Cloud Workload Protection Platform

Troubleshooting

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Troubleshooting Intrusions on Linux

Last updated：2023-12-26 16:40:00

This topic describes how to troubleshoot the intrusions into servers running on Linux and provides security optimization suggestions.

Identifying Causes of Intrusions

I. Check for hidden accounts and weak passwords

1. Check whether **weak passwords** exist in the server system and application accounts.
Description: check the admin account, database account, MySQL account, Tomcat account, and website backend admin account for weak passwords that can be easily cracked by hackers.
Solution: Log in to the system or application backend with admin privileges and change the weak passwords to complex passwords.
Risk level: high
2. Run the command `last` to view the record of accounts recently logged in to the server and check whether there were logins from suspicious IPs.
Description: Attackers or malware often inject hidden accounts into the system to implement privilege elevation or other destructive attacks.
Solution: When you find a suspicious user, run the command `usermod -L username` to disable the user or run the command `userdel -r username` to delete the user.
Risk level: high
3. Run the command `less /var/log/secure|grep 'Accepted'` to check whether there were successful logins from suspicious IPs.
Description: Attackers or malware often inject hidden accounts into the system to implement privilege elevation or other destructive attacks.
Solution: Run the command `usermod -L username` to disable the user or run the command `userdel -r username` to delete the user.
Risk level: high
4. Check whether the system uses the **default management ports**.
Check whether the management ports (for SSH, FTP, MySQL, Redis, etc.) used by the system are the default ones. These default ports can be easily attacked by automated tools.
Solutions:

4.1. Change port 22 in the file `/etc/ssh/sshd_config` on the server to a non-default port. You need to restart the SSH service after modification.

Note:

When you change the port, you need to edit the security group configuration of the server on the CVM Console to allow the corresponding port in its inbound rule. For more information, see Adding Security Group Rules.

4.2. Run `/etc/init.d/sshd restart` (on CentOS) or `/etc/init.d/ssh restart` (on Debian or Ubuntu) to restart the server to make the updated configuration take effect.

4.3. Change the default listener ports 21, 3306, and 6379 in the configuration files of FTP, MySQL, and Reids to other ports.

4.4. Deny remote login IPs by editing the files `/etc/hosts.deny` and `/etc/hosts.allow` .

Risk level: high

5. Check the `/etc/passwd` file for unauthorized account logins.

Description: Attackers or malware often inject hidden accounts into the system to implement privilege elevation or other destructive attacks.

Solution: Run the command `usermod -L username` to disable the user or run the command `userdel -r username` to delete the user.

Risk level: medium

II. Check for malicious processes and unauthorized ports

1. Run `netstat -antlp` to check whether the server is being listened to by an unauthorized port and check the corresponding PID.

Check the server for malicious processes, which often open listener ports and connect to external controllers.

Solutions:

a. If you find an unauthorized process, run `ls -l /proc/$PID/exe` or `file /proc/$PID/exe` ($PID is the PID) to check the path to the process file identified by the PID.

b. If it is a malicious process, delete its file.

Risk level: high

2. Run the commands `ps -ef` and `top` to check for unusual processes.

Description: If you find an unauthorized process with a constantly changing name that occupies a great amount of CPU or memory resources, it may be a malicious program.

Solution: After confirming that the process is malicious, run the command `kill -9 process name` to end the process or use a firewall rule to prevent network connection by the process.

Risk level: high

III. Check for malicious programs and suspicious startup items

1. Run the commands `chkconfig --list` and `cat /etc/rc.local` to check whether suspicious startup services exist in the startup items.

Description: Malicious programs are often added to the system startup items so that they can run again after the system is restarted.
Solution: If you find a malicious process, run the command `chkconfig service name off` to close it. At the same time, check whether there are suspicious items in `/etc/rc.local` . If so, comment them out.
Risk level: high
2. Go to the cron file directory and check whether illegal scheduled task scripts exist.
Description: Check `/etc/crontab` , `/etc/cron.d` , `/etc/cron.daily` , `cron.hourly/` , `cron.monthly` , and `cron.weekly/` for suspicious scripts and programs.
Solution: If you find an unknown scheduled task, you can locate its script to verify whether it is a normal service script. If not, directly comment out the task content or delete the script.
Risk level: high

IV. Check for third-party software vulnerabilities

1. If your server runs web or database application services, restrict the application accounts' write access to the file system and try to use non-root accounts for running them.
Description: Using a non-root account to run an application can guarantee that the attacker cannot remotely control the server immediately after the application is compromised, reducing the potential losses caused by the attack.
Solutions:
a. Go to the web service's root directory or database configuration directory;
b. Run the commands `chown -R apache:apache /var/www/xxxx` and `chmod -R 750 file1.txt` to configure the website access permissions.
Risk level: medium
Reference example
2. Upgrade applications to fix vulnerabilities
Description: If a server is intruded, the reason may be that the software applications used by the system are older with more unfixed vulnerabilities, which could be exploited.
Solution: For typical vulnerabilities such as ImageMagick, openssl, and glibc, you can directly upgrade the applications to fix them through apt-get/yum or other methods according to the security notices released by Tencent Cloud.
Risk level: high

Below is an example of file permission for a website directory:Scenarios:

The user and user group running on the HTTP server is "www", the website user is "centos", and the root directory of the website is `/home/centos/web` .

Steps:

1. Run the following command to set the owner of the website directory and files to "centos" and the owner group to "www":

```
chown -R centos:www /home/centos/web
```

2. Set the website directory permission to 750, which grants the user "centos" read/write access to the directory. The user "centos" can create files in any directory. The user group has read and execute permissions so that the users in it can access the directory. Other users have no permission at all.

```
find -type d -exec chmod 750 {} \\;
```

3. Set the website file permission to 640, which means that only the user "centos" has permission to change the website files. The HTTP server only has permission to read files but cannot modify files, and other users have no permission at all.

```
find -not -type d -exec chmod 640 {} \\;
```

4. Set the permission for certain directories requiring write permission to 770. For example, some cache directories of the website need to grant the HTTP service write permission, such as the `/data/` directory of Discuz x2.

```
find data -type d -exec chmod 770 {} \\;
```

Security Optimization Suggestions

It’s recommended to log in using SSH keys to reduce the risk of brute force attacks.

Change port 22 in the file `/etc/ssh/sshd_config` on the server to a non-default port. Then you need to restart the SSH service using the following command:

```
/etc/init.d/sshd restart (on CentOS) or /etc/init.d/ssh restart (on Debian or Ubunt
```

Note:

When you change the port, you need to edit the security group configuration of the server on the CVM Console to allow the corresponding port in its inbound rule. For more information, see Adding Security Group Rules.

If you do need to use an SSH password, choose a strong one.

For application management backends (website, middleware, Tomcat, etc.), remote SSH, remote desktop, and databases, always use complex and different passwords.

See below for examples of strong passwords (spaces are allowed):

`1qtwo-threeMiles3c45jia` `caser, lanqiu streets`

See below for the examples of weak passwords:

Company name + date (coca-cola2016xxxx)

Common phrases (Iamagoodboy)

Run the following command to check which ports on the server are opened to the Internet and close ports not used for your business.

```
netstat -antp
```

Use the **Tencent Cloud security group firewall** to allow only specified IPs to access the management features. Or, restrict the IPs by editing the files `/etc/hosts.deny` and `/etc/hosts.allow` .

Avoid running applications with the **root** privileges.

For example, for Apache, Redis, MySQL, and Nginx, do not run them with the root privileges.

Fix system privilege elevation vulnerabilities and **program vulnerabilities** running under the root privileges to prevent malware from gaining root privileges to embed backdoors.

Update the OS and applications used in a timely manner, such as Struts 2, Nginx, ImageMagick, and Java.

Disable remote management of applications such as Redis and NTP. If there is no need for remote management, you can disable the external listener ports or configuration.

Back up your CVM business data regularly.

Perform off-site or cloud backup of important business data to ensure that the data can be recovered after the CVM instances are compromised.

In addition to the "home" and "root" directories, also back up the "/etc" and "/var/log" directories.

Install Tencent Cloud's **CWPP Agent** so that you can keep track of risks after an attack.

Intrusions on Windows

Last updated：2023-12-26 16:40:09

This topic describes how to troubleshoot intrusions into servers running on Windows.

Identifying Causes of Intrusions

I. Check accounts for weak passwords

1. Check whether weak passwords exist in the server system and application accounts.
Description: Check the system admin account, website backend account, database account, and other application accounts (FTP, Tomcat, phpMyAdmin, etc.) for weak passwords.
Note:
Set a strong account password using 12-16 characters containing uppercase and lowercase letters, special characters, and digits. You can also use a password generator to generate strong passwords.
Solution: Please check as needed.
Risk level: high
2. Check whether there are any accounts on the server that are not created by the system and you.
Description: The names of suspicious accounts created by hackers are generally displayed in the local user group.
Solution: Open the Command Prompt window and enter the command `lusrmgr.msc` to check whether there are any new accounts. If new accounts are found in the Administrators group, disable or delete them immediately.
Risk level: high
3. Check for hidden account names.
Description: To evade inspection, hackers often create hidden accounts on your server that are not visible in the local user group.
Solution (you can also check for hidden accounts by downloading the LD_check security tool):
 a. Open the Run window (or press Win + R) on the desktop, and enter `regedit` to open the Registry Editor.
 b. Select HKEY_LOCAL_MACHINE/SAM/SAM. The content of this key is invisible by default. Right-click the key and select **Permissions**.
 c. Select the current user (usually administrator), check **Full Control** for the permissions, click "OK", and close the Registry Editor.
 d. Open the Registry Editor again and select HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users.
 e. You can see all the user names of the instance under Names. Any account that is not in the list of local accounts can be considered a hidden account. You can delete the user if you confirm it is a non-system user.
Risk level: high

II. Check for malicious processes and ports

1. Check whether there are malicious processes running in the system background.

Description: After intruding into the system, attackers often run malicious processes to communicate with the external network. By analyzing the processes that connect to the external network, you can identify the processes that have intruded into the system.

Solution:

a. Log in to the server and select **Start** > **Run**.

b. Enter "cmd", and then "netstat –nao" to check whether the server is being listened to by an unauthorized port.

c. Open the Task Manager and check whether the process corresponding to the PID is a normal process. If not, check the path to the running file via the PID and delete the file. You can also use the Process Explorer provided by Microsoft for troubleshooting.

Risk level: high

III. Check for malicious programs and startup items

1. Check whether unusual startup items exist on the server.

Description: After intruding into the system, attackers often put malicious programs in startup items so that they can run upon the system's startup.

Solution:

a. Log in to the server and select **Start** > **All Programs** > **Startup**.

b. By default, this directory is empty. Check whether there are non-business programs in it.

c. Select **Start** >**Run**, and enter "msconfig" to check whether startup items with an abnormal name exist. If so, uncheck them and go to the paths displayed in the commands to delete the files.

d. Select **Start** >**Run**, and enter "regedit" to open the Registry Editor. Check whether the startup items are normal. Especially, check the following three registry entries:

HKEY_CURRENT_USER\\software\\micorsoft\\windows\\currentversion\\run
HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Runonce

Check whether unusual startup items exist on the right of the Registry Editor. If so, delete them. It is recommended to install an anti-virus program for detecting and killing residual viruses and trojans.

Risk level: high

2. Check the connected sessions.

Description: Check ongoing sessions between the server and other servers on the network or scheduled tasks.

Solution: a. Log in to the server and select **Start** > **Run**.

b. Enter "cmd", and then "netstat -ano" to check the session between the server and other servers on the network, and verify whether the connection is normal. Enter "schtasks", check the scheduled tasks on the server, and verify whether it is a normal scheduled task.

Risk level: medium

IV. Check for third-party software vulnerabilities

If your server runs service applications (WWW, FTP, etc.), configure them to **restrict their permissions and prohibit directory browsing or write access to files**.

FAQs

How to restore a compromised website or system

After a system is intruded, the system files are often modified and replaced. At this point, the system has become untrusted. The best choice is to reinstall the system and install all patches to the new system.

How to prevent the website or system from being intruded again

1. Change the passwords of all system accounts to **complex passwords** (at least different from those before the intrusion).
2. **Change the default remote desktop port** by following the steps below:
2.1 Select **Start** > **Run**, and enter "regedit".
2.2 Open the Registry Editor, and go to the following path:
HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\Wds\\rdpwd\\Tds\\tcp
2.3 KEY_LOCAL_MACHINE\\SYSTEM\\CurrentContro1Set\\Control\\Tenninal Server\\WinStations\\RDP-Tcp
2.4 Modify the PortNumber value on the right.
3. Configure the security group firewall to allow only **the specified IPs to access the remote desktop port**.
4. **Back up important business data and files** regularly.
5. **Update the OS and application components (FTP, Struts 2, etc.) regularly** to prevent vulnerability exploitation.
6. Install **CWPP Agent** and an anti-virus program for regular checkups and scans.

Offline Agent on Linux

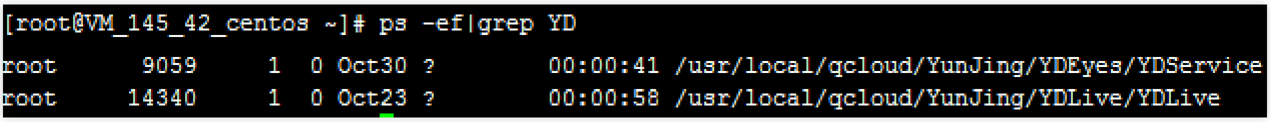
Last updated：2023-12-26 16:40:17

This topic describes how to troubleshoot the CWPP agent running on Linux, including how to troubleshoot the failed startup of CWPP agent processes and network failures.

Failed Startup of CWPP Agent Processes

1. Enter the command `ps -ef|grep YD` to check whether the CWPP processes exist.

Normally, CWPP has two processes as shown below:



```
[root@VM_145_42_centos ~]# ps -ef|grep YD
root      9059     1  0 Oct30 ?        00:00:41 /usr/local/qcloud/YunJing/YDEyes/YDService
root     14340     1  0 Oct23 ?        00:00:58 /usr/local/qcloud/YunJing/YDLive/YDLive
```

If the processes do not exist, possible reasons include the following:

The CWPP agent is not installed on the server or has been uninstalled from the server. Please install it by following the steps described in Getting Started

The agent has a conflict or crash, which leads to the failed startup of processes.

2. If CWPP agent has been installed on the server, troubleshoot the problem using the following method:

View the agent log stored in `/usr/local/qcloud/YunJing/log` .

Run the command `sh /usr/local/qcloud/YunJing/startYD.sh` to start CWPP.

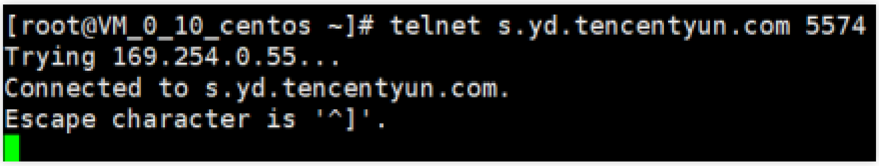
Network Failures

If the processes exist, but CWPP is offline, the issue is caused by network disconnection in most cases. Troubleshoot the issue by following the steps below:

1. If you are unable to access the CWPP security domain, try changing the DNS. Run the following command line to check whether the CWPP security domain is accessible:

VPC or CPM environment: telnet s.yd.tencentyun.com 5574.

Normally, the returned result is as shown below:

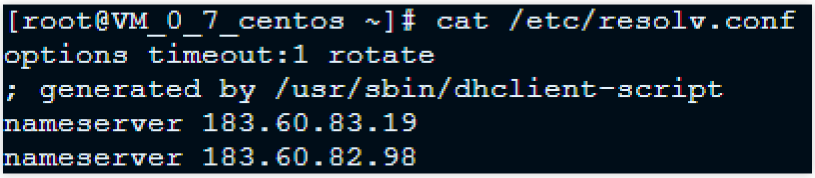


```
[root@VM_0_10_centos ~]# telnet s.yd.tencentyun.com 5574
Trying 169.254.0.55...
Connected to s.yd.tencentyun.com.
Escape character is '^]'.
```

If it is inaccessible：

a. Change the field `dns nameserver`： `vim /etc/resolv.confnameserver 183.60.83.19nameserver 183.60.82.98`

b. Then run `telnet s.yd.tencentyun.com 5574` again to check whether you can connect to it.

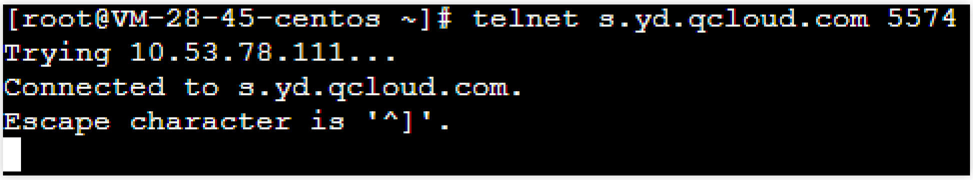


```
[root@VM_0_7_centos ~]# cat /etc/resolv.conf
options timeout:1 rotate
; generated by /usr/sbin/dhclient-script
nameserver 183.60.83.19
nameserver 183.60.82.98
```

c. If it can be connected, wait for a few minutes (the time length depends on the network conditions), and then you will see that the server is online again.

Basic network environment (non-VPC servers): `telnet s.yd.qcloud.com 5574` .

Normally, the returned result is as shown below:



```
[root@VM-28-45-centos ~]# telnet s.yd.qcloud.com 5574
Trying 10.53.78.111...
Connected to s.yd.qcloud.com.
Escape character is '^]'.
```

If it is inaccessible：

a. Change the field `dns nameserver`： `vim /etc/resolv.conf` . Comment the original field `nameserver` first, and then add a new `nameserver` field.

b. Then run `telnet s.yd.qcloud.com 5574` again to check whether you can connect to it.

c. If it can be connected, wait for a few minutes (the time length depends on the network conditions), and then you will see that the server is online again.

2. Make sure your firewall policies allow the TCP ports 5574, 8080, 80, and 9080.

3. If the CWPP processes exist and the offline state of the CWPP agent is not caused by network issues, package the agent logs (log path: `/usr/local/qcloud/YunJing/log`) and submit a ticket for feedback.

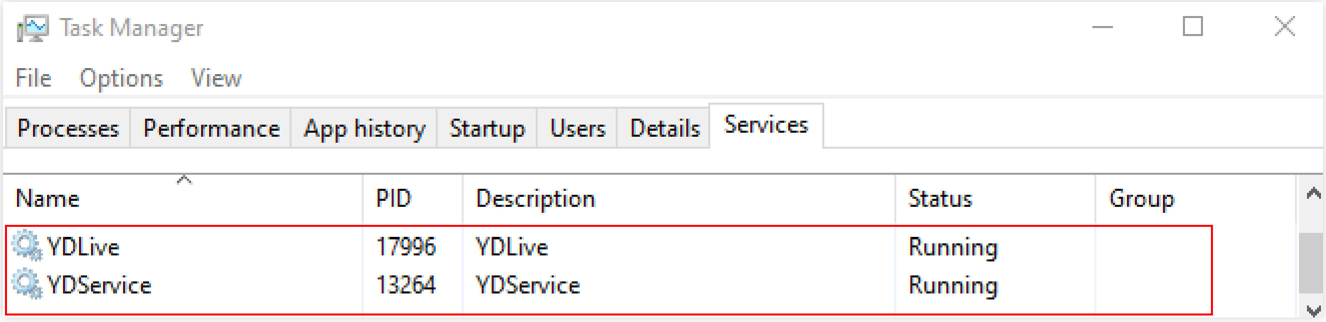
Offline Agent on Windows

Last updated：2023-12-26 16:40:30

Failed Startup of CWPP Agent Processes

1. Check whether the CWPP process exists.

Open Windows Task Manager and check whether the `YDService.exe` process exists.



Name	PID	Description	Status	Group
YDLive	17996	YDLive	Running	
YDService	13264	YDService	Running	

2. If the process does not exist, possible reasons include the following:

The CWPP agent is not installed on the server or has been uninstalled from the server. Please install it by following the steps described in Getting Started

The agent has a conflict or crash, which leads to the failed startup of processes.

3. Troubleshooting methods:

View the agent log stored in `C:\\Program Files\\QCloud\\YunJing\\log` .

Run the command `sc start ydservice` to manually start the agent.

Network Failures

If the process exists, but CWPP is offline, the issue is caused by network disconnection in most cases. Troubleshoot the issue by following the steps below:

1. Check whether the DNS has been modified by running the following commands. If a normal result is returned, the DNS is correct:

Download address for the basic network (non-VPC servers): `telnet s.yd.qcloud.com 5574` .

Download address for VPC and CPM: `telnet s.yd.tencentyun.com 5574` .

2. Make sure the ports 5574, 8080, 80, and 9080 are open in the firewall rules.

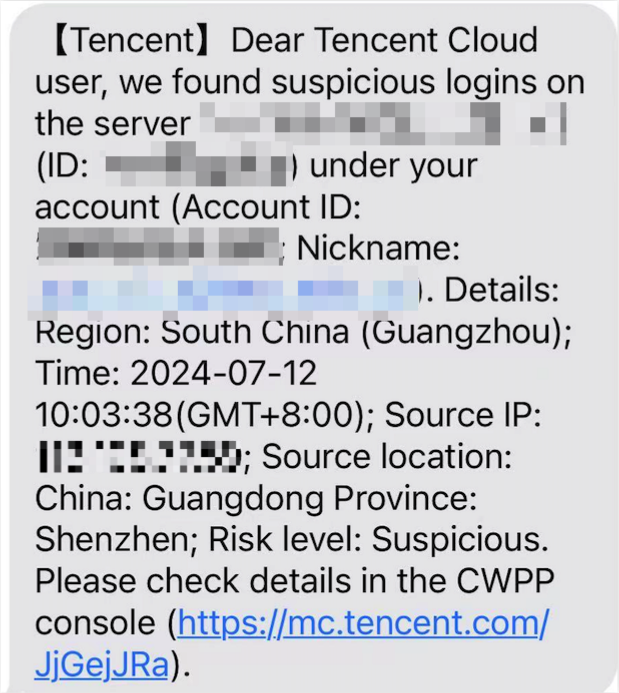
3. If the CWPP process exists and the offline state of the CWPP agent is not caused by network issues, package the agent logs (log path: `C:\\Program Files\\QCloud\\YunJing\\log`) and submit a ticket for feedback.

An Abnormal Log-in Notification

Last updated：2024-08-13 16:34:25

Phenomenon Description

The user receives a notification from Tencent Cloud about an abnormal log-in to the server. Take the SMS below as an example:



【Tencent】Dear Tencent Cloud user, we found suspicious logins on the server [redacted] (ID: [redacted]) under your account (Account ID: [redacted]; Nickname: [redacted]). Details: Region: South China (Guangzhou); Time: 2024-07-12 10:03:38(GMT+8:00); Source IP: [redacted]; Source location: China: Guangdong Province: Shenzhen; Risk level: Suspicious. Please check details in the CWPP console (https://mc.tencent.com/JjGejJRa).

Possible Causes

When log-in activities occur on the servers under your Tencent Cloud account, if Tencent Cloud CWPP founds that the log-in does not match any entries in the log-in allowlist, it will use intelligent algorithms to mark the log-in record as "Suspicious" or "High-risk” and trigger real-time alarms.

Note

By default, you can enable triggering alarms by going to Settings > and tick **Alarm Settings** only for those abnormal log-in events with a hazard level of "High-risk".

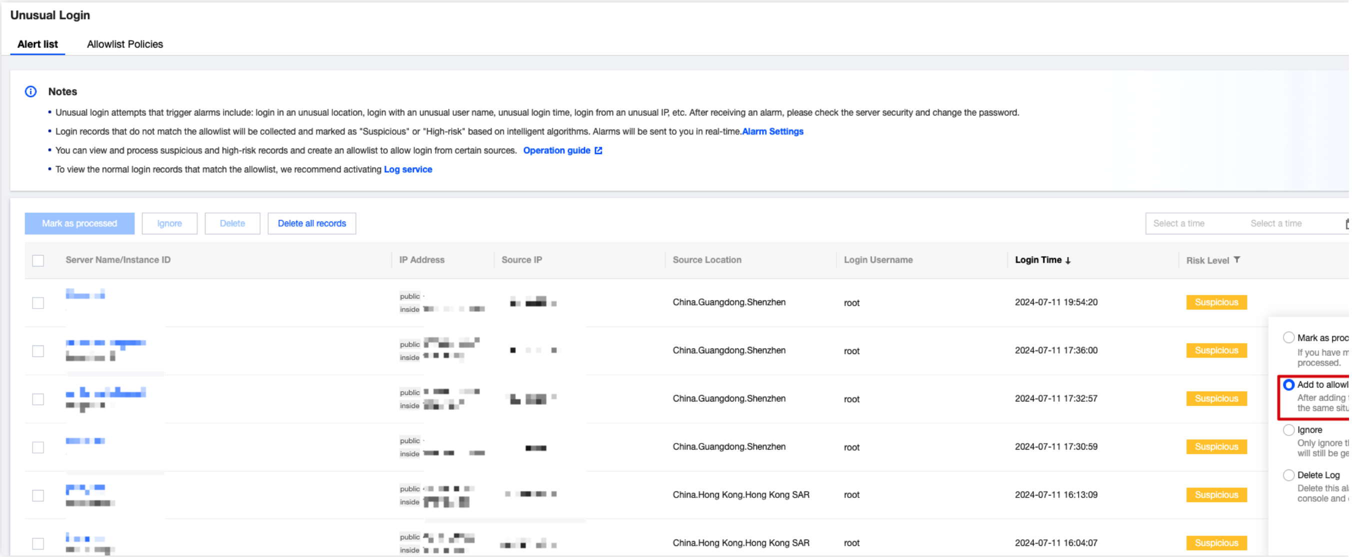
The hazard level of an abnormal log-in is determined by an algorithm that comprehensively evaluates previous log-in patterns on the server.

Directions

After receiving an abnormal log-in alarm, please follow these steps for confirmation:

1. Verify if this log-in behavior is authorized.

If yes, add this log-in record to the allowlist. If this behavior occurs again, no alarms will be generated.



Unusual Login

Alert list | Allowlist Policies

Notes

- Unusual login attempts that trigger alarms include: login in an unusual location, login with an unusual user name, unusual login time, login from an unusual IP, etc. After receiving an alarm, please check the server security and change the password.
- Login records that do not match the allowlist will be collected and marked as "Suspicious" or "High-risk" based on intelligent algorithms. Alarms will be sent to you in real-time.Alarm Settings
- You can view and process suspicious and high-risk records and create an allowlist to allow login from certain sources. Operation guide
- To view the normal login records that match the allowlist, we recommend activating Log service

□	Server Name/Instance ID	IP Address	Source IP	Source Location	Login Username	Login Time ↓	Risk Level
□	[redacted]	public [redacted] inside [redacted]	[redacted]	China.Guangdong.Shenzhen	root	2024-07-11 19:54:20	Suspicious
□	[redacted]	public [redacted] inside [redacted]	[redacted]	China.Guangdong.Shenzhen	root	2024-07-11 17:36:00	Suspicious
□	[redacted]	public [redacted] inside [redacted]	[redacted]	China.Guangdong.Shenzhen	root	2024-07-11 17:32:57	Suspicious
□	[redacted]	public [redacted] inside [redacted]	[redacted]	China.Guangdong.Shenzhen	root	2024-07-11 17:30:59	Suspicious
□	[redacted]	public [redacted] inside [redacted]	[redacted]	China.Hong Kong.Hong Kong SAR	root	2024-07-11 16:13:09	Suspicious
□	[redacted]	public [redacted] inside [redacted]	[redacted]	China.Hong Kong.Hong Kong SAR	root	2024-07-11 16:04:07	Suspicious

○ Mark as proc
If you have m
processed.

● Add to allowl
After adding
the same situ

○ Ignore
Only ignore t
will still be ge

○ Delete Log
Delete this al
console and

If not, go to step 2.

2. If you have determined that the log-in is unauthorized, it is preliminarily concluded that the alarm for an abnormal log-in event on your server is due to a less frequently used user account being compromised. It is recommended that you immediately change the log-in password and update any related authentication credentials stored on the server. You can see Linux Intrusion Issue Troubleshooting Approach and Windows Intrusion Issue Troubleshooting Approach for routine investigations on your server.

Reinforcement Methods

Subsequently, you can enhance server security through the following reinforcement methods:

Set a complex password for the server which consists of a combination of uppercase letters, lowercase letters, special characters, and numbers, with a length of 12 to 16 characters.

Change the default remote log-in port for the Linux-based CVM as shown below:

Modify file /etc/ssh/sshd_config.

```
Port 22 # is located in the third or fourth line. If there is a hash tag in front o
```

You can use the vi command in a remote connection or download the file to your local machine via sftp and modify it there. After modifying the file, use the following command to restart the SSH service:

```
/etc/init.d/sshd restart #centos system, which is used to restart the sshd service
etc/init.d/ssh restart #debian/ubuntu system, which is used to restart the ssh serv
```

Tencent Cloud Platform provides a Security Group feature. We suggest you only use it to only allow the necessary protocols and ports required for your business operations, and not to open all protocols and all ports. For details, refer to Creating Security Groups.

To configure the system firewall for your CVM, it is recommended to enable CFW and set Internet boundary rules.

Ensure that the protection software installed on the CVM CWPP agent process is running normally and that the real-time alarm is enabled. This will promptly notify you in case of any abnormal log-in.

Promptly fix any security vulnerabilities in the CVM system components and Web components.

Note

While implementing the aforementioned CVM system security measures effectively reduces security risks, it cannot guarantee absolute security. Therefore, it is recommended to regularly conduct security inspections and data backups for CVM system to prevent data loss or service unavailability due to unexpected incidents.

In addition to security reinforcement, it is also strongly recommended to back up your data by creating system images, creating data snapshots, and setting up automatic periodic snapshots to ensure data safety.

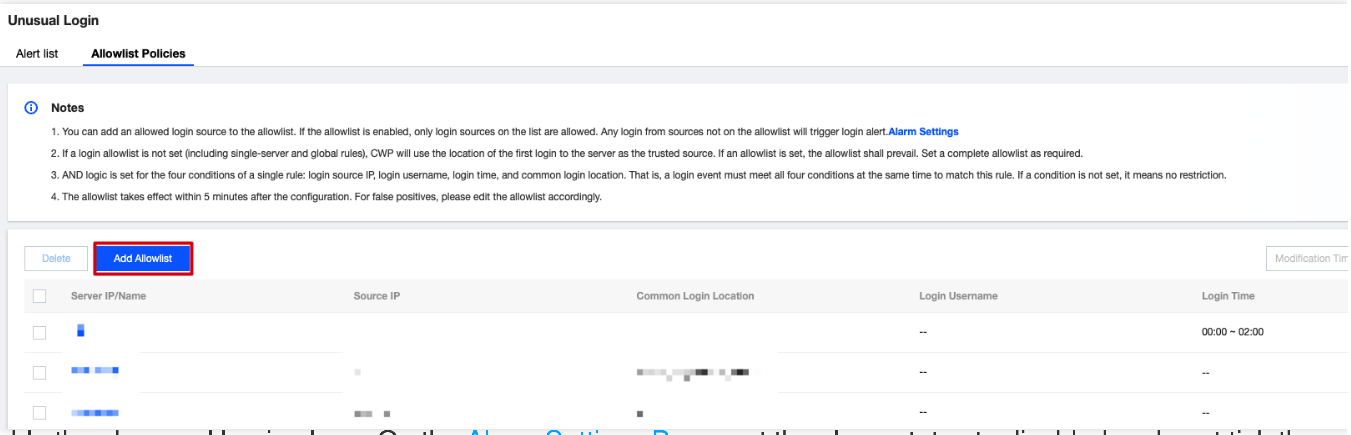
FAQs

Can abnormal log-in detection be disabled?

Abnormal log-in detection cannot be disabled.

If you do not want to receive alarm notifications for abnormal log-in, you can try to complete the log-in allowlist or disable the abnormal log-in alarm.

To complete the log-in allowlist: On the Unusual Login Page, select **Allowlist Management** > **Add to Allowlist** and add commonly used log-in source IPs to the allowlist.

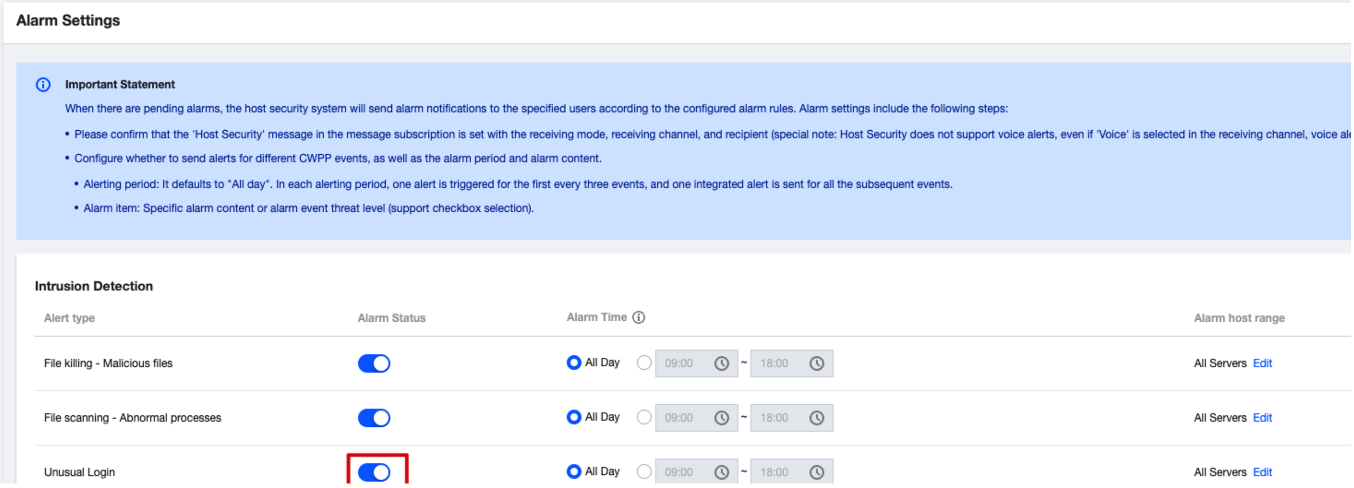


Notes

1. You can add an allowed login source to the allowlist. If the allowlist is enabled, only login sources on the list are allowed. Any login from sources not on the allowlist will trigger login alert.**Alarm Settings**
2. If a login allowlist is not set (including single-server and global rules), CWP will use the location of the first login to the server as the trusted source. If an allowlist is set, the allowlist shall prevail. Set a complete allowlist as required.
3. AND logic is set for the four conditions of a single rule: login source IP, login username, login time, and common login location. That is, a login event must meet all four conditions at the same time to match this rule. If a condition is not set, it means no restriction.
4. The allowlist takes effect within 5 minutes after the configuration. For false positives, please edit the allowlist accordingly.

□	Server IP/Name	Source IP	Common Login Location	Login Username	Login Time
□	[redacted]			--	00:00 ~ 02:00
□	[redacted]	[redacted]	[redacted]	--	--
□	[redacted]	[redacted]	[redacted]	--	--

To disable the abnormal log-in alarm: On the Alarm Settings Page, set the alarm status to disabled or do not tick the alarm item High-risk or Suspicious.



Alarm Settings

Important Statement

When there are pending alarms, the host security system will send alarm notifications to the specified users according to the configured alarm rules. Alarm settings include the following steps:

- Please confirm that the 'Host Security' message in the message subscription is set with the receiving mode, receiving channel, and recipient (special note: Host Security does not support voice alerts, even if 'Voice' is selected in the receiving channel, voice al
- Configure whether to send alerts for different CWPP events, as well as the alarm period and alarm content.
  - Alerting period: It defaults to "All day". In each alerting period, one alert is triggered for the first every three events, and one integrated alert is sent for all the subsequent events.
  - Alarm item: Specific alarm content or alarm event threat level (support checkbox selection).

Intrusion Detection

Alert type	Alarm Status	Alarm Time	Alarm host range
File killing - Malicious files	●	● All Day ○ 09:00 ~ 18:00	All Servers Edit
File scanning - Abnormal processes	●	● All Day ○ 09:00 ~ 18:00	All Servers Edit
Unusual Login	●	● All Day ○ 09:00 ~ 18:00	All Servers Edit