

SecurityInfo

Best Practices

Issue 03
Date 2025-07-18



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property 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 Cloud 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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1

Best Practices for Using Huawei Accounts.....

1

2

Best Practices in Enabling High-Risk Ports.....

7

3

Disposal of Spam Mails Sent to External Systems.....

13

3.1

What Is Spam Email and How It Is Harmful.....

13

3.2

How Huawei Cloud Handles Resources That Send Spam Email.....

14

4

UDP-based Amplification Attack Check.....

15

4.1

Overview.....

15

4.2

Detecting UDP-based Amplification Attacks.....

16

4.3

Solution and Prevention Measures.....

17

5

Host Security Checks.....

18

5.1

Hosts Security Issues.....

18

5.1.1

Overview.....

18

5.1.2

External Attacks: Port Scan.....

18

5.1.3

Mining.....

20

5.1.4

Ransomware.....

21

5.2

Host Security Check (Windows).....

22

5.2.1

Troubleshooting Methods.....

22

5.2.2

Troubleshooting Process.....

22

5.2.2.1

Method 1: Using Tools to Detect Security Issues.....

22

5.2.2.1.1

Step 1: Analyzing All Processes.....

22

5.2.2.1.2

Step 2: Detecting Automatic Startup Programs.....

25

5.2.2.1.3

Step 3: Analyzing the Network.....

28

5.2.2.1.4

Step 4: Detecting Abnormal Users.....

29

5.2.2.2

Method 2: Using DOS System Commands to Check Processes.....

32

5.2.2.3

Security Hardening Suggestions for Windows Hosts.....

36

5.3

Host Security Check (Linux).....

37

5.3.1

Troubleshooting Methods.....

37

5.3.2

Troubleshooting Process.....

37

5.3.3

Security Hardening Suggestions for Linux Hosts.....

40

1 Best Practices for Using Huawei Accounts

To safeguard your Huawei Cloud accounts and help you set up a secure channel to access Huawei Cloud resources, we recommend the following settings on IAM.

Enabling Login Protection

After login protection is enabled, you and users created using your account will be authenticated by a virtual MFA device, SMS, or email during console login. This improves account security and prevents phishing attacks or accidental password leakage.

Step 1 Enable login protection for the account. [Table 1-1](#) shows an example.

Table 1-1 User roles

User Roles	Procedure
Huawei Cloud Account	Access the Security Settings page . Select Critical Operations > Login Protection , click Enable . In the displayed pane, select Enable .

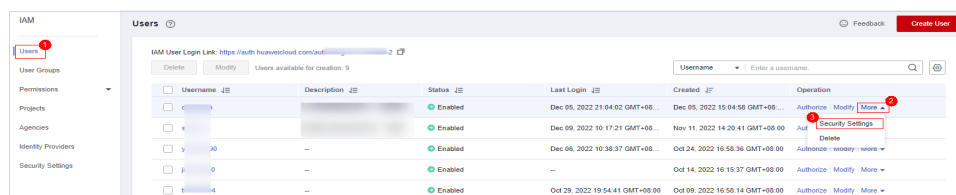
NOTE

- Your Huawei Cloud account is created after you successfully register with Huawei Cloud. Your account has full access permissions for your cloud resources and makes payments for the use of these resources.
- Your HUAWEI ID is a unified identity that you can use to access all Huawei services.

Step 2 Enable login protection for each IAM user under your Huawei Cloud account.

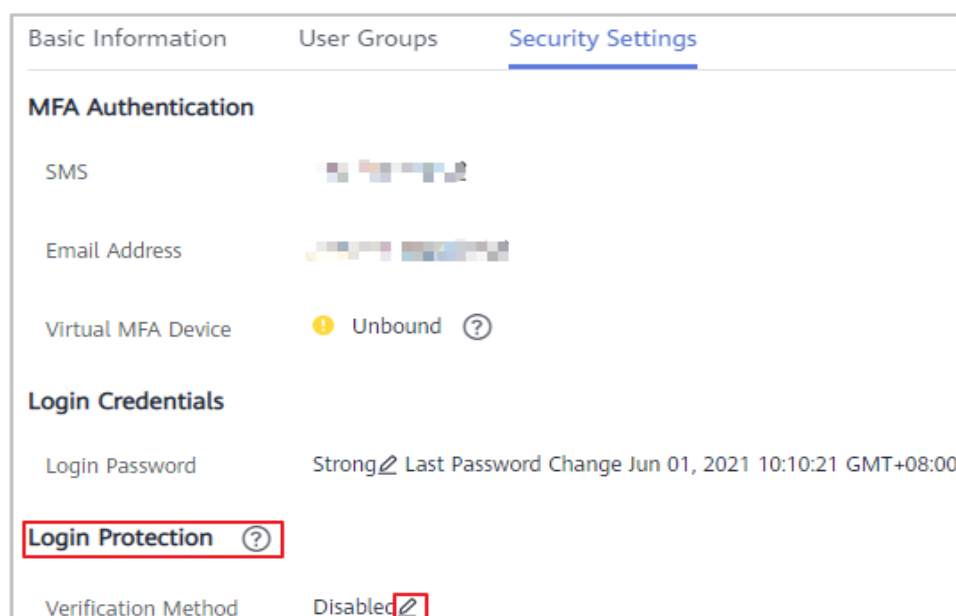
1. Choose **Identity and Access Management > Users** and click **Security Settings** in the row where an IAM user resides.

Figure 1-1 Users



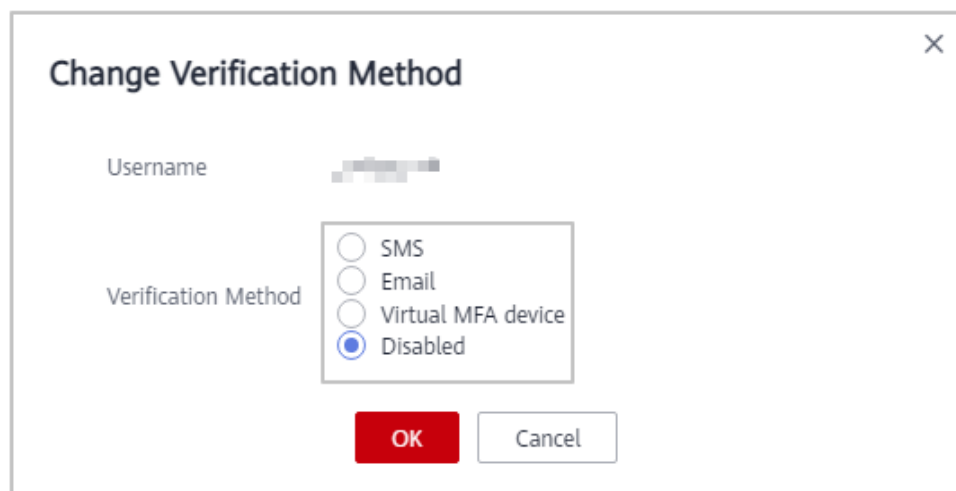
- Click  in the **Login Protection** area.

Figure 1-2 Security Settings



- In the displayed **Change Verification Method** dialog box, select **SMS**, **Email**, or **Virtual MFA device** for **Verification Method**, and click **OK**.

Figure 1-3 Change Verification Method



----End

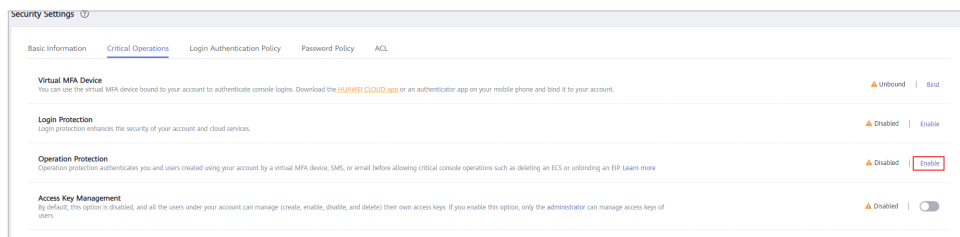
Enabling Critical Operation Protection

After critical operation protection is enabled, if you or users created using your account perform a **critical operation**, such as deleting a resource and generating an access key, a password and a verification code are required for additional authentication. This prevents risks and loss caused by misoperations.

Step 1 Access the **Security Settings** page as an administrator.

Step 2 Select **Critical Operations**, locate the **Operation Protection** row, and click **Enable**.

Figure 1-4 Critical Operations



Step 3 On the displayed pane, select **Enable** for **Operation Protection**. Then, select **Self-verification** or **Verification by another person**.

- **Self-verification:** You or IAM users themselves perform verification when performing a critical operation.
- **Verification by another person:** The specified person completes verification when you or IAM users perform a critical operation. Only SMS and email verification is supported.

Figure 1-5 Operation Protection

Operation Protection

Operation protection provides an additional layer of security for cloud resources.
You and users created using your account will be authenticated by a virtual MFA device, SMS, or email before being allowed to perform a critical operation.

Operation Protection ☒ **Enable**

You and users created using your account will need to perform identity verification by using the method you specify here.

☐ Self-verification
☒ **Verification by another person**
Specify a mobile number for identity verification.

+86 (Chinese... Enter a mobile number.

6-digit code Send Code

[Email Address Verification](#)

☐ **Disable**
Identity verification will not be required for performing a critical operation.

Cancel OK

Step 4 Click **OK**.

-----End

Configuring a Login Authentication Policy

A login authentication policy includes many aspects of account security, including session timeout, account lockout, recent login information, and custom login

prompt. You can configure a login authentication policy to better safeguard your account, preventing password leakage caused by forgetting to log out or phishing attacks.

Step 1 Access the [Security Settings page](#) as an administrator.

Step 2 Select **Login Authentication Policy** and configure required parameters as shown in the following figure.

Figure 1-6 Login Authentication Policy

The screenshot shows the 'Security Settings' page with the 'Login Authentication Policy' tab selected. The page includes sections for Session Timeout, Account Lockout, Account Disabling, Recent Login Information, and Custom Information. The 'Session Timeout' section shows a value of 1 hour. The 'Account Lockout' section shows a value of 15 minutes. The 'Account Disabling' section has a checkbox for 'Disable account upon login if it is not used within the validity period'. The 'Recent Login Information' section has a checkbox for 'Display last login information upon successful login'. The 'Custom Information' section has a text area with the value 'welcome'.

Security Settings ?

Basic Information Critical Operations **Login Authentication Policy** Password Policy ACL

Session Timeout

Log out if no operations are performed within 1 hours .

Account Lockout Takes effect for both you and IAM users created using your account

Lock the account for 15 minutes if 5 login attempts fail within 15 minutes.

Account Disabling Takes effect only for IAM users created using your account

☐ Disable account upon login if it is not used within the validity period

Recent Login Information

☒ Display last login information upon successful login

Custom Information

Display custom information upon login.

welcome

7/60

Save

NOTE

You can provide your custom information which will be displayed when you log in.

----End

Configuring Password Policies

You can specify minimum password length, restrict consecutive identical character, and disallow previously used passwords to ensure that strong passwords of high complexity are used.

- Step 1** Access the **Security Settings** page as an administrator.
- Step 2** Select **Password Policy** and configure required parameters as shown in the following figure.

Figure 1-7 Password Policy

The screenshot shows the 'Security Settings' page with the 'Password Policy' tab selected. The page is divided into three main sections: 'Password Composition & Reuse', 'Password Expiration', and 'Minimum Password Age'. In the 'Password Composition & Reuse' section, the 'Must contain at least' field is set to 3, the 'Minimum Number of Characters' is 8, and the 'Disallow previously used passwords' checkbox is checked. In the 'Password Expiration' section, the 'Prompt password change 15 days before expiration and force password change upon expiration' checkbox is checked, and the 'Password Validity Period (days)' is 90. In the 'Minimum Password Age' section, the 'Allow a password to be changed only after it is used for a specified time' checkbox is unchecked. A red 'Save' button is located at the bottom left of the form.

Security Settings ?

Basic Information Critical Operations Login Authentication Policy **Password Policy** ACL

Password Composition & Reuse

Must contain at least of the following character types: uppercase letters, lowercase letters, digits and special characters.

Minimum Number of Characters

☐ Restrict consecutive identical characters

☒ Disallow previously used passwords

Number of Recent Passwords Disallowed

Password Expiration

☒ Prompt password change 15 days before expiration and force password change upon expiration

Password Validity Period (days)

Minimum Password Age

☐ Allow a password to be changed only after it is used for a specified time

Save

----End

2 Best Practices in Enabling High-Risk Ports

To safeguard your Huawei Cloud resources and help you set up a secure access channel to your Huawei Cloud resources, we recommend the following security policies for enabling high-risk ports.

Configuring Security Groups and Network ACL to Control Inbound Access

You can configure inbound rules in security groups and network ACLs to protect the ECSs in the security group and the subnets associated with the network ACL.

- Step 1 Go to the **Security Groups** page.
1. [Log in to the management console](#).

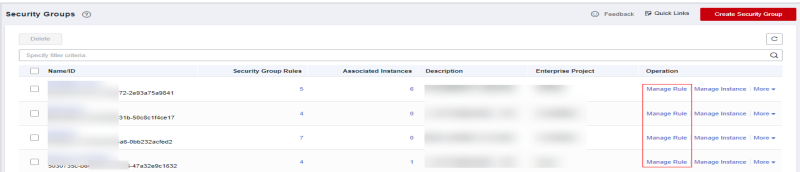
2. Click  in the upper left corner of the management console and select a region and a project.

3. In the navigation pane on the left, click  and choose **Network > Virtual Private Cloud**.

4. In the navigation pane on the left, choose **Access Control > Security Groups**.

- Step 2 Check each security group and delete high-risk port inbound rules.
1. On the **Security Groups** page, locate a security group and click **Manage Rule** in the **Operation** column.

Figure 2-1 Security Groups page



2. Click the **Inbound Rules** tab, check for the protocols and ports listed in **Protocol & Port** in [Table 2-1](#), and find the policy whose **Action** is **Allow** and **Source** is **0.0.0.0/0**.

Figure 2-2 Checking security group policies

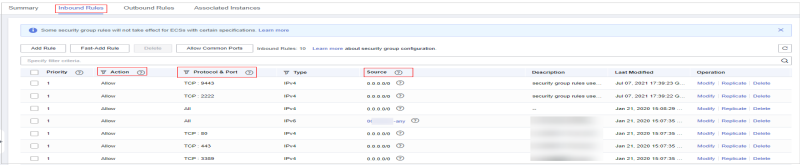


Table 2-1 High-risk ports

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 20, 21	File Transfer Protocol (FTP)	TCP: 3306	MySQL (database)
TCP: 22	Secure Shell (SSH)	TCP: 3389	Windows Remote desktop protocol (RDP)
TCP: 23	Telnet (remote terminal protocol)	TCP: 3690	Subversion (SVN, an open-source version control system)
TCP: 25	Simple Mail Transfer Protocol (SMTP)	TCP: 4848	GlassFish (application server)
TCP/UDP: 53	Domain Name System (DNS)	TCP: 5000	Sybase/DB2 (database)
TCP: 69	Trivial File Transfer Protocol (TFTP)	TCP: 5432	PostgreSQL (database)
TCP: 110	Post Office Protocol 3 (POP3)	TCP: 5900-5902	Virtual Network Console (VNC)
TCP: 111, 2049	Network File System (NFS)	TCP: 5984	CouchDB (database)
TCP: 137, 139, 445	Server Message Block (SMB) protocol (NetBIOS)	TCP: 6379	Redis (database)
TCP: 143	Internet Message Access Protocol (IMAP)	TCP: 7001-7002	WebLogic (web app system)
TCP: 389, 636	Lightweight Directory Access Protocol (LDAP)	TCP: 7199, 7000, 7001, 9160, 9042	Apache Cassandra
TCP: 512-514	Linux rexec (remote login)	TCP: 7778	Kloxo (virtual host management system)

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 873	Rsync (data image backup tool)	TCP: 8000	Ajenti (Linux server management panel)
TCP: 1194	OpenVPN (virtual private channel)	TCP: 8069, 10050-10051	Zabbix (system network monitoring)
TCP: 1352	Lotus	TCP: 8443	Plesk (virtual server management panel)
TCP: 1433	SQL Server (database management system)	TCP: 8080, 28015, 29015	RethinkDB
TCP: 1521	Oracle (database)	TCP: 8080-8089	Jenkins and JBoss (application server)
TCP: 1500	ISPmanager (server control panel)	TCP: 8088, 50010, 50020, 50030, 50070	Hadoop (distributed file system)
TCP: 1723	Point-to-Point Tunneling Protocol (PPTP)	TCP: 8848, 9848, 9849, 7848	Nacos service
TCP: 2082-2083	cPanel (VM control system)	TCP: 9080-9081, 9090	WebSphere (application server)
TCP: 2181	ZooKeeper (reliable coordination service for distributed systems)	TCP: 9200, 9300	Elasticsearch (Lucene search server)
TCP: 2601-2604	Zebra (route)	TCP: 11211	Memcached (cache system)
TCP: 3128	Squid (caching proxy)	TCP: 27017-27018	MongoDB (database)
TCP: 3311-3312	kangle (web server)	TCP: 50000	SAP Management Console

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 8080	DisConf (distributed configuration management platform)	TCP: 60010, 60030	HBase
TCP: 8888	Spring Cloud Config (distributed configuration center)	TCP: 3000	Grafana (data visualization)
TCP: 8761	Eureka (service registration and discovery component)	TCP: 8983	Solr (open-source enterprise-search platform)
TCP: 8500, 8502	Consul (service registration and discovery component)	TCP: 3123-3124, 8081, 6123	Flink (big data processing platform)
TCP: 8070, 8080	Apollo (distributed configuration management platform)	TCP: 4040, 7077, 8080-8081	Spark (big data processing platform)
TCP: 8090	Diamond (distributed configuration management system)	TCP: 8080, 11800, 12800	SkyWalking (distributed system monitoring)
TCP: 2379-2380	Etcd (distributed key-value storage system)	TCP: 8080	WebTTY (Web TTY management page)
TCP: 15672	RabbitMQ (message queue)	TCP: 80, 443	NextCloud (private network hard disk)
TCP: 8161, 61616	ActiveMQ (message queue)	TCP: 9001, 9090	Minio (cloud storage management tool)
TCP: 8083, 8086, 8635	InfluxDB (time series database)	TCP: 18083	EMQX (IoT access platform)
TCP: 6030-6032, 6041	TDengine (time series database)	TCP: 1090, 1099	Java-RMI protocol (Java remote method invocation protocol)
TCP: 9092-9095, 9999	Kafka (distributed stream processing platform)	TCP: 8000	JDWP (Java remote debugging interface)
TCP: 2375	Docker (application container engine)	TCP: 8009	Tomcat AJP protocol (binary communication protocol)

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 5601	Kibana (data visualization)	TCP: 8888	Jupyter Notebook (web applications for interactive computing)
TCP: 177	xmanager/xwin (Linux remote GUI)	TCP: 6443, 8443, 10250-10256	Kubernetes (container orchestration engine)
TCP: 8081	Nexus (repository manager)	TCP: 80/443, 8080	GitLab (code hosting platform)
UDP: 161, 162	Simple Network Management Protocol (SNMP)	TCP: 5555	ADB (Android debugging tool)
TCP: 1883, 8883	MQTT (IoT message protocol)	TCP: 6000-6063	X11 (Linux remote GUI)
TCP: 8888	Napster (P2P file sharing protocol)	-	-

3. Check for and eliminate high-risk port policies. You can click **Modify** or **Delete** in the **Operation** column.

Figure 2-3 High-risk port policies for security groups

Priority	Action	Protocol & Port	Type	Source	Description	Last Modified	Operation
1	Allow	TCP: 8443	IPv4	0.0.0.0	security group rules use...	Jul 07, 2021 17:39:23 G...	Modify Replicate Delete
1	Allow	TCP: 2222	IPv4	0.0.0.0	security group rules use...	Jul 07, 2021 17:39:22 G...	Modify Replicate Delete
1	Allow	All	IPv4	0.0.0.0	-	Jan 21, 2020 15:08:29 ...	Modify Replicate Delete

NOTE

- You are advised to delete the **Allow** policies for ports that do not need to be open to the external network.
- To allow external access from certain IP addresses, you are advised to set **Source** to the IP addresses in the whitelist. For details, see [Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group](#).
- You are not advised to enable high-risk port policies for all IP addresses.

Step 3 In the navigation pane on the left, choose **Access Control > Network ACLs**.

Step 4 Check all the network ACLs that are enabled and associated with subnets. Delete high-risk port policies from the inbound rules.

1. In the network ACL list, locate a rule and click **Manage Rule** in the **Operation** column.

Figure 2-4 Network ACL page

NameID	Status	Network A...	Associated...	Description	Operation
9b0c0000-0000-0000-0000-000000000000	Enabled	5	1	test	Associate Subnet Manage Rule More

- Click the **Inbound Rules** tab, check for the protocols and ports listed in **Protocol & Port** in [Table 2-1](#), and find the policy whose **Action** is **Allow** and **Source** is **0.0.0.0/0**.

Figure 2-5 Checking network ACL policies

Priority	Action	Protocol & Port	Type	Source	Description	Last Modified	Operation
1	Allow	TCP: 8443	IPv4	0.0.0.0/0	security group rules use...	Jul 07, 2021 17:39:23 (s)	Modify Refresh Delete
1	Allow	TCP: 2222	IPv4	0.0.0.0/0	security group rules use...	Jul 07, 2021 17:39:23 (s)	Modify Refresh Delete
1	Allow	All	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:55:26	Modify Refresh Delete
1	Allow	All	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:38	Modify Refresh Delete
1	Allow	TCP: 80	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:38	Modify Refresh Delete
1	Allow	TCP: 443	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:38	Modify Refresh Delete
1	Allow	TCP: 3389	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:38	Modify Refresh Delete

- Check for and eliminate high-risk port policies. You can click **Modify** or **Delete** in the **Operation** column.

NOTE

- You are advised to delete the **Allow** policies for ports that do not need to be open to the external network.
- To allow external access from certain IP addresses, you are advised to set **Source** to the IP addresses in the whitelist.
- You are not advised to open high-risk ports to all IP addresses.

----End

Using VPN/IPsec to Control Internal Access to Ports

By default, ECSs in a VPC cannot communicate with your physical data center or private network. To connect ECSs in a VPC to your data center or private network, you are advised to use Huawei Cloud **Virtual Private Network (VPN)**.

Using Huawei Cloud Native Services to Enhance Security

Our cloud native services provide a range of features to enhance security.

Databases

Relational Database Service (RDS) provides a comprehensive performance monitoring system, implements **a range of security measures**, and offers a professional database management platform, allowing you to easily configure and scale databases on the cloud. On the RDS console, you can perform almost all necessary tasks and no programming is required. The console simplifies operations and reduces routine O&M workloads, so you can stay focused on application and service development.

Application middleware

Distributed Cache Service (DCS) provides **multiple features** to improve the reliability and security of tenant data, such as VPC, security group, whitelist, SSL encrypted connection for public network access, automatic backup, data snapshot, and cross-AZ deployment.

3 Disposal of Spam Mails Sent to External Systems

3.1 What Is Spam Email and How It Is Harmful

What Is Spam Email?

Spam email is unsolicited and unwanted junk email that is sent out in bulk to an indiscriminate recipient without the permission of the recipient. Usually, spam email always:

- Has no title, no sender, or source address.
- Has false information in the subject or content.
- Includes fraud information.
- Contains immoderate or illegal content.
- Hides harmful information such as viruses in the content.

How Is Spam Email Harmful?

Email is one of the important communication tools in today's society. Spam email will:

- Reduce communication quality: Spam email occupies a large amount of network bandwidth, affects the network transmission speed, and may cause mail server congestion.
- Damage the interests of the recipient: Spam usually contains hidden phishing links that may cause data leakage of recipients. Recipients may be then tricked into leaking credentials or business secrets. Spam email is repeated and spread quickly, it takes a lot of time and money for the recipient to stop it.
- Spread harmful information: Spam email is always used to spread harmful information such as rumors.

3.2 How Huawei Cloud Handles Resources That Send Spam Email

Overview

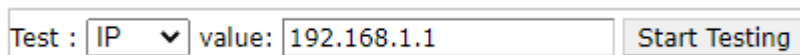
Using resources on Huawei Cloud to send spam email violates [Huawei Cloud User Agreement](#) and other related laws and regulations. IP addresses that are used to send out spam email in bulk will be recorded in the blocklist by the international anti-spam organization. IP addresses in the blocklist cannot be used for accessing websites, receiving emails, or sending emails. Once the IP address you obtained from Huawei Cloud is in the blocklist, the image of Huawei Cloud is severely damaged. If Huawei Cloud receives an external complaint that spam email is sent by resources of a Huawei Cloud user, Huawei Cloud will send a warning email to the user and take risk control measures (including but not limited to blocking ports and freezing IP addresses involved).

Rectification Suggestion

Huawei Cloud will implement risk control measures based on the complaint types.

You can open the [anti-spam organization](#) address, enter your IP address, and click **Start Testing** to check whether the IP address is listed by the organization as a spammer. Then handle the complaint accordingly.

Figure 3-1 Anti-spam organization



- If no IP address records are displayed on the page and the initial page is displayed, the IP address has not been blocked by the anti-spam organization.
Stop using the server with this IP address to send spam email as soon as possible and protect the mail address from malicious use. If the rectification is not completed within the time specified in the warning email, your resources may be blocked (including but not limited to blocking ports and freezing IP addresses).
- If your IP address is displayed on the page, the IP address has been blocked by the anti-spam organization.
The anti-spam organization has added your IP address to their blocklist. This means this IP address cannot be used to access websites or send emails anymore. Stop using this IP address to send spam email as soon as possible and protect your mail address.
Since the IP address blocklisted by the anti-spam organization is managed by Huawei Cloud, the image of Huawei Cloud is severely damaged. Huawei Cloud will permanently freeze the IP address. The IP address cannot be unfrozen in any cases. Bind a new IP address to the server.

4 UDP-based Amplification Attack Check

4.1 Overview

What Are DDoS Attacks

DoS (Denial of Service) attacks are also called flood attacks. They are intended to exhaust the network or system resources on the target computer, causing service interruption or suspension. Consequently, legitimate users fail to access network services. A DDoS attack involves multiple compromised computers controlled by an attacker flooding the targeted server with superfluous requests.

What Are UDP-based Amplification Attacks

UDP-based amplification attacks are a form of DDoS attacks that are highly destructive, easy to trigger, and difficult to trace.

Figure 4-1 shows how such an attack works. An UDP-based amplification attack does not directly work on the target server. Instead, the attacker sends special UDP-based request packets to some open internet servers via IP addresses forged as that of the target server. These request packets will bring out high volumes of data to overwhelm the target server.

Figure 4-1 How a UDP-based amplification attack works



4.2 Detecting UDP-based Amplification Attacks

This section describes how to detect UDP amplification attacks on your server.

1. Log in to the server as user **root**.

NOTE

In this example, the server sends ten 800-byte UDP packets per second when it is running properly.

2. Run the following command to check the current network connections and processes:

netstat -anpt

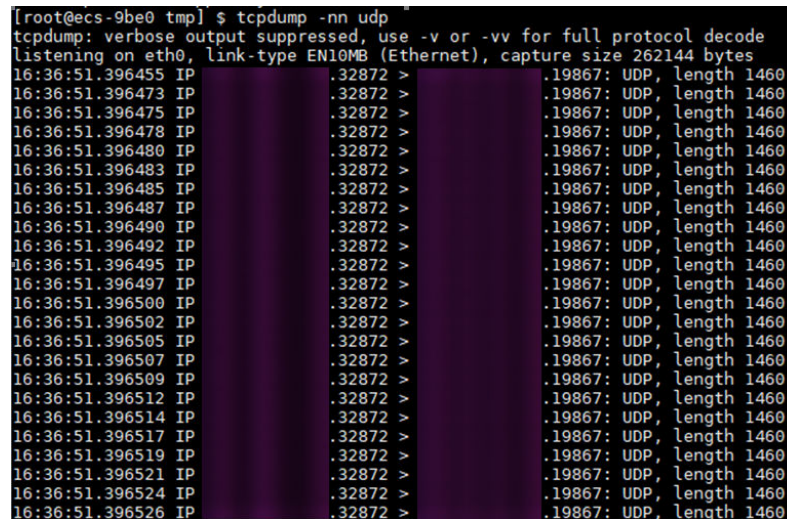
You are advised to run the **netstat -anpt** command to check whether the current network connections and processes are normal. If the current connections and processes have been stopped or hidden, you can use the **tcpdump** packet capture tool to capture packets for analysis.

3. Run the following command to capture packets and analyze UDP traffic attacks:

tcpdump -nn udp

Figure 4-2 shows an example of the captured packets.

Figure 4-2 UDP attack packets



```
[root@ecs-9be0 tmp] $ tcpdump -nn udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:36:51.396455 IP .32872 > .19867: UDP, length 1460
16:36:51.396473 IP .32872 > .19867: UDP, length 1460
16:36:51.396475 IP .32872 > .19867: UDP, length 1460
16:36:51.396478 IP .32872 > .19867: UDP, length 1460
16:36:51.396480 IP .32872 > .19867: UDP, length 1460
16:36:51.396483 IP .32872 > .19867: UDP, length 1460
16:36:51.396485 IP .32872 > .19867: UDP, length 1460
16:36:51.396487 IP .32872 > .19867: UDP, length 1460
16:36:51.396490 IP .32872 > .19867: UDP, length 1460
16:36:51.396492 IP .32872 > .19867: UDP, length 1460
16:36:51.396495 IP .32872 > .19867: UDP, length 1460
16:36:51.396497 IP .32872 > .19867: UDP, length 1460
16:36:51.396500 IP .32872 > .19867: UDP, length 1460
16:36:51.396502 IP .32872 > .19867: UDP, length 1460
16:36:51.396505 IP .32872 > .19867: UDP, length 1460
16:36:51.396507 IP .32872 > .19867: UDP, length 1460
16:36:51.396509 IP .32872 > .19867: UDP, length 1460
16:36:51.396512 IP .32872 > .19867: UDP, length 1460
16:36:51.396514 IP .32872 > .19867: UDP, length 1460
16:36:51.396517 IP .32872 > .19867: UDP, length 1460
16:36:51.396519 IP .32872 > .19867: UDP, length 1460
16:36:51.396521 IP .32872 > .19867: UDP, length 1460
16:36:51.396524 IP .32872 > .19867: UDP, length 1460
16:36:51.396526 IP .32872 > .19867: UDP, length 1460
```

- a. Run the following command to temporarily save the captured packet information to the **udp.pcap** file in the **/home** folder:
- b. Run the following command to analyze the captured packet information.

tcpdump -nn -r /home/udp.pcap|awk -F'.' '{print \$1}'|sort|uniq -c

Figure 4-3 Captured packet analysis result

```
[root@ecs-9be0 home] $ tcpdump -nn -r /home/udp.pcap|awk -F"." '{print $1}'|sort|uniq -c
reading from file /home/udp.pcap, link-type EN10MB (Ethernet)
 1701 16:40:45
 55566 16:40:46
 56007 16:40:47
 55692 16:40:48
 56272 16:40:49
 55062 16:40:50
 56007 16:40:51
 55188 16:40:52
 55944 16:40:53
 56952 16:40:54
 55818 16:40:55
 56196 16:40:56
 55188 16:40:57
 55314 16:40:58
 55629 16:40:59
```

According to step 3, the checked device is sending dozens of 1460-byte UDP data packets to another IP address, which is far greater than the normal traffic. This indicates that the device is likely being used as an amplifier for UDP reflection attacks.

According to step b, the number of UDP connections per second is more than 50,000, indicating that the services provided by the device are used by attackers to launch UDP amplification attacks. So, necessary protection measures must be taken to prevent server resources from being exhausted by attack traffic.

4.3 Solution and Prevention Measures

You can take measures to defend against UDP amplification attacks based on service requirements. The following provides some recommended protection measures for your reference.

- Pay attention to the latest security advisories and bulletins released by security vendors, and implement targeted protection policies against such attacks in a timely manner.
- Use firewalls to control access to the UDP ports of ECSs.
- Configure security groups to control access to UDP ports. For details, see [Configuring Security Group Rules](#).
- Configure local IP addresses, disable external access, disable the UDP protocol, and enable login authentication.
- Adjust some parameters and restart the server to disable UDP.
- Create a profile of normal packet sizes based historical data, so you can easily detect overly small or overly large packets that may be part of the attack traffic.

5 Host Security Checks

5.1 Hosts Security Issues

5.1.1 Overview

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.

This document describes how to defend against the following threats to host security:

- External attacks: port scan
- Mining
- Ransomware

5.1.2 External Attacks: Port Scan

What Is Port Scan?

In a port scan attack, an attacker sends a request to the IP address of a target server or workstation to discover open ports, and exploit vulnerabilities through the port to launch attacks.

Cases

The following are several cases of port scan attacks on hosts:

- Case 1:
 - a. The host is scanning a large number of external ports 6379, as shown in [Figure 5-1](#).

Figure 5-1 Port scan

```
(root@ecs-2 ~)# netstat
```

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	1	kafka01:34934	1: 6:6379	SYN_SENT
tcp	0	1	kafka01:47186	1: 45:6379	SYN_SENT
tcp	0	1	kafka01:56582	1: 16:6379	SYN_SENT
tcp	0	1	kafka01:55246	1: 11:6379	SYN_SENT
tcp	0	1	kafka01:54158	1: 1:6379	SYN_SENT
tcp	0	1	kafka01:36218	1: 1:6379	SYN_SENT
tcp	0	1	kafka01:51348	1: 7:6379	SYN_SENT
tcp	0	1	kafka01:48172	1: 21:6379	SYN_SENT
tcp	0	1	kafka01:35938	1: 39:6379	SYN_SENT
tcp	0	1	kafka01:54252	1: 4:6379	SYN_SENT
tcp	0	1	kafka01:43734	1: 17:6379	SYN_SENT
tcp	0	1	kafka01:36836	1: 34:6379	SYN_SENT
tcp	0	1	kafka01:57958	1: 36:6379	SYN_SENT
tcp	0	1	kafka01:57958	1: 5:6379	SYN_SENT
tcp	0	1	kafka01:53292	1: 48:6379	SYN_SENT
tcp	0	1	kafka01:51384	1: 61:6379	SYN_SENT
tcp	0	1	kafka01:56862	1: 26:6379	SYN_SENT
tcp	0	1	kafka01:53856	1: :6379	SYN_SENT
tcp	0	1	kafka01:57512	1: 31:6379	SYN_SENT
tcp	0	1	kafka01:55324	1: 43:6379	SYN_SENT
tcp	0	1	kafka01:48428	1: 98:6379	SYN_SENT
tcp	0	1	kafka01:41912	1: 11:6379	SYN_SENT
tcp	0	1	kafka01:43682	1: 68:6379	SYN_SENT
tcp	0	1	kafka01:47736	1: 83:6379	SYN_SENT
tcp	0	1	kafka01:kitim	1: 7:6379	SYN_SENT
tcp	0	1	kafka01:47298	1: 6:6379	SYN_SENT

- b. The query result shows that these IP addresses are from different countries/regions.
- Case 2:
 - a. An abnormal process is detected on the host, as shown in [Figure 5-2](#).

Figure 5-2 Abnormal process

0	0	0.0.0.0:13562	0.0.0.0:*	LISTEN	28873/java
0	0	0.0.0.0:2181	0.0.0.0:*	LISTEN	27514/java
0	0	1: 93:4181	1: 17:36524	ESTABLISHED	27514/java
0	0	1: 93:8042	1: 1:58934	TIME_WAIT	-
0	0	1: 93:48110	1: 17:7184	ESTABLISHED	27514/java
0	0	1: 93:48128	1: 17:7184	ESTABLISHED	27515/java
0	0	1: 93:45182	1: 17:7182	ESTABLISHED	24954/python2
0	0	1: 93:52768	2: 0:81	ESTABLISHED	9487/Sofia
0	0	1: 93:22	1: 233:7847	ESTABLISHED	18718/sshd: root@pt
0	0	1: 93:2181	1: 17:58834	TIME_WAIT	-
0	0	1: 93:9810	1: 17:49586	ESTABLISHED	27514/java
0	0	1: 93:39552	1: 2.111:18188	ESTABLISHED	8134/hostguard
0	0	1: 93:41288	1: 74:3181	ESTABLISHED	27514/java
0	0	1: 93:34736	1: 17:9995	ESTABLISHED	24954/python2
0	0	1: 93:51410	1: 17:8831	ESTABLISHED	28873/java
0	0	1: 93:9864	1: 3:58596	TIME_WAIT	-
0	0	1: 93:9866	1: 17:57468	TIME_WAIT	-
0	0	1: 93:22	1: 233:7846	ESTABLISHED	338/sshd: root@pts/
0	0	1: 93:47758	1: 17:9997	ESTABLISHED	24954/python2
0	0	1: 93:9810	1: 17:49592	ESTABLISHED	27514/java
0	0	1: 1:19881	1: 36238	ESTABLISHED	24953/python2
0	0	1: 93:4181	1: 74:37818	ESTABLISHED	27514/java
0	0	1: 93:9810	1: 17:49562	ESTABLISHED	27514/java
0	0	1: 1:33364	1: 48174	TIME_WAIT	-
0	0	1: 1:36238	1: 19881	ESTABLISHED	24954/python2
0	0	1: 93:58846	1: 17:8822	ESTABLISHED	27515/java
0	0	1: 9288	1: *	LISTEN	38648/java

- b. The query result shows that the IP address connects to C&C.
C&C refers to command and control, a communication mode between hosts.
A C&C host sends commands to a victim system and receives data from the system.

5.1.3 Mining

What Is Mining?

Digital currency, which is decentralized and valuable, is getting more attention nowadays. Black and gray markets obtain digital currency through malicious mining.

Mining is a process of occupying victims' system and network resources and obtaining digital currency through a large amount of computing without permissions.

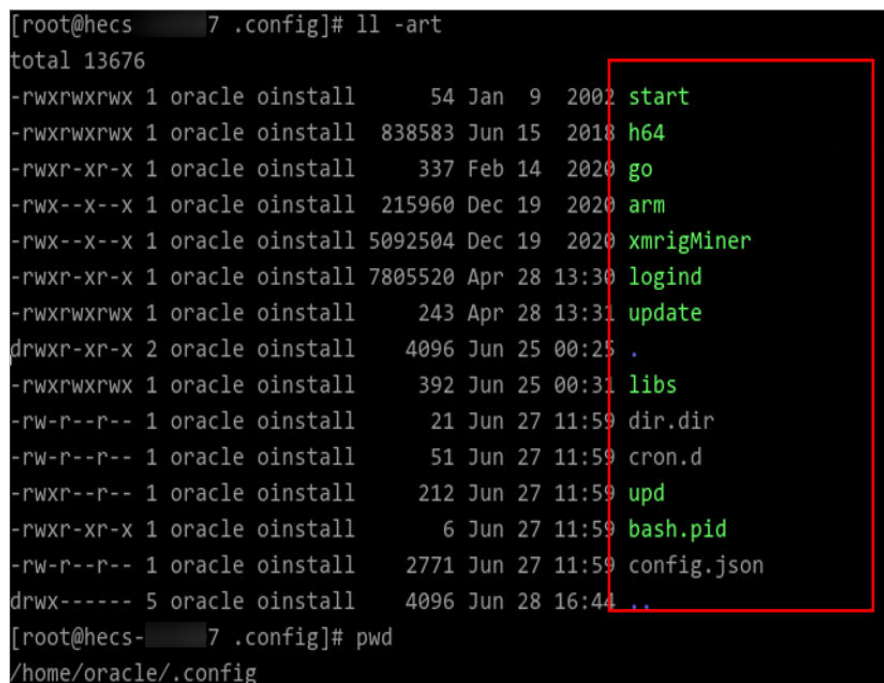
The machines that can be remotely controlled by attackers are called zombies, which can be the Windows, Linux, or Unix servers of companies, schools, or even governments and militaries.

Mining occupies a large number of system resources and leads to performance deterioration of other software or services. In addition, hackers may use mining programs to obtain confidential information, such as confidential files and the usernames and passwords of key assets.

Cases

The following are several cases of mining:

- Case 1:
 - a. An abnormal file (usually marked with **xmr** or **mine**) is detected.



```
[root@hecs-7 .config]# ll -art
total 13676
-rwxrwxrwx 1 oracle oinstall      54 Jan  9  2002 start
-rwxrwxrwx 1 oracle oinstall 838583 Jun 15  2018 h64
-rwxr-xr-x 1 oracle oinstall    337 Feb 14  2020 go
-rwx--x--x 1 oracle oinstall 215960 Dec 19  2020 arm
-rwx--x--x 1 oracle oinstall 5092504 Dec 19  2020 xmrigMiner
-rwxr-xr-x 1 oracle oinstall 7805520 Apr 28 13:30 logind
-rwxrwxrwx 1 oracle oinstall    243 Apr 28 13:31 update
drwxr-xr-x 2 oracle oinstall    4096 Jun 25 00:25 .
-rwxrwxrwx 1 oracle oinstall    392 Jun 25 00:31 libs
-rw-r--r-- 1 oracle oinstall    21 Jun 27 11:59 dir.dir
-rw-r--r-- 1 oracle oinstall    51 Jun 27 11:59 cron.d
-rwxr--r-- 1 oracle oinstall    212 Jun 27 11:59 upd
-rwxr-xr-x 1 oracle oinstall     6 Jun 27 11:59 bash.pid
-rw-r--r-- 1 oracle oinstall   2771 Jun 27 11:59 config.json
drwx----- 5 oracle oinstall    4096 Jun 28 16:44 ..
[root@hecs-7 .config]# pwd
/home/oracle/.config
```

- b. Analyze the file. A mining pool is detected. Verify that the URL is a malicious mining pool address.
- Case 2:

- a. A mining process is detected from a Windows host.
- b. Abnormal files are detected from the host.
- c. Analyze the file. A mining pool is detected.

```
~ donate-over-proxy : 1,  
"pools" : [  
  {  
    "algo" : null,  
    "coin" : null,  
    "url" : "ok.xmrpool.ru:1081",  
    "user" : "abc1081",  
    "pass" : "x",  
    "rig-id" : null,  
    "nicehash" : true,  
    "keepalive" : false,
```

- d. Verify that the URL is a malicious mining pool address.

5.1.4 Ransomware

What Is 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.

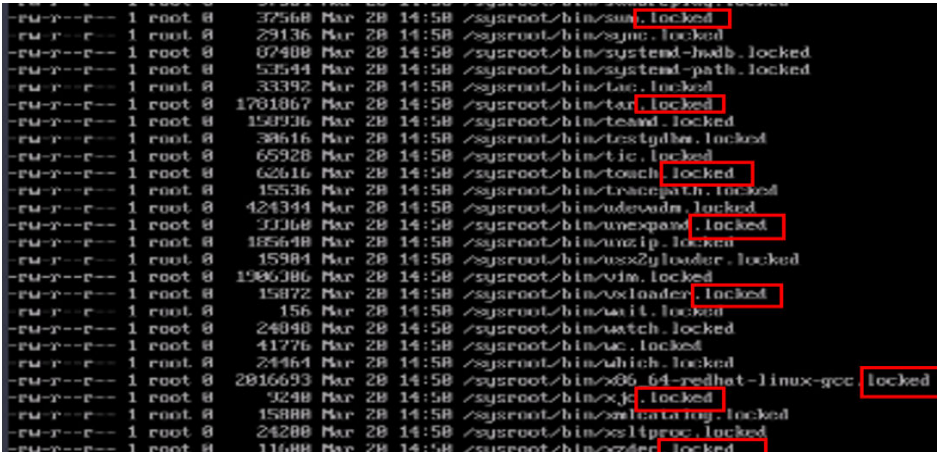
Ransomware interrupts businesses and can cause serious economic losses. We need to know how it works and how we can prevent it.

Ransomware can intrude servers in various ways and is difficult to remove.

Cases

The following are several cases of ransomware:

- Case 1: Files in a Windows host are encrypted and ransomware messages exist in the host.
- Case 2: Files in a Windows host are encrypted and suffixes are added to the files.
- Case 3: Files in a Linux host are encrypted and suffixes are added to the files.



5.2 Host Security Check (Windows)

5.2.1 Troubleshooting Methods

- You can check Windows hosts by using the methods described below. **Method 1: Using Tools to Detect Security Issues** is recommended.
- Method 1: **Method 1: Using Tools to Detect Security Issues** (recommended)
 - You are advised to use the following software.

Table 5-1 Software

Tool	Link
ProcessExplorer	https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer
Tcpview	https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
Autoruns	https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
busybox-x86_64	https://busybox.net/downloads/binaries/1.16.1/busybox-x86_64

- Method 2: **Method 2: Using DOS System Commands to Check Processes**

5.2.2 Troubleshooting Process

5.2.2.1 Method 1: Using Tools to Detect Security Issues

5.2.2.1.1 Step 1: Analyzing All Processes

This section describes how to detect Trojans from official Windows processes.

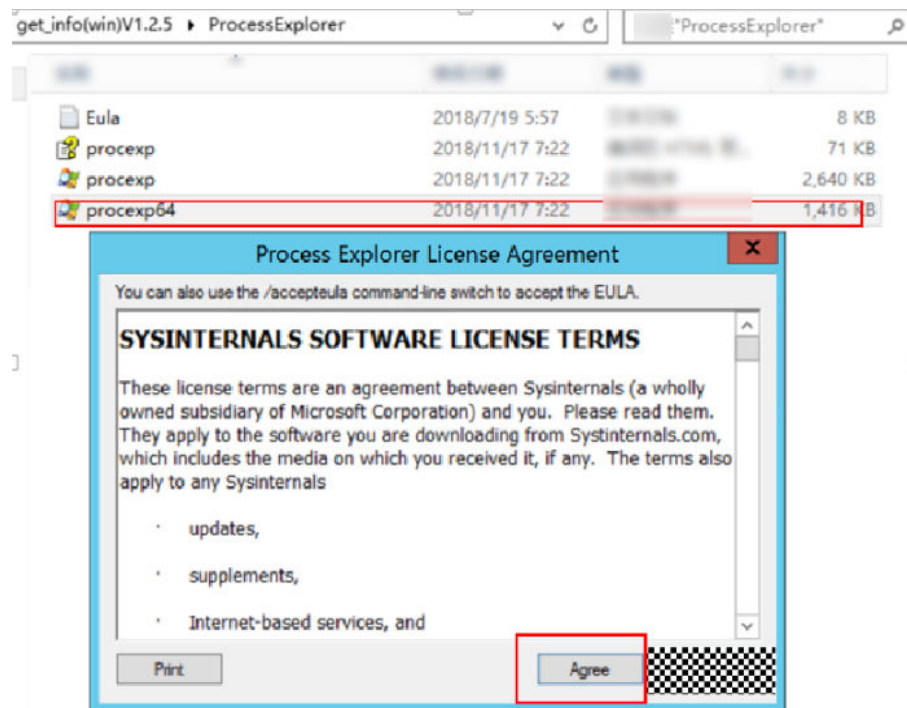
Prerequisites

You have downloaded **Process Explorer**.

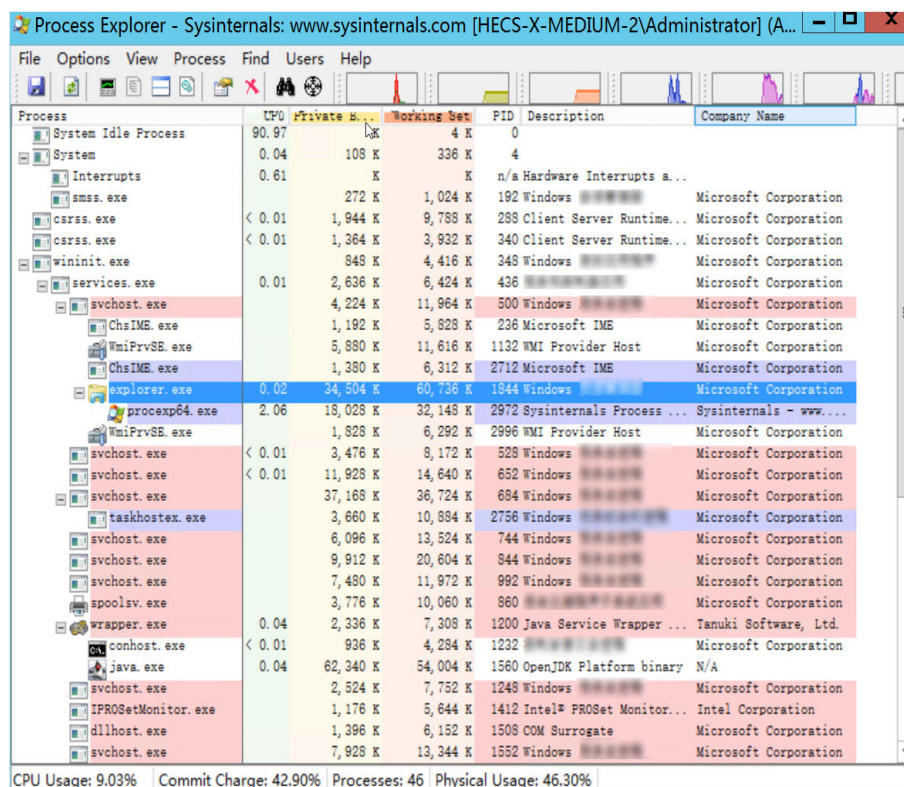
Procedure

Step 1 Open the **ProcessExplorer** folder and double-click the **procexp64.exe** file.

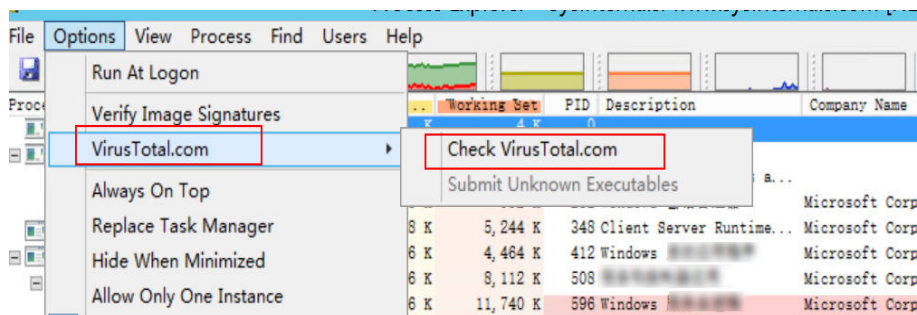
Figure 5-3 processExplorer



Step 2 In the dialog box that is displayed, click **Agree** to view the process information and check the processes online.

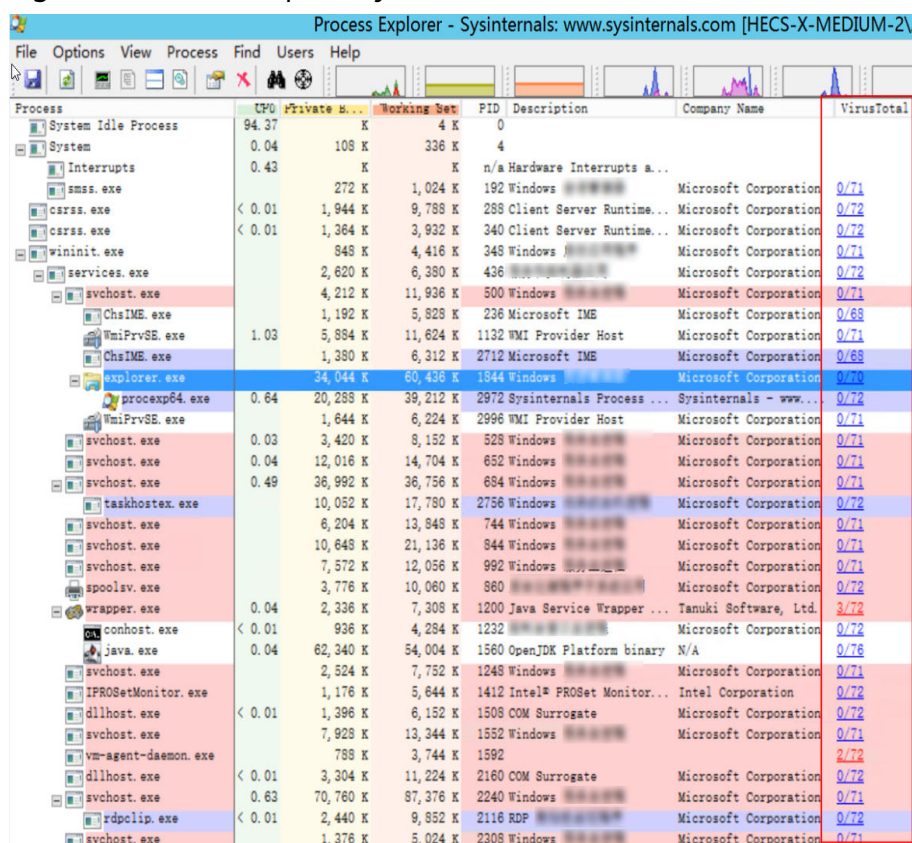
Figure 5-4 Viewing the current process

Step 3 On the menu bar, choose **Options > VirusTotal.com**, and select **Check VirusTotal.com** and **Submit Unknown Executables**.

Figure 5-5 options > VirusTotal.com

The system compares the hash values of the current processes with that in the **VirusTotal** database to quickly detect Trojans.

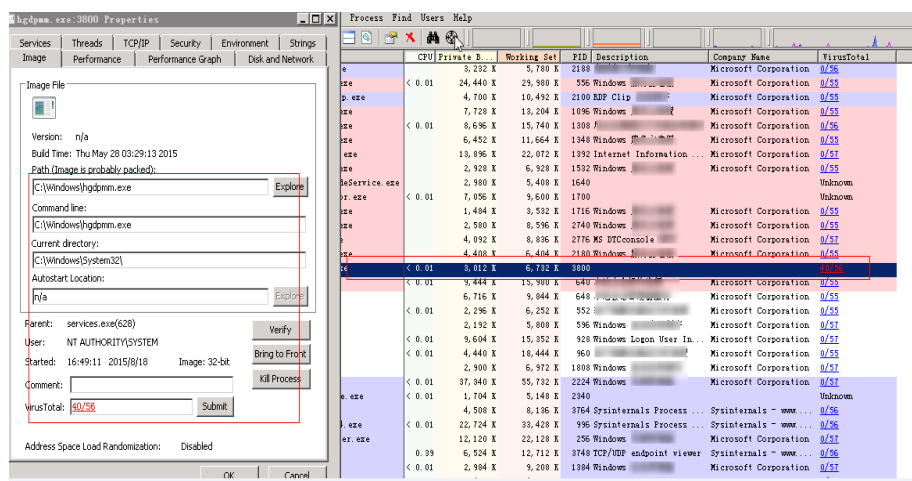
Figure 5-6 Process Explore-Sysinternals



Process	CPU	Private B...	Working Set	PID	Description	Company Name	VirusTotal
System Idle Process	94.37	K	4 K	0			
System	0.04	108 K	336 K	4			
Interrupts	0.43	K	K	n/a	Hardware Interrupts a...		
smss.exe		272 K	1,024 K	192	Windows ...	Microsoft Corporation	0/71
csrss.exe	< 0.01	1,944 K	9,788 K	288	Client Server Runtime...	Microsoft Corporation	0/72
csrss.exe	< 0.01	1,364 K	3,932 K	340	Client Server Runtime...	Microsoft Corporation	0/72
wininit.exe		848 K	4,416 K	348	Windows ...	Microsoft Corporation	0/71
services.exe		2,620 K	6,380 K	436	Windows ...	Microsoft Corporation	0/72
svchost.exe		4,212 K	11,936 K	500	Windows ...	Microsoft Corporation	0/71
ChsiME.exe		1,192 K	5,828 K	236	Microsoft IME	Microsoft Corporation	0/68
WmiPrvSE.exe	1.03	5,884 K	11,624 K	1132	WMI Provider Host	Microsoft Corporation	0/71
ChsiME.exe		1,380 K	6,312 K	2712	Microsoft IME	Microsoft Corporation	0/68
explorer.exe		34,044 K	60,436 K	1844	Windows ...	Microsoft Corporation	0/71
procexp64.exe	0.64	20,288 K	39,212 K	2972	Sysinternals Process ...	Sysinternals - www...	0/72
WmiPrvSE.exe		1,644 K	6,224 K	2996	WMI Provider Host	Microsoft Corporation	0/71
svchost.exe	0.03	3,420 K	8,152 K	528	Windows ...	Microsoft Corporation	0/71
svchost.exe	0.04	12,016 K	14,704 K	652	Windows ...	Microsoft Corporation	0/71
svchost.exe	0.49	36,992 K	36,756 K	684	Windows ...	Microsoft Corporation	0/71
taskhost.exe		10,052 K	17,780 K	2756	Windows ...	Microsoft Corporation	0/72
svchost.exe		6,204 K	13,848 K	744	Windows ...	Microsoft Corporation	0/71
svchost.exe		10,648 K	21,136 K	844	Windows ...	Microsoft Corporation	0/71
svchost.exe		7,572 K	12,056 K	992	Windows ...	Microsoft Corporation	0/71
spoolsv.exe		3,776 K	10,060 K	860	Windows ...	Microsoft Corporation	0/72
wrapper.exe	0.04	2,336 K	7,308 K	1200	Java Service Wrapper ...	Tanuki Software, Ltd.	3/72
conhost.exe	< 0.01	936 K	4,284 K	1232	Windows ...	Microsoft Corporation	0/72
java.exe	0.04	62,340 K	54,004 K	1560	OpenJDK Platform binary	N/A	0/76
svchost.exe		2,524 K	7,752 K	1248	Windows ...	Microsoft Corporation	0/71
IPROSetMonitor.exe		1,176 K	5,644 K	1412	Intel® PROSet Monitor...	Intel Corporation	0/72
dllhost.exe	< 0.01	1,396 K	6,152 K	1508	COM Surrogate	Microsoft Corporation	0/72
svchost.exe		7,928 K	13,344 K	1552	Windows ...	Microsoft Corporation	0/71
vm-agent-daemon.exe		788 K	3,744 K	1592			2/72
dllhost.exe	< 0.01	3,304 K	11,224 K	2160	COM Surrogate	Microsoft Corporation	0/72
svchost.exe	0.63	70,760 K	87,376 K	2240	Windows ...	Microsoft Corporation	0/71
rdpclip.exe	< 0.01	2,440 K	9,852 K	2116	RDP	Microsoft Corporation	0/72
svchost.exe		1,376 K	5,024 K	2308	Windows ...	Microsoft Corporation	0/71

Step 4 Check the value of **VirusTotal**. Right-click a process name and choose **Properties** from the shortcut menu. On the page that is displayed, click **Image** from the menu bar to view the process path and determine whether the process is a Trojan.

Figure 5-7 Checking whether a program is a Trojan horse program



----End

5.2.2.1.2 Step 2: Detecting Automatic Startup Programs

This section describes how to use **Autoruns** to check which programs are configured to automatically start upon system startup and login.

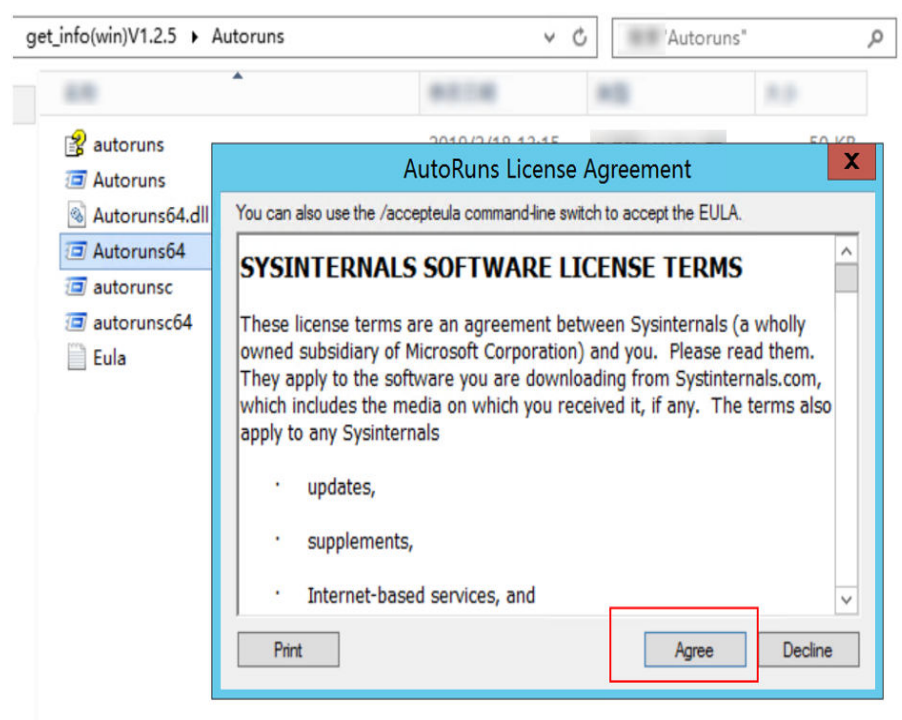
Prerequisites

You have downloaded **Autoruns**.

Procedure

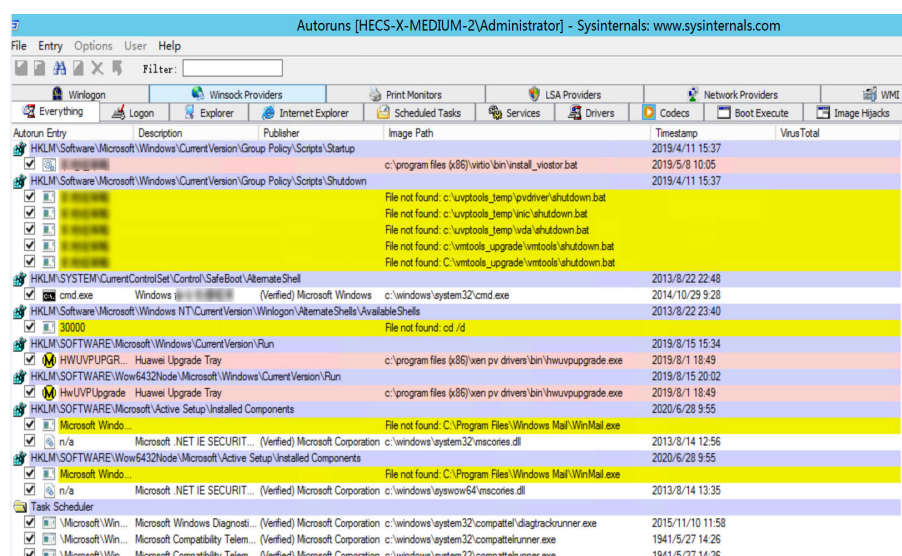
Step 1 Open the **Autoruns** folder and double-click the **Autoruns.exe** file.

Figure 5-8 Opening the AutoRuns folder

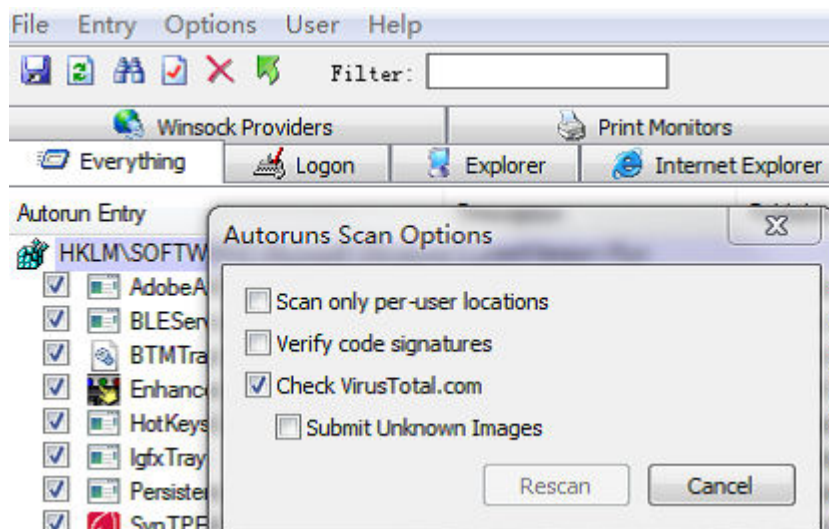


Step 2 In the displayed dialog box, click **Agree**.

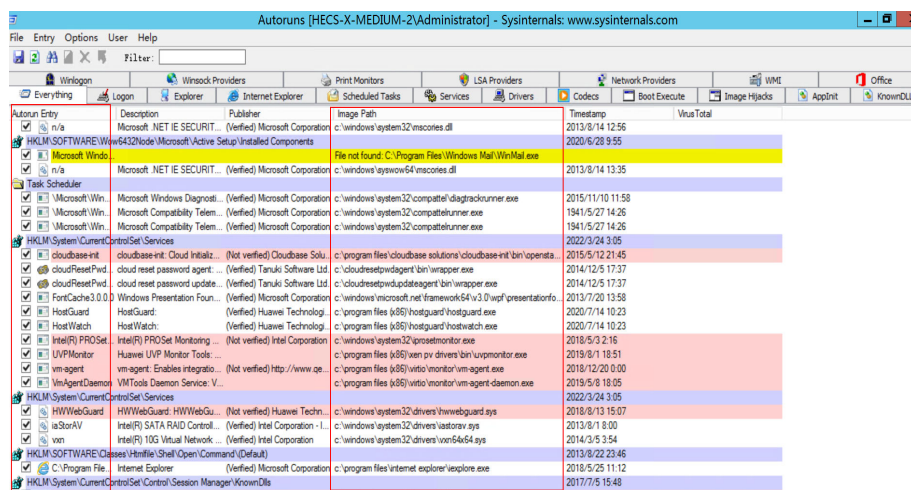
Figure 5-9 AutoRuns



- Step 3** On the menu bar, choose **Options > Scan Options** and select **CheckVirusTotal.com** to enable the online process detection function.

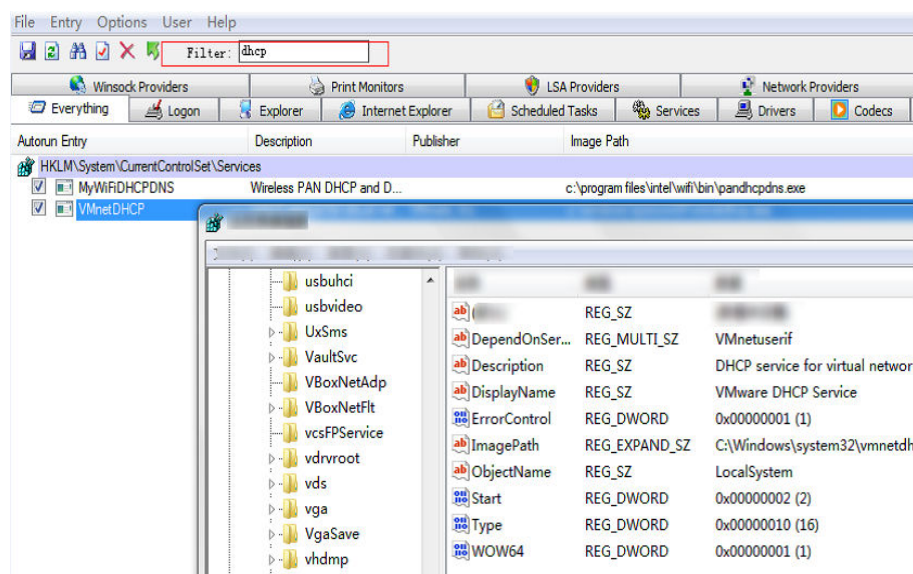


- Step 4** Check whether abnormal files (not created for system or normal service deployment) exist in the **Autorun** and **Images Path** columns.



- Step 5** If a suspicious process is found, double-click the process name to locate the registry. You can search for the names of suspicious processes in the **Filter** box.

Figure 5-10 Opening the Registry Editor



----End

5.2.2.1.3 Step 3: Analyzing the Network

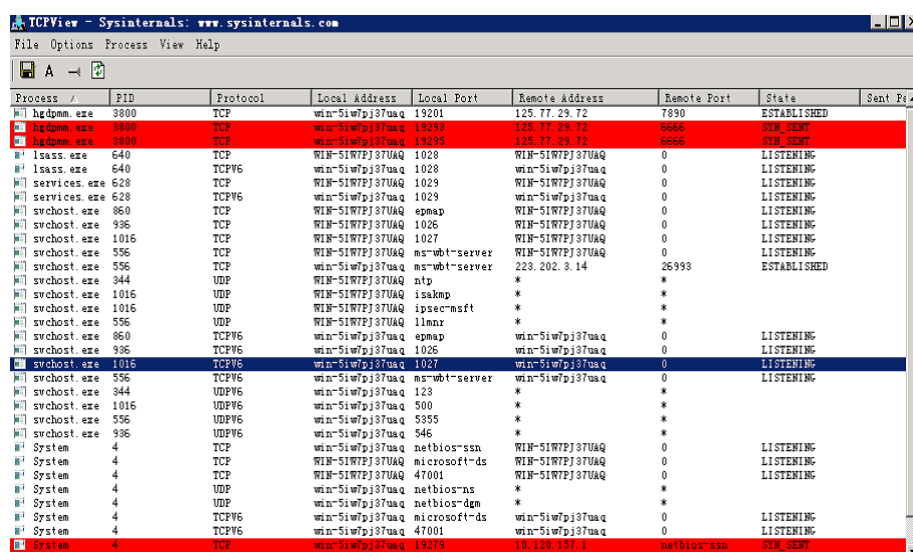
This section describes how to use **TCPView** to view the current TCP connection status and detect suspicious processes. Suspicious processes are highlighted in red.

Prerequisites

You have downloaded the **TCPView** tool.

Procedure

Step 1 Open the **TCPView** folder and double-click the **Tcpview.exe** file. In the displayed dialog box, click **Agree**.



Step 2 Check the TCP connection status of the target process to analyze whether it is a Trojan.

- If an unknown process has a large number of connections in the **SYN_SENT** state, the process may be a Trojan.
- If a process connects to regular ports (for example, 6666 or 2333), or its host automatically parsed in the **RemoteAddress** column contains keywords such as **mine**, **pool**, or **xmr**, the process may be infected with viruses.

Process	Port	Protocol	Local Address	Remote Address	State	Remote Address	State
cmd.exe	1620	TCP	192.168.1.40	53318	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53319	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53320	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53321	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53322	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53324	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53326	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53327	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53328	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53329	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53330	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53331	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53332	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53333	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53334	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53335	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53336	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53337	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53338	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53339	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53340	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53341	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53342	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53343	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53344	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53345	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53346	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53347	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53348	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53349	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53350	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53351	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53353	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53354	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53355	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53356	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53357	119.90.12.136	6431	SYN_SENT
cmd.exe	1620	TCP	192.168.1.40	53358	119.90.12.136	6431	SYN_SENT

Step 3 (Optional) You can use the security detection websites to check external remote addresses or URLs.

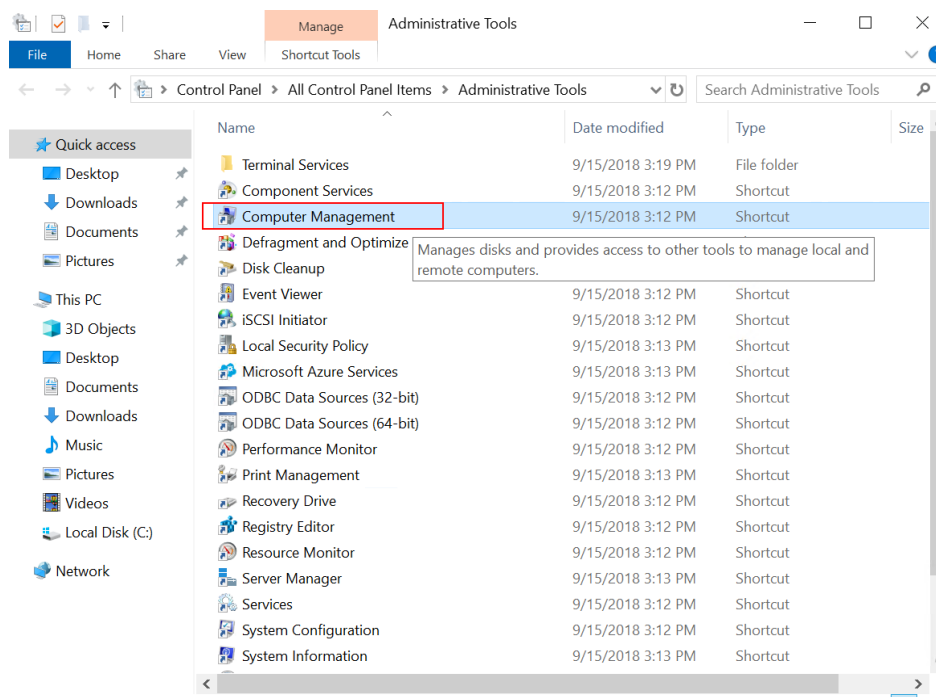
----End

5.2.2.1.4 Step 4: Detecting Abnormal Users

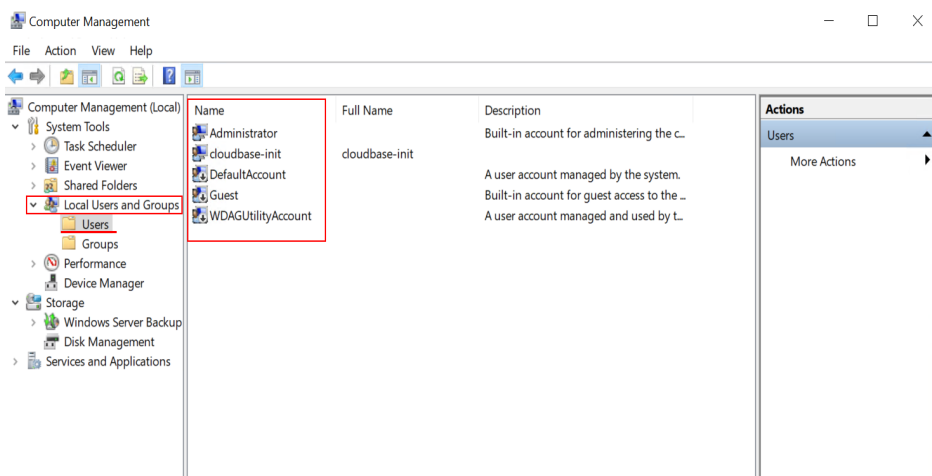
This section describes how to detect abnormal users.

Procedure

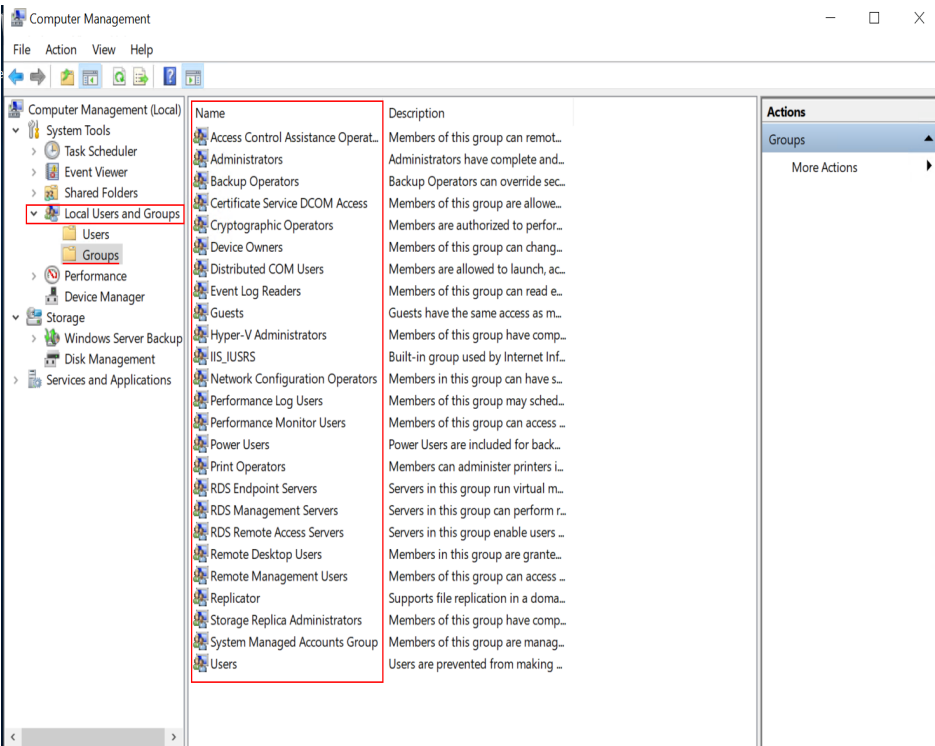
Step 1 Choose **Control Panel > Administrative Tools > Computer Management**.



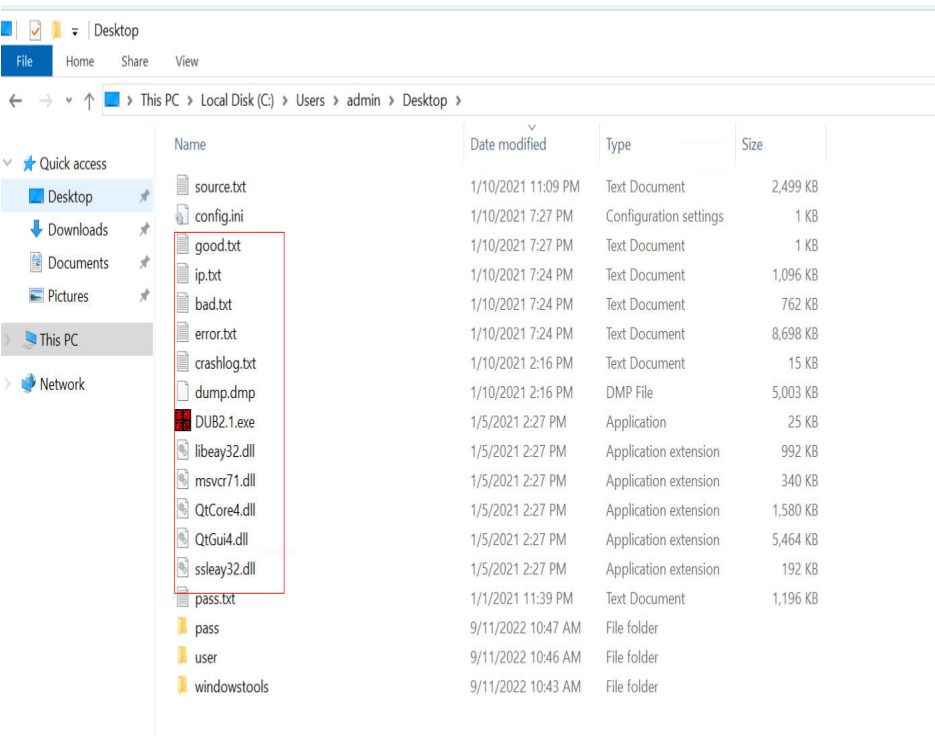
Step 2 In the navigation pane on the left, choose **Local Users and Groups > Users** to check whether abnormal users exist in the host.



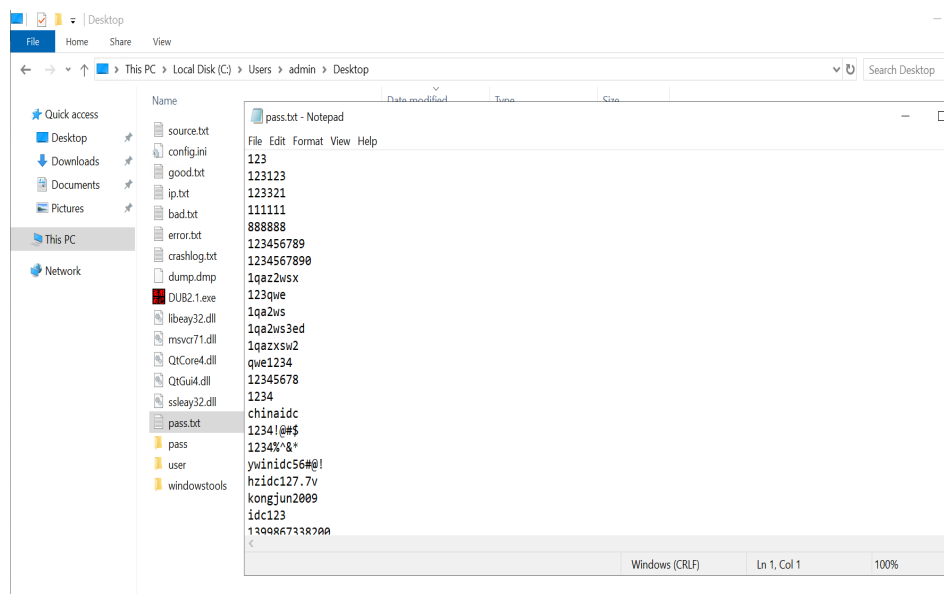
Step 3 In the navigation pane on the left, choose **Local Users and Groups > Groups** to check whether abnormal groups exist in the host.



Step 4 Check whether abnormal files (not created by the system or service deployment) exist in the abnormal user directory.



Step 5 Check whether the abnormal files are used for normal services, or use antivirus software to scan the abnormal files.



5.2.2.2 Method 2: Using DOS System Commands to Check Processes

This section describes how to use DOS commands to check processes.

Common Commands

Command	Description
cd	Switch to the following directory: • Current directory: [./] It can be omitted. • One level up: [../] • Two levels up: [../../]
dir /a: (disk)	Display all files (including system files and hidden files) by default.
more	Display file contents in the split-screen mode.
tasklist	Check process status.
netstat -ano	View links.
wmic startup list full	View automatic startup programs.
net user	View users.
Example commands are as follows: • Search for the files that contain DR under the D:\Apps\ directory: dir /a-d /s "D:\Apps\IDE" findstr "DR" • Search for the files and directories that contain exe in drive C: dir /s C: findstr "exe"	

Procedure

Step 1 Check whether abnormal processes exist.

Command: **tasklist**

Based on the query result, locate abnormal processes that are neither system processes nor service application processes.

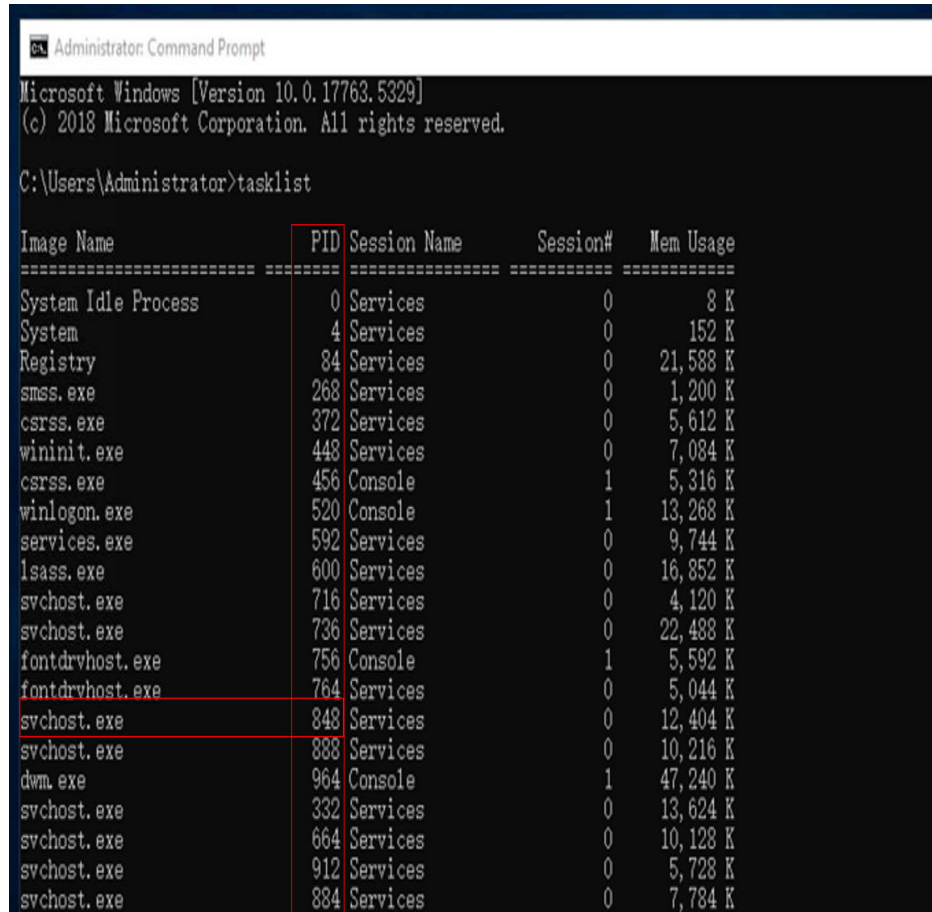


Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	152 K
Registry	84	Services	0	21,588 K
smss.exe	268	Services	0	1,200 K
csrss.exe	372	Services	0	5,612 K
wininit.exe	448	Services	0	7,084 K
csrss.exe	456	Console	1	5,316 K
winlogon.exe	520	Console	1	13,268 K
services.exe	592	Services	0	9,744 K
lsass.exe	600	Services	0	16,852 K
svchost.exe	716	Services	0	4,120 K
svchost.exe	736	Services	0	22,488 K
fontdrvhost.exe	756	Console	1	5,592 K
fontdrvhost.exe	764	Services	0	5,044 K
svchost.exe	848	Services	0	12,404 K
svchost.exe	888	Services	0	10,216 K
dwm.exe	964	Console	1	47,240 K
svchost.exe	332	Services	0	13,624 K
svchost.exe	664	Services	0	10,128 K
svchost.exe	912	Services	0	5,728 K
svchost.exe	884	Services	0	7,784 K

Step 2 View the network analysis result to check whether abnormal IP addresses are connected to the host.

Query command: **netstat -ano**

1. Based on the query result, locate the suspicious addresses that are neither service connection ports nor external addresses used for service connections.
2. Check whether the suspicious address is an international address of malicious or abnormal services.
3. Locate the target process (for example, **svchost.exe**) from the query result based on the PID value of the abnormal connection (for example, **2240**).

```
C:\Users\Administrator>netstat -ano

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING   848
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:3389             0.0.0.0:0               LISTENING   332
TCP   0.0.0.0:5357             0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:5985             0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:5986             0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:47001            0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:49664            0.0.0.0:0               LISTENING   448
TCP   0.0.0.0:49665            0.0.0.0:0               LISTENING   1100
TCP   0.0.0.0:49666            0.0.0.0:0               LISTENING   1616
TCP   0.0.0.0:49667            0.0.0.0:0               LISTENING   2196
TCP   0.0.0.0:49668            0.0.0.0:0               LISTENING   2580
TCP   0.0.0.0:49669            0.0.0.0:0               LISTENING   2392
TCP   0.0.0.0:49670            0.0.0.0:0               LISTENING   592
TCP   0.0.0.0:49696            0.0.0.0:0               LISTENING   600
TCP   192.168.1.125:139        0.0.0.0:0               LISTENING   4
TCP   192.168.1.125:49672     100.125.11.131:10180    ESTABLISHED 2240
TCP   [::]:135                 [::]:0                  LISTENING   848
TCP   [::]:445                 [::]:0                  LISTENING   4
TCP   [::]:3389                [::]:0                  LISTENING   332
TCP   [::]:5357                [::]:0                  LISTENING   4
TCP   [::]:5985                [::]:0                  LISTENING   4
```

Step 3 Check for abnormal users.

1. Run the following command: **net user**

```
C:\Users\Administrator>net user

User accounts for \\ECS-9808

-----
Administrator      c:\windows\system32\cmd.exe /d /s /q %*
Guest               W\*****ount
The command completed successfully.
```

2. Run the following command to query the time when the user changed the host password: **net user username** (for example, **administrator**)

```
Administrator: Command Prompt

C:\Users\Administrator>net user Administrator
User name                Administrator
Full Name                Administrator
Comment                  Administrator
User's comment            Administrator
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set        8/20/2024 10:15:45 AM
Password expires         Never
Password changeable      8/20/2024 10:15:45 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script             
User profile             
Home directory           
Last logon               9/4/2024 2:49:14 PM
Logon hours allowed      All
```

3. Run the following command to check whether the system has been restarted: **systeminfo**

After a host is restarted, data is automatically deleted. To query file directories, perform [Step 4](#).

```
C:\Users\Administrator>systeminfo

Host Name: ECS
OS Name: Microsoft Windows Server 2019 Standard
OS Version: 10.0.17763 N/A Build 17763
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows
Registered Organization:
Product ID: 0042
Original Install Date: 1/6/2022, 11:20:28 AM
System Boot Time: 9/4/2024, 2:48:25 PM
System Manufacturer: OpenStack Foundation
System Model: OpenStack Nova
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel®64 Family 6 Model 106 Stepping 6 GenuineIntel ~2800 Mhz
BIOS Version: SeaBIOS rel-1.12.1-0-ga5cab58-20230305_150410-szxrtsoc10000, 4/1/2014
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: zh-cn;Chinese (China)
Input Locale: zh-cn;Chinese (China)
Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Total Physical Memory: 4,095 MB
Available Physical Memory: 2,312 MB
Virtual Memory: Max Size: 4,255 MB
Virtual Memory: Available: 3,071 MB
Virtual Memory: In Use: 1,184 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\ECS-9808
Hotfix(s): 7 Hotfix(s) Installed.
[01]: KB5033904
[02]: KB4548947
[03]: KB4539208
[04]: KB5012170
[05]: KB5024127
```

Step 4 Check for abnormal files.

Run the following command: **dir /s *file_directory* (for example, C:) | findstr "exe"**

Query the **.exe** files and directories in a disk (for example, **C:**). Based on the query result, locate abnormal files that are not system files or application-created files. Lock abnormal files.

[illegible]

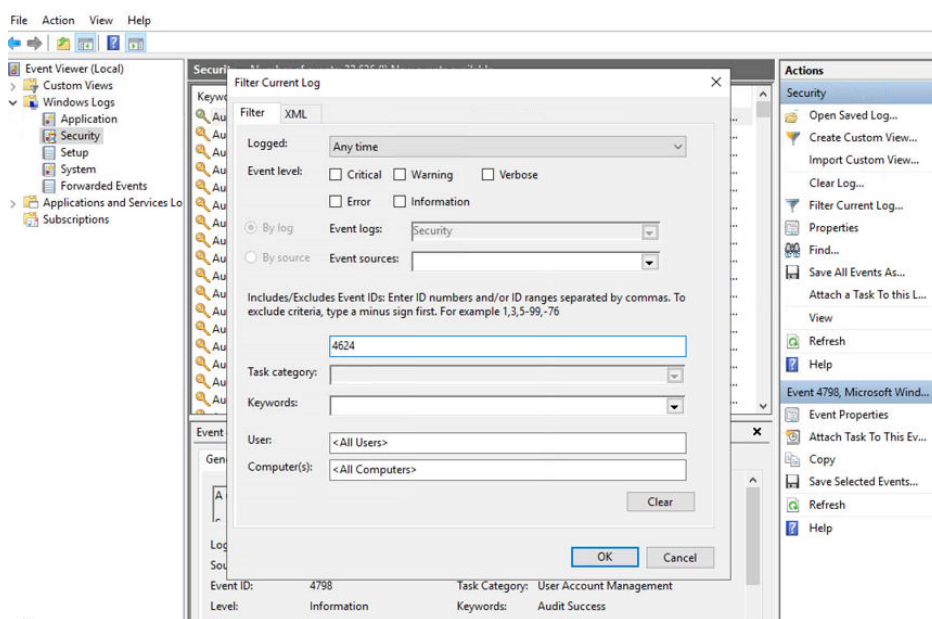
 NOTE

You are advised to check the following directories: **windows, windows\system32, windows/system32 \drivers, c:\program files\internet explorer/, c:\program files \internet explorer\plugin, and c:\program files\common files\microsoft shared.**

Step 5 View the Windows host login log (login success event ID: **4624**) to check for abnormal logins to the host.

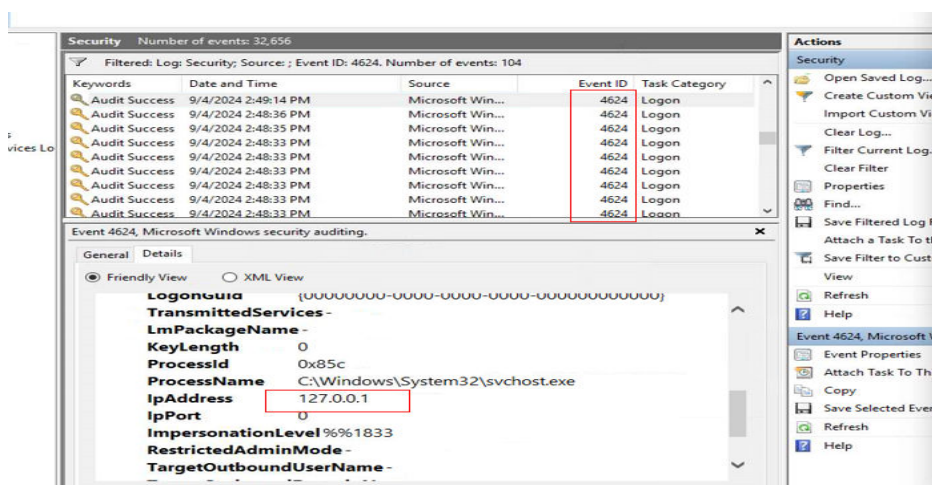
1. Open **Control Panel**, choose **Administrative Tools > Computer Management > System Tools > Event Viewer > Windows Logs > Security**, and click **Filter Current Log** on the right.
2. Enter **4624** in the **Includes/Excludes Event IDs** box.

Figure 5-11 Filtering current logs



3. The query results are displayed. See [Figure 5-12](#).

Figure 5-12 Viewing results



Step 6 If the problem persists, you can submit a service ticket.

----End

5.2.2.3 Security Hardening Suggestions for Windows Hosts

- Configure security groups and open only necessary ports to the public network. Protect the service web console ports and LAN internal communication ports from being exposed to the public network. Disable high-risk ports (**135**, **139**, and **445**) or allow limited source IP addresses to access the ports.
- Do not run applications using the administrator account. Disallow applications (such as webs) to use the database administrator account to interact with databases.

- Periodically back up service data remotely to prevent data loss caused by intrusions.
- Periodically detect security vulnerabilities in the system and software, update system security patches in a timely manner, and upgrade the software to the latest official version.
- Download and install the software from official channels. For the software downloaded from non-official channels, use antivirus software to scan it before running.
- Do not open suspicious email links or web page links.
- Do not use the default password or a weak password for the default account.
- Set OS system passwords (including administrators and common users) and database account passwords. Set strong passwords for the management account of the web application system. The passwords must contain at least 12 characters.
- To improve password strength,
 - Do not use empty passwords or default passwords.
 - Set a long and complex password.
 - Do not set duplicate consecutive characters (for example, AAAAAAAA) or a combination of repeated characters (for example, 123123).
 - Use complex combinations. For example, ensure that your password contains uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and special characters.
 - Do not use the name, date of birth, commemorative date, login name, email address, or words in the dictionary.
 - Do not use common acronyms or abbreviations, for example, **passwd**.
 - Change the password periodically.
 - Do not contain **Huawei** or adjacent characters on the keyboard, for example, **123qwe!@#** and **passwd**.

5.3 Host Security Check (Linux)

5.3.1 Troubleshooting Methods

You need to check both the users and applications of your Linux hosts.

- **Users:** Check processes and networks and view the users of the running processes. Check for abnormal files in the username directory under the **/home** directory, and check for abnormal logins and brute-force attacks.
- **Applications:** Check whether abnormal files exist in the directory of the application to which a process belongs.

5.3.2 Troubleshooting Process

This section describes how to troubleshoot security issues in a Linux host.

Procedure

Step 1 Check whether abnormal processes exist in the host.

Query command: **top**

Check whether abnormal processes exist based on the CPU usage and process names. For example, the CPU usage of the following suspicious process exceeds 100%:

```
top - 15:26:55 up 5 days, 21:08, 3 users, load average: 3.54, 3.36, 3.29
Tasks: 115 total, 1 running, 114 sleeping, 0 stopped, 0 zombie
%Cpu(s):100.0 us, 0.0 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3879812 total, 528792 free, 1769656 used, 1581364 buff/cache
KiB Swap: 524284 total, 208680 free, 315604 used. 1124856 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
 25267 oracle    20   0 824248 270772 3480 S 149.2   7.0   4540:04 logind
13493 oracle    20   0 315280 266712 1384 S  50.2   6.9   3728:28 [kthreaddi]
 2107 oracle    -2   0 1790412 1364 1168 S   0.3   0.0    9:19.83 oracle
 2120 oracle    20   0 1795020 27780 23392 S   0.3   0.7   13:02.99 oracle
33463 ssh      20   0 3533356 330630 5340 S   0.3   8.6   2:36:27 java
```

Step 2 Check the file directory based on the PID of the abnormal process.

Query command: **lsuf -p PID** (for example, 25267)

```
root@h [ ~ ]# lsuf -p25267
COMMAND  PID  USER  FD   TYPE    DEVICE  SIZE/OFF      NODE NAME
logind   25267 oracle cwd     DIR    253,1     4096   2498248 /home/oracle/.config
logind   25267 oracle rtd     DIR    253,1     4096         2 /
logind   25267 oracle txt     REG    253,1  7805520  2498251 /home/oracle/.config/logind
logind   25267 oracle mem     REG    253,1  109976  1836518 /usr/lib64/libresolv-2.17.so
logind   25267 oracle mem     REG    253,1   31344  1836506 /usr/lib64/libnss_dns-2.17.so
logind   25267 oracle mem     REG    253,1   61560  1836508 /usr/lib64/libnss_files-2.17.so
logind   25267 oracle mem     REG    253,1  2156344  1836490 /usr/lib64/libc-2.17.so
logind   25267 oracle mem     REG    253,1  1136944  1836498 /usr/lib64/libm-2.17.so
logind   25267 oracle mem     REG    253,1   19248  1836496 /usr/lib64/libdl-2.17.so
logind   25267 oracle mem     REG    253,1   43712  1836520 /usr/lib64/librt-2.17.so
logind   25267 oracle mem     REG    253,1  142144  1836516 /usr/lib64/libpthread-2.17.so
logind   25267 oracle mem     REG    253,1  163312  1844706 /usr/lib64/ld-2.17.so
logind   25267 oracle 0r      CHR     1,3        0t0    1031 /dev/null
logind   25267 oracle 1w      CHR     1,3        0t0    1031 /dev/null
logind   25267 oracle 2w      CHR     1,3        0t0    1031 /dev/null
logind   25267 oracle 3u      a_inode 0,10        0    6394 [eventpoll]
```

Step 3 Locate abnormal files, which are marked with **xmr** or **mine**.

1. View files: **ll -art**

```
[root@h7 .config]# ll -art
total 13676
-rwxrwxrwx 1 oracle oinstall      54 Jan  9  2002 start
-rwxrwxrwx 1 oracle oinstall 838583 Jun 15  2018 h64
-rwxr-xr-x 1 oracle oinstall    337 Feb 14  2020 go
-rwx--x--x 1 oracle oinstall 215960 Dec 19  2020 arm
-rwx--x--x 1 oracle oinstall 5092504 Dec 19  2020 xmrMiner
-rwxr-xr-x 1 oracle oinstall 7805520 Apr 28 13:30 login
-rwxrwxrwx 1 oracle oinstall    243 Apr 28 13:31 update
drwxr-xr-x 2 oracle oinstall    4096 Jun 25 00:25 .
-rwxrwxrwx 1 oracle oinstall    392 Jun 25 00:31 libs
-rw-r--r-- 1 oracle oinstall     21 Jun 27 11:59 dir.dir
-rw-r--r-- 1 oracle oinstall     51 Jun 27 11:59 cron.d
-rwxr--r-- 1 oracle oinstall    212 Jun 27 11:59 upd
-rwxr-xr-x 1 oracle oinstall      6 Jun 27 11:59 bash.pid
-rw-r--r-- 1 oracle oinstall   2771 Jun 27 11:59 config.json
drwx----- 5 oracle oinstall    4096 Jun 28 16:44 ..
[root@h7 .config]# pwd
/home/oracle/.config
[root@h7 .config]#
```

2. Query the Trojan path: **pwd**

Detect the file that contains abnormal addresses: **strings file_name** (for example, config.json) **|grep xmr**

```
[root@h7 .config]# pwd
/home/oracle/.config
[root@h7 .config]# strings config.json |grep xmr
"url": "xmr.flooder.org:80",
[root@h7 .config]# pwd
/home/oracle/.config
```

 NOTE

You are advised to check the following directories: **/etc** (configuration files), **/tmp** (temporary files), and **/bin** (executable files).

- In user commands, **/lib** refers to library files, **/etc** refers to configuration files, and **/sbin** refers to executable files.
- In management commands, **/lib** refers to library files, **/etc** refers to configuration files, **/usr/** refers to read-only files, and **shared read-only** and **/usr/local** refer to third-party software.

3. Check whether the URL (xmr.flooder.org:80) is a mining pool.

Step 4 View the permissions of the host user.

Query command: **cat /etc/passwd|grep username** (for example, **bash**)

```
dr-xr-xr-x.  2 root root      16384 Feb 26 12:38 .
[root@hecs-144007 sbin]# cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
csp:x:1000:1000:./home/csp:/bin/bash
oracle:x:1001:1001:./home/oracle:/bin/bash
```

 NOTE

The **nologin** user does not have the login permission. You are advised to check the users who have the login permission.

Step 5 Check the abnormal login records from the host login logs.

Query command: **cat file_name** (for example, **secure**) **|grep Acc|grep username** (for example, **oracle**)

Find the time that the host is usually logged in to from the success login logs, which may be the time when the Trojan is implanted.

```
[root@ ~]# cat secure*|grep Acc|grep oracle
Jun 27 11:44:52 l... sshd[24188]: Accepted password for oracle from 1... 13 port 34288 ssh2
Jun 27 11:59:06 / sshd[25220]: Accepted password for oracle from 1... port 42032 ssh2
Jun 28 16:43:53 h... 37 sshd[348]: Accepted password for oracle from 5:... 44 port 37048 ssh2
Jun 25 23:15:26 h... 7 sshd[13281]: Accepted password for oracle from 1... port 60690 ssh2
```

Based on the login time, check the login IP addresses and login frequency (including the number of successful or failed logins). If there are a large number of abnormal IP address logs, brute-force attacks may have taken place.

```
Jun 25 23:15:00 hcs-14400 sshd[13235]: Failed password for root from 1... port 59376 ssh2
Jun 25 23:15:00 7 sshd[13235]: Connection closed by 1.15... port 59376 [preauth]
Jun 25 23:15:01 7 sshd[13239]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:03 7 sshd[13239]: Failed password for root from 1... port 59464 ssh2
Jun 25 23:15:03 7 sshd[13239]: Connection closed by 1.15... port 59464 [preauth]
Jun 25 23:15:03 7 sshd[13243]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:04 7 sshd[13243]: Failed password for root from 1... port 59552 ssh2
Jun 25 23:15:04 7 sshd[13243]: Connection closed by 1.15... port 59552 [preauth]
Jun 25 23:15:04 7 sshd[13246]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:06 7 sshd[13246]: Failed password for root from 1... port 59616 ssh2
Jun 25 23:15:06 7 sshd[13246]: Connection closed by 1.15... port 59616 [preauth]
Jun 25 23:15:06 7 sshd[13250]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:09 7 sshd[13250]: Failed password for root from 1... port 59698 ssh2
Jun 25 23:15:09 7 sshd[13250]: Connection closed by 1.15... port 59698 [preauth]
Jun 25 23:15:09 7 sshd[13254]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:11 7 sshd[13254]: Failed password for root from 1... port 59778 ssh2
Jun 25 23:15:11 7 sshd[13254]: Connection closed by 1.15... port 59778 [preauth]
Jun 25 23:15:12 7 sshd[13258]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:14 7 sshd[13258]: Failed password for root from 1... port 59958 ssh2
Jun 25 23:15:14 7 sshd[13258]: Connection closed by 1.15... port 59958 [preauth]
Jun 25 23:15:14 7 sshd[13262]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:16 7 sshd[13262]: Failed password for root from 1... port 60218 ssh2
Jun 25 23:15:16 7 sshd[13262]: Connection closed by 1.15... port 60218 [preauth]
Jun 25 23:15:16 7 sshd[13265]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:18 7 sshd[13265]: Failed password for root from 1... port 60342 ssh2
Jun 25 23:15:18 7 sshd[13265]: Connection closed by 1.15... port 60342 [preauth]
Jun 25 23:15:18 7 sshd[13269]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:20 7 sshd[13269]: Failed password for root from 1... port 60414 ssh2
Jun 25 23:15:20 7 sshd[13269]: Connection closed by 1.15... port 60414 [preauth]
Jun 25 23:15:20 7 sshd[13273]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:23 7 sshd[13273]: Failed password for root from 1... port 60496 ssh2
Jun 25 23:15:23 7 sshd[13273]: Connection closed by 1.15... port 60496 [preauth]
Jun 25 23:15:23 7 sshd[13277]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1... 3 us
Jun 25 23:15:25 7 sshd[13277]: Failed password for root from 1... port 60606 ssh2
Jun 25 23:15:25 7 sshd[13277]: Connection closed by 1.1... port 60606 [preauth]
Jun 25 23:15:26 7 sshd[13281]: Accepted password for oracle from 1... port 60690 ssh2
```

Step 6 If the problem persists, you can submit a service ticket.

----End

5.3.3 Security Hardening Suggestions for Linux Hosts

- Set OS system passwords (including administrators and common users) and database account passwords. Set strong passwords for the management account of the web application system. The passwords must contain at least 12 characters.
- Set the host login mode to key login.
- Do not run applications using the administrator account. Disallow applications (such as webs) to use the database administrator account to interact with databases. Open only necessary ports to the public network. Do not allow public network access to service web console ports and LAN internal communication ports. Disable high-risk ports (such as the SSH port),

allow limited source IP addresses to access the ports, or use the O&M stream established by VPNs or bastion hosts.

- Periodically back up service data remotely to prevent data loss caused by intrusions.
- Periodically detect security vulnerabilities in the system and software, update system security patches in a timely manner, and upgrade the software to the latest official version.
- Download and install the software from official channels. For the software downloaded from non-official channels, use antivirus software to scan it before running.
- You are advised to use HSS to thoroughly detect the potential security risks of your hosts and applications.

For details about HSS, visit <https://www.huaweicloud.com/intl/en-us/product/hss.html>.