Alibaba Cloud Threat Detection

User Guide

Issue: 20190415

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

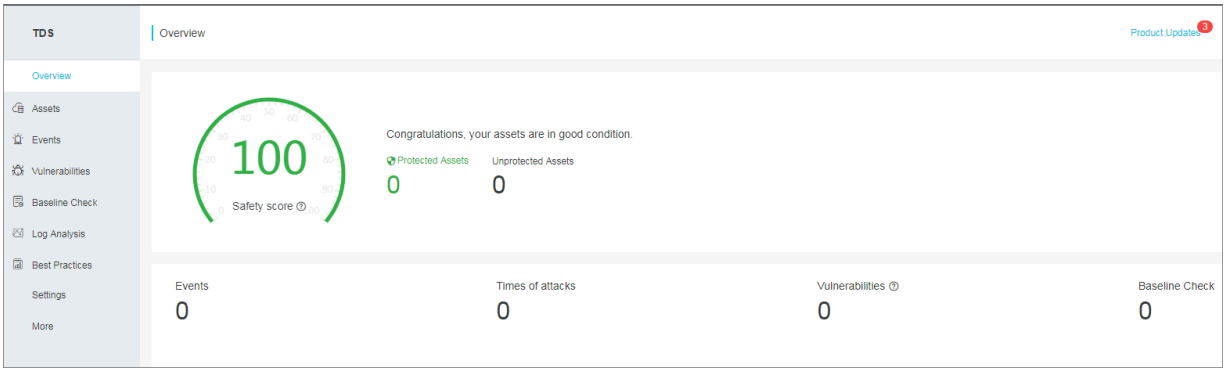
Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich {stand | slave}`

Contents

1 Overview

As the security operation center of Alibaba Cloud, the Overview page of the Cloud Security Center console displays the threats to, and the safety score of all your assets, and all the Alibaba Cloud Security services you have bought. You can upgrade Cloud Security Center, renew your Cloud Security Center service, scale up your assets, and modify the notification method.

On the Overview page, you can view important security information of your assets and execute related operations.



The Overview page includes the following modules:

- Cloud Security Center edition: Click Upgrade to Enterprise Edition/Renewon the top right of the Overview page, you can upgrade to your Cloud Security Center to the Enterprise Edition, scale up your assets, or renew your Cloud Security Center service.

  Basic Edition:

  Enterprise Edition:

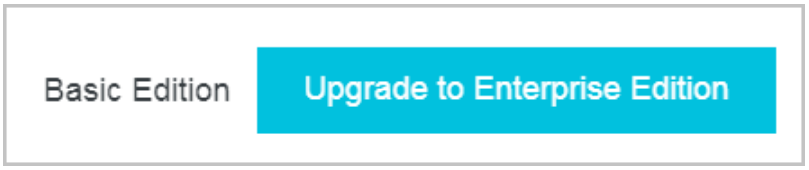
- Safety score: Safety score displays your assest's security score evaluated by Cloud Security Center, and the number of protected and unprotected assets. For specific score descriptions, see the Safety score table below.

  To add unprotected assets under the protection of Cloud Security Center, click the number under Unprotected Assets and on the displayed Install/Uninstall Cloud Security Center Agent page, install the Cloud Security Center agent. For more information, see *Install the Cloud Security Center agent*.
- Urgent Vulnerabilities: Urgent Vulnerabilities displays the latest discovered urgent vulnerabilities of your assets.
- Threat statistics: Threat statistics includes the number of security events, attacks, vulnerabilities, and vulnerable baseline configurations.
- Cloud platform best security practices: This module displays the detected baseline risks of your cloud products.
- Safe operation: This module displays the number of events, vulnerabilities, and vulnerable baseline configurations handled during the week in the form of column charts.
- Information on the Alibaba Cloud Security products you have bought.

Upgrade to the Enterprise Edition, scale up assets, and renew your Cloud Security Center service

Cloud Security Center provides a Basic Edition and an Enterprise Edition. You can view information on your specific edition in the upper-right corner of the Overview page. For more information on the differences in features of the Basic Edition and the Enterprise Edition, see *Features*.

- Basic Edition: The edition of Cloud Security Center is shown in the upper-right corner of the page. An Upgrade to Enterprise Edition button is also displayed. If you upgrade your Cloud Security Center Basic Edition to the Enterprise Edition, you are able to use such advanced functions as baseline checks, asset fingerprints, malicious processes (malware checking), and log analysis.



- Enterprise Edition: The expiration date of your Cloud Security Center service, and the size of your assets (the number of servers) are displayed in the upper-right corner of the page. A Renew button is also displayed.

Note:
If your current number of servers exceeds the number that you specified when purchasing Cloud Security Center, an Asset Scaling button is displayed in the upper-right corner of the page. To guarantee the availability of all features, we recommend that you scale up your assets.

Security score table

Security score	Description
95–100	Your assets are fully secured.
85–94	There are some security risks to your assets. We recommend that you strengthen the security of your servers and your system as soon as possible.
70–84	There are many security risks in your assets detected by Cloud Security Center. We highly recommend that you strengthen the security and protection of your system as soon as possible.
69 and lower	Your assets are exposed to security risks and may be easily compromised. We recommend that you immediately strengthen the security and protection of your system.

Table 1-1: Impacts to safety score table

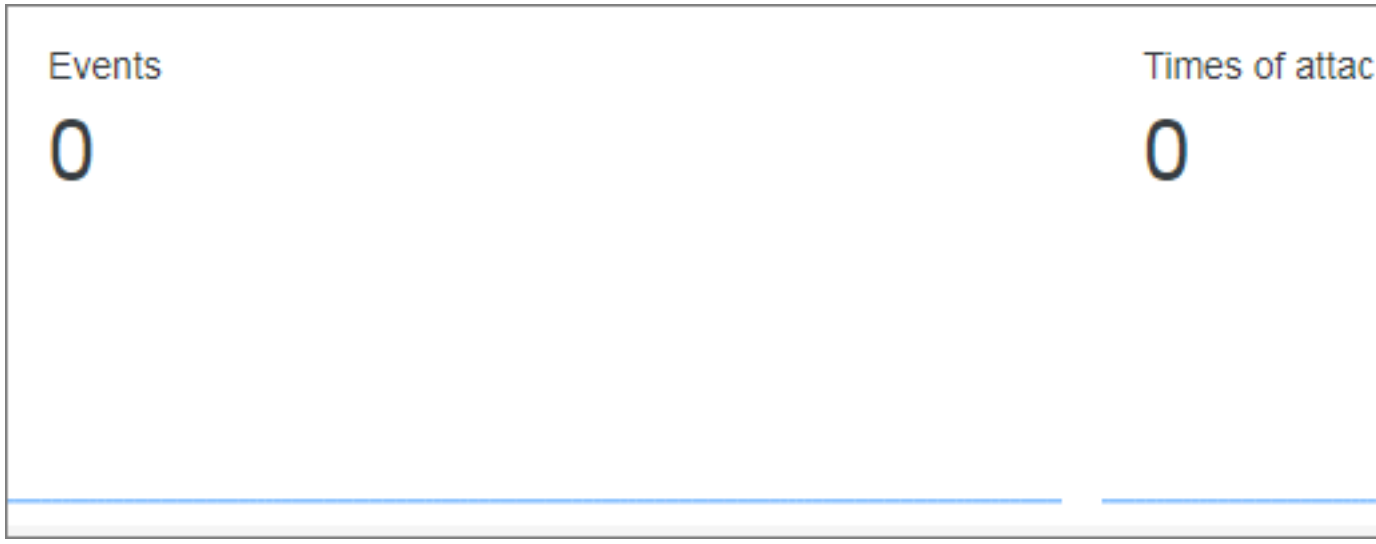
Impact	Strengthening suggestion
Lack of a security operation center	Establish an in-depth defense system. If you have any queries, submit a ticket for technical support.

Impact	Strengthening suggestion
Unfixed vulnerabilities	Fix the vulnerabilities. For more information, see Vulnerabilities.
Unhandled security events	Handle the security events in a timely manner.
Lack of host protection	Enable the enterprise edition of Server Guard.
The protection status is offline (the Cloud Security Center agent is not installed or offline).	Install the Cloud Security Center agent. For more information.
Web-CMS vulnerabilities	Fix the Web-CMS vulnerabilities.
System software vulnerabilities	Fix the software vulnerabilities.
Risks detected by baseline checks	Fix the vulnerabilities of baseline.
Unexpected logons	Check and handle the unexpected logons.
Webshell threats	Check and handle the webshell files.
Host exceptions	Handle the host exception events.

Threat statistics

The Overview page displays the statistics of the threats that Cloud Security Center detects in all your assets, and the corresponding trend diagrams, including:

- Events: Number of unhandled security events.
- Times of attacks: Number of attacks today.
- Vulnerabilities: Number of unhandled vulnerabilities.
- Baseline check: Number of vulnerable baseline configurations.


Events
0
Times of attac
0

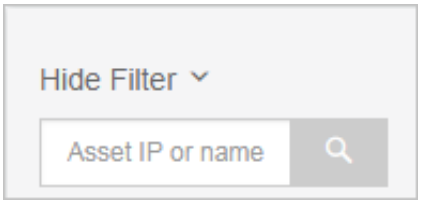
2 Assets

The Assets page in the Cloud Security Center console allows you to view the security status of the assets that have been protected by Cloud Security Center. You can use the asset group and tag functions on the Assets page to manage the security of specific assets. You can view security events by asset group. You can also use tags to filter and view assets that have the same attributes.

View the security status of assets

To view the security status of your assets, follow these steps:

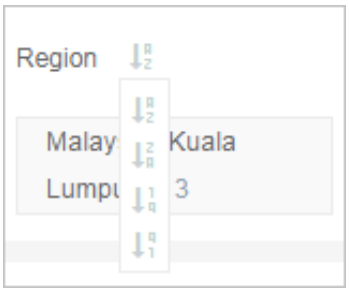
1. Log on to the *Cloud Security Center console* .
2. In the left-side navigation pane, click Assets to view the security status of the assets that have been protected by Cloud Security Center.
3. You can show the filter pane, and use the search and filtering functions in the pane to quickly find your expected assets.
   - Enter the IP address of a server in the search box to view the security status of the server.

   - You can use the filtering items to filter assets, including Category, Tag, Region, Security Issue Type, Agent, OS, and All Groups.

     Note:
     When a filtering item contains too many criteria, you can click the sort button next to the filtering item to sort these criteria. You can sort the criteria in the

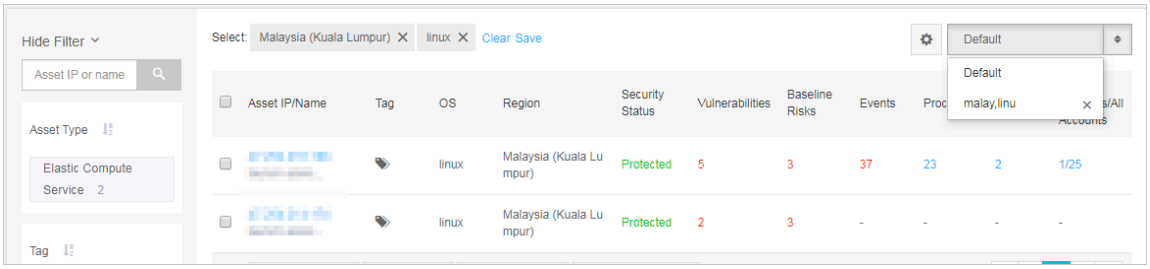
alphabetical ascending order (A to Z), alphabetical descending order (Z to A), numerical ascending order (1 to 9), and numerical descending order (9 to 1).



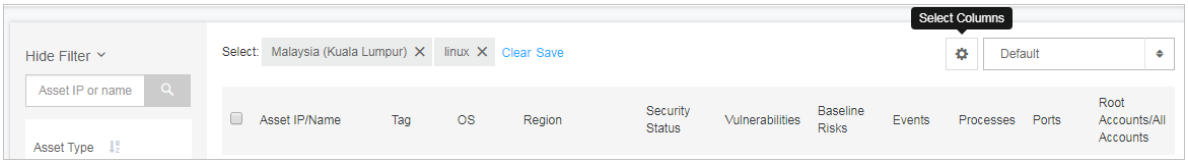
- You can select a criterion under a filtering item to view assets that match the specified criterion. For example, you can select Malaysia (Kuala Lumpur) under the Region item to view servers in the Malaysia (Kuala Lumpur) region.
- You can also select multiple criteria under a filtering item, and then click Apply to view assets that match all these criteria. For example, you can select Baseline Check and Vulnerability for the Security Issue Type item, and then click Apply to view servers that have baseline risks or vulnerabilities.
- You can select multiple filtering items to filter assets. For example, you can select Malaysia (Kuala Lumpur) for the Region item and select linux for the OS item to only view Linux servers in the Malaysia (Kuala Lumpur) region.

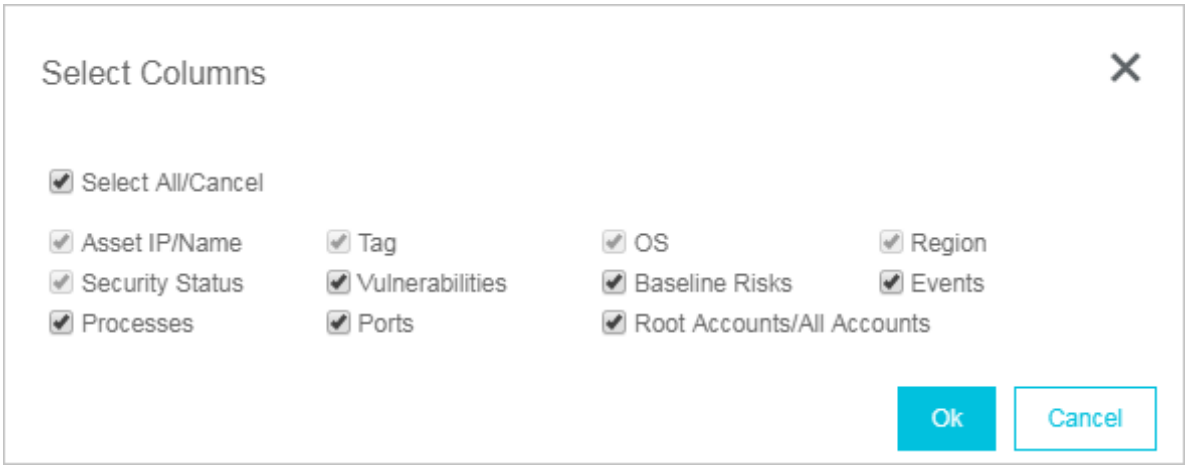
Note:

You can save filtering items that have been applied as a filtering condition. To perform this task, click Save, and enter a filtering condition name (for example, malay-li). You can then select the condition from the filtering condition list in the upper-right corner of the asset list page.



4. You can click Select Columns in the upper-right corner of the Assets page to customize the columns to be shown in the asset list.

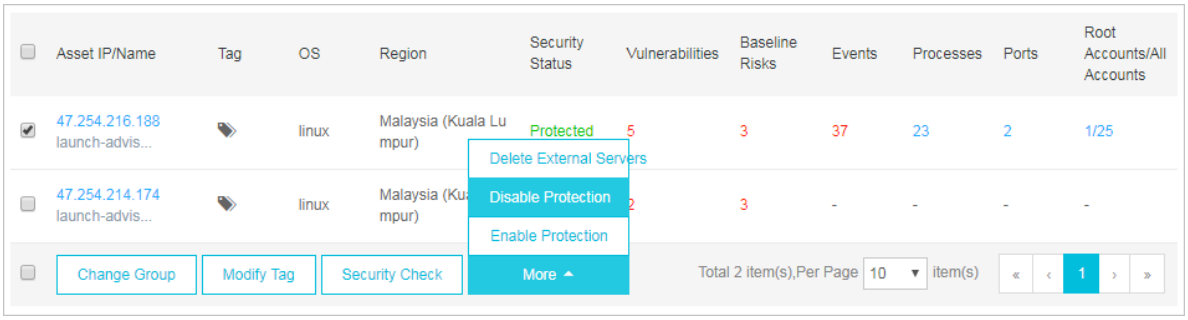




Disable/Enable Cloud Security Center protection

If you want the Cloud Security Center agent to stop consuming resources on your assets for a specific period of time, follow these steps to disable Cloud Security Center protection for your assets:

1. Select one or more assets whose Security Status is Protected from the Assets page.
2. Click More > Disable Protection under Assets.



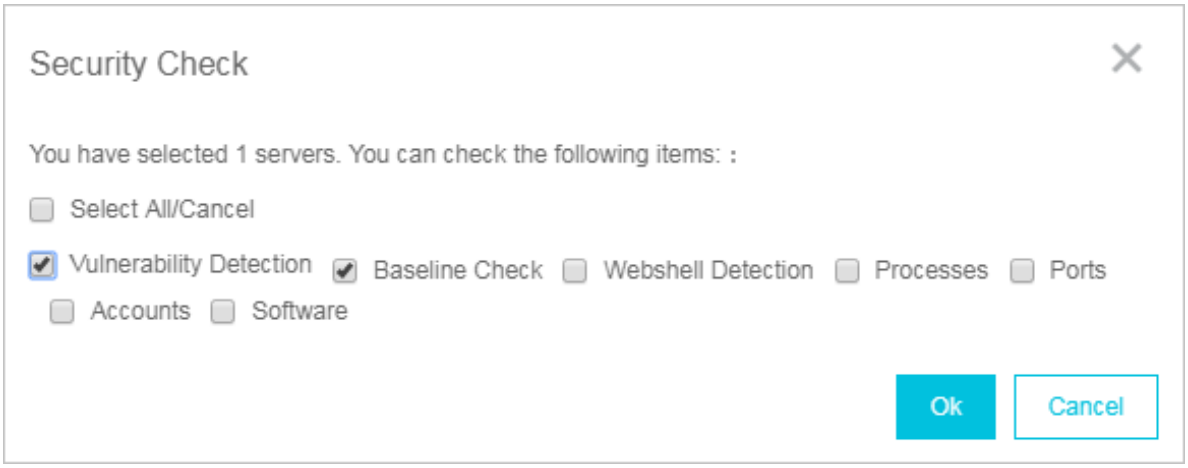
After Cloud Security Center protection has been disabled, the Cloud Security Center agent no longer collects security information on your servers, reports security information, or occupies system resources. You can select More > Enable Protection to enable Cloud Security Center protection for your assets.

Quick security check

You can use the Security Check function on the Assets page to perform a security scan for specific assets and update information about vulnerabilities, baseline configuration risks, and asset summary.

Follow these steps to perform a quick security check:

1. Select one or more assets from the Assets page.
2. Click Security Check under Assets.
3. Select security check entries in the Security Check dialog box.



4. Click OK to perform a quick security check.

The security check results will be automatically updated to the relevant page in the Cloud Security Center console.

Asset group management

If the Assets page contains multiple assets under your account, we recommend that you use the asset group function to create an asset group for these assets so that you can search and manage these assets by group.

Follow these steps to create and manage asset groups:

1. Show the filter pane. At the bottom of the filter pane, click Manage under All Groups to open the Manage Asset Groups dialog box.

2. Create an asset group.

Note:
The Default group contains assets that have not been added to any asset group. If you delete an asset group, all assets in that group will be moved to the Default group.

a. Click Add Group.
b. Enter a group name, and click OK.
c. You can click the + button on the right side of a group to create a sub group. You can also rename or delete a group.

Note:
The system supports up to three levels of sub groups.

3. Sort asset groups. When there are multiple groups with the same level, you can click the ↑ or ↓ button next to a group to sort the groups.
4. Delete an asset group. You can click the × button on the right side of a group to delete the group.

Note:
When you delete an asset group that contains sub groups, all of the assets in this group and sub groups will be moved to the Default group.

Add assets to a specific asset group

You can add assets to an asset group to operate multiple assets at one time. We recommend that you add the same type of assets to an asset group. For example, when you configure an asset baseline check policy, you can specify an asset group to apply the policy to all assets in the group. You can also filter assets on the Assets page by asset group.

To add assets to a specific asset group, follow these steps:

1. Select one or more assets on the Assets page and click Change Group under the asset list.
2. Select an asset group to add these assets to the specified group.

Note:
You cannot add both assets and sub groups to the same asset group. For example, asset group A contains sub group B. In this case, you cannot add asset C to asset group A.

3. Click OK.

Add/Modify tags

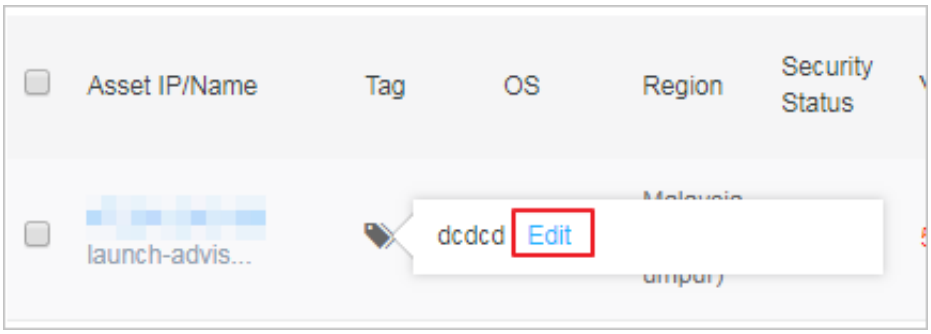
You can use tags to label your assets and filter assets on the Assets page by tag.

Follow these steps to add a tag to an asset:

1. Select an asset on the Assets page.
2. Hover your cursor over the tag icon in the Tag column, and click Add. (If the asset already has tags, click Edit.)

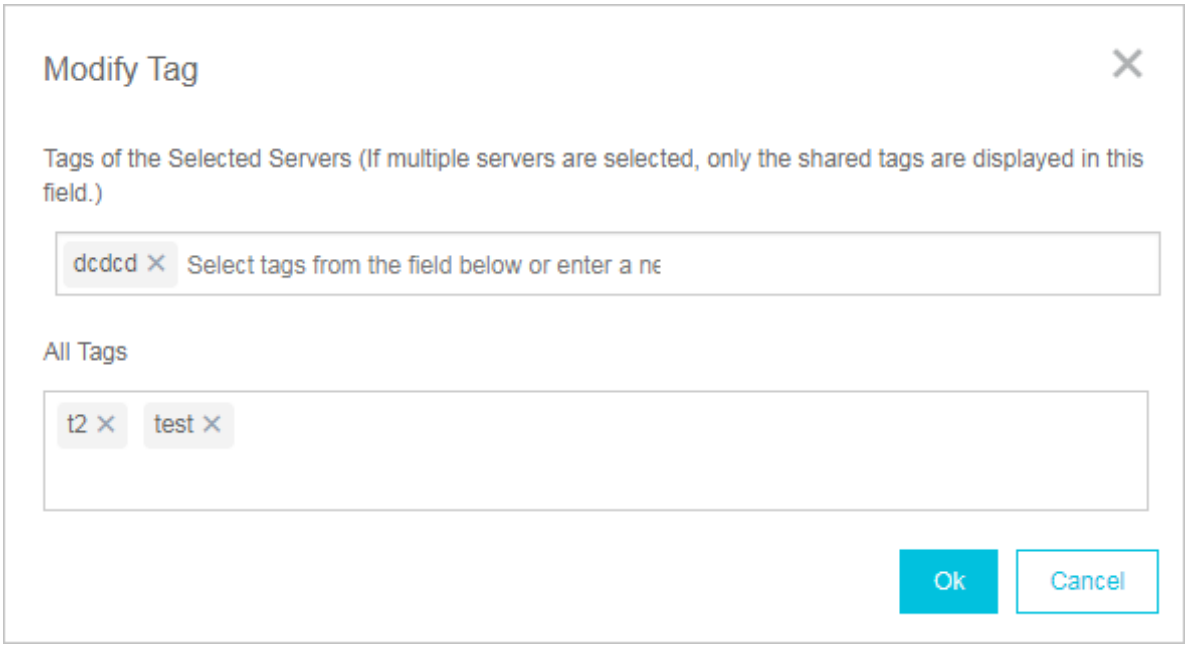
Note:

You can select one or more assets, and click Modify Tag under the asset list to modify tags for these assets at the same time.



3. Enter a tag name or select one or more existing tags.

Note:
You can add multiple tags to an asset.



4. Click OK.

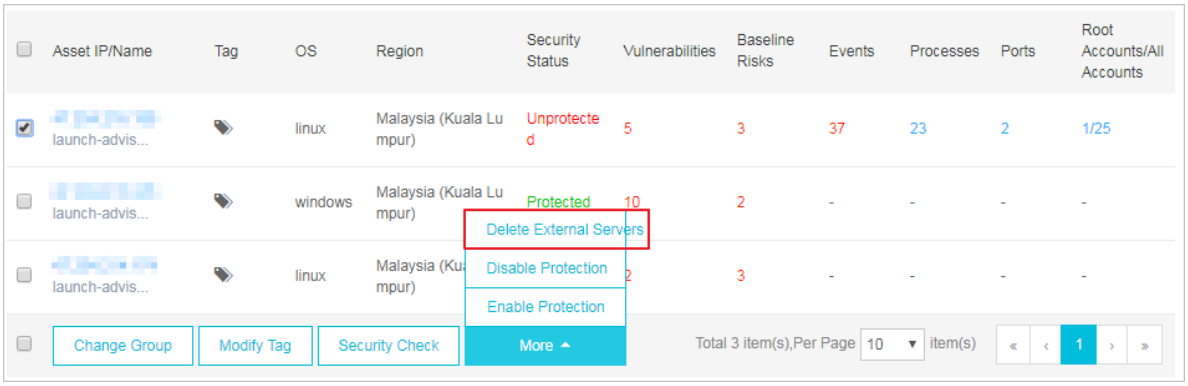
Remove external server

You can remove external servers from the asset list to completely disable Cloud Security Center protection for these servers.

Note:
Uninstalling the Cloud Security Center agent on an ECS instance does not remove the instance from the asset list. In this case, the security status of the ECS instance appears unprotected.

Follow these steps to remove external servers from the asset list:

1. Select one or more external servers from the Assets page.
2. Click More > Delete External Servers under Assets.



3. Click OK. The system will automatically uninstall the Cloud Security Center agent on your servers and then remove the servers from the asset list.

3 Events

3.1 Security events

TDS can monitor the security status of your servers and trigger alarms when it detects any network intrusions. This allows you to manage potential security risks and quickly respond to the risks.

Function Description

TDS detects network intrusion behaviors such as:

- Unusual logon: After you specify valid logon IP addresses, logon times, and accounts, TDS can then monitor your logon behavior against these conditions and triggers an alarm when any unusual logon behavior is detected. Usual logon locations can also be added. TDS can then trigger alarms when logons to a specified asset from an unfamiliar location are detected.
- Webshell: TDS detects common Webshells using an autonomous detection engine that supports scheduled detection, and real-time safeguard. You can then one click quarantine any detected Webshells.
  - Modifications made to scan targets will trigger a dynamic Webshell analysis. A static Webshell analysis is performed daily at 12:00 am.
  - You can customize scan targets for Trojan horse scanning and removal.
  - You can quarantine, restore, or ignore detected Trojan horse files.
- Suspicious host: You can view suspicious processes, sensitive file tampering, and unusual network connections that are detected on your servers.
- Virus: TDS and the control center on the cloud collaborate to provide a virus scanning and removal mechanism. TDS records information generated by running processes and reports the information to the control center on the cloud for virus scanning. When a virus is detected, TDS determines the method to remove the virus, for example, by terminating the process and quarantining the file.

View and process security events

To view and process network intrusions that occur on your servers, follow these steps :

1. Log on to the *TDS console*.
2. In the left-side navigation pane, click Events.
3. In the event list, view all the network intrusions that are detected.
4. You can quickly locate a specific event by search and selecting its event type, severity level, and processing status. For example, you can search for an event by using the IP address or name of the server on which the event occurred, or the event name.
5. Process events using applicable methods.
   - View: View event details.
   - Handle Offline: Remove the record from the list after the event has been confirmed and processed offline.
   - Ignore Once: Ignore the event and remove the record from the list.
   - Label as False Positive: Label the event as a false positive and remove it from the list.
   - (Webshell only) Handle Online: Quarantine the webshell file. The quarantined files can be viewed by clicking Quarantine in the upper-right corner of the page.

     Note:
     The system only keeps a quarantined file for 30 days. You can restore any quarantined file before the system deletes the file.

Settings

You can customize your usual logon locations and scan targets. You can also set alarm severity levels and configure advanced logon detection.

Note:
Advanced logon detection is provided only in TDS Enterprise Edition. With TDS Enterprise Edition, you can specify more precise conditions of unusual logons, such as specifying valid logon IP addresses, logon times, and accounts.

To set security events, follow these steps:

1. Log on to the *TDS console*.
2. In the left-side navigation pane, click Events.

3. In the upper-right corner, click Settings and then configure the settings.
   - Add usual logon locations
     a. Click Add next to Usual Logon Locations.
     b. Select a usual logon location and its associated servers or server groups.
     c. Click OK.

     You can Edit or Delete an added usual logon location.

     - Click Edit next to a usual logon location to change its associated servers.
     - Click Delete next to a usual logon location to delete the configurations for this usual logon location.
   - Configure advanced logon alarming

      Note:
     You can specify valid logon IP addresses, logon times, and accounts. TDS sets alarms to trigger when unusual logon attempts are detected. Operations related to the following functions are similar to the configurations of usual logon

locations. You can perform the operations of Add, Edit, Delete by referring to the preceding section.

- Click the switch next to Valid Logon IPs to enable or disable IP address check. If the IP check is enabled, alarms are triggered when logons are performed from unspecified IP addresses.
- Click the switch next to Valid Logon Time to enable or disable logon time check. If the logon time check is enabled, alarms are triggered when logons are performed at unspecified times.
- Click the switch next to Valid Logon Accounts to enable or disable account check. If account check is enabled, alarms are triggered when logons are performed using unspecified accounts.

· Customize scan targets

TDS automatically detects the scan targets that are on your servers. It then performs dynamic and static scans. You can also customize your scan targets.

a. Click Add next to Add Scan Targets.
b. Specify a valid scan target and select the server on which the scan target is stored.


Note:
Adding the root directory is not supported.

c. Click OK.

· Set alarm severity levels

At the bottom of the Settings sidebar, select the severity levels of the events to be detected.

The alarm severity levels are as follows:

- Reminder: An event of this severity level indicates an event that requires you to verify its validity, for example, account creation.
- Warning: An event of this severity level indicates a possible intrusion event, for example, a logon record to your ECS instance from an unfamiliar location.
- Urgency: An event of this severity level indicates a successful hacker attack, for example, virus or a denial-of-service attack.

3.2 Cloud Threat Detection

Cloud Threat Detection of TDS integrates the features of popular antivirus engines, and provides you with comprehensive and real-time virus detection and protection service. This service features a unique detection model, which is based on machine learning and deep learning techniques, and large amount of threat information gathered by Alibaba Cloud.

Cloud Threat Detection checks hundreds of millions of files every day and serves millions of cloud servers.

Detection capabilities of Cloud Threat Detection

TDS collects the process information on servers and upload it onto cloud for viruses detection. If a malicious process has been detected, you can directly stop the process and quarantine the related files.

- Virus detection engine (self-developed by Alibaba) is built on deep learning techniques and a large amount of attack samples and protection policies. The engine specializes in detecting malicious files in the cloud, can effectively identify potential threats, and cover the shortages of traditional antivirus engines.
- Cloud sandbox (self-developed by Alibaba) simulates cloud environments and allow you to monitor attacks from malicious samples. Based on big data analysis and machine learning modeling techniques, cloud sandbox automatically checks and detects potential threats and offers dynamic analysis and detection capabilities.
- Integration with antivirus engines popular in the world enables the service to timely update the virus database.
- Based on the threat data provided by TDS, the service also integrates a server detection model to detect suspicious processes and malicious activities from various perspectives.

Supported virus types

Cloud Threat Detection provides a comprehensive solution based on the experience of Alibaba Cloud's security and defense experts. It covers data collection, masking, recognition, analysis, quarantine and recovery. You can quarantine malicious files and restore quarantined files on TDS console.

Cloud Threat Detection can detect the following virus types :

Virus	Description
Mining program	A mining program illegally consumes server resources to mine virtual currencies.
Computer worm	A computer worm is a malware computer program that replicates itself and spread to a large number of computers within a short time.
Ransomware	Ransomware such as WannaCry uses encryption algorithms to encrypt files and prevent users from accessing their files.
Trojans	A trojan is a malicious program that allows the attacker to access users' personal information, to gain control of the server, and to consume system resources.
DDoS trojan	A DDoS trojan hijacks servers and uses zombie servers to launch DDoS attacks, which can interrupt your normal service.
Backdoor	A backdoor is a malicious program injected by an attacker, who uses the backdoor to control the server or launch attacks.
Computer virus	A computer virus is a type of malicious program that can replicate itself by modifying other programs and insert malicious code into other programs to infect the whole system.
Malicious program	Programs that brings harm to a computer system and data security.

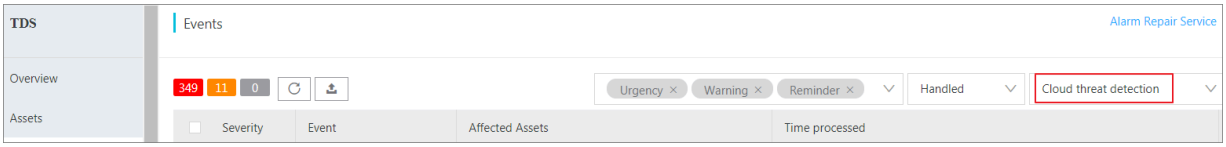
Benefits

- Reliable : Based on big data, deep learning, and machine learning techniques, the service integrates the capabilities of multiple detection engines to provide a comprehensive and real-time virus detection service.
- Lightweight: The service only takes 1% CPU usage and 50 MB memory.
- Real-time: The service obtains process initiation logs and monitors malicious programs in real time.

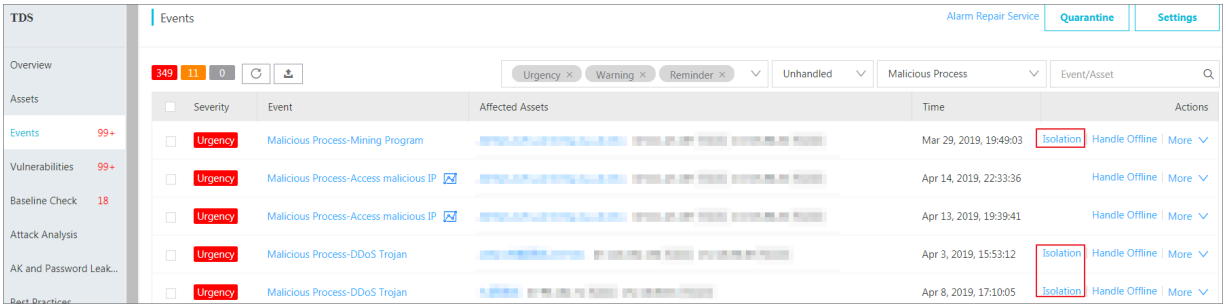
- Easy management: You can manage all servers and view their real-time status in the Alibaba Cloud Security console.

Scenarios

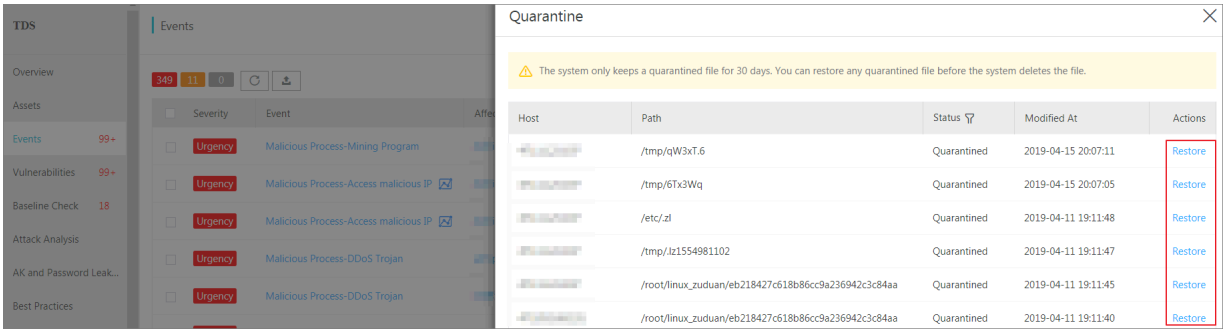
Detect



Quarantine



Recover



3.3 View and handle security events

You can view and handle security events in TDS console. TDS allows you to handle multiple events at a time.

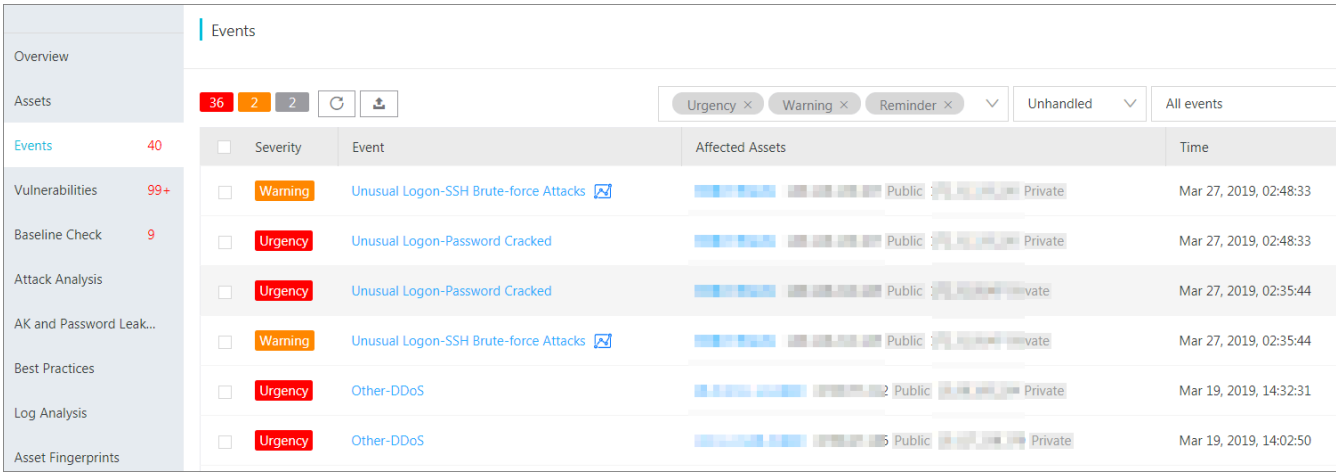
Procedure

1. Log on to *Threat Detection Service console*.
2. In the left-side navigation pane, click Events to go to the Events page.

3. On the Events page, view or search for the detected intrusion or threat events, and check their details.

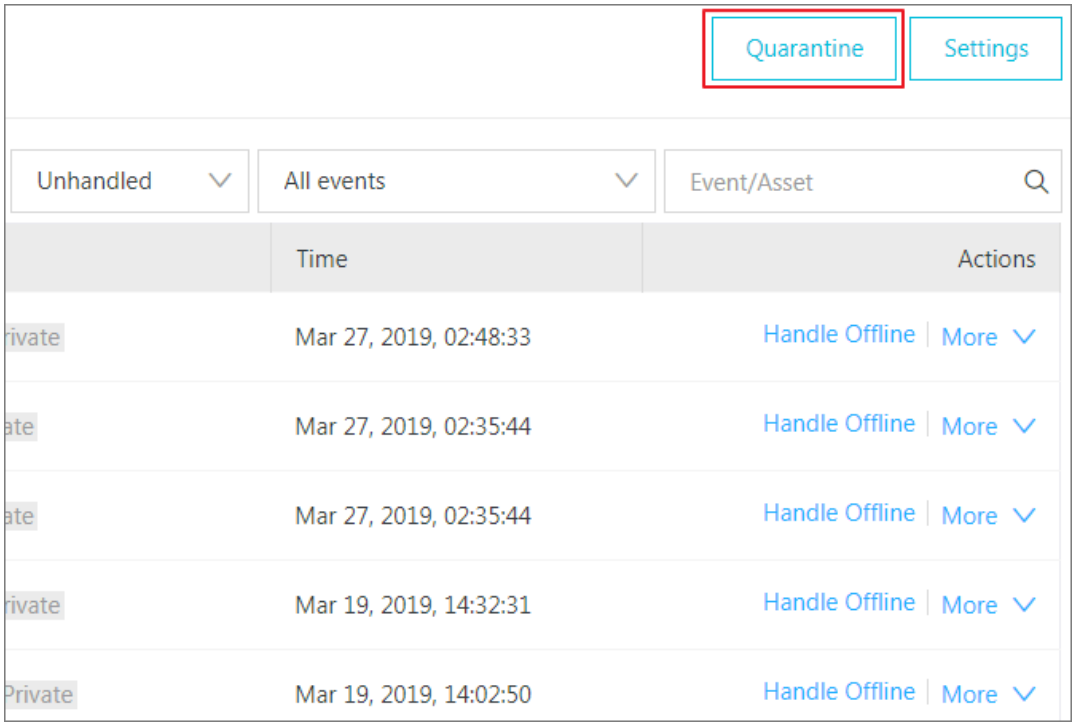
   You can find a certain event based on specified search conditions. For example, you can search for events by event or asset name, severity level, event status, or event type.

4. You can handle different events with the following operations.



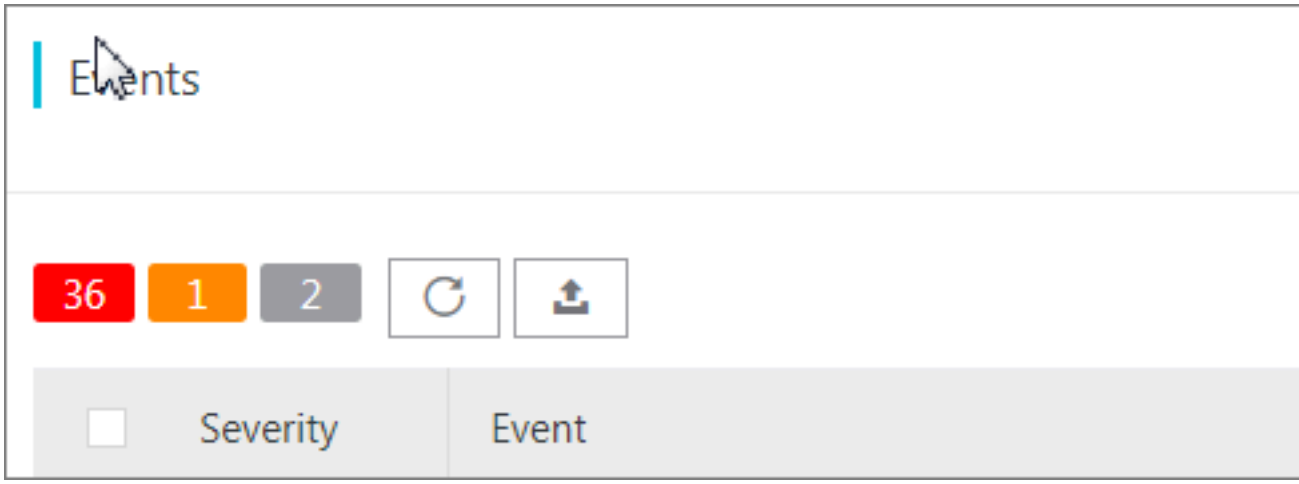
   - Quarantine: Quarantine only the Webshell and Malicious Process events. You can click Quarantine in the Actions column corresponding to a Webshell event

to quarantine the relevant webshell file. Quarantined files no longer pose threats to the host.



Note:
The system keeps a quarantined file for only 30 days. You can restore any quarantined file before the system deletes the file.

- Handle Offline: After handling an event offline, you can click Handle Offline in the Actions column. The event status then changes to Handled.



- Ignore Once: You can click More in the Actions column corresponding to an event and choose Ignore Once from the shortcut menu to ignore the event. The

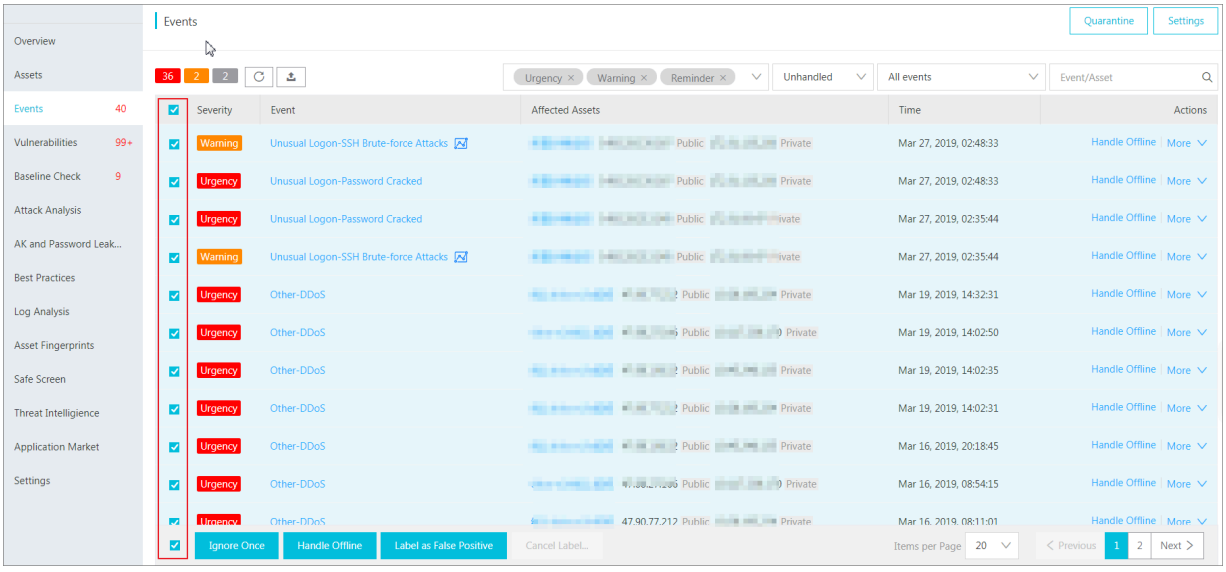
event status then changes to Handled. The event will no longer be reported in TDS console.

- Label as False Positive: You can click More in the Actions column corresponding to an event and choose Label as False Positive from the shortcut menu to label the event as a false positive. The event status then changes to Handled. The event will no longer be reported in TDS console. You can find the event that you labeled as a false positive in the Handled event list, and click Cancel Labeling as False Positive in the Actions column to unlabel the event.

> **Note:**
> False positives are alerts generated for normal processes. The *Unusual TCP Packets* event is a common false positive. It is reported when a process on your server initiated a suspected scan on other devices.

Handle security events in batches

You can use the batch-handling toolbar in the lower-left corner of the Events page to handle security events in batches.



> **Note:**
> Check the details of each event before you handle the events in batches.

4 Vulnerabilities

4.1 Linux software vulnerability fix

This topic introduces attributes of Linux software vulnerabilities to help you understand Linux software vulnerabilities that have been detected by Threat Detection Service (TDS).

View Linux software vulnerabilities

Log on to the *TDS console* , go to the Vulnerabilities > Server Vulnerabilities page, and then click the Linux Software Vulnerabilities tab to view all Linux software vulnerabilities that TDS has detected on your server.

You can click a vulnerability name on the Vulnerabilities page to go to the corresponding detail page.

Linux software vulnerability attribute descriptions

The following table describes Linux software vulnerability attributes on the detail page.

Attribute	Description
Vulnerability	Name of the Linux software vulnerability. The vulnerability name typically starts with CVE or RHSA. Example: *CVE-2018-1123 on Ubuntu 14.04 LTS (trustly).*

Attribute	Description
CVSS Score	The Common Vulnerability Scoring System (CVSS) score that is assigned to the vulnerability by the CVSS according to the open industry standard. A CVSS score is used to rate the severity of a vulnerability to help you prioritize responses to the vulnerability. CVSS v3.0 rates the severity of vulnerabilities as follows: · 0.0: None. · 0.1-3.9: Low. - Vulnerabilities that will cause denial of service issues. - Vulnerabilities that have minor impacts. · 4.0-6.9: Medium. - Vulnerabilities that will impact users during system and user interactions. - Vulnerabilities that will be exploited to perform unauthorized activities. - Vulnerabilities that can be exploited after attackers have changed the local configuration or obtained important information. · 7.0-8.9: High. - Vulnerabilities that can be exploited to indirectly obtain user permissions to your server and application systems. - Vulnerabilities that can be exploited to read, download, write, or delete arbitrary files. - Vulnerabilities that will cause sensitive data leaks. - Vulnerabilities that will cause business disruption or remote denial of service issues. · 9.0-10.0: Critical. - Vulnerabilities that can be exploited to directly obtain permissions to the operating system of your server. - Vulnerabilities that can be exploited

Attribute	Description
Revealed At	Time when the vulnerability was revealed.
CVEID	Common Vulnerabilities and Exposures (CVE) ID. The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. You can use CVE IDs, such as `CVE - 2018 - 1123` , to quickly search vulnerability fix information in any CVE-compatible databases to resolve security issues.
Affected Assets	Servers where the vulnerability has been detected.
Vulnerability Fix Priority	Priority of the vulnerability rated by TDS based on multiple factors, such as the vulnerability severity, time when the vulnerability was revealed, and actual ECS environment. The vulnerability fix priorities include the following: · Urgent · Less urgent · Not urgent Note: For more information about how to prioritize vulnerability fixes, see *Vulnerability fix prioritization*.

Attribute	Description
Details	Software directory, version, configurations, and affected items. · Software: Version of the software in the operating system of the current server. · Cause: Reason why the software has this vulnerability. Typically, the main cause is that the current software version is lower than the specified software version. Another cause is that this vulnerability has already been detected in the current software version. · You can click More to view Path: Path of the software on the server.
First/Last Detected At	The first and last time when the Linux software vulnerability was detected by TDS.

4.2 Vulnerability fix prioritization

The prioritization of vulnerability fixes is essential to cloud asset protection. If you have a large number of assets, Threat Detection Service may discover thousands of vulnerabilities on your assets. Such a large number means it is difficult to prioritize the vulnerabilities. To resolve this issue, Cloud Security Center provides a set of prioritization standards for you to prioritize these vulnerabilities.

Vulnerability severity score

Cloud Security Center uses vulnerability severity scores to prioritize Linux software vulnerabilities and Windows vulnerabilities. Vulnerability fix priorities calculated based on vulnerability severity scores include Urgent, Less urgent, and Not urgent.

> Note:
> Emergency vulnerabilities and web content management system (WCMS) vulnerabilities are critical vulnerabilities confirmed by Alibaba Cloud security engineers, which must be fixed immediately.

Vulnerability severity scores can be calculated by using the following formula:

Vulnerability Severity Score = Vulnerability CVSS Base Score x Temporal Score x Environmental Score x Asset Importance Score

The descriptions for these scores are as follows:

- **Vulnerability CVSS Base Score: Specifies the CVSS2/3 base score of the vulnerability, in the range of 0 to 10.**
- **Temporal Score: A temporal score is derived from multiple metrics in the range of 0 to 1. These metrics include the vulnerability exploit maturity and remediation latency.**

  In the first three days of the revealing of the vulnerability, the probability of the vulnerability being exploited greatly increases as the public awareness of the vulnerability increases. The temporal score raises from 0 to reach a peak value that is smaller than 1, and then drops quickly. However, as the time passes, the vulnerability becomes more likely to be exploited based on the rapid development of exploit techniques. The temporal score then gradually increases and approaches 1 within 100 days.

- Environmental Score: Your actual environment is essential to vulnerability prioritization. An environmental score is measured based on your server and the exploitability of the corresponding vulnerability.

  The following environmental factors are currently used to calculate an environmental score:

  - Your server receives traffic from the public network:
    - If the vulnerability can be remotely exploited, the environmental score is 1.5.
    - If the vulnerability can be exploited by attackers in a neighboring network, the environmental score is 1.2.
    - If the vulnerability can be locally exploited, the environmental score is 1.
    - If the vulnerability can only be exploited in a complex environment that cannot be recreated in the cloud, the environmental score greatly decreases.
  - Your server receives traffic only from VPCs:
    - If the vulnerability can be remotely exploited, the environmental score greatly decreases. In this case, the environmental score is set to 0.
    - If the vulnerability can be exploited by attackers in a neighboring network, the environmental score is 1.2.
    - If the vulnerability can be locally exploited, the environmental score is 1.
    - If the vulnerability can only be exploited in a complex environment that cannot be recreated in the cloud, the environmental score greatly decreases.
- Asset Importance Score: Asset importance scores are assigned to servers or assets based on scenarios when large amounts of servers or assets exist.

  Note:
  The default asset importance score is 1.

It takes 48 hours for Cloud Security Center to calculate a vulnerability severity score from the time that the vulnerability was detected by Cloud Security Center.

Note:

- When a vulnerability is identified, the corresponding authority may have not yet assigned a CVSS base score to the vulnerability. Cloud Security Center will provide the vulnerability severity score 48 hours after the authority has posted the CVSS base score.

- Network malfunctions, such as Cloud Security Center agent offline issues, may cause environmental score calculation failures. In this case, the vulnerability severity score is available in 48 hours after your network has recovered.

Vulnerability fix priorities

- Urgent: The recommended vulnerability severity score is in the range of 13.5 to 15.
- Less urgent: The recommended vulnerability severity score is in the range of 7.1 to 13.5.
- Not urgent: The recommended vulnerability severity score is smaller than 7.

Vulnerability fix priorities in special scenarios

- Cloud Security Center weights the priority of a vulnerability that has just been detected based on the environment of your server. This process takes 48 hours. During this process, the priority of the vulnerability is measured based on the severity of the vulnerability as follows:
  - If the severity of the vulnerability is critical, the priority is Urgent.
  - If the severity of the vulnerability is high or medium, its priority is Less urgent.
  - If the severity of the vulnerability is low, its priority is Not urgent.
- If the environmental score of a vulnerability cannot be measured due to network convergence, the priority of the vulnerability is set to Not urgent.

4.3 Software vulnerability fix

This topic introduces the best practice for fixing software vulnerabilities on servers.

You can use the following method to fix vulnerabilities that have been detected on your server by the vulnerability detection feature of Threat Detection Service.

Note:
This method is designed to successfully fix vulnerabilities detected in the operating system, network devices, databases, and middleware on servers.

How to fix software vulnerabilities

Unlike fixing vulnerabilities on PCs, fixing software vulnerabilities on servers requires expert knowledge. You must follow these steps to fix software vulnerabilities :

Prerequisites

1. You must check all assets on the target server and log on to the Cloud Security Center console to check system vulnerabilities on the server. For more information about descriptions of Linux software vulnerability attributes in Cloud Security Center, see *Linux software vulnerability attribute descriptions*.
2. After checking the system vulnerabilities on the target server, determine the vulnerabilities that need to be fixed urgently. You can determine which vulnerabilities need to be fixed urgently based on the business status, server status, and impacts caused by vulnerability fixes.
3. Upload vulnerability patches to the testing environment, test the compatibility and security of these patches, and then generate a vulnerability fix testing report. The vulnerability fix testing report must include vulnerability fix results, vulnerability fix duration, patch compatibility, and impacts caused by vulnerability fixes.
4. To prevent exceptions, before fixing the software vulnerabilities, you must use the backup and recovery feature to back up the system of the target server. For example, you can use the snapshot feature of ECS to create a snapshot of the target ECS instance.

Fix vulnerabilities

1. Upload the vulnerability patches to the target server and use the patches to fix the vulnerabilities. This task requires a minimum of two administrators: One administrator takes charge of fixing vulnerabilities and the other one takes charge of making records. Exercise all operations with caution.
2. The administrator must follow the system vulnerability list sequentially to upgrade the system and fix vulnerabilities.

Validate vulnerability fixes and generate a report

1. Validate the vulnerability fixes on the target server. Make sure that the vulnerabilities have been successfully fixed and that no exceptions have occurred on the target server.
2. Generate a vulnerability fix report based on the entire vulnerability fix process and archive the relevant documents.

Software vulnerability fix guidelines

To make sure that the operating system of the target server can run normally during the software vulnerability fix process, and to minimize the possibility of exceptions, follow these guidelines when you fix vulnerabilities:

- Create a vulnerability fix plan

  You must inspect the operating system and application system of the target server and create a applicable vulnerability fix plan. The feasibility of the vulnerability fix plan must be discussed and verified in the testing environment. You must strictly follow the instructions and steps in the vulnerability fix plan to fix vulnerabilities and make sure that no damage is made to the systems of the target server.

- Use a testing environment

  You must use a testing environment to verify the feasibility of your vulnerability fix plan. Make sure that the plan has no impacts on the online business system to be fixed.

   Note:
  The testing environment must use the same operating system and database system as your online business system. The application system version of the testing environment must be the same as your online business system. We recommend that you use the latest replica of the entire business system for testing.

- Back up your business system

  You must back up the entire business system, including the operating system, applications, and data. After backup, you must validate the backup by restoring your system. System backup guarantees the availability of your business. If a system exception or data loss occurs, you can use the backup to restore your system. We recommend that you use the snapshot feature of ECS to quickly back up your business system.

5 Baseline check

5.1 Server baseline check

Threat Detection Service (TDS) supports baseline checks to automatically detect vulnerable configurations on servers and provides resolutions. This article describes how to use the server baseline check to locate and optimize vulnerable configurations on servers.

Function description

After you enable the server baseline check, TDS automatically detects risks related to systems, accounts, databases, passwords, and compliance configurations of your servers, and provides resolutions. For more information about the check items, see *Details of the server baseline check*.

By default, TDS automatically performs the server baseline check once between 00:00 and 06:00 each day. You can add and maintain a scan policy that specifies the check items, target instances, check cycle, and trigger time.

Note:
For some checked items, such as detecting weak passwords in MySQL and SQL Server services, TDS may use certain instance resources for logon attempts, and generate some logon failure records. Therefore, these checked items are disabled by default. If you require these items, confirm the preceding risks, customize the server baseline scan policy, and then check these items.

You can configure a whitelist for the server baseline check. TDS skips items that are included in the whitelist. You can also add notes to the items in the whitelist to facilitate tracking.

Add a scan policy

When you enable the server baseline check, the default policy is used. You cannot change the check items and check cycle of the default policy.

Follow these steps to create a scan policy:

1. Log on to the *Threat Detection Service console*.

2. In the left-side navigation pane, click Baseline Check.
3. Click Create Policy to create a scan policy and follow these configurations:
   a. Enter a policy name.
   b. Select the items to check related to compliance configurations, passwords, systems, accounts, and databases. For more information, see *Details of the server baseline check*.
   c. Specify the check cycle (1, 3, 7, or 30 days), and trigger time (00:00-06:00, 06:00-12:00, 12:00-18:00, or 18:00-24:00).
   d. Select the target assets.

      
      Note:
      By default, new instances are sent to All Groups > default. To apply this policy to new instances, select Default.

   e. Click OK.

   The new policy takes effect immediately, and runs a scan according to the specified cycle and trigger time. You can also click Check Now on a target policy on the Servers tab page to run the scan immediately.
4. Click Settings in the upper-right corner on the Baseline Check page. Then, in the dialog box that appears, select a target policy from the list under Scan Policy, and click Edit to edit this policy, or click Delete to delete this policy.

View and fix vulnerable configurations

Follow these steps to locate and optimize vulnerable configurations on your instance:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click Baseline Check.
3. On the Servers tab page, check vulnerable configurations on your instance.
4. You can quickly locate a vulnerable configuration by specifying its name, category, severity, and status.

   
   Note:
   When you specify a category, you can then choose a sub-category.

5. On the Servers tab page, perform the following actions as needed:
   - Select risk items and click Ignore to ignore them. The ignored items do not trigger alarms any more.
   - Select risk items and click Add to Whitelist to add them to the whitelist. TDS does not check the items in the whitelist.
6. Click the name of a risk to enter the details page, and view the details of the risk and affected assets.
7. Refer to the suggestion in Details > More to fix the risk on servers.

   Note:
   You can select one or more affected assets and apply the bulk operations at the bottom of the Affected Assets list.

   - Once you fix the risk, click Verify in the Actions column to verify if the risk has been fixed successfully. If you do not perform a manual verification, the system automatically verifies the resolution 72 hours after the resolution is applied.
   - If you do not want to receive an alarm for this risk item, you can click Ignore in the Actions column to ignore the risk. The ignored risk does not trigger any alarm.
   - If you do not want to check for the specified risk, click Add to Whitelist in the upper-right corner of the page, and add a note to this item. You can remove a risk item from the whitelist in *Settings*.

Settings

Follow these steps to change server baseline check settings:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click Baseline check.
3. Click Settings in the upper right corner of the page. You can perform the following settings:
   - Edit or Delete scan policies. For more information, see *Add a scan policy*.
   - Set a time frame for Retain Invalid Risks for: 7 days, 30 days, or 90 days.

     Note:

If you do not take any actions on the detected risks, the system determines that these risks are invalid. The system deletes them when the retention period expires.

- Maintain the Baseline Check Whitelist: Click Remove under a risk to remove this item from the whitelist. Then, the system performs a new scan and generates the corresponding alarms.

Details of the server baseline check

Category	Check item
Compliance with Security Standards	httpd2.2
	Windows 2008 R2
	Memcached
	CentOS 7
	MySQL 5.6 Database
	SQL Server 2008 R2
	Tomcat 7
	MongoDB
	Ubuntu 14
Weak Password	PostgreSQL Weak Password
	SSH Weak Password
	Anonymous FTP Logon
	SQL Server Weak Password
	MySQL Weak Password
	RDP Weak Password
	FTP Weak Password
System	Group Policy
	Baseline Policy
	System File Changes
	Registry
Account	System Account Security
Database	Redis Configurations

6 Settings

On the Threat Detection Service (TDS) settings page, you can perform the following tasks: Install/Uninstall TDS agent, and Configure alert policies. This document introduces how to configure TDS settings.

Install/Uninstall TDS agent

> Note:
> The TDS agent is a security plug-in that runs on servers. To use TDS to protect your servers, you must first install the TDS agent to the operation system of your servers.

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click Settings.
3. Go to the Install/Uninstall TDS Agent page.
4. If the server is in the Unprotected status, follow the instructions on the page to download and install the latest version of the TDS agent. For more information, see *Install the Threat Detection Service agent*.
5. To disable TDS protection, click Uninstall in the upper-right corner to uninstall the agent. For more information about uninstalling the TDS agent, see *Uninstall the Threat Detection Service agent*.

Configure alert settings

Alert settings allow you to modify the alert policies for TDS. The operation is as follows:

> Note:
> By default, the alarm message recipient is your account contact. You can also go to the *Message Center*, and add more message recipients in Message Settings > Common Settings > Security Message.

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click Settings.
3. Go to the Alert Settings page.

4. Specify the alert Severity level and Notification Method for Events, Vulnerabilities, and Baseline Check.

 Note:
Changes made on this page are applied immediately.

You can also modify the alert policy on the Overview page. The operation is as follows:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click Overview.
3. Click the Alert Settings button at the top of the page.
4. In the Alert Settings dialog box, select a alert policy: Critical, Not Critical, All, or Customize. We recommend that you use the first three policies.

 Note:
Click Save for the changes to take effect.

7 Asset fingerprints

The asset fingerprint feature periodically collects the following information on your servers: processes, system accounts, listener ports, software, and website backgrounds. You can view the status of your assets and perform retrospective analysis using this information. This document describes how to view different asset fingerprints.

Function description

The asset fingerprint feature contains the following modules:

- Processes: Periodically collects information about processes on the server. Scenarios: to check which server is running a specific process, and to check which processes are initiated by a specific server.
- Accounts: Periodically collects system account information on the server. Scenarios: to check which server has created a specific account, and to check which accounts are created by a specific server.
- Listener ports: Periodically collects information about listener ports on the server . Scenarios: to check which server is listening on a specified port, and to check which ports are enabled on a specified server.
- Software: Periodically collects software version information on the server. Scenarios: to check for illegal software installations, to check for obsolete software versions, and to quickly find the affected assets when vulnerabilities are exploited.
- Website backgrounds: Periodically collects logon information at website backgrounds, detects weak passwords and user enumeration attempts, and monitors background security. Scenarios: to view logon records at backgrounds, to check whether weak passwords exist, and to view user enumeration attempts.

Additionally, for information about processes, system accounts, listener ports, and software, you can specify the frequency of data collection.

View asset fingerprints for an individual asset

You can access the asset details of a specific asset through the Assets page and view the asset fingerprints of this asset. The individual asset fingerprints include processes, accounts, listener ports, and software.

1. Log on to the *Cloud Security Center console*.

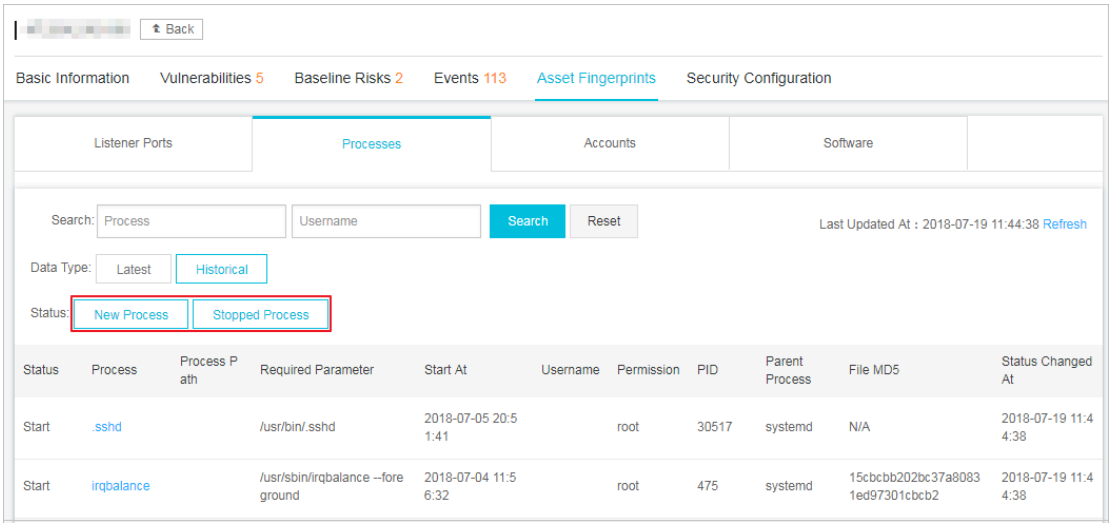
2. Go to the Assets page, select the asset you want to view, and click its Asset IP/Name.

3. On the asset details page, click Asset Fingerprints.

- View processes

a. Go to the Processes page to view all the running processes on the asset. You can search by process name or user.

b. Set Data Type to Historical to view the process changes, including New Process and Stopped Process.

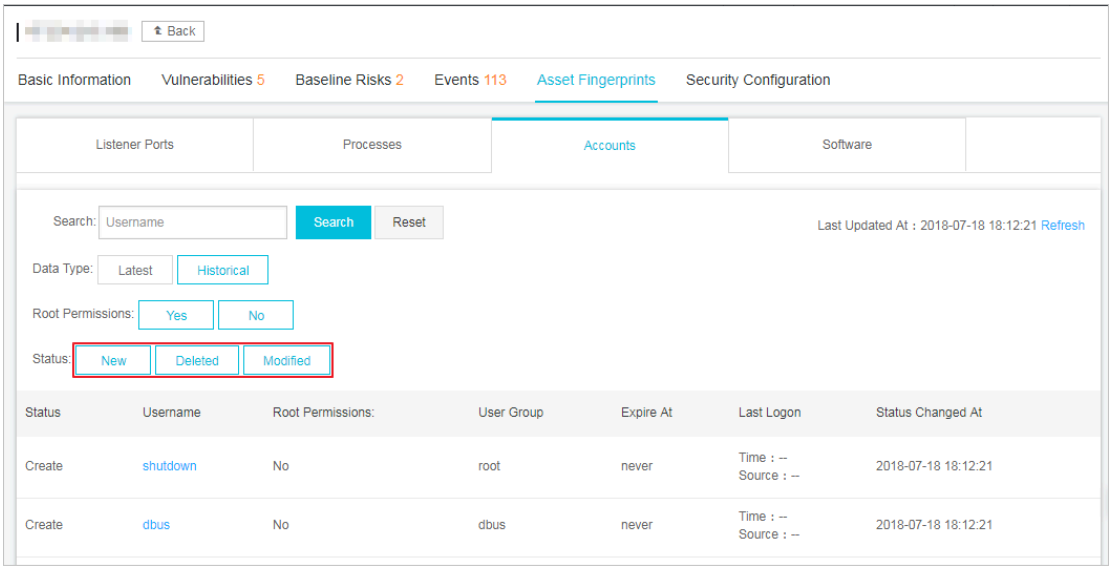


c. Click a process name to view the details.

- View accounts

a. Go to the Accounts page to view all the logged-on system accounts on the asset. You can search by account name.

b. Set Data Type to Historical to view the system account changes, including New, Modified, and Deleted.

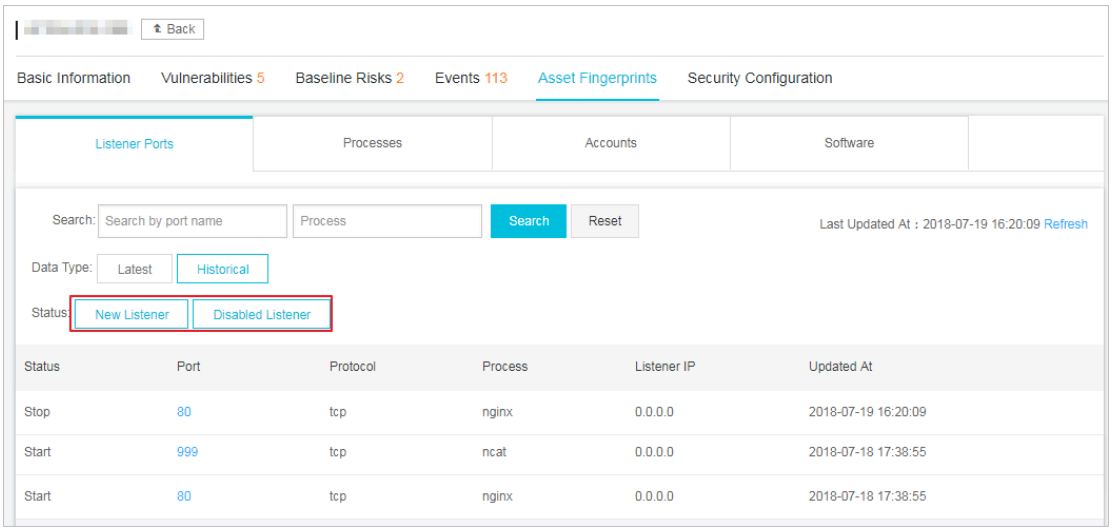


c. Click an account name to view account details.

- View listener ports

  a. Go to the Listener Ports page to view all the enabled ports and the network protocols on the asset. You can search by port number or process name.

  b. Set Data Type to Historical to view the listener port changes, including New Listener and Disabled Listener.

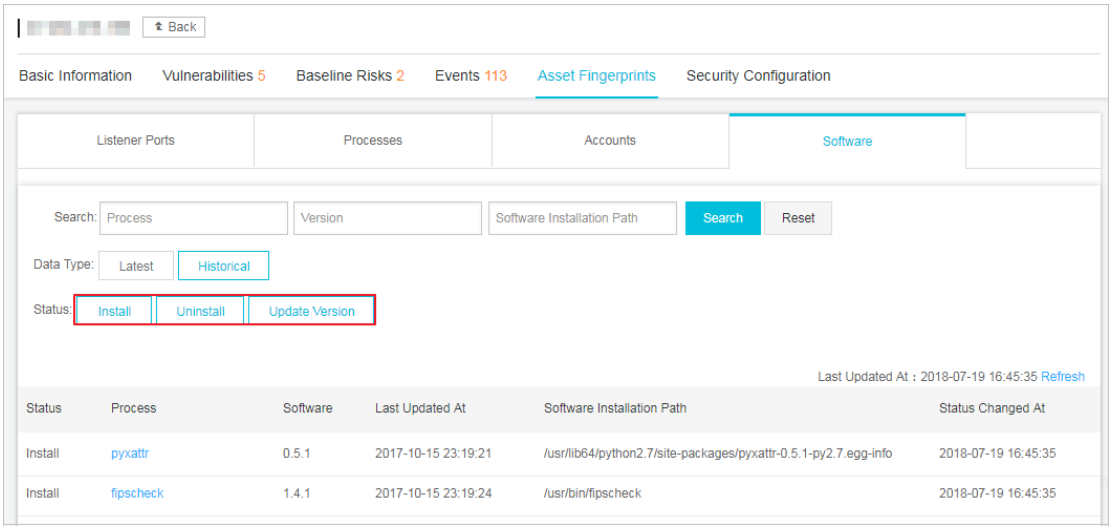


  c. Click a port number to view the details.

- View software

  a. Go to the Software page to view all the software on the asset. You can search by process, version, or installation directory.

  b. Set Data Type to Historical to view the software changes, including Install, Uninstall, and Update Version.



  c. Click a software name to view the details.

View asset fingerprints for all assets

You can view the asset fingerprints for all assets on the Asset Fingerprints page. The Asset Fingerprints page displays the real-time information for processes, accounts, listener ports, software, and website backgrounds.

Follow these steps to view asset fingerprints for all assets:

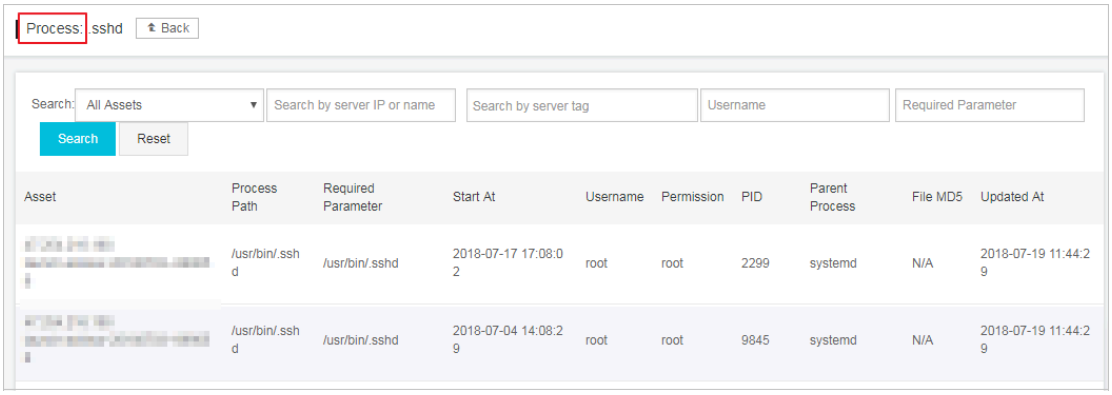
1. Log on to the *Cloud Security Center console*.
2. In the left-side navigation pane, click More.

3. Click Asset Fingerprints.

- View processes

  a. Go to the Processes page to view all the processes and servers that are running them. You can search by process name or user.

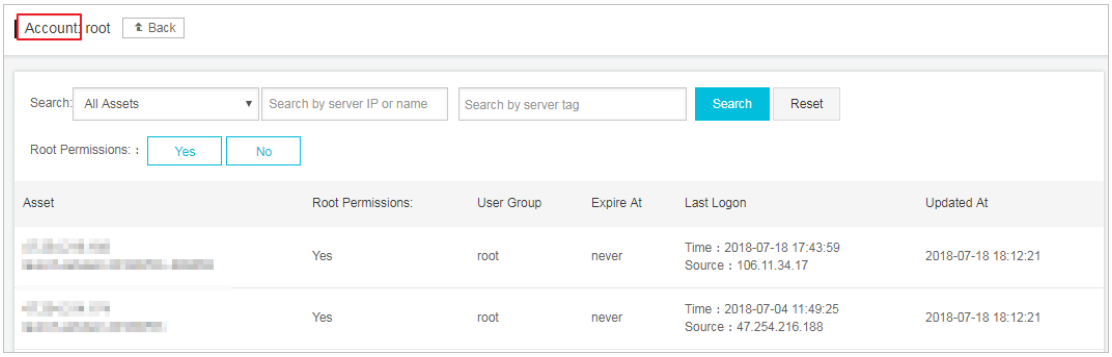
  b. Click a process name to view the details.



- View system accounts

  a. Go to the System Accounts page to view all the logged-on accounts and servers that are using them. You can search by account name.

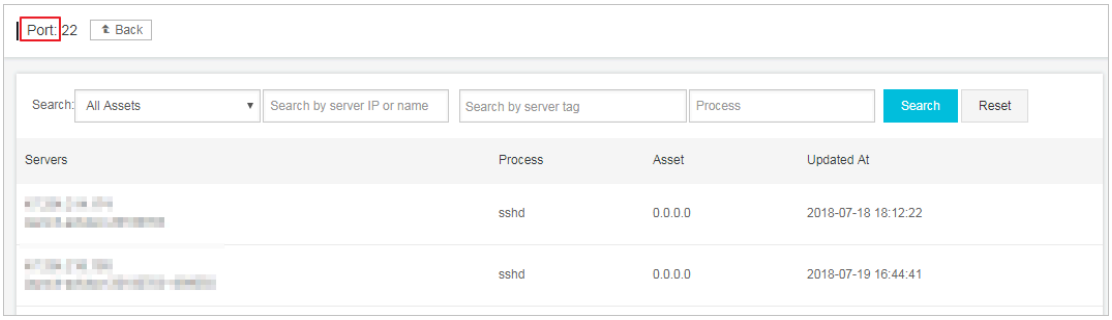
  b. Click an account name to view account details.



- View listener ports

  a. Go to the Listener Ports page to view all the enabled ports, protocols, and servers that are using them. You can search by port number or process name.

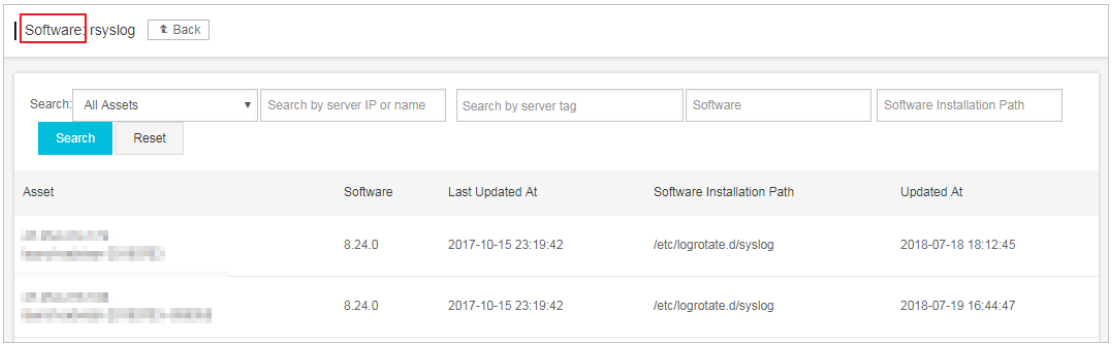
  b. Click a port number to view the details.



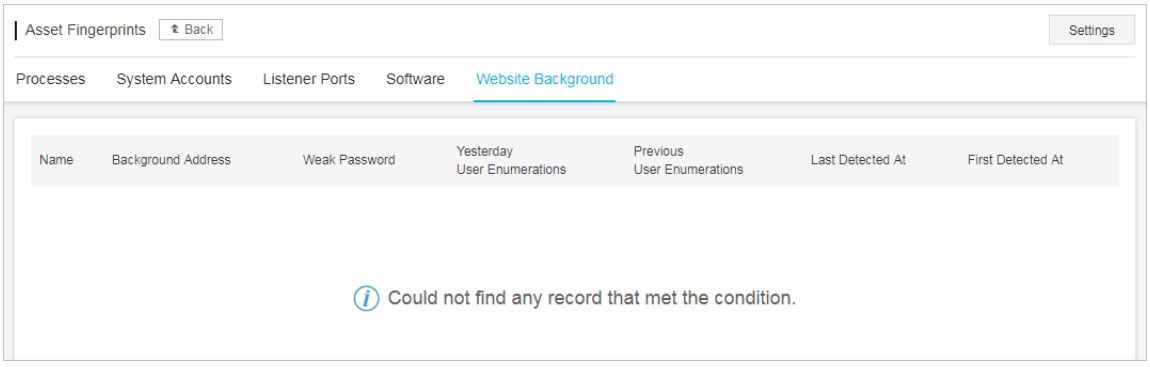
- View software

  a. Go to the Software page to view all the software and servers that are using them. You can search by process, version, or by installation directory.

  b. Click a software name to view the details.



- View website background logon records: Go to the Website Background page to view the background logon records, weak logon passwords, and user enumerations attempts.



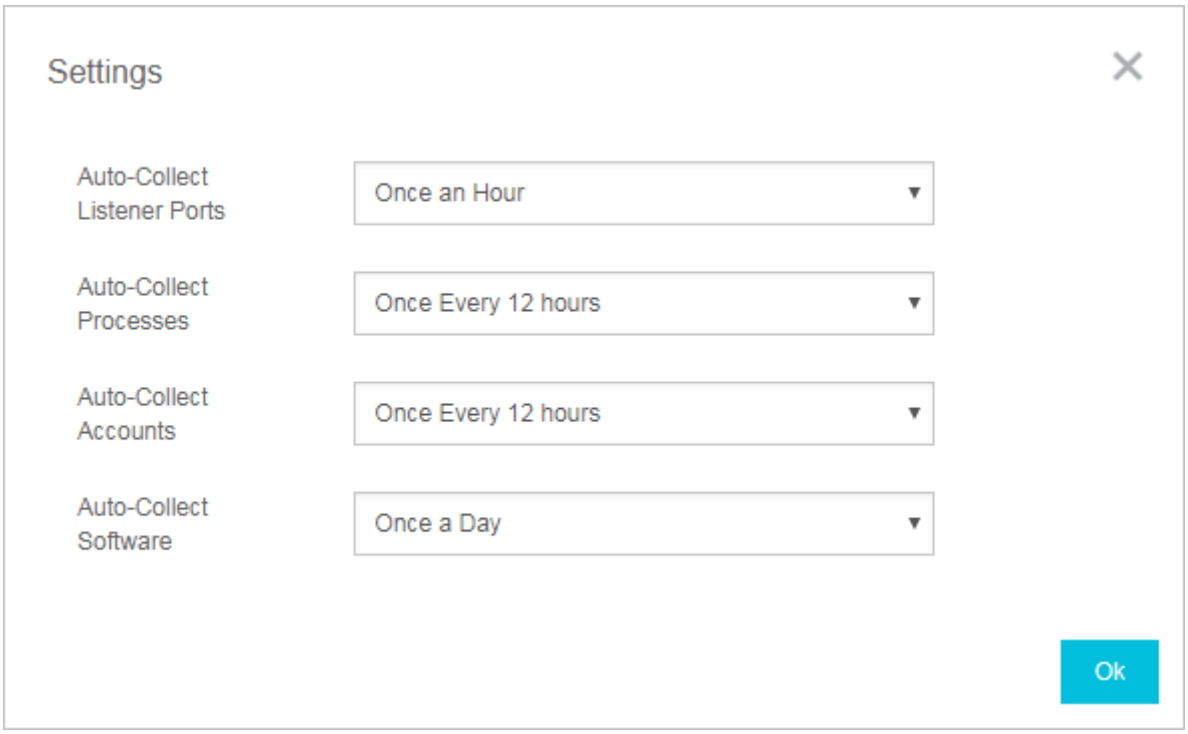
Settings

On the Asset Fingerprints Settings page, you can specify the frequency of data collection for processes, system accounts, listener ports, and software.

You can specify the frequency of data collection by following these steps:

1. Log on to the *Cloud Security Center console*.
2. In the left-side navigation pane, click More.

3. Click Asset Fingerprints.
4. In the upper right corner of the page, click Settings.
5. Complete the following settings:



- Select Auto-Collect Listener Ports and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
- Select Auto-Collect Processes and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
- Select Auto-Collect System Accounts and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
- Select Auto-Collect Software and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.

6. Click OK to apply the settings.

8 Log retrieval

9 Server vulnerability management

Threat Detection Service provides server vulnerability management to automatica lly detect system vulnerabilities on your servers. This article introduces how to use server vulnerability management.

Function description

Server vulnerability management helps you detect and fix the following system vulnerabilities on servers:

- Web content management system (WCMS) vulnerabilities

  TDS uses vulnerability patch databases in the cloud to provide automatic vulnerability detection and quick vulnerability repair as follows:

  - TDS automatically detects vulnerabilities, reports detection results, and sends alerts.
  - TDS allows you to easily fix vulnerabilities by replacing common web files (MD5 checksum validated).
  - TDS also allows you to verify vulnerability fixes. You can also use the undo fix function to restore the web files that have been replaced by TDS.
- Vulnerabilities of Linux software

  TDS scans the software that has been installed on your servers against the Common Vulnerabilities and Exposures (CVE) list to discover matching vulnerabil ities in your software and send alerts. TDS also provides commands for you to fix vulnerabilities that have been detected and allows you to verify these vulnerability fixes.
- Windows vulnerabilities

  TDS automatically checks if your servers have the latest Microsoft updates installed, and sends alerts if it finds any vulnerabilities. TDS also can automatically detect and fix major vulnerabilities on your servers.

View and fix vulnerabilities

Follow these steps to view and fix vulnerabilities that have been detected in the operating system (Linux or Windows) and WCMS of your servers:

1. Log on to the *Threat Detection Service console*.

2. In the left-side navigation pane, click Vulnerabilities.
3. Go to the Server Vulnerabilities page to view all server vulnerabilities.
4. You can use the vulnerability search and tag functions to quickly find a vulnerability. For example:
   - Search for a vulnerability by name.
   - Select vulnerability tags to quickly search for a vulnerability. For example, you can select the Unhandled, Urgent, and WCMS Vulnerabilities tags to search for a critical WCMS vulnerability that needs to be fixed urgently.
5. Perform the following actions according to your needs:
   - To disable TDS alerts for a specific vulnerability, select the vulnerability, and then click Ignore under the vulnerability list.
   - To exclude a specific vulnerability from the vulnerability detection list, select the vulnerability, and click Add to Whitelist under the vulnerability list. TDS does not detect vulnerabilities in the whitelist.
6. Click a vulnerability name to go to the vulnerability details page. You can view detailed vulnerability information and affected assets on this page.
7. Select an action to manage a vulnerability, depending on the type of the vulnerability.

 Note:

- You can select an action in the Actions column to manage an affected server. You can also select multiple affected servers, and then select an action to manage the selected servers.
- To manage multiple vulnerabilities, use the batch management tool in the upper-right corner of the Affected Assets page. Enter a batch name, and click Save to create a batch to fix all vulnerabilities that have been filtered out. You

can then track the relevant servers and verify vulnerability fixes by specifying the batch name.

- Linux software vulnerabilities
  - You can click Fix to directly fix a vulnerability. You can also click Generate Fix Command to automatically generate a command, log on to the relevant server, and then run the command to fix the vulnerability.

    Note:
    If a vulnerability fix requires a server restart to take effect, you must not restart the server until the Status of the vulnerability changes to Fixed (To Be Restarted), and then restart the server and click Restarted and Verified.
  - You can click Ignore to ignore a vulnerability. The system will no longer alert you for this vulnerability.
  - You can click Verify to verify the vulnerability fix. If you do not perform a manual verification, the system will automatically perform a verification 48 hours after the vulnerability fix procedure has completed.
- Windows system vulnerabilities
  - You can click Fix to fix a vulnerability. The system caches an official Windows patch in the cloud for your server to download and update.

    Note:
    If a vulnerability fix requires a server restart to take effect, you must not restart the server until the Status of the vulnerability changes to Fixed (To Be Restarted), and then restart the server and click Restarted and Verified.
  - You can click Ignore to disable TDS from alerting you for a specific vulnerability.
  - If your server has been installed with a vulnerability patch, you can click Verify to verify the vulnerability fix.
- WCMS vulnerabilities
  - You can click Fix to fix a WCMS vulnerability by replacing the web files that contain the vulnerability on your server.

    Note:

> Before you fix a WCMS vulnerability, we recommend that you back up the relevant web files. You can reference the path in the vulnerability management instructions to back up the web files.

- You can click Ignore to ignore a vulnerability. The system will no longer alert you for this vulnerability.
- You can click Verify to verify a vulnerability fix. If you do not perform a manual verification, the system will automatically perform a verification 48 hours after the vulnerability fix procedure has completed.
- For vulnerabilities that have been fixed, you can click Undo Fix to restore the web files that have been replaced by TDS.

Vulnerability management settings

The vulnerability management settings allow you to enable or disable automatic detection for different types of vulnerabilities, select a server for application vulnerability detection, set a time window to remove invalid vulnerabilities, and configure the vulnerability whitelist.

You can click Add to Whitelist under the vulnerability list to add multiple vulnerabilities to the whitelist (see *View and fix vulnerabilities step 5*). After the vulnerabilities have been added to the whitelist, the system no longer detects these vulnerabilities. The vulnerability management settings allow you to maintain the vulnerability whitelist.

Follow these steps to perform vulnerability management settings:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click Vulnerabilities.
3. Click Settings on the Server Vulnerabilities page.
4. You can perform the following tasks on this page:
   - You can select a vulnerability type, and click the toggle to enable or disable detection for the specified vulnerability type.
   - You can select a vulnerability type, and click Manage to specify servers on which TDS detects the specified vulnerability.
   - You can set a time window to remove invalid vulnerabilities: 7 days, 30 days, or 90 days.

> Note:

If you do not take any action on the detected vulnerabilities, the system determines that the alert settings for the vulnerabilities are invalid. The system removes the vulnerabilities when the specified period expires.

- **You can select vulnerabilities in the whitelist, and click Remove to enable TDS to detect these vulnerabilities and send alerts.**