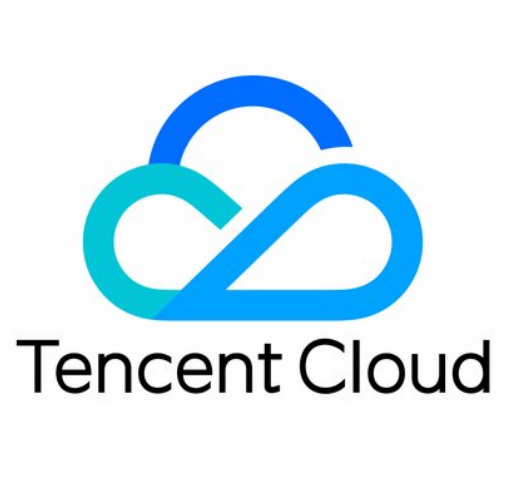
Cloud Workload Protection

Troubleshooting

Product Documentation



Contents

Troubleshooting Intrusions on Linux

Last updated：2020-02-27 19:30:33

Finding Causes of Intrusions

1. Check for hidden accounts and weak passwords

1. Check whether there are **weak passwords** 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 `last` command to view the record of accounts that 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 `usermod -L username` command to disable the user or run the `userdel -r username` command to delete the user.
   - Risk level: high
3. Run the `less /var/log/secure|grep 'Accepted'` command 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: when you find a suspicious user, run the `usermod -L username` command to disable the user or the `userdel -r username` command 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 intruded by automated tools.
   - Solutions:
     a. Change port 22 in the `/etc/ssh/sshd_config` file on the server to a non-default port. You need to restart the SSH service after modification.
     b. 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 configuration take effect.

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

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

- Risk level: high

5. Check the `/etc/passwd` file to see whether there were unauthorized account logins.
   - 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 `usermod -L username` command to disable the user or the `userdel -r username` command to delete the user.
   - Risk level: medium

2. 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 corresponding PID) to check the path to the process file corresponding to the PID.

     b. If it is a malicious process, delete the corresponding file.
   - Risk level: high
2. Run the `ps -ef` and `top` commands to check whether there are exceptional processes.
   - Description: run the commands above. If you find an unauthorized processes 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 `kill -9 process name` command to end the process or use a firewall to prevent network connection by the process.
   - Risk level: high

3. Check malicious programs and suspicious startup items

1. Run the `chkconfig --list` and `cat /etc/rc.local` commands to check whether there are suspicious startup services 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 `chkconfig service name off` command to close it. Plus, check whether there are suspicious items in `/etc/rc.local`, and if yes, comment them out.
   - Risk level: high

2. Go to the cron file directory and check whether there are illegal scheduled task scripts.
   - 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 a scheduled task that you do not know, you can locate its script to confirm whether it is a normal service script, and if not, directly comment out the task content or delete the script.
   - Risk level: high

4. Check for third-party software vulnerabilities

1. If your server runs web or database application services, limit 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 attacks.
   - Solutions:
     a. Enter the web service's root directory or database configuration directory;
     b. Run the `chown -R apache:apache /var/www/xxxx` and `chmod -R 750 file1.txt` commands to configure website access permissions.
   - Risk level: medium
   - Reference example
2. Upgrade applications to repair 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 repair them through apt-get/yum or other methods according to the security notices released by Tencent Cloud.
   - Risk level: high

Below is a reference example of file permission of a website directory:

Scenario:

Assume that the HTTP server runs user and user group “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 permission 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 permissions at all.

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

3. Set the website file permission to 640. 640 means that only the centos user 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 permissions 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

1. It’s recommended to log in using SSH keys to reduce the risk of brute force attacks.
2. Change port 22 in the `/etc/ssh/sshd_config` file on the server to a non-default port. You need to restart the SSH service after modification by running the following command:

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

3. If you do need to use password login, choose a strong password.
   - For application management backends (website, middleware, Tomcat, etc.), remote SSH, remote desktop, and databases, always use complex and different passwords.
   - See below for the 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)
4. 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 -anltp
```

5. Use the **Tencent Cloud security group firewall** to allow only specified IPs to access the management features. Or, limit the IPs by editing the `/etc/hosts.deny` and `/etc/hosts.allow` files.
6. Prevent running applications with the **root** privileges.
   For example, for Apache, Redis, MySQL, and Nginx, do not run them with the root privileges.
7. Repair 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, 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.
8. Regularly **back up** your CVM business data.
   - 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, you should also back up the “/etc” and “/var/log” directories.
9. Install the **CWP Agent** so that you can understand the risk situation after an attack.

Intrusions on Windows

Last updated : 2020-04-20 12:20:26

Finding Causes of Intrusions

1. Check accounts and weak passwords

1. Check whether there are weak passwords in the existing server system and application accounts:
   - Description: check system admin account, website backend account, database account, and other application accounts (FTP, Tomcat, phpMyAdmin, etc.) for weak passwords.
   - Inspection method: do so based on the actual situation.
   - Risk level: high
2. Check whether there are any accounts on the server that are not created by the system and you.
   - Description: names of suspicious accounts created by hackers are generally displayed in the local user group.
   - Solution: open the Command Prompt window and enter the `lusrmgr.msc` command to see whether there are any new accounts. If there are new accounts in the Administrators group, disable or delete them immediately.
   - Risk level: high
3. Check whether there are hidden account names.
   - Description: hackers often create hidden users on your server to evade inspection. Hidden accounts are not visible in the local user group.
   - Solution: (you can also check whether there are 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 to select HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users.
     e. Under the Names entry, you can see all the usernames on the instance. If there is an account that is not in the local account group, it is a hidden account. After confirming that it is not a system user, delete it.
   - Risk level: high

2. Check malicious processes and ports

1. Check whether there are malicious processes running in the system background.
   - Description: after intruding the system, attackers often run malicious processes to communicate with external services. By analyzing the outbound processes, the intrusion control processes can be identified.
   - Solution:
     a. Log in to the server and select **Start** > **Run**.
     b. Enter `cmd` and enter `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, and if not, use the PID to view the path to the running file and delete it. You can also use the official Process Explorer tool provided by Microsoft for troubleshooting.
   - Risk level: high

3. Check malicious programs and startup items

1. Check whether there are abnormal startup items on the server.
   - Description: after intruding the system, attackers often put malicious programs in startup items so that they can run at system 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 see whether there are startup items with abnormal names, and if yes, 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 there are any abnormal startup items on the right, and if yes, delete them. It is recommended to install an anti-virus program for detecting and killing residual viruses and trojans.
   - Risk level: high

2. View the connected sessions.

- Description: check ongoing sessions between your computer and other computers on the network or scheduled tasks.
- Solution:
  a. Log in to the server and select **Start** > **Run**.
  b. Enter `cmd` and then enter `netstat -ano` to check ongoing sessions between your computer and other computers on the network and confirm whether they are normal. Enter `schtasks` to check scheduled tasks on your computer and confirm whether they are normal.
- Risk level: medium

4. Check third-party software vulnerabilities

1. If your server runs service applications (WWW, FTP, etc.), configure them to **restrict their permissions and prohibit directory browsing or file write**.
2. **Activate Web Application Firewall (WAF)** to view the WAF attack logs.

How to Restore a Website or System

1. **After the system is intruded, the system files are often modified and replaced. At this point, the system has become untrusted, and the best choice is to reinstall the system and install all patches to the new system.**
2. Change the passwords of all system accounts to **complex passwords** (at least different from those before the intrusion).
3. **Change the default remote desktop port** in the following steps:
   i. Select **Start** > **Run** and enter `regedit` .
   ii. Open the Registry Editor and go to the following path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
   iii. KEY_LOCAL_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp
   iv. Modify the `PortNumber` value on the right.
4. Configure the security group firewall to allow only **the specified IPs to access the remote desktop port**.
5. **Back up important business data and files** on a regular basis.
6. **Update the OS and application components (FTP, Struts 2, etc.) on a regular basis** to prevent vulnerability exploitation.
7. Install **CWP Agent** and an anti-virus program for regular checkups and scans.

Offline Agent on Linux

Last updated : 2020-02-27 19:34:02

Agent Processes Are not Started

1. Run the following command to check whether the CWP processes exist: `ps -ef|grep YD` .
2. In normal state, CWP has two processes as shown below:

```
[root@VM_145_42_centos ~]# ps -ef|grep YD
root      2890  2857  0 11:05 pts/0    00:00:00 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
```

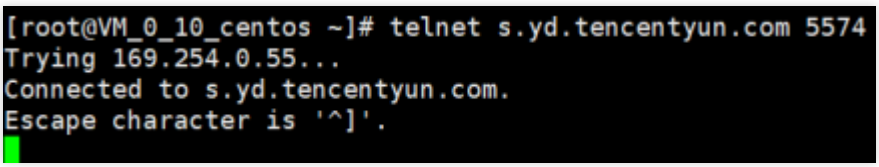
3. If the processes do not exist, possible reasons include the following:
   - The CWP agent is not installed on or has been uninstalled from the server. Please see Getting Started and follow the instructions to install the agent.
   - The agent has a conflict or crash and thus cannot be started.
4. Troubleshooting methods:
   - View the agent log stored in `/usr/local/qcloud/YunJing/log` .
   - Run the following command to manually start the agent: `/usr/local/qcloud/YunJing/YDEyes/YDService` .

Network Failures

If the processes exist, but CWP is offline, the issue is caused by network disconnection in most cases. Troubleshoot the network issue as shown below:

1. Run the following command to check whether the DNS has been modified:
   - Basic network environment (non-VPC servers): telnet s.yd.qcloud.com 5574.
   - VPC or CPM environment: telnet s.yd.tencentyun.com 5574.

In normal state, the returned result is as shown below:



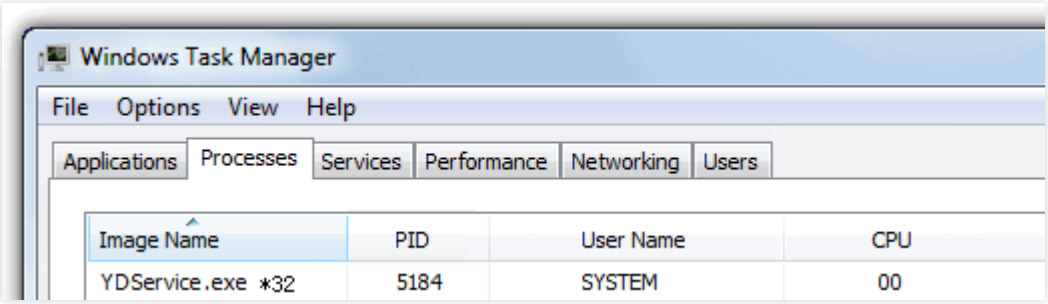
2. Make sure your firewall policies allows the following TCP ports: 5574, 8080, 80, and 9080.

Offline Agent on Windows

Last updated：2020-03-02 19:26:09

Agent Process Not Started

1. Check whether the CWP process exist.
   Open Windows Task Manager and check whether the `YDService.exe` process exists.



2. If the agent process do not exist, possible reasons include the following:
   - The CWP agent is not installed on or has been uninstalled from the server. Please see Getting Started and follow the instructions to install the agent.
   - The agent has a conflict or crash and thus cannot be started.
3. Troubleshooting methods:
   - View the agent log stored in `C:¥Program Files¥QCloud¥YunJing¥log` .
   - Run the following command to manually start the agent: `sc start ydservice` .

Network Failures

If the process exists, but CWP is offline, the issue is caused by network disconnection in most cases. Please check the following:

1. Check whether the DNS has been modified. If any of the following commands returns a normal result, 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 following ports are open: 5574, 8080, 80, and 9080.