Alibaba Cloud Threat Detection

User Guide

Issue: 20190115

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 intellectu

al 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 instructio ns, 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]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

1 Access Threat Detection Service

1.1 Threat Detection Service agent

How Threat Detection Service (TDS) agent works

The TDS agent automatically sends online data to the TDS server at an interval of five hours.

If the TDS server has not received any information from the agent for 12 hours, the server determines that the server where the agent runs is offline. The TDS server then changes the security status of the server to **Unprotected** in the console.

Agent processes

TDS runs the following TDS agent processes on a server:

Note:
TDS uses the root account to run the TDS agent processes on a Linux server. TDS uses the system account to run the TDS agent processes on a Windows server.

- **AliYunDun**

  TDS runs this process on a server to establish a connection to the TDS server.

  The directory of the process file varies by operating system, as follows:

  - Windows 32-bits: *C:\Program Files\Alibaba\aegis\aegis_client*
  - Windows 64-bits: *C:\Program Files (x86)\Alibaba\aegis\aegis_client*
  - Linux: /usr/local/aegis/aegis_client

- **AliYunDunUpdate**

  TDS periodically runs this process on a server to verify if an update is available for the TDS agent.

  The path of the process file varies depending on the operating system, as follows:

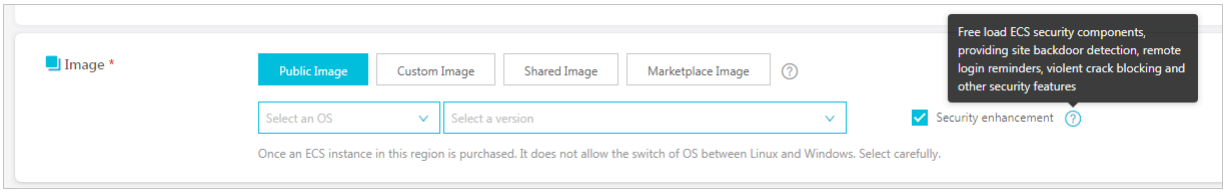
  - Windows 32-bits: *C:\Program Files\Alibaba\aegis\aegis_update*
  - Windows 64-bits: *C:\Program Files (x86)\Alibaba\aegis\aegis_update*
  - Linux: */usr/local/aegis/aegis_update*

1.2 Install the TDS agent

The Threat Detection Service (TDS) agent is a security plug-in running on servers. To use TDS to protect your servers, you must first install the TDS agent in the guest operating system of your servers.

Automatically install the TDS agent through Alibaba Cloud public images

The TDS agent has been integrated into Alibaba Cloud public images. When you create an ECS instance, select a public image and enable **Security enhancement** to automatically install the TDS agent on your instance.

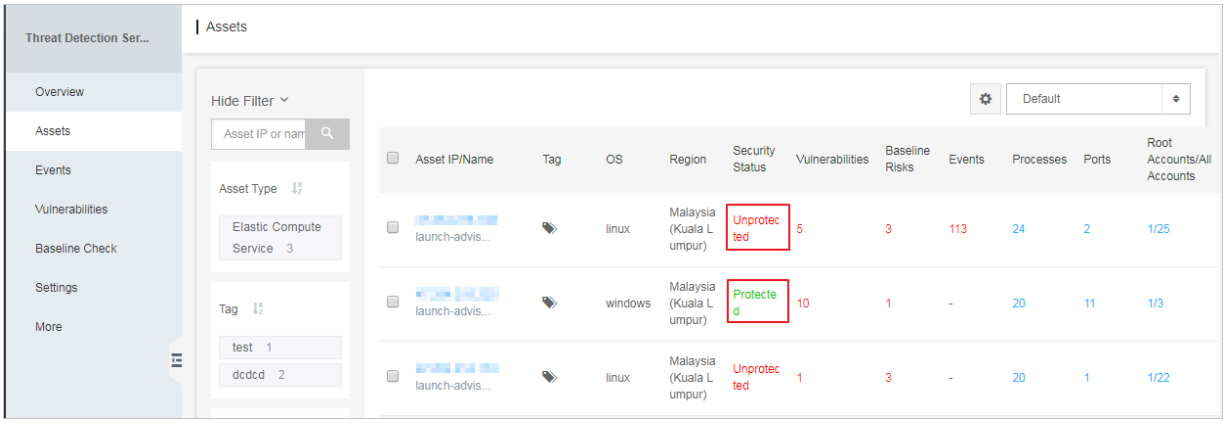


View the security status of your instance

The security status of an instance indicates whether or not the TDS agent is installed or working properly on the instance.

Log on to the *Threat Detection Service console*, and view the **Security Status** of all your instances on the **Assets** page.

- **Protected** indicates that the TDS agent is installed on the instance and is online.
- **Unprotected** indicates that the TDS agent is not installed on the instance or is offline.



If the security status of your servers appears unprotected, use the following method to manually download and install the TDS agent on your servers.

Manually install the TDS agent on a server (including external servers)

> **Note:**
> If security software such as Fortinet FortiGate has been installed on your server, the system may fail to install the TDS agent correctly. We recommend that you check whether security software already exists on your server before installing the TDS agent. If you have already installed security software to your server, disable or uninstall the software before you install the TDS agent.

Prerequisites

Before you install the TDS agent, make sure that your server meets the following requirements:

- If the server has been deployed in Alibaba Cloud, you can directly install the TDS agent on the server.
- If the server is not in Alibaba Cloud and communicates with Alibaba Cloud over the Internet, make sure that your server has access to the Internet.
- If the server is not in Alibaba Cloud and communicates with Alibaba Cloud through a leased line, add the following lines to the host file in the operating system of your server for TDS host names to be resolved.
  - `100.100.25.3 jsrv.aegis.aliyun.com`
  - `100.100.25.4 update.aegis.aliyun.com`

Procedure

Follow these steps to manually install the TDS agent:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click **Settings**.
3. Click **Install/Uninstall TDS Agent**.
4. Select the installation method that is applicable to the operating system of your server to download and install the latest TDS agent version:
   - **Windows**
     a. Click **Download** to download the latest version of TDS agent package to your PC.
     b. Upload the TDS agent package to your server. For example, you can use an FTP client to upload the package to the server.
     c. Run the package on your server as an administrator.

> **Note:**
> The installation of the TDS agent requires a verification key. The verification key is used to associate the TDS agent with your Alibaba Cloud account. You can view the verification key on the **Install/Uninstall TDS Agent** page.

- **Linux**

  a. Depending on the type of your server, select **Alibaba Cloud Servers** or **External Servers**.

  b. Log on to your Linux instance as an administrator.

  c. Upload the TDS agent package to your Linux server, and then select an install command that is applicable to the operating system of your server.

  d. Run the command to download and install the TDS agent.

> **Note:**
> The install command will download the latest version of TDS agent package from Alibaba Cloud. Before you run the command, make sure that your server has access to the Internet.

5. The TDS agent installation may take five minutes to complete. After the TDS agent has been installed, log on to the TDS console and verify the server security status on the **Assets** page:
   - If the server is an ECS instance, the security status of the server changes from **Unprotected** to **Protected**.
   - If the server is an external server, the server is added to the asset list.

Verify TDS agent installation

Follow these steps to verify the TDS agent installation:

1. Verify if the TDS agent processes, including `AliYunDun` and `AliYunDunUpdate`, are running correctly. For more information about the TDS agent processes, see *Threat Detection Service agent*.
2. Verify that your instance can communicate with TDS servers by running the following telnet commands on your instance:

> **Note:**
> Make sure that your server can access at least one of the following jsrv domain names and one of the following update domain names.

- `telnet jsrv.aegis.aliyun.com 80`
- `telnet jsrv2.aegis.aliyun.com 80`
- `telnet jsrv3.aegis.aliyun.com 80`
- `telnet update.aegis.aliyun.com 80`
- `telnet update2.aegis.aliyun.com 80`
- `telnet update3.aegis.aliyun.com 80`

If the verification fails, follow the instructions in *Troubleshoot the problem of TDS agent going offline* to resolve the issue.

Restrictions and guidelines

For an external server that runs Windows, you must use the TDS agent package to install the agent. For an external server that runs Linux, you must run the relevant command to install the agent.

To make sure that the agent can run correctly in the following situations, delete the TDS agent directory and follow the preceding steps to manually reinstall the agent.

- You have used an image that includes the TDS agent to install the TDS agent on multiple external servers.
- You have directly copied the TDS agent files to your external servers.

TDS agent directory

- Windows: *C:\Program Files (x86)\Alibaba\Aegis*
- Linux: */usr/local/aegis*

1.3 Install the TDS agent on servers in private networks

The following sections describe how to install the Threat Detection Service (TDS) agent to connect instances in private networks (such as instances used in Alibaba Cloud's Financial Service Solutions, or instances in Alibaba Cloud VPC) to the TDS server.

Procedure

Follow these steps to install the TDS agent on servers in private networks:

Note:

If security software such as Fortinet FortiGate has been installed on your server, the system may fail to install the TDS agent correctly. We recommend that you check whether security software

already exists on your server before installing the TDS agent. If security software is already installed on your instances, we recommend that you temporarily disable or uninstall the software before you install the TDS agent.

1. Log on to the *Threat Detection Service console*.
2. Go to the **Settings** page.
3. Click **Install/Uninstall TDS Agent**.
4. Depending on the operating system running on your instance, select the applicable installation method.

   - **Windows**

     a. Click **Download** on the **Install/Uninstall TDS Agent** page to download the latest version of TDS agent package to your PC.

     b. Upload the TDS agent package to your instance. For example, you can use an FTP client to upload the package to the instance.

     c. Run the package on your instance as an administrator.

     Note:

     The installation of the TDS agent requires a verification key. The verification key is used to associate the TDS agent with your Alibaba Cloud account. You can view the verification key on the **Install/Uninstall TDS Agent** page.

   - **Linux**

     a. Depending on your system requirements, click one of the following links to download the TDS agent package to your PC.

        - 32-bit Linux: *TDS agent package*
        - 64-bit Linux: *TDS agent package*

     b. Upload the TDS agent package to your instance. For example, you can use an FTP client to upload the package to the instance.

     c. Log on to your Linux instance as an administrator.

     d. Locate the directory that stores the uploaded TDS agent package, depending on your system requirements, run one of the following commands to install the TDS agent:

        - 32-bits Linux: `chmod +x AliAqsInstall_32.sh && . /AliAqsInstall_32.sh xxxxxx`
        - 64-bits Linux: `chmod +x AliAqsInstall_64.sh && . /AliAqsInstall_64.sh xxxxxx`

> **Note:**
> Replace `xxxxxx` at the end of each command with the verification key that is provided on the **Install/Uninstall TDS Agent** page. This verification key is the same as that used to install the TDS agent to a Windows running instance. The verification key is used to associate the TDS agent with your Alibaba Cloud account.

5. Once the TDS agent is installed and synced with your instances (this process may take up to 5 minutes), you can log on to the TDS console and view the Security Status of your instances on the **Assets** page. The Security Status of your instances will change from **Unprotected** to **Protected**.

Verify TDS agent installation

To verify your TDS agent installation, follow these steps:

1. Verify that the *AliYunDun* and *AliYunDunUpdate* processes of the TDS agent are running normally. For more information about the TDS agent processes, see *Threat Detection Service agent*.
2. Verify that your instance can communicate with TDS servers by running the following telnet commands on your instance:

> **Note:**
> Make sure that your instance can communicate with the following two TDS servers properly:
>
> - `telnet jsrv3.aegis.aliyun.com 80`
> - `telnet update3.aegis.aliyun.com 80`

If your instance cannot communicate with the TDS servers properly, see *Troubleshoot the problem of TDS agent going offline* to resolve the issue.

1.4 Troubleshoot the problem of TDS agent going offline

If you have followed instructions in *Install the TDS agent* and successfully installed the Threat Detection Service (TDS) agent on your server, but the security status of the server is still **Unprotected**, then the agent goes doffline. This article describes how to resolve this issue.

Context

If your TDS agent is offline, follow these steps to resolve the issue:

Procedure

1. Log on to your server and check whether the TDS agent processes (*AliYunDun* and *AliYunDunUpdate*) are running.

   If the TDS agent processes are not running, we recommend that you restart your server or reinstall the TDS agent. For more information, see *Install the TDS agent*.

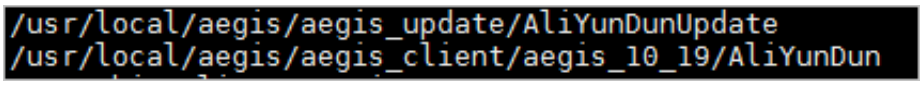
   - **Windows**

     Open the Task Manager and check whether the following processes are running.

   - **Linux**

     Run the `top` command to check whether the following processes are running.

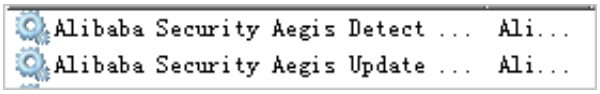
     

2. If you have installed the TDS agent on a server for the first time and the security status of the server is **Unprotected** after installation, you can restart the TDS agent using the following methods:

   - Linux: Run the following command: `killall AliYunDun && killall AliYunDunUpdate && /usr/local/aegis/aegis_client/aegis_10_xx/AliYunDun`.

     Note:
     You must replace `xx` with the largest number in the directory.

   - Windows: Restart the two services displayed in the following screenshot by right-clicking and selecting Restart.

3. Check whether the network connection on your server is normal.

   - Servers with public IP addresses (for example, servers connected to classic networks, EIPs, or external hosts)
     - Windows: Run the following command: `ping jsrv.aegis.aliyun.com -l 1000`
     - Linux: Run the following command: `ping jsrv.aegis.aliyun.com -s 1000`
   - Servers without public IP addresses (for example, servers connected to the Financial Cloud, or VPCs)
     - Windows: Run the following command: `ping jsrv3.aegis.aliyun.com -l 1000`

- Linux: Run the following command: `ping jsrv3.aegis.aliyun.com -s 1000`

4. If the ping command does not work, try the following methods:

   a. Make sure that the DNS service is running on your server. If the DNS service is not running , restart your server or check whether a DNS error has occurred.

   b. Check whether firewall ACL rules or Alibaba Cloud security group rules have been configured on your server. If firewall rules or security group rules have been configured, make sure that the IP address of the TDS server is added to the whitelist (both in the inbound and outbound directions).

   Note:
   Allow the following network segments to access your server on port 80. For the last network segment, both port 80 and 443 must be enabled.

   - 140.205.140.0/24 80
   - 106.11.68.0/24 80
   - 110.173.196.0/24 80
   - 106.11.68.0/24 80
   - 100.100.25.0/24 80 443

   c. Check whether the public network bandwidth on your server is zero. If the public network bandwidth on your server is zero, try the following methods:

      A. Add the following name resolution rules to the hosts file on your server:

      - `100.100.25.3 jsrv.aegis.aliyun.com`
      - `100.100.25.4 update.aegis.aliyun.com`

      B. After changing the hosts file, run the following command: `ping jsrv.aegis.aliyun.com`.

      Note:
      If `100.100.25.3` is not returned, restart your server or check whether a DNS error has occurred.

      C. If the ping command does not return expected results, change the values of `t_srv_domain` and `h_srv_domain` in the `network_config` file under the TDS agent installation directory (*conf*) to `100.100.25.3` and `100.100.25.4` respectively. After making the changes, restart the TDS agent.

> **Note:**
> You must create a copy of the `network_config` file before making the changes.

This method only applies when the public network bandwidth on the server is zero and the TDS agent is offline.

d. If the ping command returns the correct IP address, run the following telnet command to verify connectivity: `telnet 140.205.140.205 80`. If no connectivity is found, check firewall restrictions.

5. Check whether high CPU or memory usage (maintained at 95% or higher for a long period) has occurred. High CPU or memory usage may prevent the TDS agent from running properly.
6. Check whether third-party security products (such as Fortinet FortiGate) have been installed on your server. Some third-party security software may prevent the TDS agent from accessing the network.

   If security software is installed on your servers, we recommend that you temporarily disable or uninstall the software before reinstalling the TDS agent.

1.5 Uninstall the TDS agent

You can use the following methods to uninstall the Threat Detection Service (TDS) agent and disable the protection. After you have uninstalled the TDS agent, there is a waiting period of six hours before the Security Status of the server in the TDS console changes to unprotected.

> **Note:**
> After you have uninstalled the agent, TDS initializes self protection. The protection duration is 24 hours. During this period, you can only manually reinstall the agent. When you reinstall the agent, you must ignore all the error messages that the system displays and run the install command more than three times.

Automatically uninstall the TDS agent

Prerequisites

To uninstall the TDS agent, you must make sure that the status of the agent on the current server is online. An offline server cannot receive the uninstall instruction.

Procedure

Follow these steps to automatically uninstall the TDS agent:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click **Settings**.
3. Click **Install/Uninstall TDS Agent**.
4. Click **Uninstall Agent** in the upper-right corner.
5. Specify the server where the TDS agent runs in the **Uninstall Agent** dialog box, and click **Uninstall Now**.
6. Wait for the system to uninstall the TDS agent on the specified server.

Manually uninstall the TDS agent

Select a method that is applicable to the operating system of your server to manually uninstall the TDS agent:

Linux servers

1. Log on to your server.
2. Run the following command to download the script for uninstalling the TDS agent.

```
wget http://update.aegis.aliyun.com/download/uninstall.sh
```

3. Sequentially run the following commands to uninstall the TDS agent.
   - `chmod +x uninstall.sh`
   - `./uninstall.sh`

Windows servers

1. Log on to your server.
2. *Download the script for uninstalling the TDS agent* to your server.

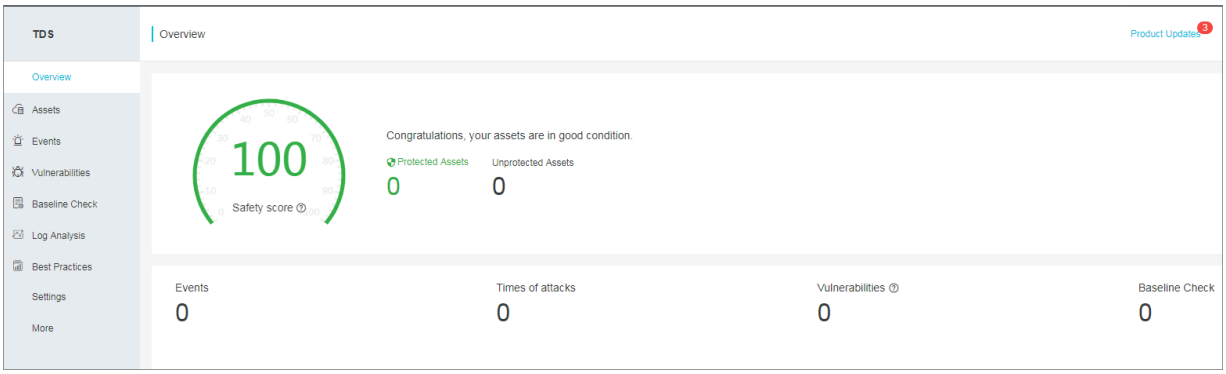
Note:
You can also download the script to your computer and use an FTP client to upload the script to your server.

3. Double-click the *uninstall.bat* file to run the script and uninstall the agent.

2 Overview

As the security operation center of Alibaba Cloud, the **Overview** page of the Threat Detection Service (TDS) 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 TDS, renew your TDS 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:

- TDS edition: Click **Upgrade to Enterprise Edition**/**Renew**on the top right of the Overview page, you can upgrade to your TDS to the Enterprise Edition, scale up your assets, or renew your TDS service.

  Basic Edition :

  Enterprise Edition :

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

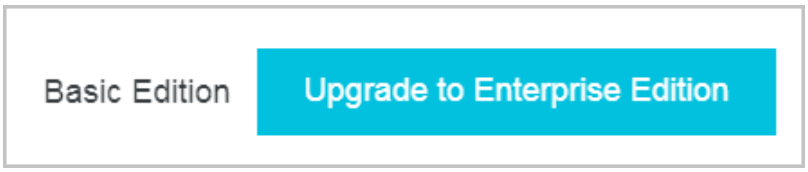
To add unprotected assets under the protection of TDS, click the number under **Unprotected Assets** and on the displayed **Install/Uninstall TDS Agent** page, install the TDS agent. For more information, see *Install the TDS agent*.

- **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 TDS service

TDS 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 TDS is shown in the upper-right corner of the page. An **Upgrade to Enterprise Edition** button is also displayed. If you upgrade your TDS 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 TDS 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 TDS, 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 TDS. 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 2-1: Impacts to safety score table

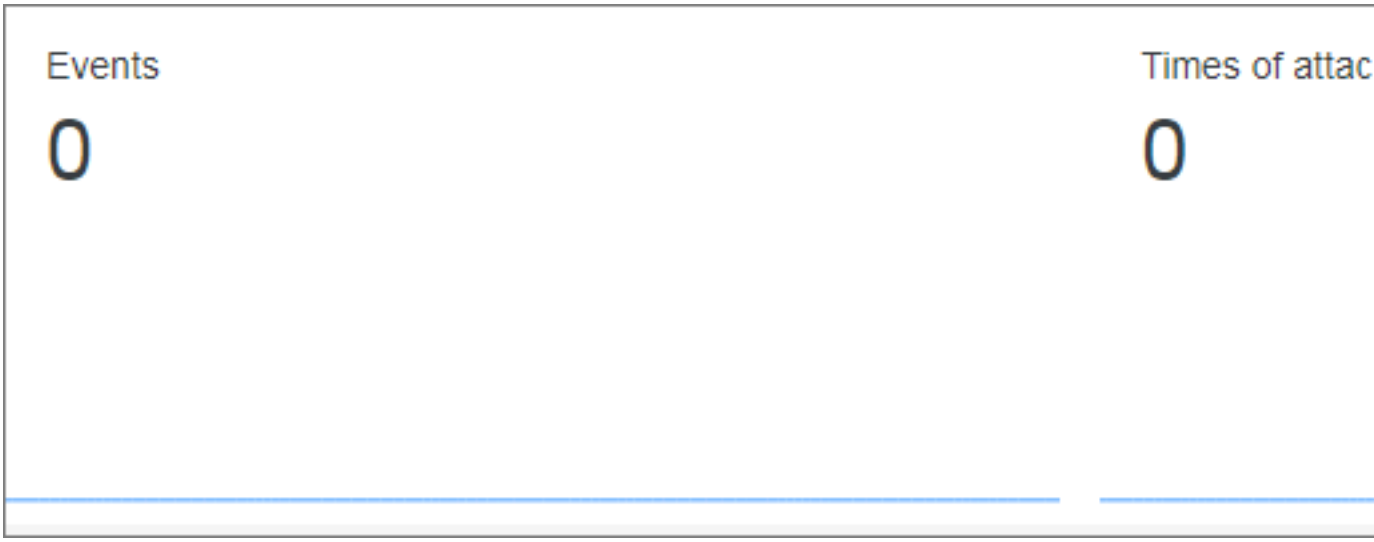
Impact	Strengthening suggestion
Lack of a security operation center	Establish an in-depth defense system. If you have any queries, submit a ticket for technical support.
Unfixed vulnerabilities	Fix the vulnerabilities. For more information, see Vulnerabilities.
Unhandled security events	Handle the security events in a timely manner.
Lack of host protection	Enable the enterprise edition of Server Guard.
The protection status is offline (the TDS agent is not installed or offline).	Install the TDS 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.

Impact	Strengthening suggestion
Host exceptions	Handle the host exception events.

Threat statistics

The **Overview** page displays the statistics of the threats that TDS 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.



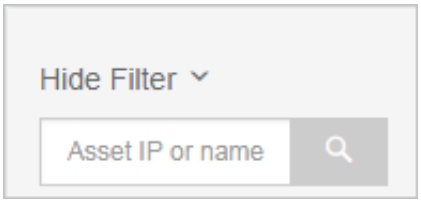
3 Assets

The Assets page in the Threat Detection Service (TDS) console allows you to view the security status of the assets that have been protected by TDS. 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

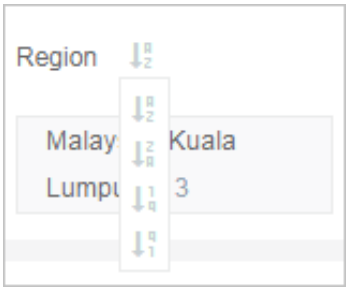
To view the security status of your assets, follow these steps:

1. Log on to the *Threat Detection Service console* .
2. In the left-side navigation pane, click **Assets** to view the security status of the assets that have been protected by TDS.
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**.

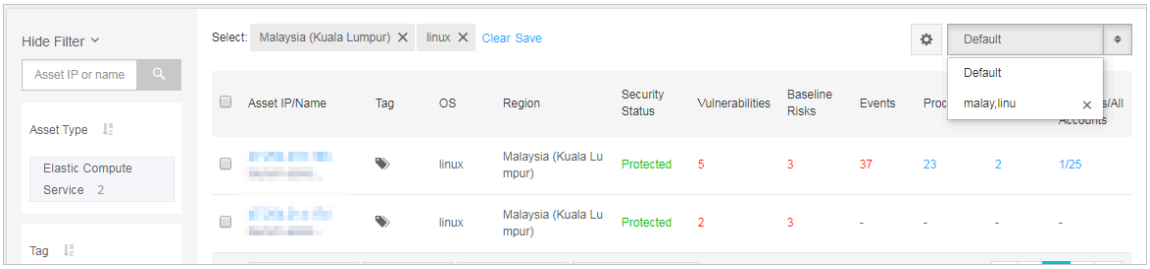
Note:
When a filtering item contains too many criteria, you can click the sort button next to the filtering item to sort these criteria. You can sort the criteria in the alphabetical ascending order (A to Z), alphabetical descending order (Z to A), numerical ascending order (1 to 9), and numerical descending order (9 to 1).



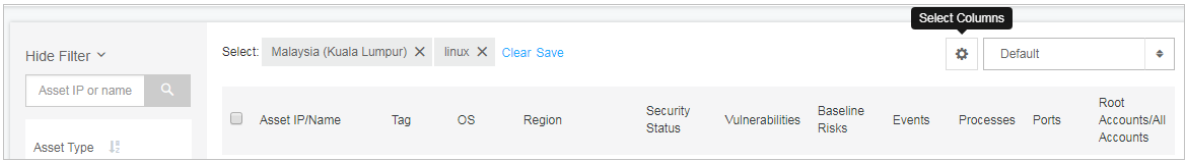
- You can select a criterion under a filtering item to view assets that match the specified criterion. For example, you can select **Malaysia (Kuala Lumpur)** under the **Region** item to view servers in the Malaysia (Kuala Lumpur) region.
- You can also select multiple criteria under a filtering item, 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.

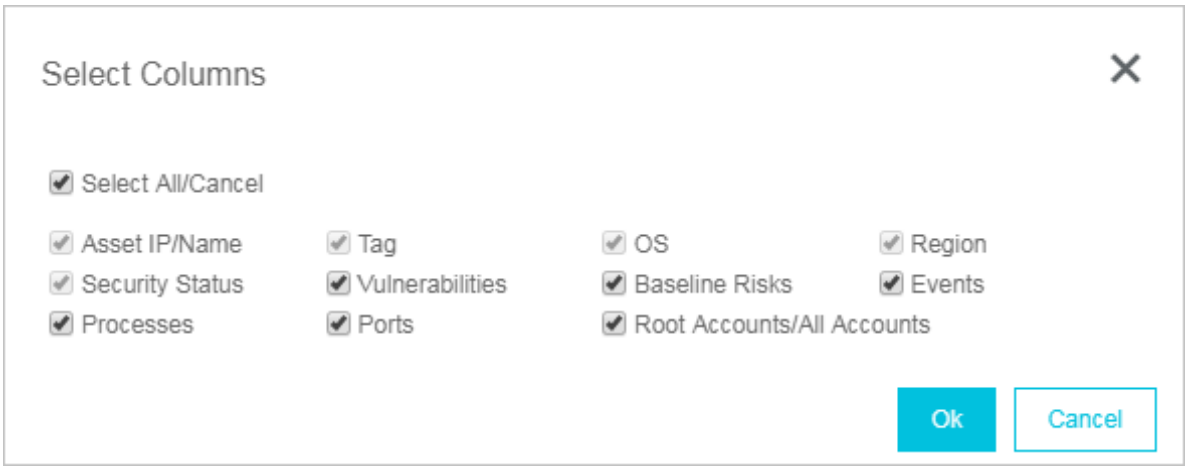
Note:

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.

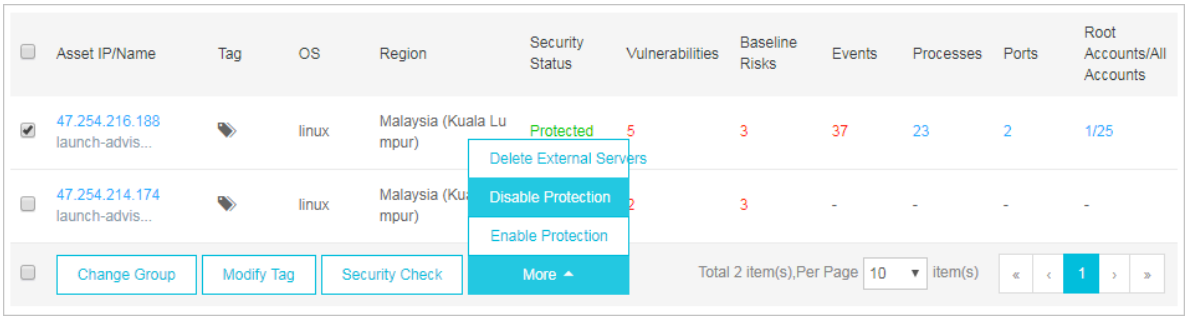




Disable/Enable TDS protection

If you want the TDS agent to stop consuming resources on your assets for a specific period of time, follow these steps to disable TDS 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**.



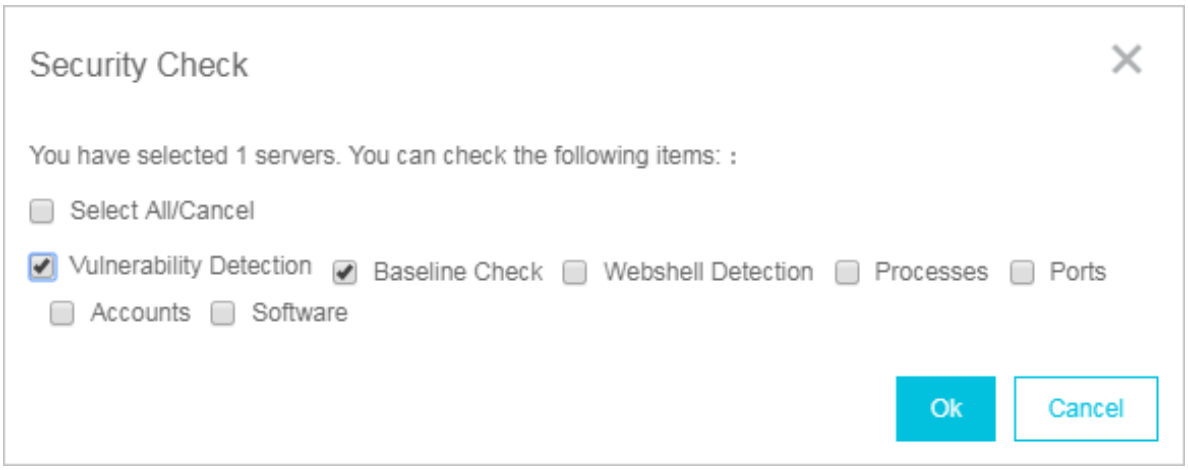
After TDS protection has been disabled, the TDS agent no longer collects security information on your servers, reports security information, or occupies system resources. You can select **More** > **Enable Protection** to enable TDS protection for your assets.

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 TDS 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

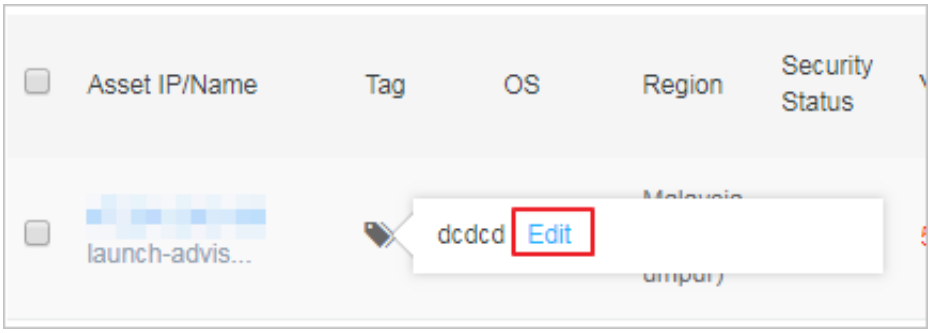
You can use tags to label your assets and filter assets on the Assets page by tag.

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:

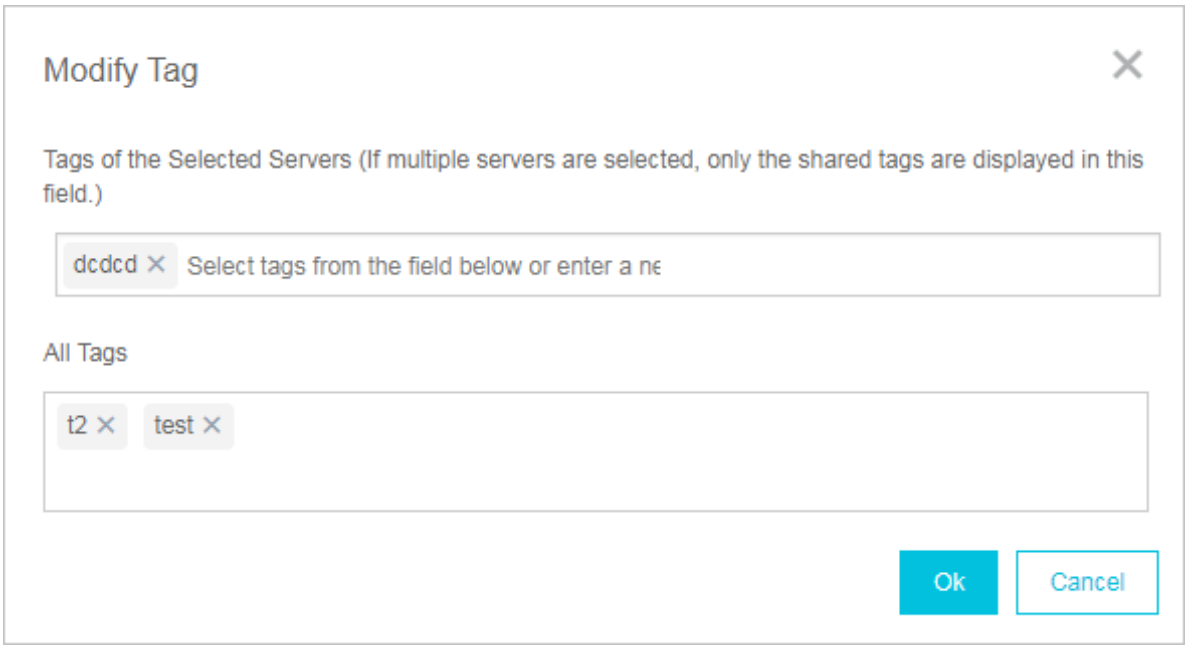
You can select one or more assets, and click **Modify Tag** under the asset list to modify tags for these assets at the same time.



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

Note:

You can add multiple tags to an asset.



4. Click **OK**.

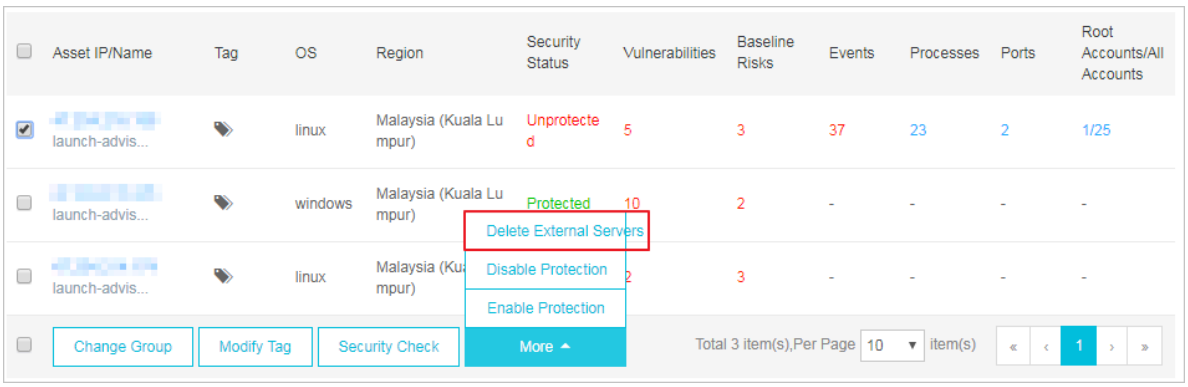
Remove external server

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

> **Note:**
> Uninstalling the TDS 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 TDS agent on your servers and then remove the servers from the asset list.

4 Vulnerabilities

4.1 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 (TDS) may discover thousands of vulnerabilities on your assets. Such a large number means it is difficult to prioritize the vulnerabilities. To resolve this issue, TDS provides a set of prioritization standards for you to prioritize these vulnerabilities.

Vulnerability severity score

TDS 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 TDS to calculate a vulnerability severity score from the time that the vulnerability was detected by TDS.

Note:

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

- Network malfunctions, such as TDS 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

- TDS 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**.

4.2 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 (TDS).

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 TDS console to check system vulnerabilities on the server. For more information about descriptions of Linux software vulnerability attributes in TDS, 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

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.

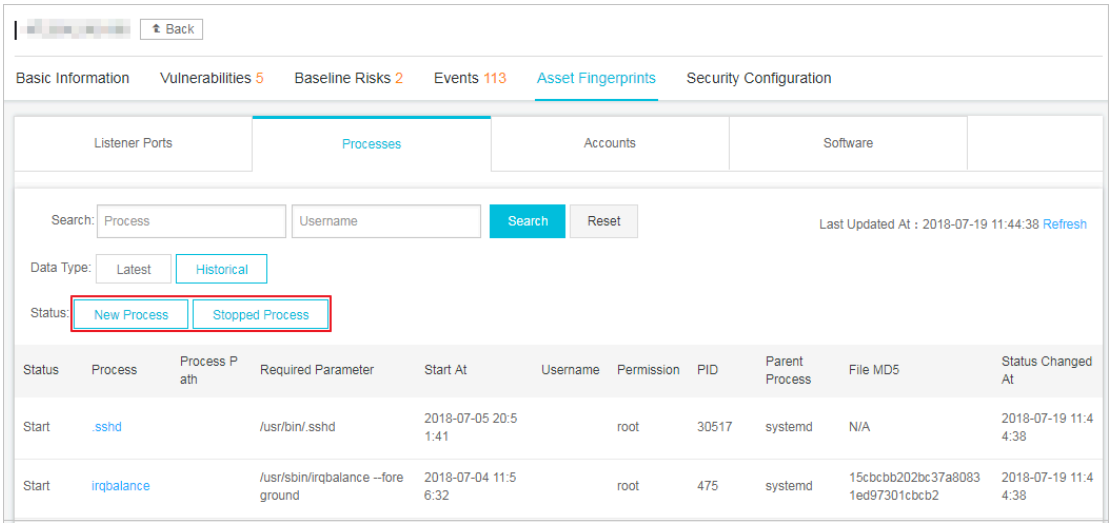
1. Log on to the *Threat Detection Service console*.
2. Go to the **Assets** page, select the asset you want to view, and click its **Asset IP/Name**.

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**.

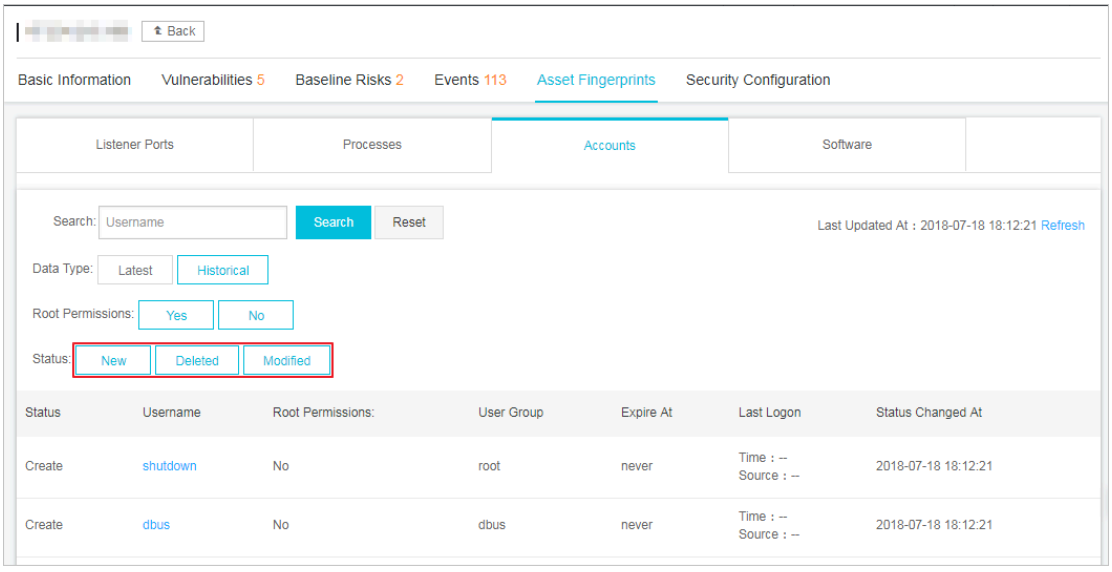


     c. Click a process name to view the details.

   - **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**.

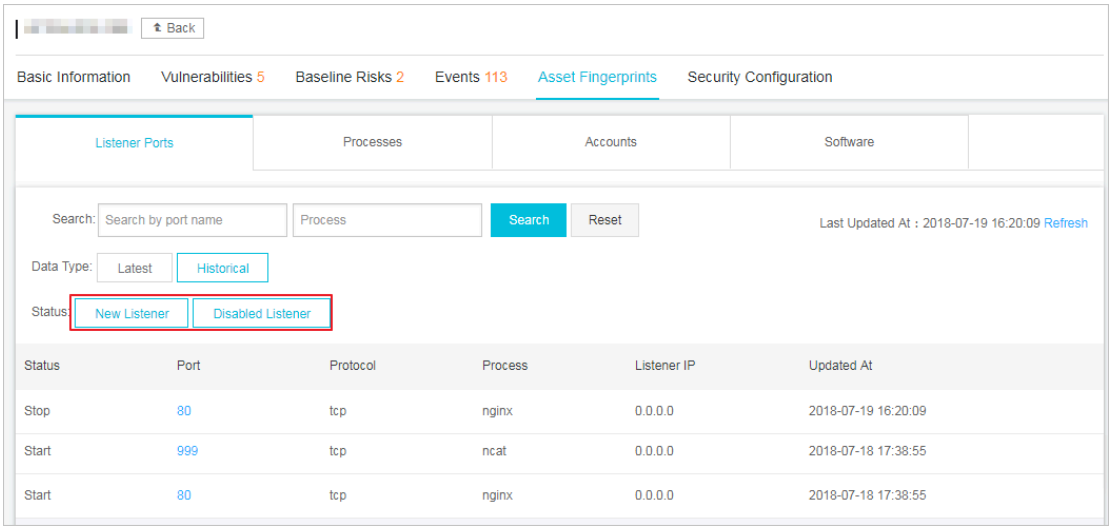


c. Click an account name to view account details.

- **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**.

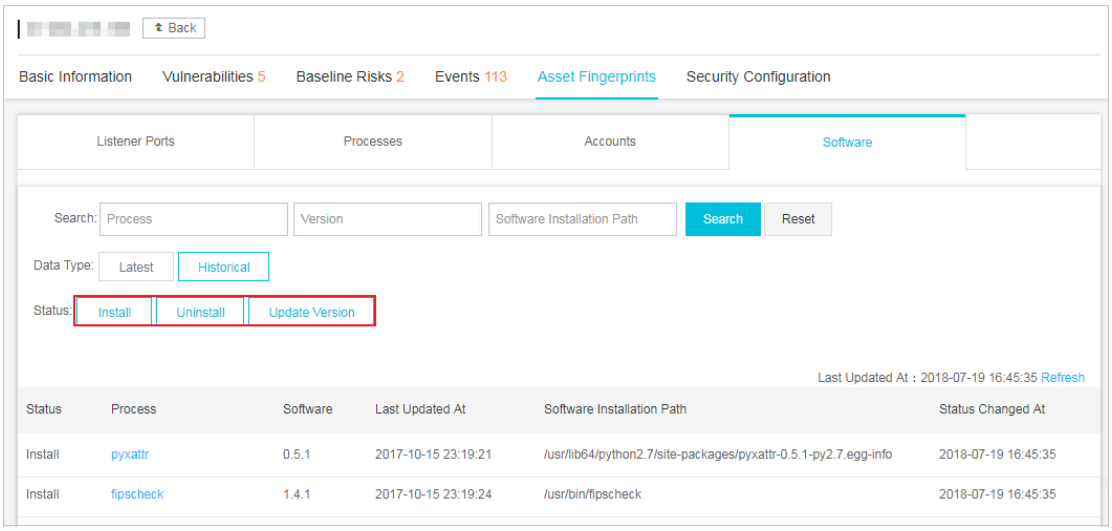


c. Click a port number to view the details.

- **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.

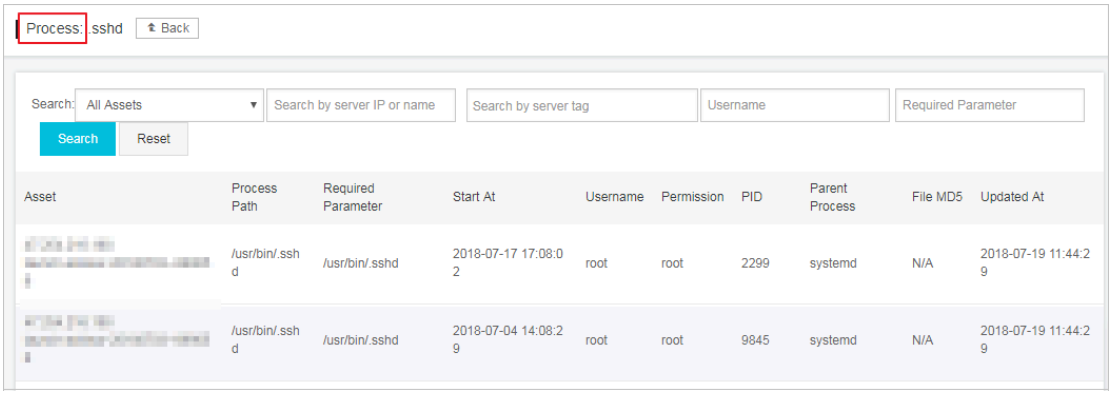
Follow these steps to view asset fingerprints for all assets:

1. Log on to the *Threat Detection Service 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.

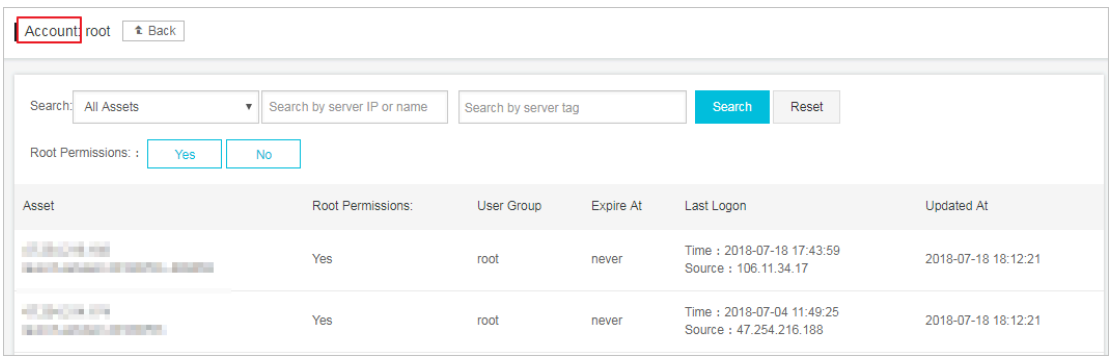
  b. Click a process name to view the details.



- **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.

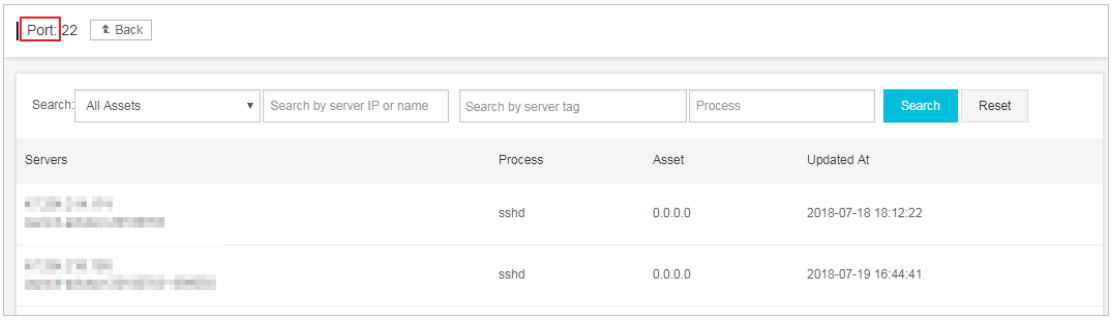
  b. Click an account name to view account details.



- **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.

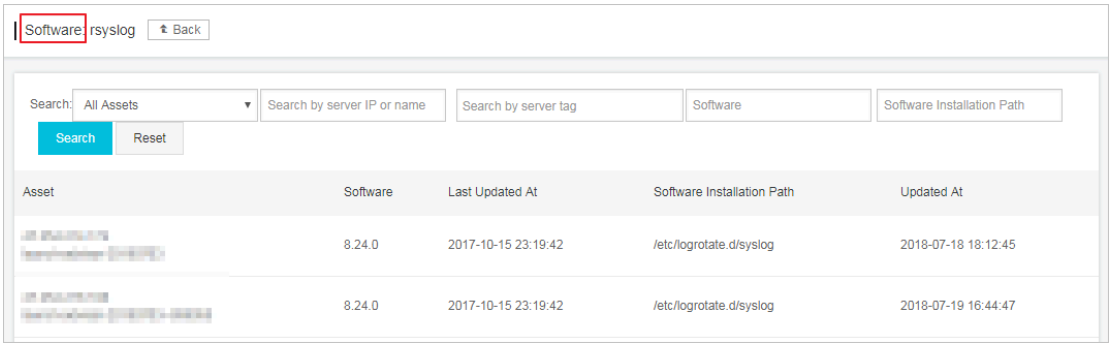
b. Click a port number to view the details.



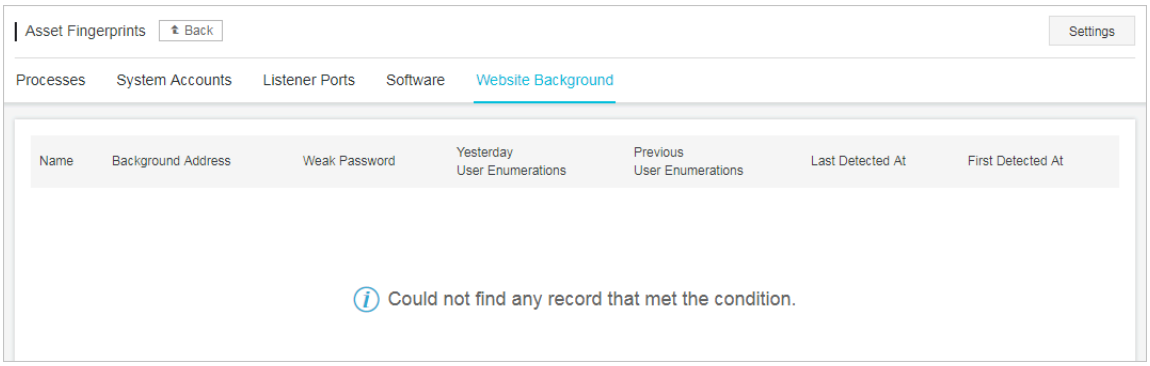
- **View software**

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.

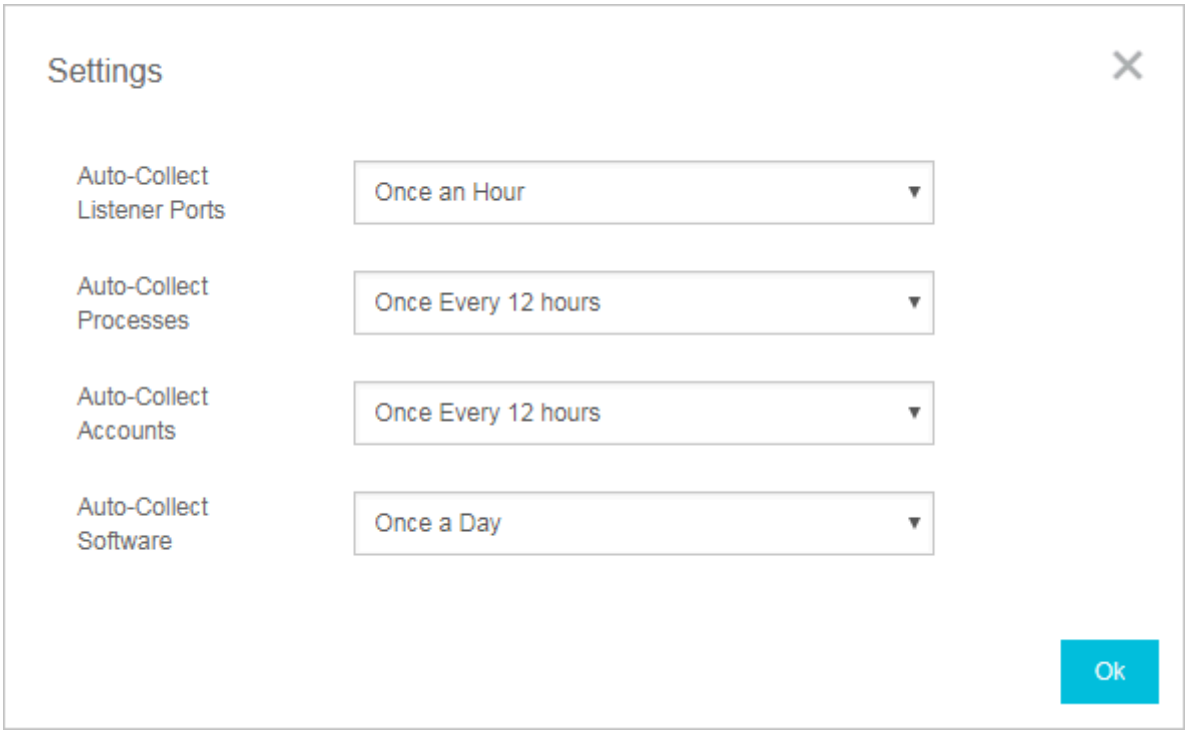


Settings

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 *Threat Detection Service 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

8.1 Log retrieval

Threat Detection Service (TDS) provides the log retrieval feature to help you manage logs on your Alibaba Cloud systems. You can easily identify the causes of problems that occur on your servers.

Note:

You must upgrade to the Threat Detection Service Enterprise Edition to use the log retrieval feature. TDS records your logs and supports retrieval only when the Log retrieval feature is enabled. Currently, TDS retains logs for 180 days and allows you to retrieve the logs of the last 30 days.

Benefits

The log retrieval feature provides the following benefits:

- One-stop log retrieval platform. You can retrieve all logs on your Alibaba Cloud systems and trace problems easily.
- Web-based log retrieval. Without the need for additional deployment, you can log on to the TDS console using a browser and use the log retrieval feature directly.
- Supports TB sized data retrieval. You can add multiple operators in a search condition and get full-text search results within several seconds.
- Supports various kinds of server logs and Web logs.

Scenarios

You can use log retrieval to achieve the following scenarios:

- Security incident analysis: When a security incident occurs on your server, you can retrieve the logs to investigate the cause, and evaluate the damage and affected assets.
- Operation review: You can review operation logs on your server, and troubleshoot high-risk operations or serious problems with fine granularity.
- Business traffic statistics: You can analyze Web access logs to track your visitors and their requests, and evaluate your service responses.

Supported logs

You can retrieve the following types of logs:

Type	Log	Description
Server log	Logon history	Logs of successful logons
	Brute force cracking	Logs of brute force cracking attacks
	Process snapshot	Logs of processes on the server at a specific time
	Port snapshot	Logs of listener ports on the server at a specific time
	Account snapshot	Account logon information on the server at a specific time
	Process initiation log	Logs of process initiation on the server
	Network connection log	Logs of outgoing connections from the server
Web log	Web access log	HTTP logs of the cloud services
	Network session log	Logs of the 5-tuples of the cloud services
	DNS log	Domain name resolution logs

Note:

For more information, see *Supported logs and fields*.

Procedure

You can use the log retrieval feature by following these steps:

1. Log on to the *Threat Detection Service console*.
2. In the left-side navigation pane, click **More**.
3. Select **Log Retrieval**.
4. Select a **Log Source** and **Field**, specify a **keyword** and Duration, and then click **Search**. The duration can be the last 24 hours, the last 7 days, or a specified time period within the last 30 days.

Note:

You can click **+** on the right-side of the page to add multiple operators to a search condition, or click **Add Conditions** to add multiple search conditions. You can delete an operator by clicking **-**. For more information, see *Grammar logic instructions*.

5. Detailed log records are retrieved based on your search conditions. You can modify the fields in search results for further analysis, or click **Save Search** to save the current search conditions for future use. You can click **Saved Searches** to use saved search conditions.
6. You can view the search results based on different time granularities and export the results.

8.2 Grammar logic instructions

The log retrieval feature supports multiple search conditions. You can include multiple operators in a query on one log, or combine multiple queries on several logs based on different logic. This document describes the operators and keywords that are supported in log queries.

The following operators and keywords are supported in log queries:

Operator	Description
and	Binary operator. The format is `query1 and query2`. The result returns the records that match both `query1` and `query2`. **Note:** When no operator has been specified among multiple words, the default operator `and` is used.
or	Binary operator. The format is `query1 or query2`. The result returns all records that match either `query1` or `query2`.
not	Binary operator. The format is `query1 not query2`. The result returns the records that match `query1` but not `query2`, which is equivalent to `query1-query2`. **Note:** If only `not query1` is specified, the result returns all records that do not match `query1`.