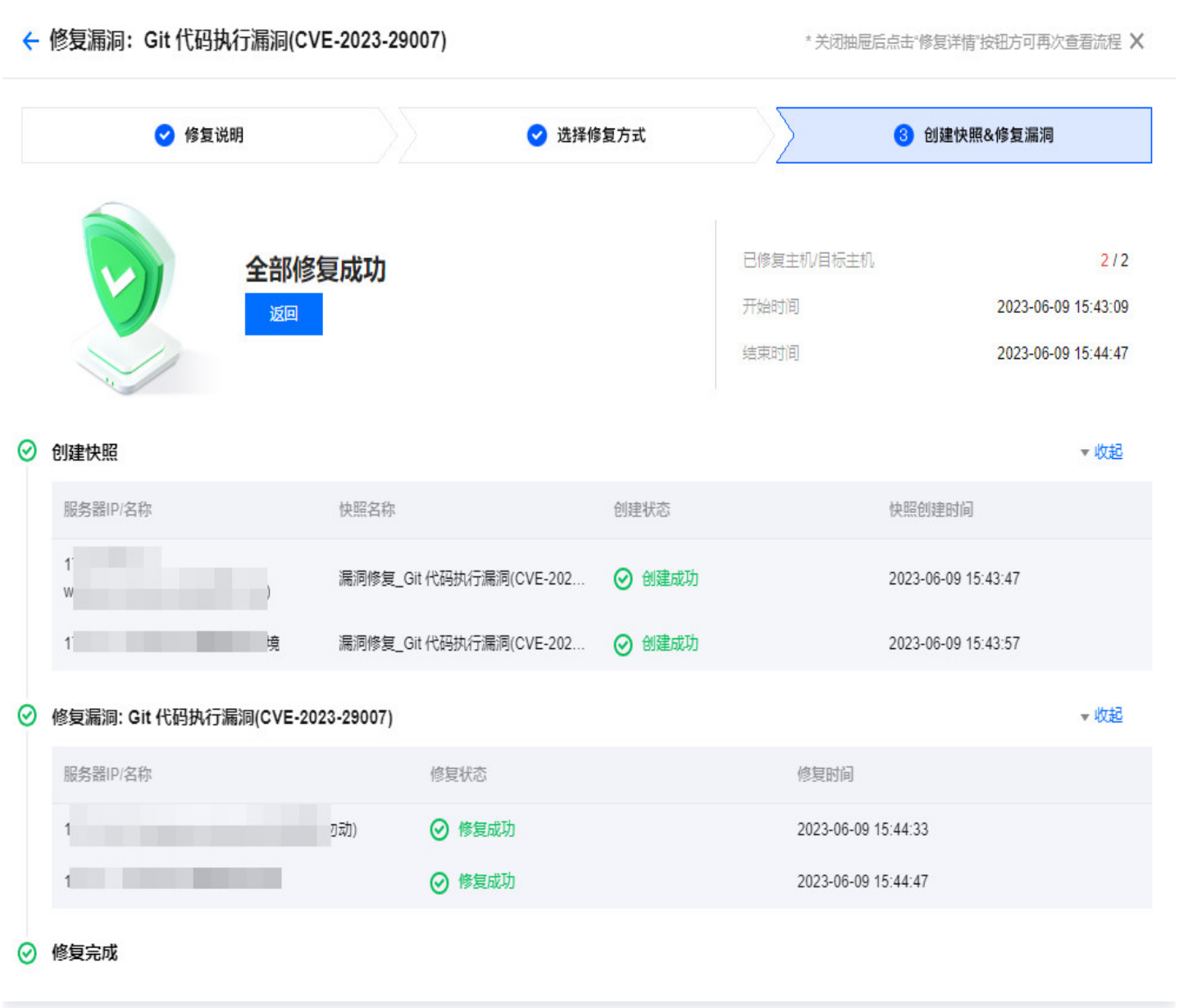
2. In the confirmation pop-up, click **Confirm** to enter the vulnerability fix page.

Step 3: Choose Whether To Create Snapshots

1. On the vulnerability modification page, confirm the range of hosts to be fixed and click **Next**.
2. Choose the repair method based on actual needs:
   - Fix and Automatically Create Snapshots: You can set the snapshot name and snapshot storage duration (3 days, 7 days, or 15 days). It is recommended to set the duration to 7 days so that the snapshots can be rolled back in time if necessary.
   - Fix Without Creating Snapshots: If snapshots have been created for all the servers selected for fixing vulnerabilities on the current day, this item becomes optional.

Step 4: Fix Vulnerabilities

Click **Confirm** to start fixing the vulnerabilities. You can keep track of the process.



Step 5: Check the Server Status Changes

Return to **Vulnerability Details** and monitor the host status changes. If the vulnerability fix fails, the status will be fix failure; if the vulnerability fix succeeds, the status will change to fixed.

- After the vulnerabilities are fixed, if your business is greatly affected, click **Rollback** to go to CVM > **Snapshot List**, and select the snapshots created before the fixing to roll back. After the rollback is successful, restart the servers to scan the vulnerabilities again.
- After the vulnerabilities are fixed, perform a **Rescan** to verify whether the vulnerabilities have been fixed.
- After the vulnerabilities are fixed, you can also click **Repair details** to view the specific repair process.

Scan Code Login Security

Last updated: 2025-02-27 11:29:19

The secure login feature via QR code scanning allows users to log in to the server by simply verifying through WeChat QR code scanning without entering a password. This feature effectively prevents brute force attacks by hackers, thereby enhancing server security and increasing login convenience. This article will introduce a practical tutorial on secure login via QR code scanning.

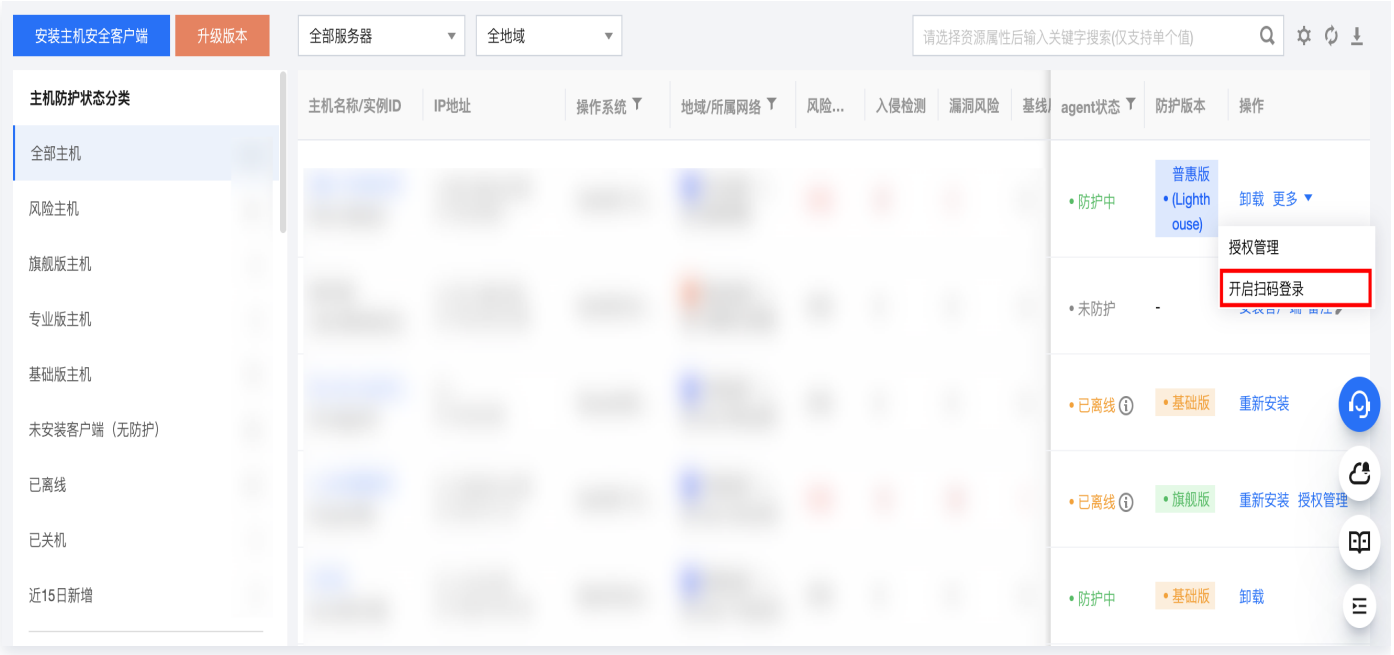
> ⚠ **Note:**
> - After enabling QR code login, WeChat QR code verification will replace password login for Tencent Cloud account, which may affect related automated business. Meanwhile, when using SSH-related protocols, although SCP, SFTP, RSYNC, GIT, MOSH, and other scenarios are supported, scenarios like folder mounting based on SSHFS protocol are not yet supported.
> - **For hosts of core business, it is recommended to fully consider before deciding whether to change the login method.**

Explanation

- Supported host types: Only CVM/Lighthouse servers on Tencent Cloud (requires Cloud Workload Protection Platform client to be online).
- Supported login users: The Tencent Cloud sub-account and its root account to which the machine belongs, or other Tencent Cloud accounts authorized by CAM.

Step 1: Configure the Login Method

1. Log in to the CWPP Console, and in the left navigation bar, click **Host List**.
2. In the host list, find the corresponding instance on the right side, and click **Enable QR Code Login**.



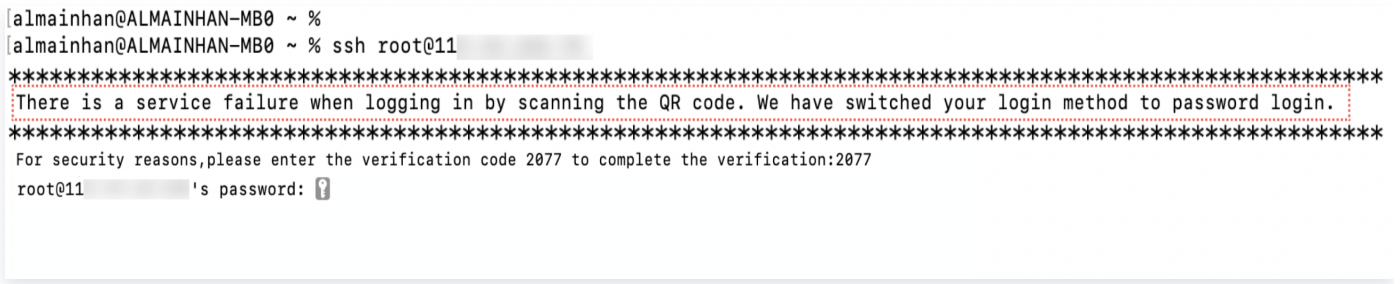
3. Click **Confirm**. After enabling, the server will preferentially log in through a Tencent Cloud account by scanning the QR code with WeChat.

Step 2: Terminal Initiates Login

1. After enabling QR code login, a QR code will pop up after entering the instance IP in the SSH command line. Use WeChat to scan the code to enter the Tencent Cloud Assistant mini program for identity authentication. After completing the authentication, you can log in.

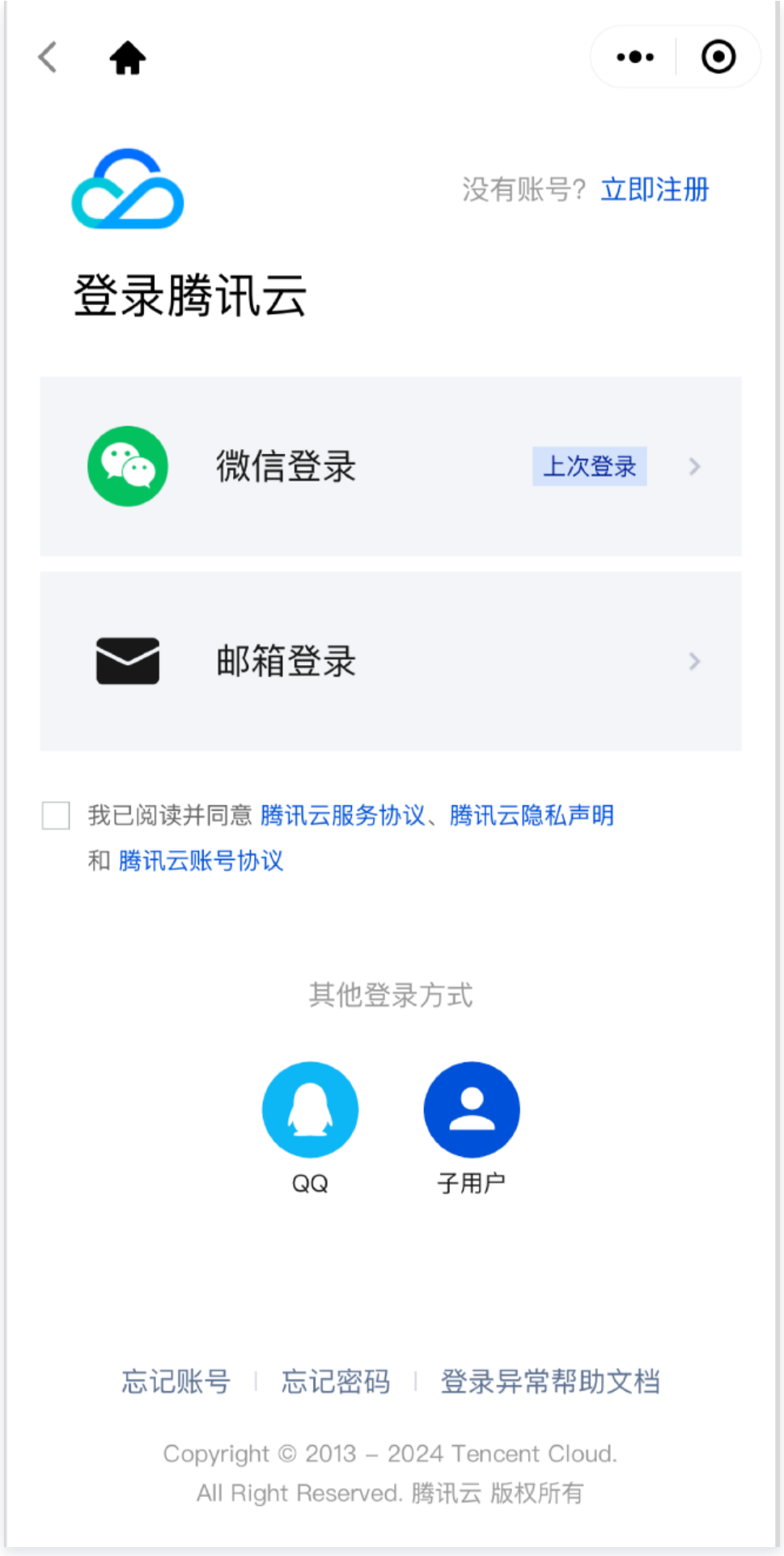
> **Note:**
> If there is an issue with the QR code display, please open the QR code image in a web page using the URL provided below.

2. When the QR code login service encounters an exception, it will automatically downgrade to the standard password login, and a captcha fallback strategy will be added. After entering the random number to complete the authentication, you can log in using the password.

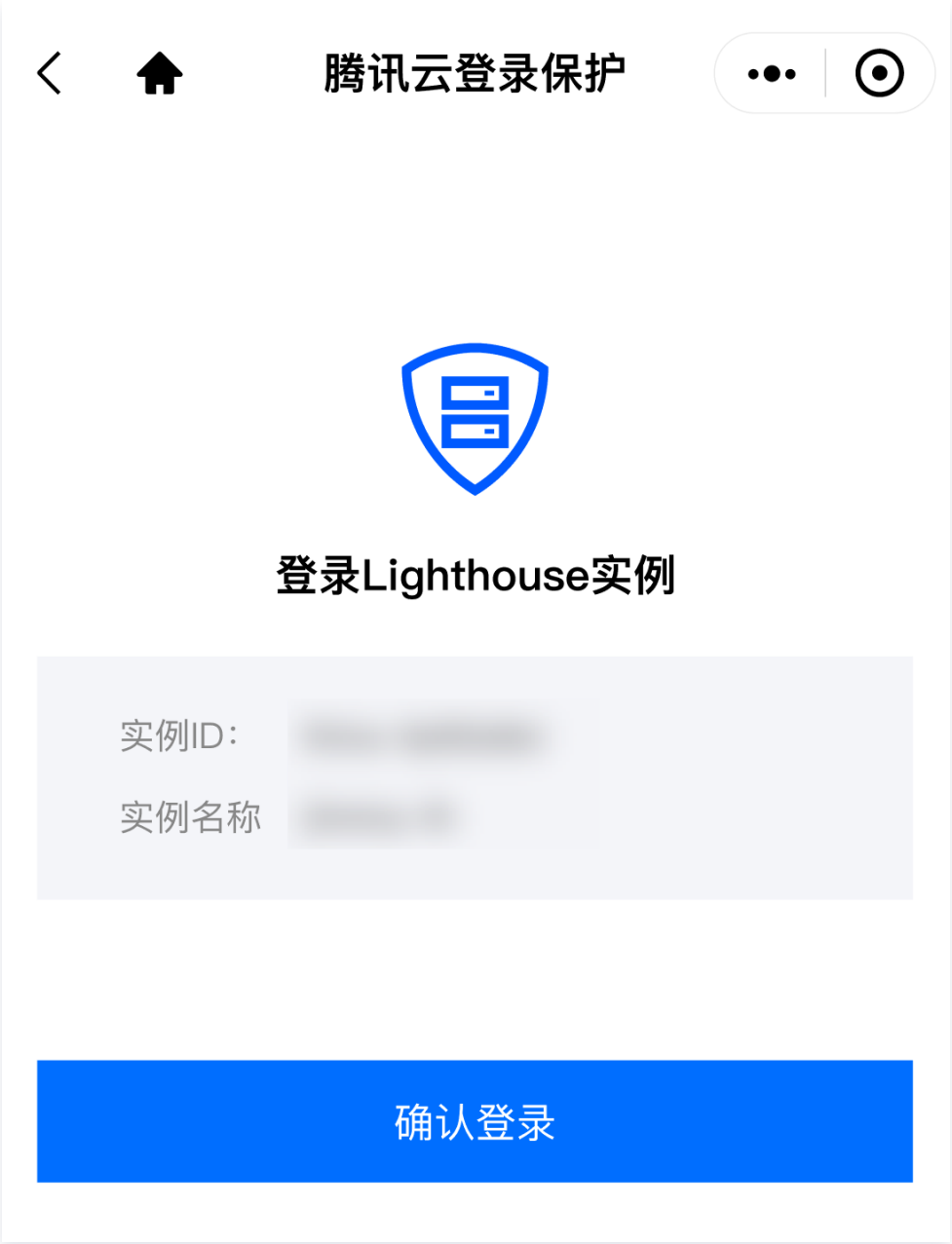


Step 3: Mini Program Verification

1. After scanning the code, open Tencent Cloud Assistant, select the login method to log in to the Tencent Cloud account to complete the verification.



2. Successfully log in to the Tencent Cloud account, click **Confirm Login**, verify the account's permission to log in to the server, and complete the login after verification.



Malicious File Handling

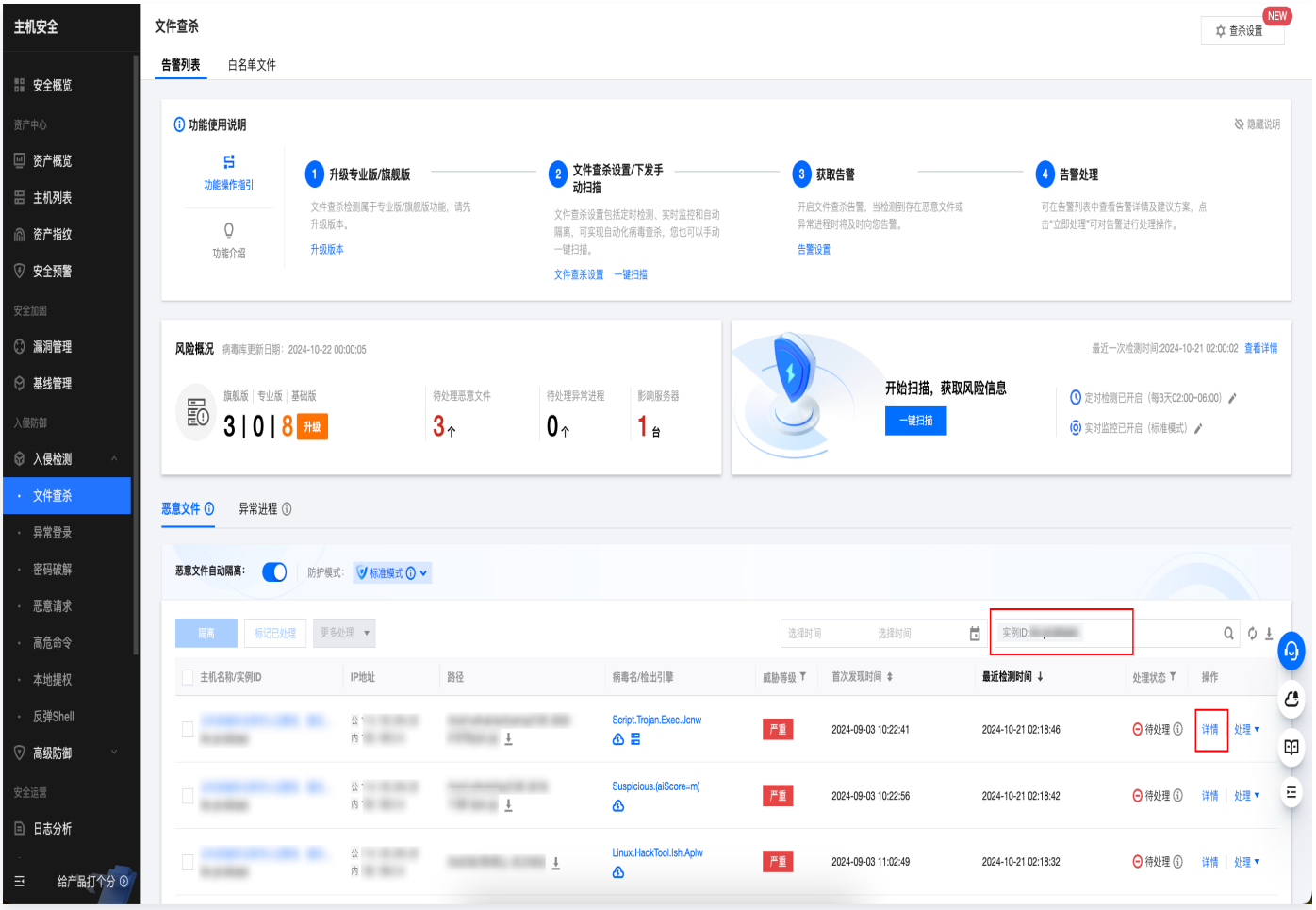
Last updated: 2025-02-27 11:52:37

When a server under a user's Tencent Cloud account is detected with a malicious file, if Host Security finds that the file is not in the allowlist, a real-time alarm will be triggered.

Processing Procedures

After receiving a malicious file alert, follow these steps:

1. Log in to the CWPP Console, and select **Intrusion Detection** > **Malicious File Scan** from the left sidebar.
2. On the Malicious File Scan page, search by **Alarm Asset ID** to locate the specific alarm and click **Details**.



3. After viewing the alarm details, confirm whether the malicious file is a false alarm. If it is a false alarm, proceed to step 4. If it is not a false alarm, proceed to step 5.

> **Note:**

Whether the malicious file is a false alarm can be determined by the following methods:

- Contact the business team to determine if the file is necessary for normal business operations.
- Query threat intelligence to determine if the file is marked as a malicious sample by the public network.
- Determine if the file's behavior triggers more alarms.
- Contact Security Expert Service.

4. If it is confirmed as a false alarm, add the file to the allowlist. Future detections of this file will be ignored and will not trigger an alarm. Contact us for Feedback on False Alarms.

5. If it is confirmed not to be a false alarm, follow the remediation suggestions in the alarm details to handle it.

- You can click **Isolation** to isolate the file and terminate the related process. The Alarm processing status will change to "Isolated".
- You can log in to the host, find the corresponding file, manually delete or isolate it and terminate the related process, then mark the Alarm as processed in the console. The Alarm processing status will change to "Processed".

6. On the Malicious File Scan page, click **Scan Settings** in the upper right corner. It is recommended to enable the automatic isolation switch to automatically isolate detected malicious files immediately.

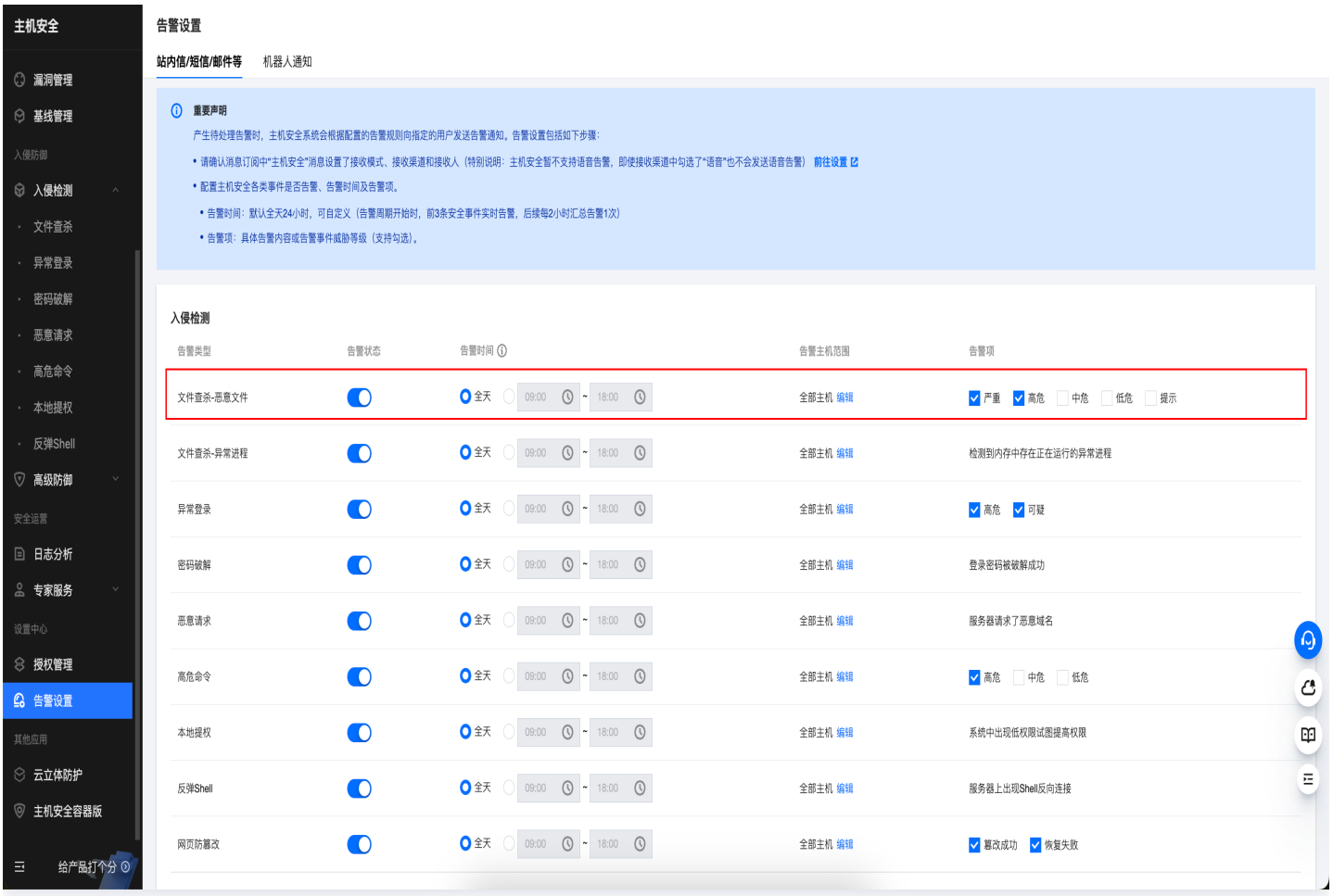
Note:

- Not all detected malicious files can be automatically isolated. Some malicious files still require manual confirmation for isolation. It is recommended to check the alarm list in file scanning to ensure all have been handled.
- If a false positive isolation occurs, please restore the file from the isolated list.
- Enabling or disabling automatic isolation requires configuration, and there is a delay of a few minutes before it takes effect.

Hot Issues

Where To Configure Alarms For Malicious Files?

On the Alarm Settings page, configure the alarm time, alarm scope, and alarm items for **Malicious File Scan – Malicious File**.



How To Set Up Periodic Detection For Malicious Files?

On the Malicious File Scan page, click **Scan Settings** in the upper right corner to open the scan settings popup and set up a scheduled scan.

If the File Has Been Deleted, What Will Be the Status Of the Original Alarm After Scanning For Malicious Files Again?

The original alarm processing status will change to "Cleared."