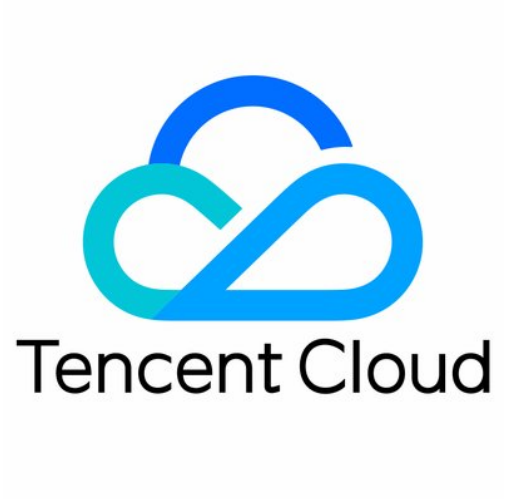
Cloud Workload Protection

FAQs

Product Documentation



FAQs

Last updated : 2020-07-30 11:14:30

What will happen when a server is intruded?

- Business interruption: databases and files are tampered with or deleted, resulting in service unavailability and system corruption.
- Data theft: hackers steal your data and sell it publicly, leading to leaks of your end users' private data, damage to your brand image, and customer loss.
- Data encryption by ransomware: hackers who intrude into your servers encrypt your data and extort ransom by embedding irreversible encryption ransomware.
- Service instability: hackers run cryptomining and DDoS trojan programs on your server to consume considerable system resources, making the servers unable to provide services normally.

How do I achieve automatic data backup through quick snapshots?

Snapshot is a data backup method provided by Tencent Cloud. It can create a fully available duplicate of the specified source cloud disk whose lifecycle is independent of the source cloud disk. You can create snapshots on a regular basis to quickly recover data in case of accidental data loss. You can create a snapshot in the console in the following steps:

1. Log in to the CBS Console.
2. Locate the row of the instance for which you want to create a snapshot and click **Create Snapshot**.
3. Confirm the relevant information on the snapshot creating page, name the snapshot, click **Submit**, and wait for the snapshot to be created.

For more information, please see Snapshot Overview and Creating Snapshot.

What should I do if my password is compromised by brute force attacks?

If your password is compromised, your server may have been intruded with backdoor programs embedded into it.

- Check the server security status to see whether there are other unknown accounts and trojan files, and if yes, delete them immediately and change the server login password. For more information, please see Intrusions on Linux and Intrusions on Windows.
- If necessary, you are recommended to reset the server and then set a complex password containing at least 15 letters, digits, and special characters.

What should I do if suspicious logins are detected?

CWP judges whether a login attempt is intended according to the list of usual login locations for admins. Please check the login log carefully. If a login was not intended, the password may have been compromised. In this case, you need to perform a thorough security check on your server.

Why does a CWP agent go offline? And how do I solve this issue?

The CWP agent is not connected to the server, which causes it to be displayed as offline on the backend. You are recommended to download and install the agent again. The agent may go offline for the following reasons:

- The agent is blocked by the firewall policy of the server. Please configure the firewall policy to allow the CWP backend access address.
- The agent is corrupted by a third-party malware on the server. In this case, please reinstall the agent.

What should I do if my server has trojan files?

For more information on how to deal with trojan files detected, please see Trojan Operation and Handling.

What should I do if trojans are not successfully detected (false negative)?

If you find an undetected trojan file, please submit a ticket to contact the Tencent Cloud security team for fast identification.

How do I uninstall the CWP agent?

Log in to the CWP Console, select **Asset Management** > **Server List** on the left sidebar, find the server from which you want to uninstall CWP, and click **Uninstall**. Or, open the installation directory and use the uninstaller there for uninstallation.

What should I do if there is a problem with identity verification for my Tencent Cloud account?

If you have encountered a problem related to the Tencent Cloud account when using CWP, please see the account documentation.

How can I reduce the probability of server intrusion?

- Fix high-risk vulnerabilities and baseline issues in a timely manner.
- Set strong passwords to defend against brute force attacks.
- Regularly inspect accounts, permissions, and ports and resolve alarms in the CWP Console in a timely manner.
- Perform snapshot backup regularly.

How long does it take before the security baseline takes effect after the product is configured?

The security baseline takes effect immediately after the product is configured

How do I fix a false positive where an intended login is mistakenly marked as suspicious?

You can log in to the CWP Console, select **Intrusion Detection** > **Login Audit** on the left sidebar, and click **Suspicious Logins** on the login audit page to find the login log that is defined as suspicious. In the "Operation" column on its right, click **Allowlist** to add it to the allowlist and eliminate the false positive.