SecurityInfo

Best Practices

Issue	02
Date	2024-09-26

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

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	**Go to the Security Settings page**. Select **Critical Operations** > **Login Protection**, click **Enable**. In the displayed pane, select **Enable**.

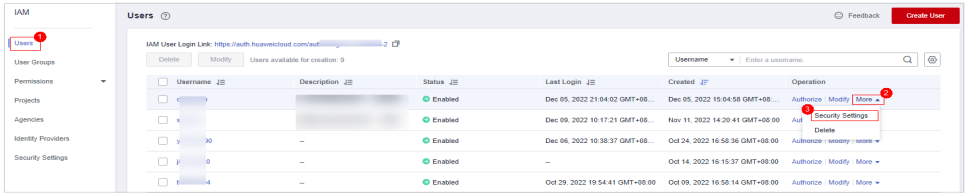
NOTE

- 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.

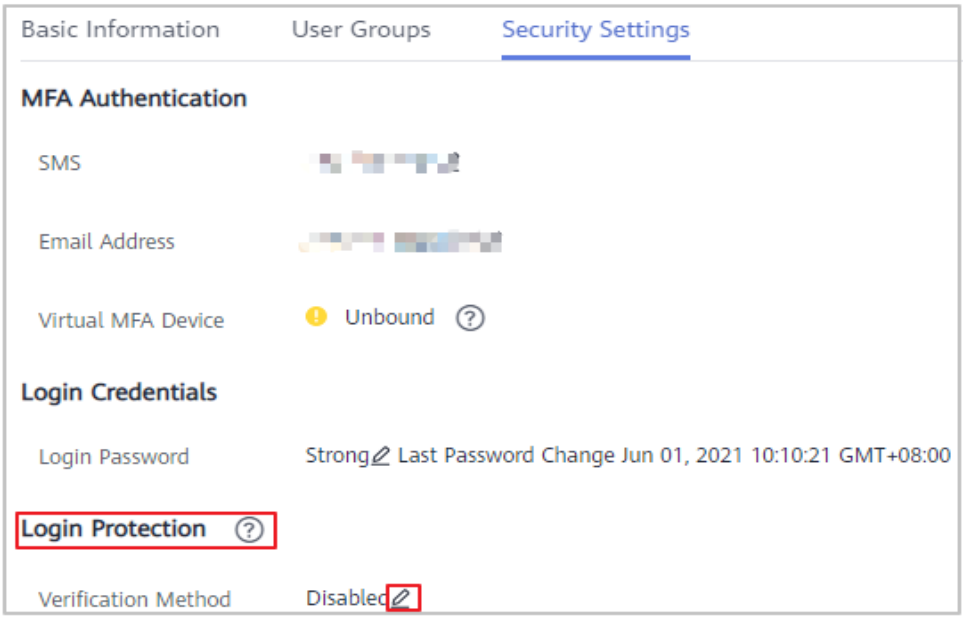
1. Choose **Identity and Access Management** > **Users** and click **Security Settings** in the row where an IAM user resides.

Figure 1-1 Users



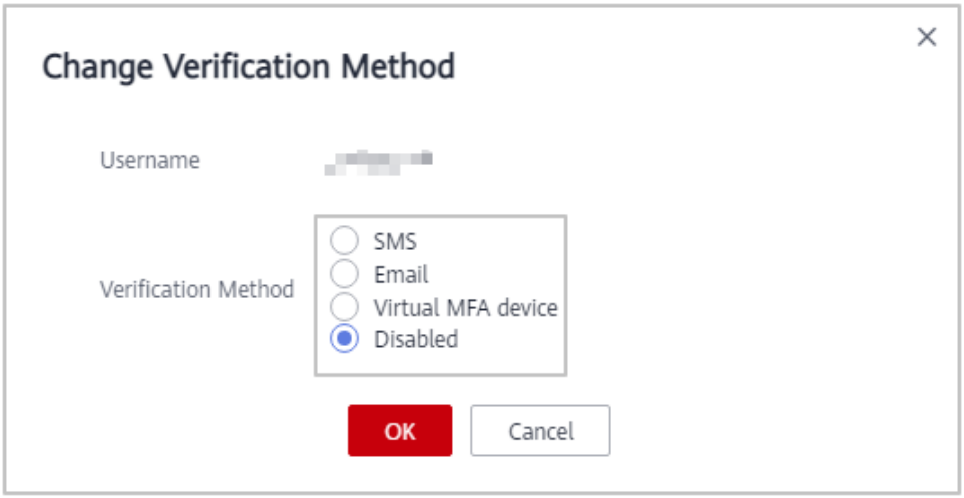
2. Click in the **Login Protection** area.

Figure 1-2 Security Settings



3. 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

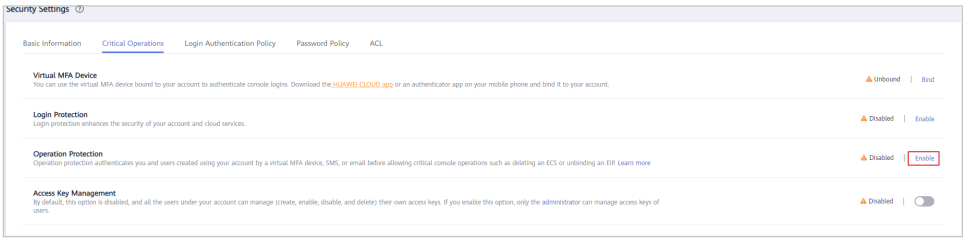
Enabling Critical Operation Protection

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 **Go to the Security Settings page** as the administrator.

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

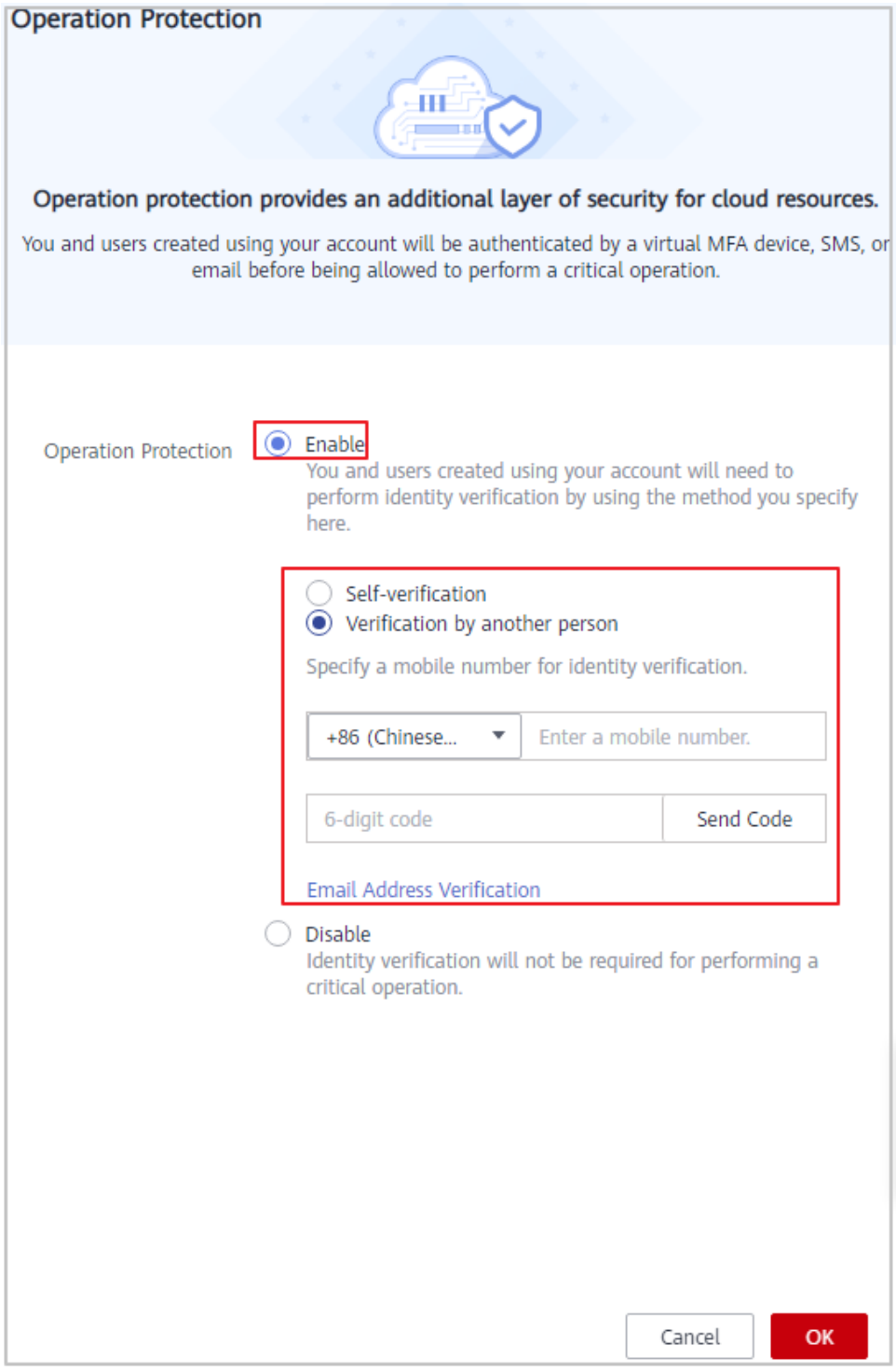
Figure 1-4 Critical Operations



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



Step 4 Click **OK**.

----End

Configuring a Login Authentication Policy

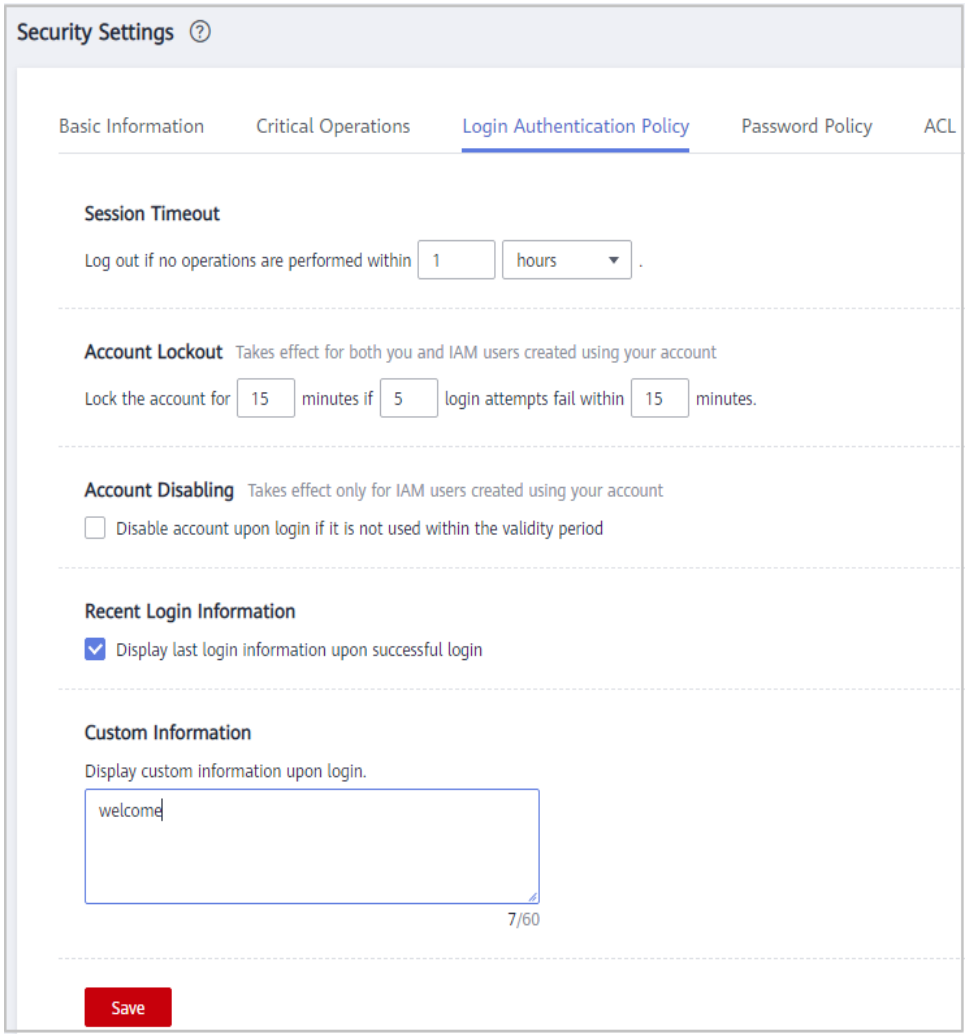
A login authentication policy includes many aspects of account security, including session timeout, account lockout, recent login information, and custom login

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 **Go to the Security Settings page** as the administrator.

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

Figure 1-6 Login Authentication Policy



NOTE

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

----End

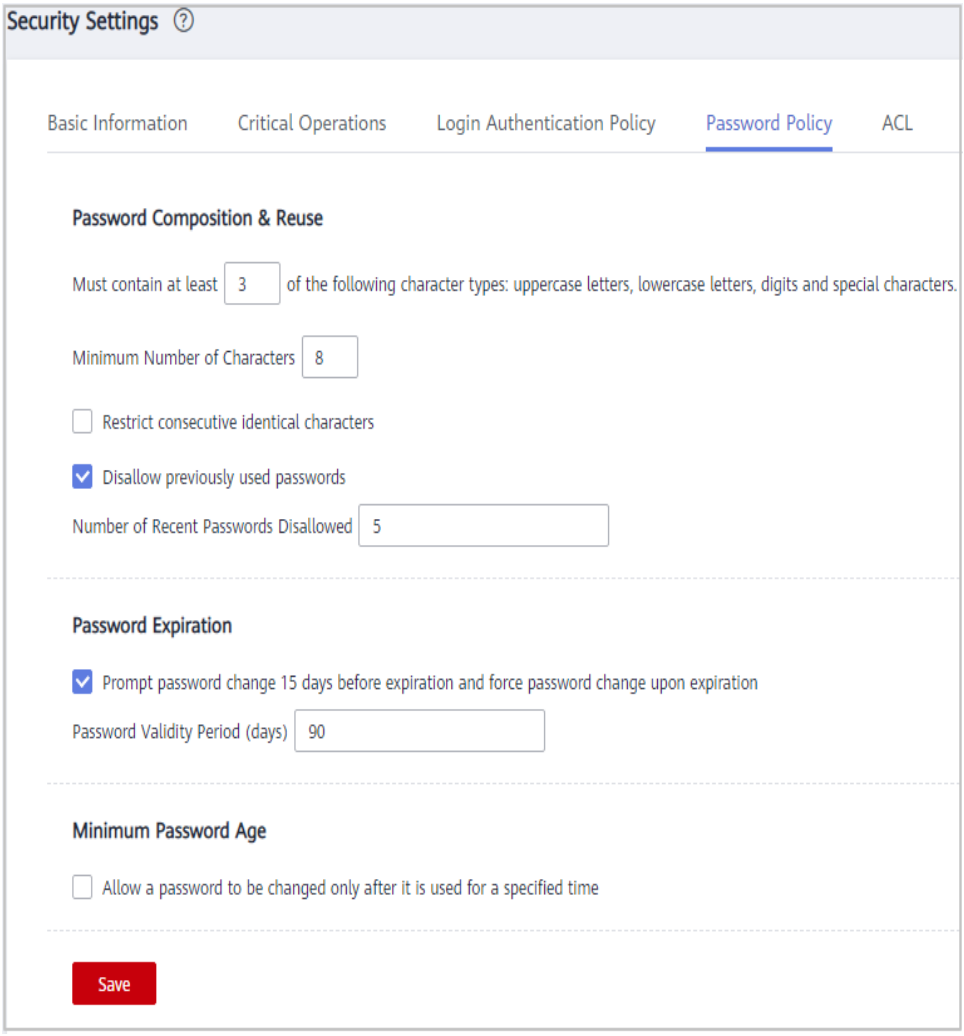
Configuring Password Policies

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 **Go to the Security Settings page** as the administrator.

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

Figure 1-7 Password Policy



----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.

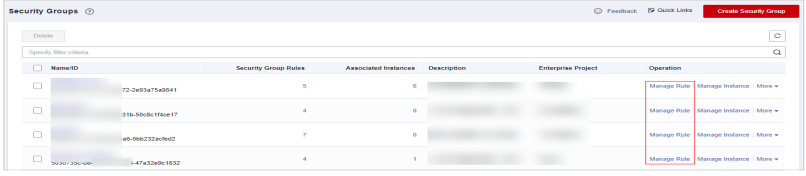
Step 1 Go to the **Security Groups** page.

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

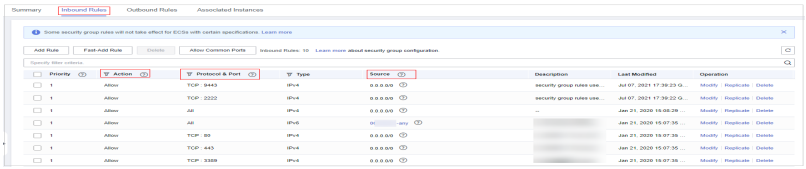


Table 2-1 High-risk ports

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

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**.

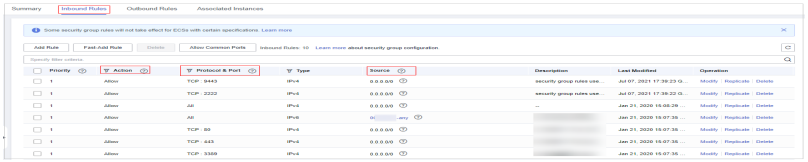
Step 4 Check all the network ACLs that are enabled and associated with subnets. Delete high-risk port policies from the inbound rules.

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

Figure 2-4 Network ACL page

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 2-5 Checking network ACL policies



3. 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

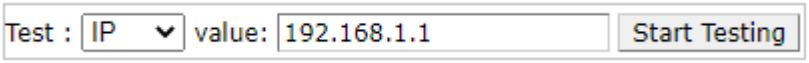
Using resources on Huawei Cloud to send spam email violates **Huawei Cloud User Agreement** and other related laws and regulations. IP addresses that are used to send out spam email in bulk will be recorded in the blocklist by the international anti-spam organization. IP addresses in the blocklist cannot 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 servery 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 unfroze in any cases. Bind a new IP address to the server.

4 UDP-based Amplification Attack Check

4.1 Overview

What Are DDoS Attacks

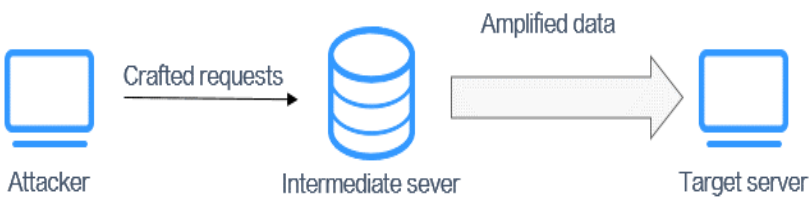
DoS (Denial of Service) attacks are also called flood attacks. They are intended to exhaust the network or system resources on the target computer, causing service interruption or suspension. Consequently, legitimate users fail to access network services. A DDoS attack involves multiple compromised computers 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 sever.

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 -anput

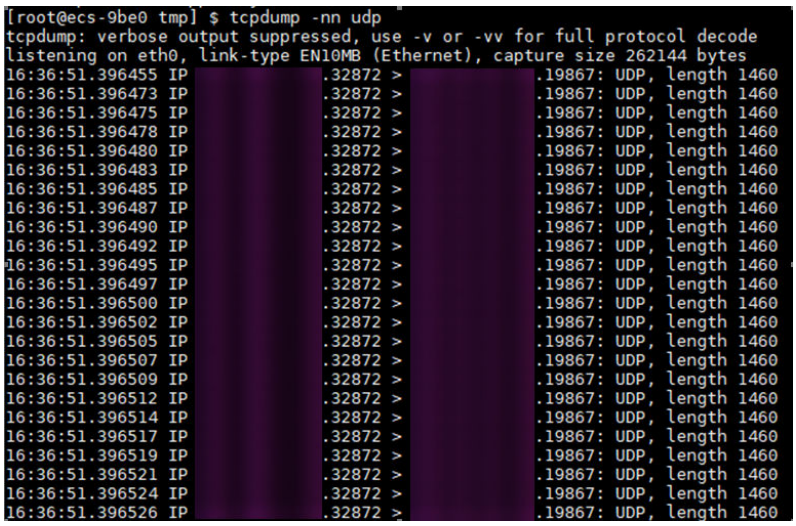
   You are advised to run the **netstat -anpt** command to check whether the current network connections and processes are normal. If the current connections and processes have been stopped or hidden, you can use the tcpdump packet capture tool to capture packets for analysis.

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

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

      nohup tcpdump -nn udp -c 1000000 -w /home/udp.pcap &

   b. Run the following command to analyze the captured packet information. Figure 4-3 shows the analysis result.

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

Figure 4-3 Captured packet analysis result

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?

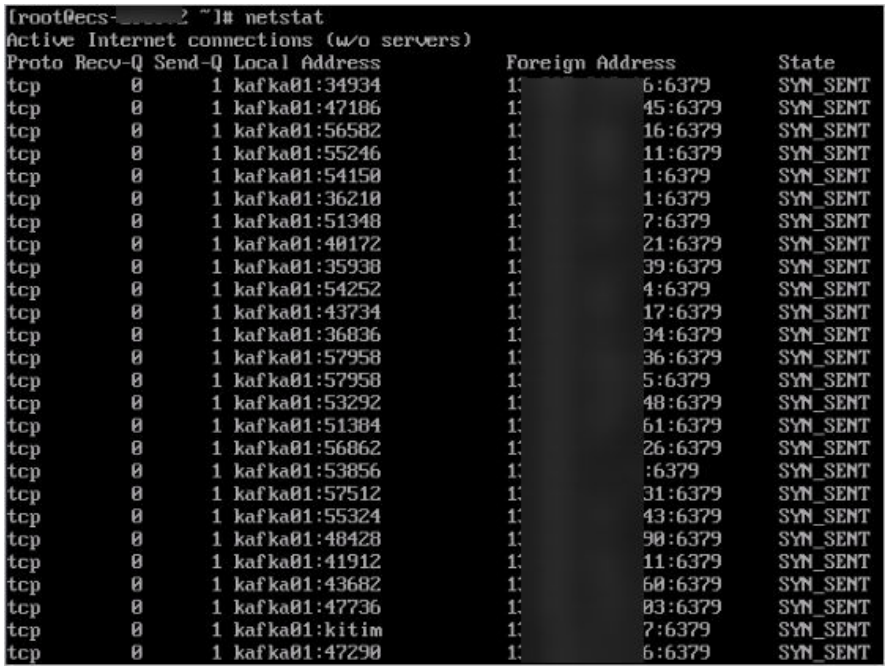
In a port scan attack, an attacker sends a request to the IP address of a target server or workstation to discover open ports, and exploit vulnerabilities through the port to launch attacks.

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



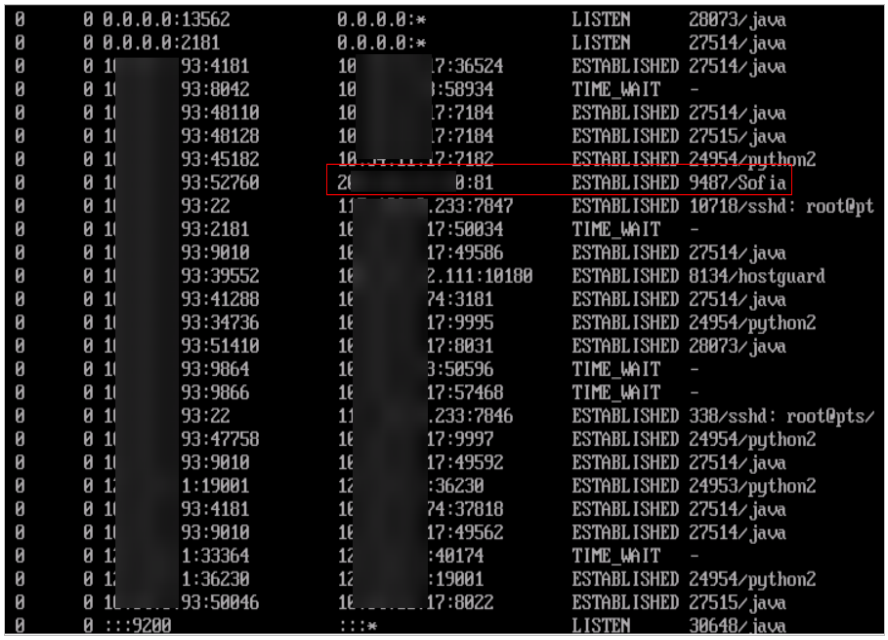
```
[root@ecs-      2 ~]# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      1 kafka01:34934           1          6:6379       SYN_SENT
tcp        0      1 kafka01:47186           1         45:6379       SYN_SENT
tcp        0      1 kafka01:56582           1         16:6379       SYN_SENT
tcp        0      1 kafka01:55246           1         11:6379       SYN_SENT
tcp        0      1 kafka01:54150           1          1:6379       SYN_SENT
tcp        0      1 kafka01:36210           1          1:6379       SYN_SENT
tcp        0      1 kafka01:51348           1          7:6379       SYN_SENT
tcp        0      1 kafka01:40172           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 kafka01:36036           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         90:6379       SYN_SENT
tcp        0      1 kafka01:41912           1         11:6379       SYN_SENT
tcp        0      1 kafka01:43682           1         60:6379       SYN_SENT
tcp        0      1 kafka01:47736           1         03:6379       SYN_SENT
tcp        0      1 kafka01:kitim           1          7:6379       SYN_SENT
tcp        0      1 kafka01:47290           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      28073/java
0      0 0.0.0.0:2181            0.0.0.0:*               LISTEN      27514/java
0      0 1          93:4181      10          7:36524     ESTABLISHED 27514/java
0      0 1          93:8042      10          :58934      TIME_WAIT   -
0      0 1          93:48110     10          7:7184      ESTABLISHED 27514/java
0      0 1          93:48128     10          7:7184      ESTABLISHED 27515/java
0      0 1          93:45182     10          7:7182      ESTABLISHED 24954/python2
0      0 1          93:52760     2           0:81        ESTABLISHED 9487/Sofia
0      0 1          93:22        1           .233:7847   ESTABLISHED 10718/sshd: root@pt
0      0 1          93:2181      1           17:50034    TIME_WAIT   -
0      0 1          93:9010      1           17:49586    ESTABLISHED 27514/java
0      0 1          93:39552     1           2.111:10180 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           17:8031     ESTABLISHED 28073/java
0      0 1          93:9864      1           3:50596     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          93:9010      1           17:49592    ESTABLISHED 27514/java
0      0 1          1:19001      1           :36230      ESTABLISHED 24953/python2
0      0 1          93:4181      1           74:37818    ESTABLISHED 27514/java
0      0 1          93:9010      1           17:49562    ESTABLISHED 27514/java
0      0 1          1:33364      1           :40174      TIME_WAIT   -
0      0 1          1:36230      1           :19001      ESTABLISHED 24954/python2
0      0 1          93:50046     1           17:8022     ESTABLISHED 27515/java
0      0 :::9200                 :::*                    LISTEN      30648/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
```

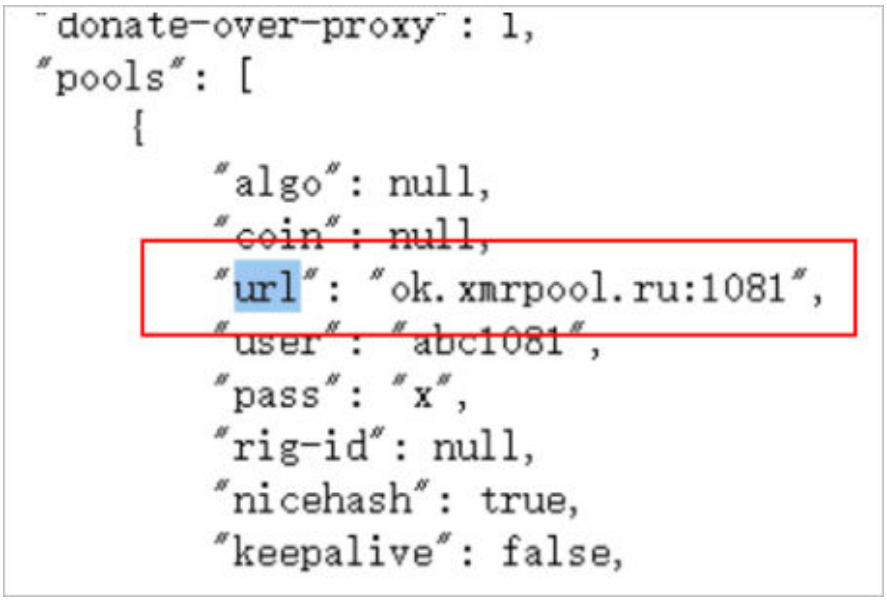
  b. Analyze the file. A mining pool is detected. Verify that the URL is a malicious mining pool address.

- 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.



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.

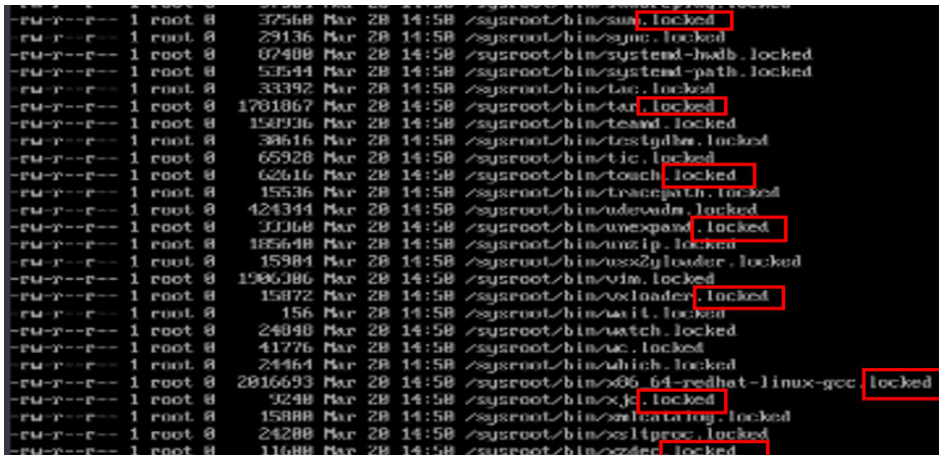
Ransomware interrupts businesses and can cause serious economic losses. We need to know how it works and how we can prevent it.

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.

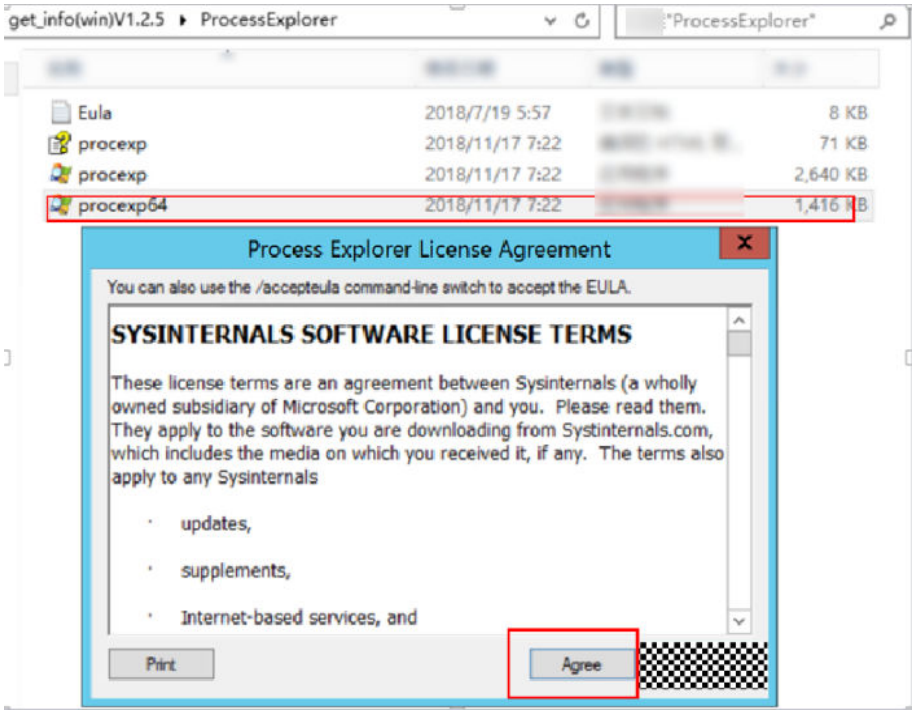
Prerequisites

You have downloaded **Process Explorer**.

Procedure

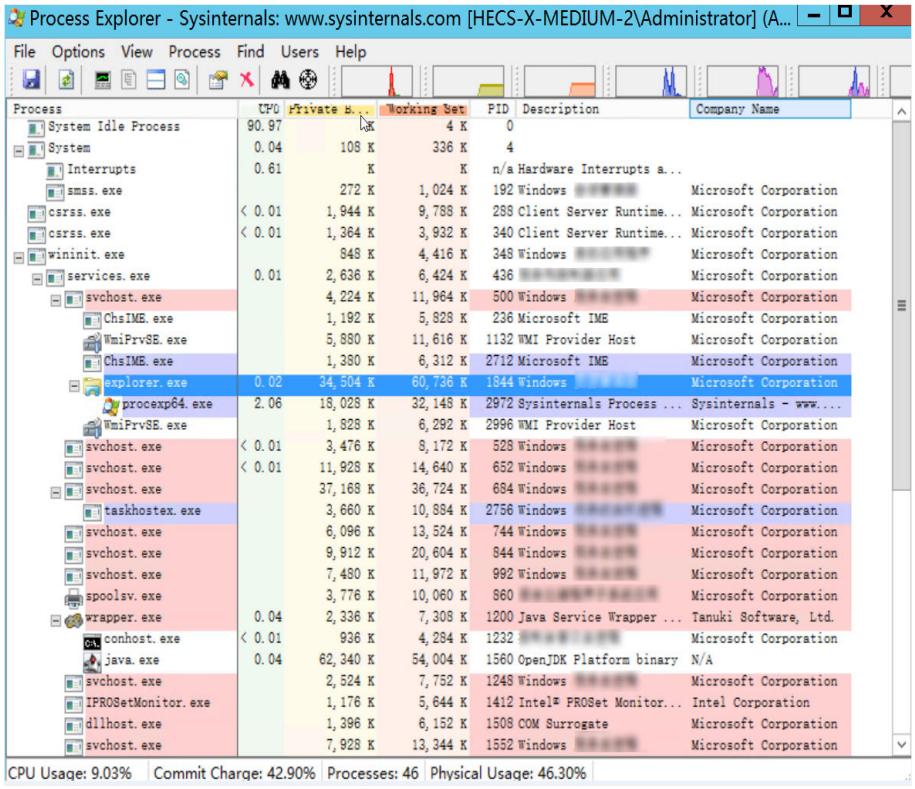
Step 1 Open the **ProcessExplorer** folder and double-click the **procexp64.exe** file.

Figure 5-3 processExplorer



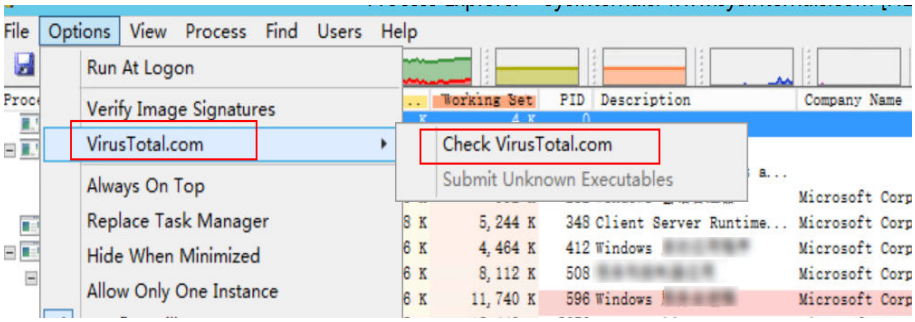
Step 2 In the dialog box that is displayed, click **Agree** to view the process information and check the processes online.

Figure 5-4 Viewing the current process



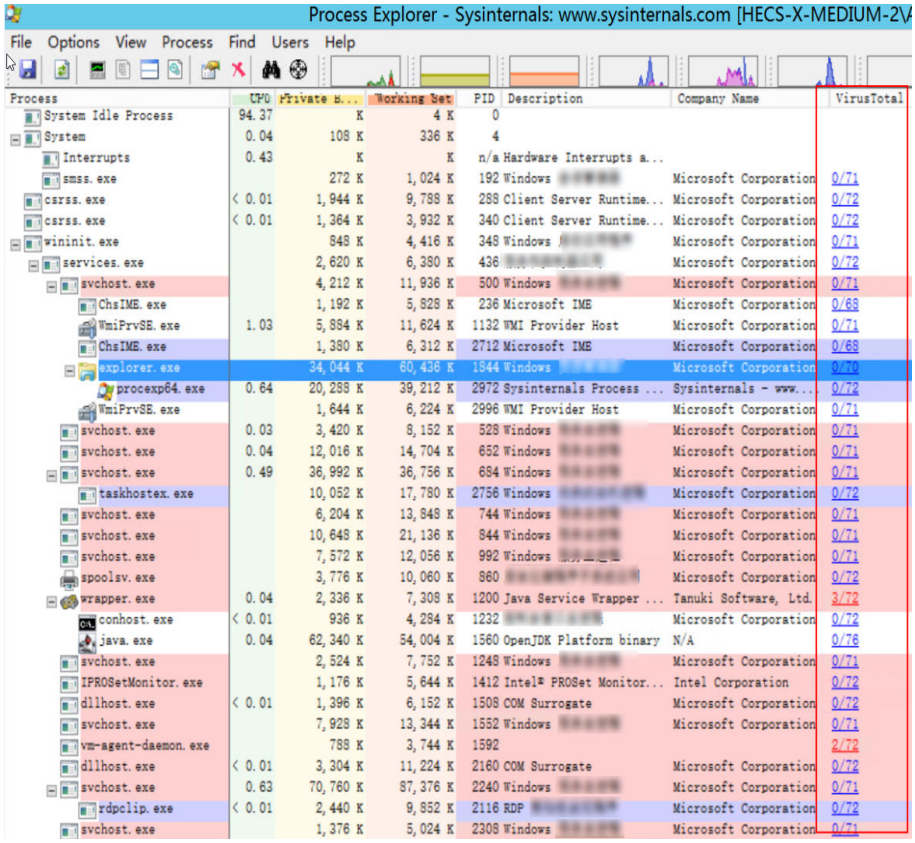
Step 3 On the menu bar, choose **Options** > **VirusTotal.com**, and select **Check VirusTotal.com** and **Submit Unknown Executables**.

Figure 5-5 options > VirusTotal.com



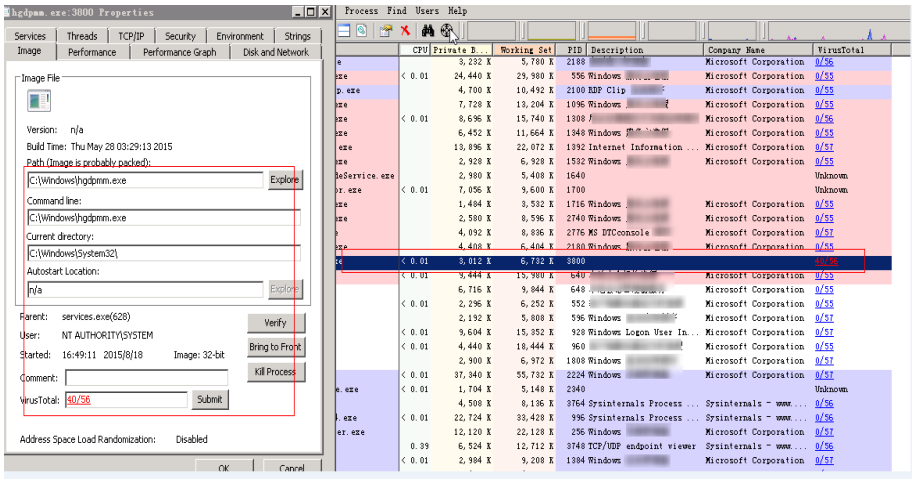
The system compares the hash values of the current processes with that in the **VirusTotal** database to quickly detect Trojans.

Figure 5-6 Process Explore-Sysinternals



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.

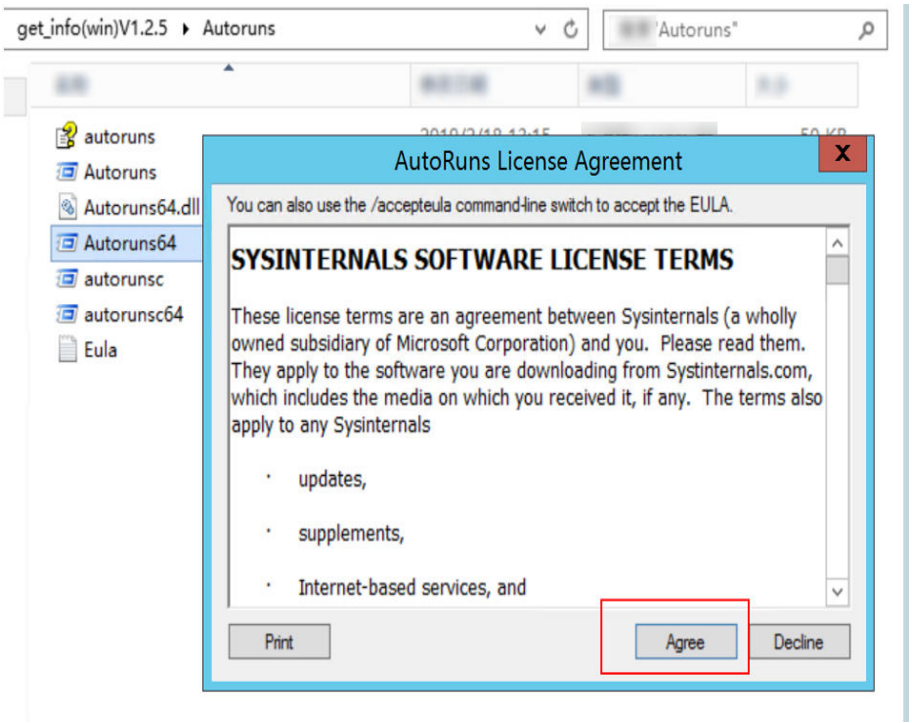
Prerequisites

You have downloaded **Autoruns**.

Procedure

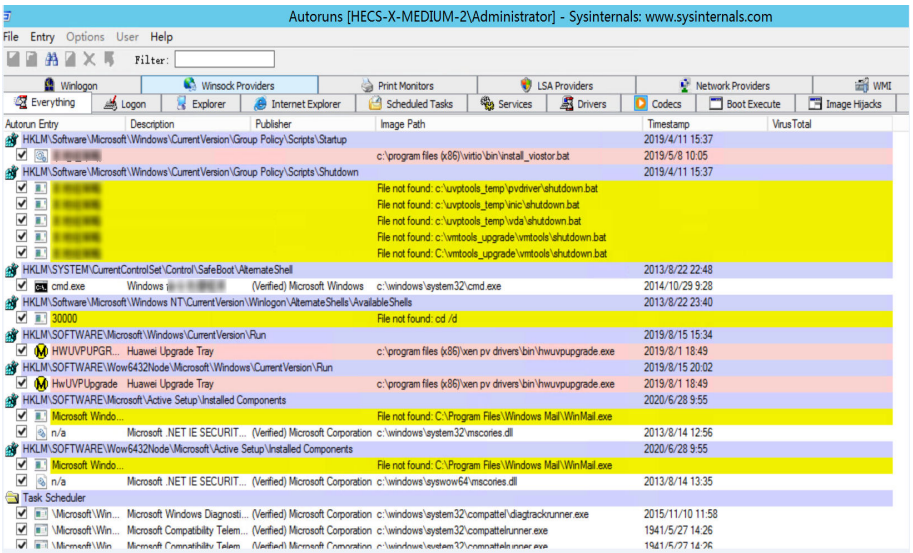
Step 1 Open the **Autoruns** folder and double-click the **Autoruns.exe** file.

Figure 5-8 Opening the AutoRuns folder

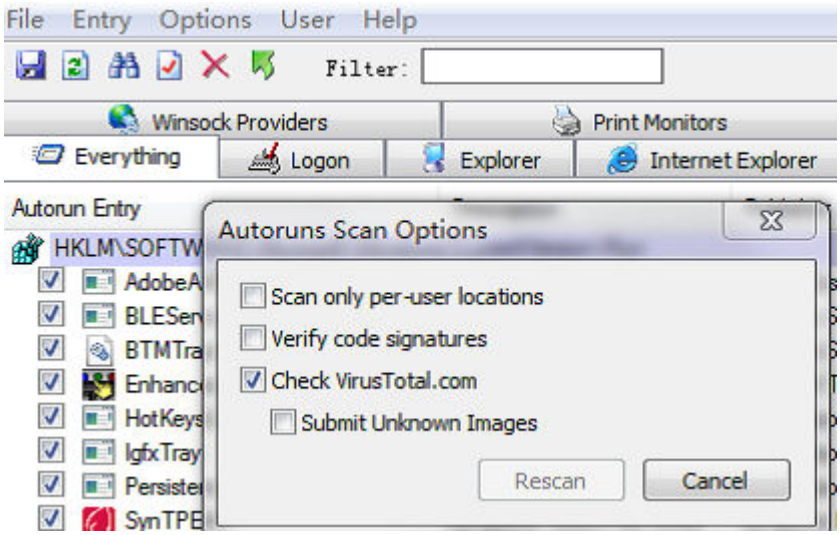


Step 2 In the displayed dialog box, click **Agree**.

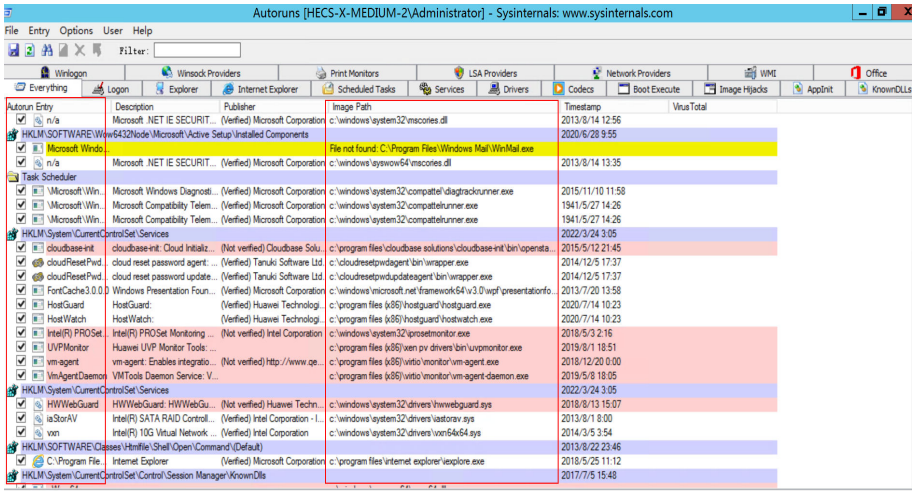
Figure 5-9 AutoRuns



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

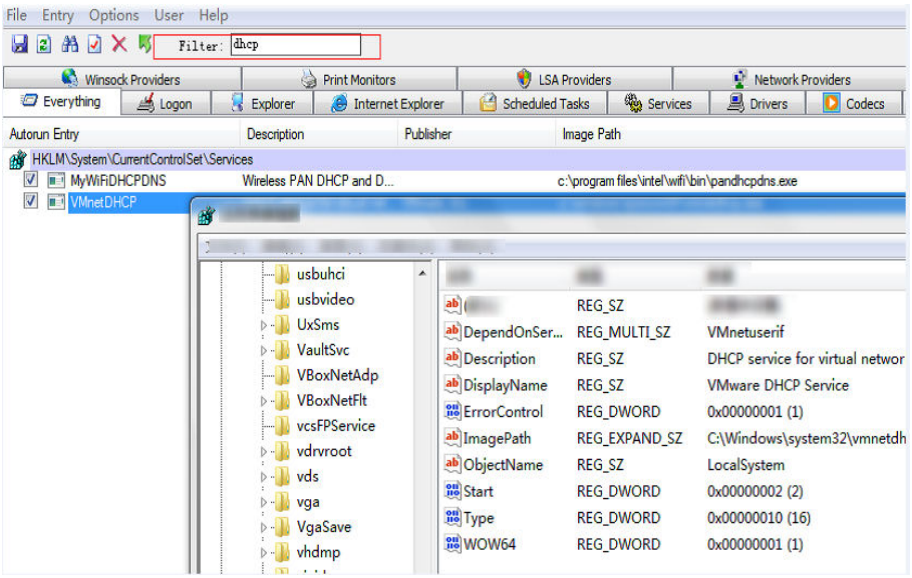


Step 4 Check whether abnormal files (not created for system or normal service deployment) exist in the **Autorun** and **Images Path** columns.



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

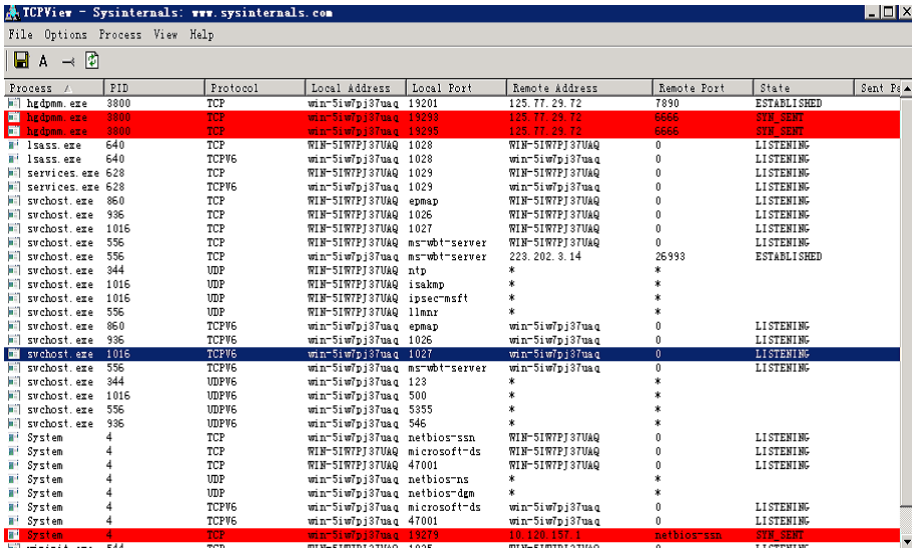
This section describes how to use **TCPView** to view the current TCP connection status and detect suspicious processes. Suspicious processes are highlighted in red.

Prerequisites

You have downloaded the **TCPView** tool.

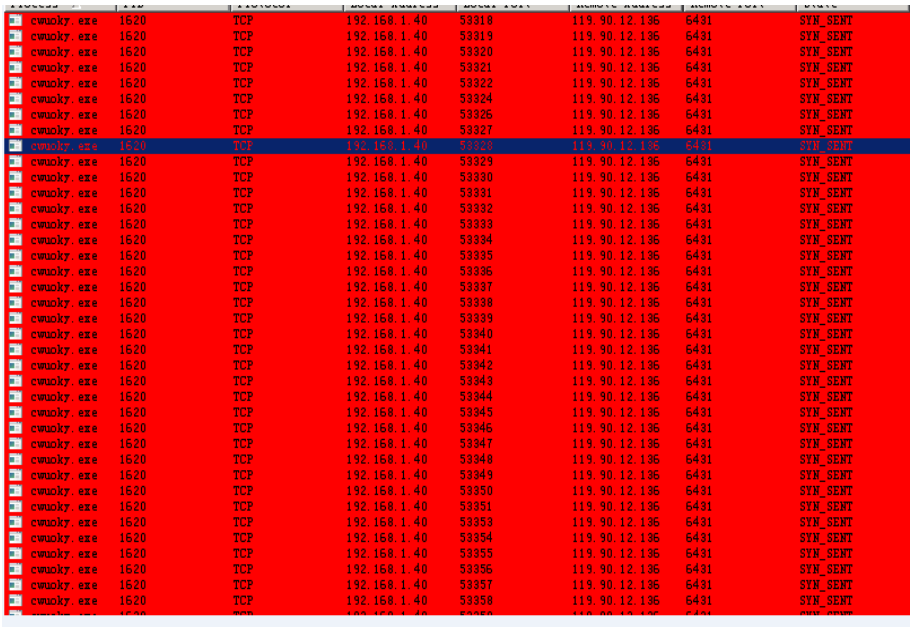
Procedure

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.



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

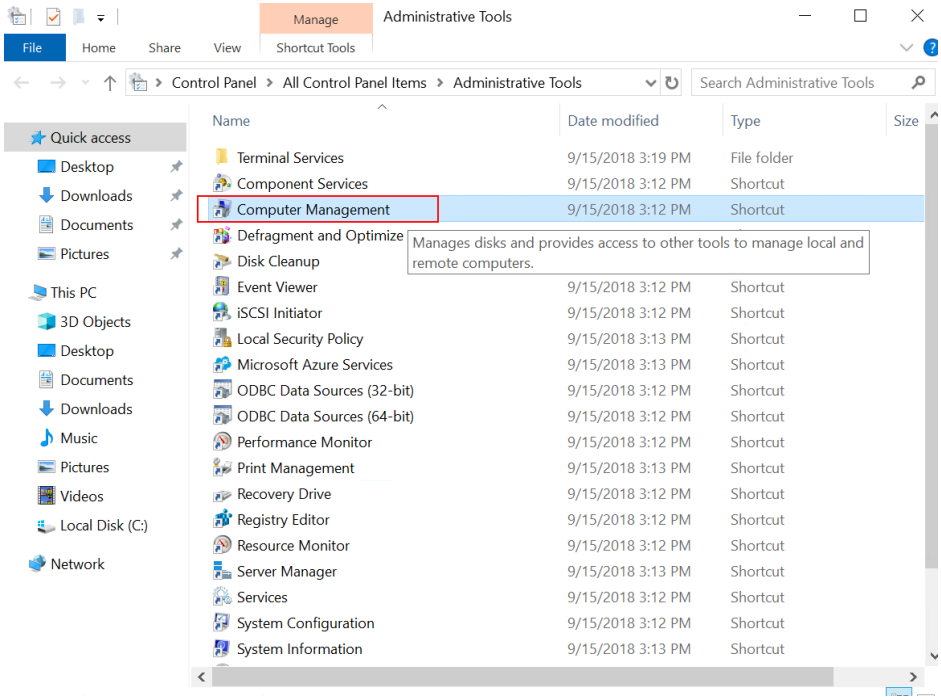
----End

5.2.2.1.4 Step 4: Detecting Abnormal Users

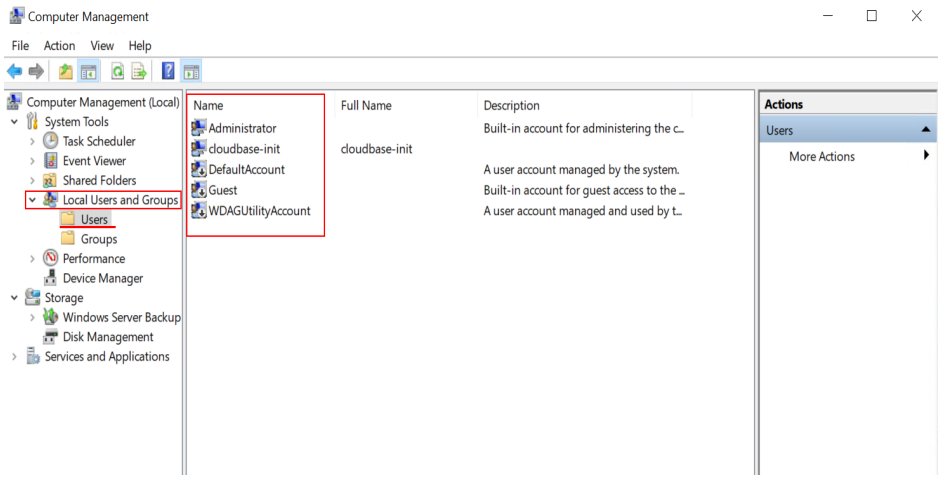
This section describes how to detect abnormal users.

Procedure

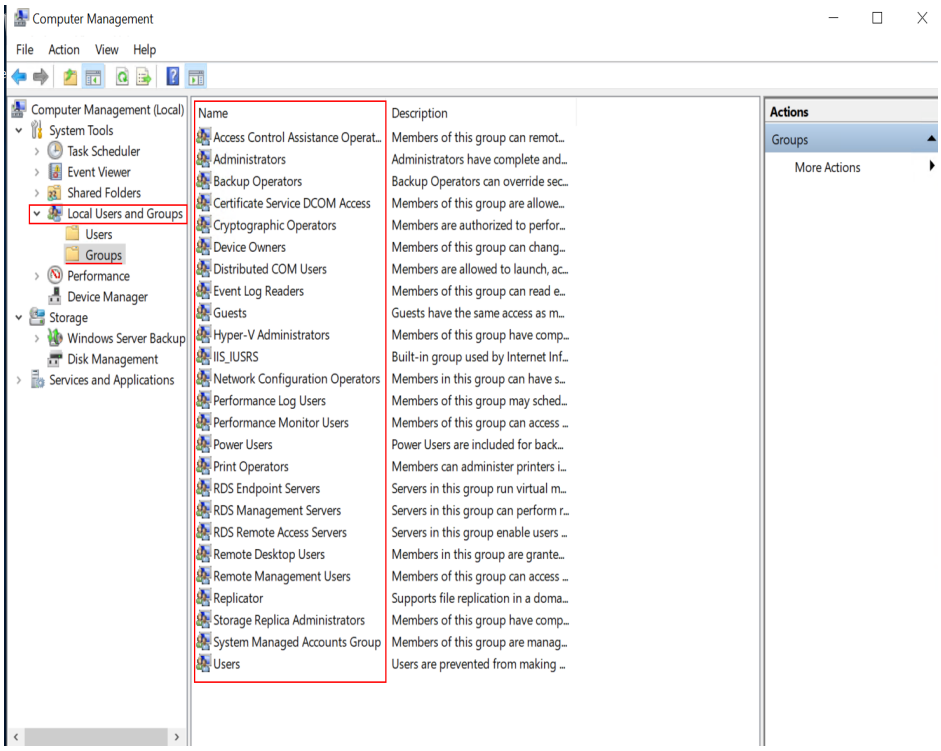
Step 1 Choose **Control Panel** > **Administrative Tools** > **Computer Management**.



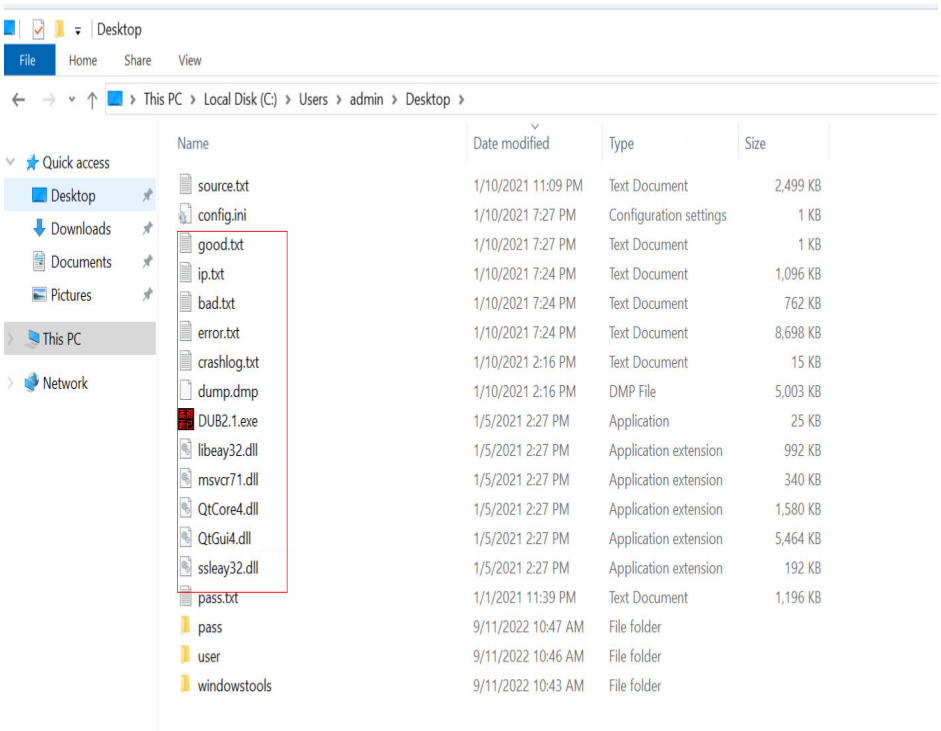
Step 2 In the navigation pane on the left, choose **Local Users and Groups** > **Users** to check whether abnormal users exist in the host.



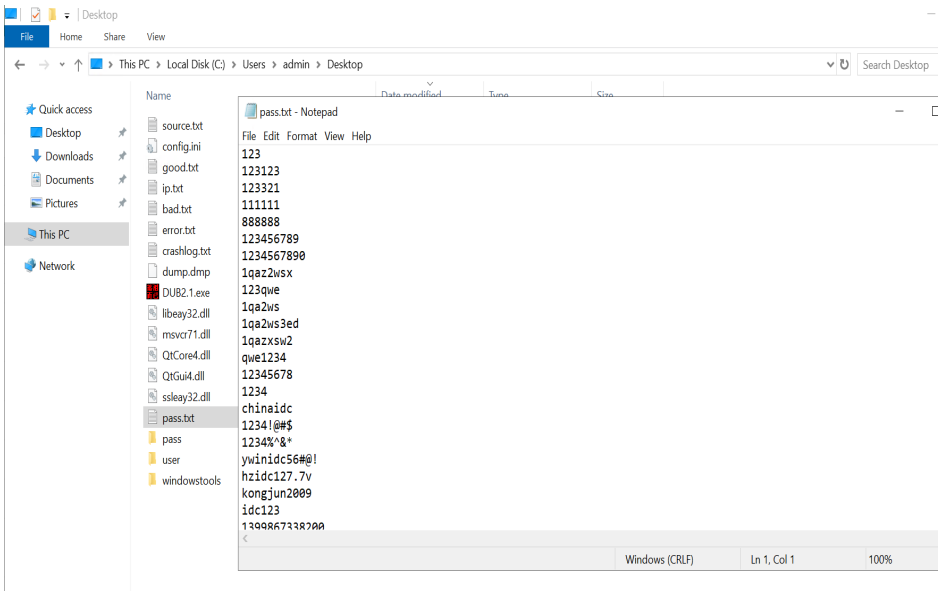
Step 3 In the navigation pane on the left, choose **Local Users and Groups** > **Groups** to check whether abnormal groups exist in the host.



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.



----End

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

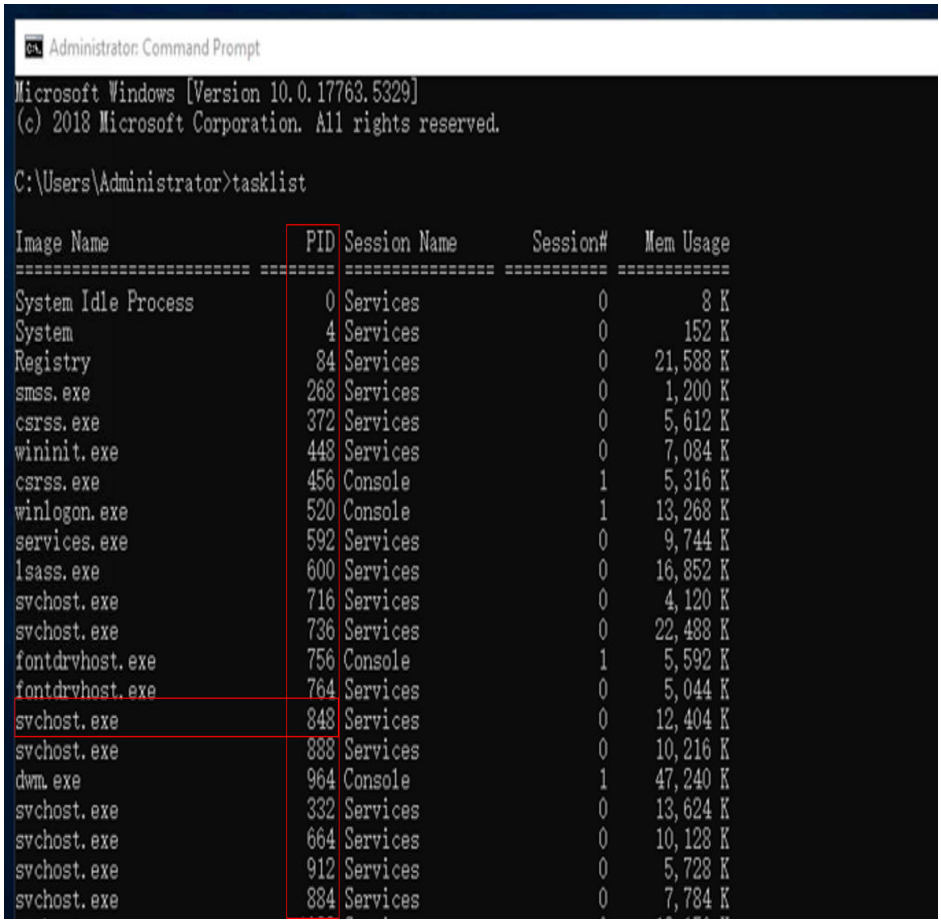
Command	Description
cd	Switch to the following directory: • Current directory: [./] It can be omitted. • One level up: [../] • Two levels up: [../../]
dir /a: (disk)	Display all files (including system files and hidden files) by default.
more	Display file contents in the split-screen mode.
tasklist	Check 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**

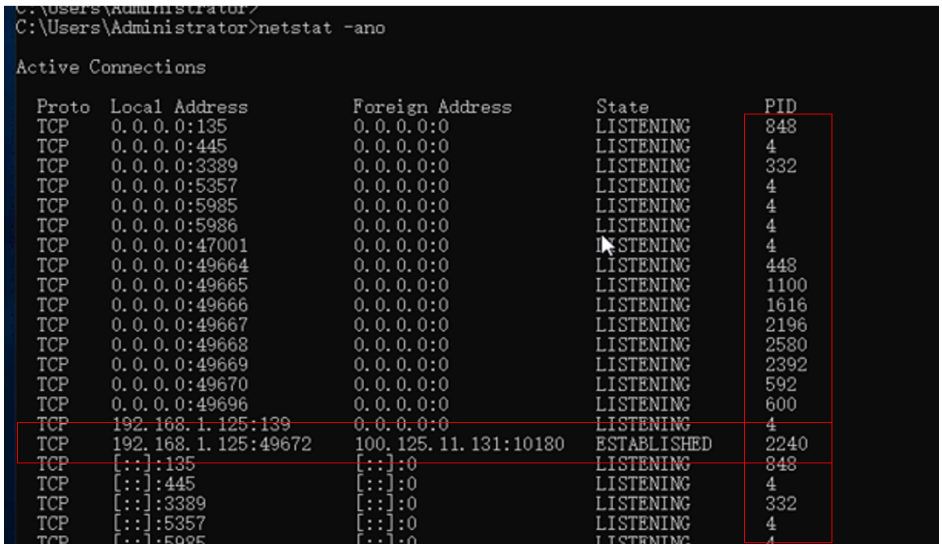
Based on the query result, locate abnormal processes that are neither system processes nor service application processes.



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

Query command: **netstat –ano**

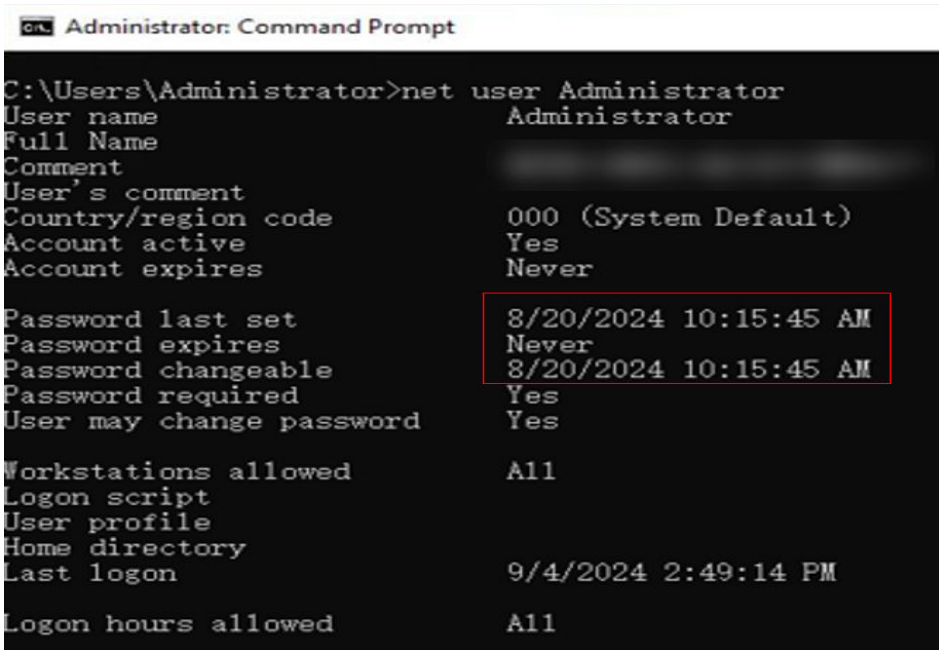
1. Based on the query result, locate the suspicious addresses that are neither service connection ports nor external addresses used for service connections.
2. Check whether the suspicious address is an international address of malicious or abnormal services.
3. Locate the target process (for example,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



Step 3 Check for abnormal users.

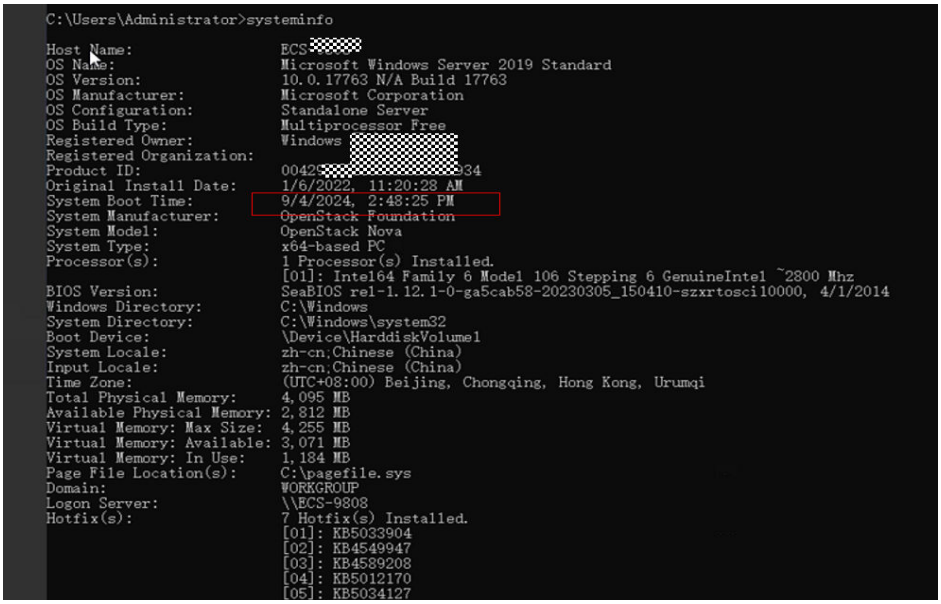
1. Run the following command: **net user**

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



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**.



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.

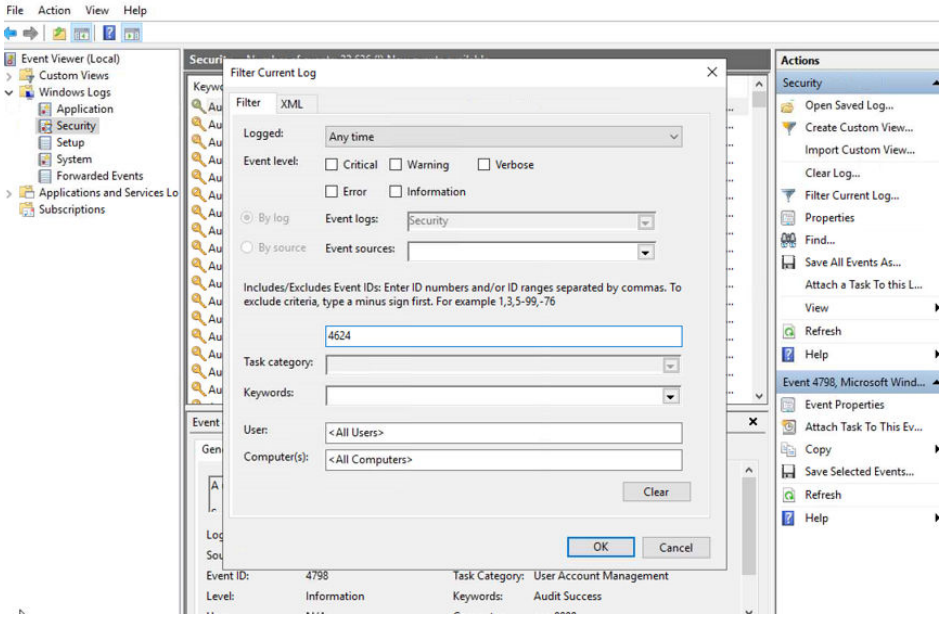
NOTE

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.

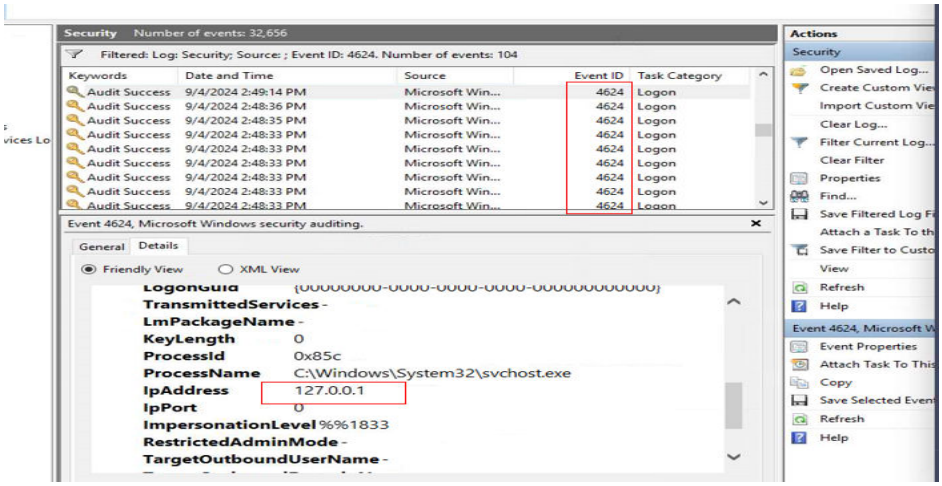
1. Open **Control Panel**, choose **Administrative Tools** > **Computer Management** > **System Tools** > **Event Viewer** > **Windows Logs** > **Security**, and click **Filter Current Log** on the right.
2. Enter **4624** in the **Includes/Excludes Event IDs** box.

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

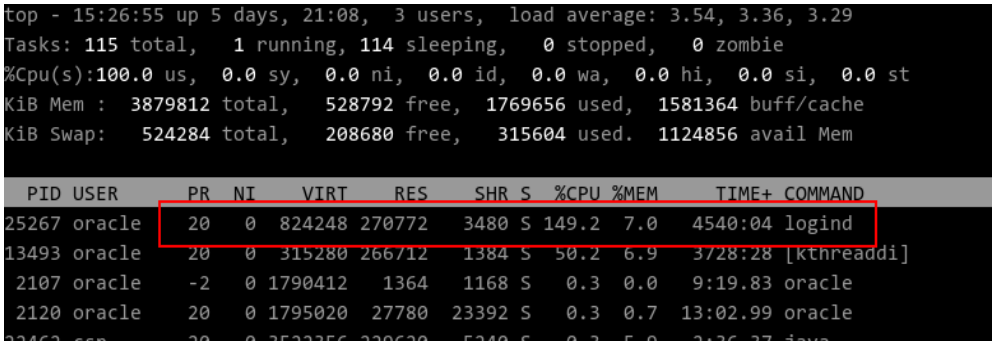
This section describes how to troubleshoot security issues in a Linux host.

Procedure

Step 1 Check whether abnormal processes exist in the host.

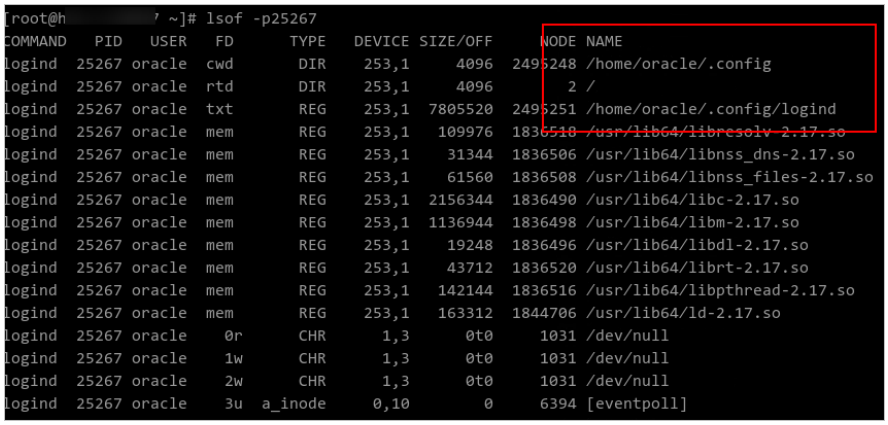
Query command: **top**

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%:



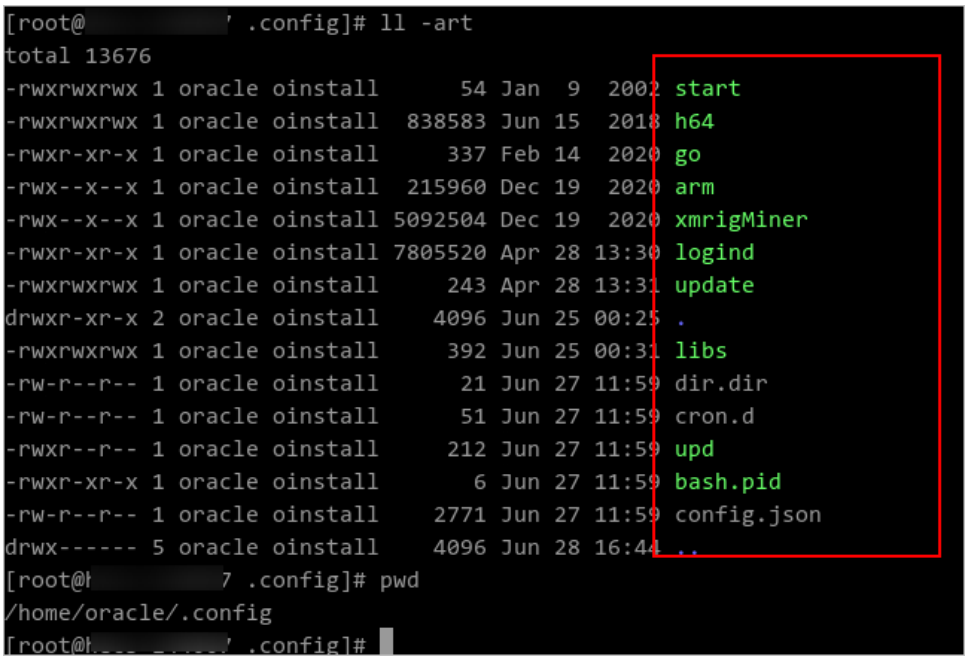
Step 2 Check the file directory based on the PID of the abnormal process.

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



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

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



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

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

   NOTE

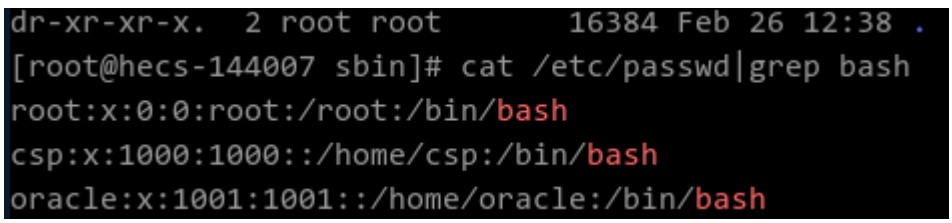
   You are advised to check the following directories: **/etc** (configuration files), **/tmp** (temporary files), and **/bin** (executable files).

   - 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**)



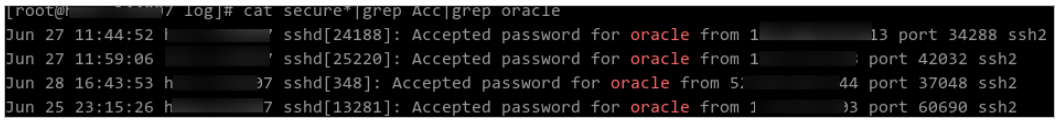
NOTE

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

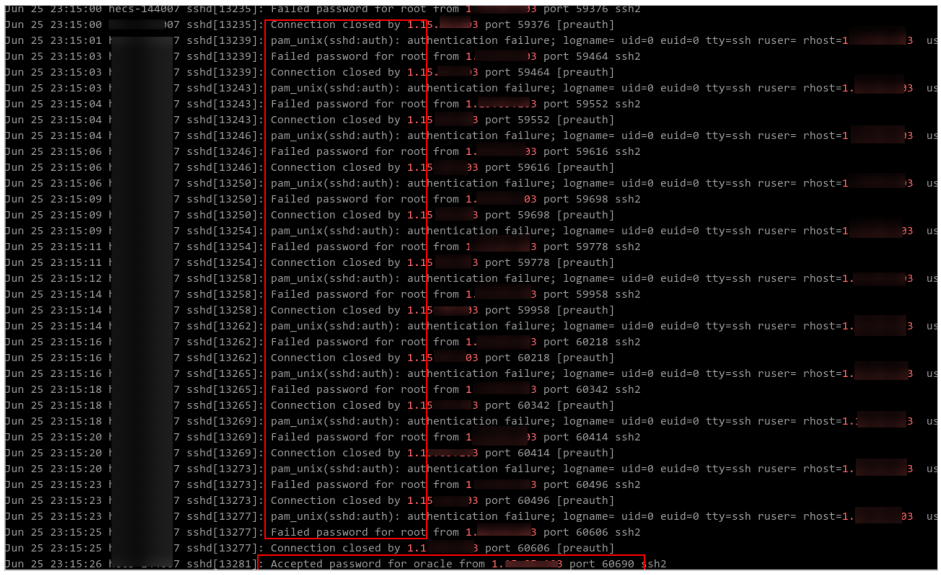
Step 5 Check the abnormal login records from the host login logs.

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.



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 logins, brute-force attacks may have taken place.



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**.

