# Alibaba Cloud Threat Detection

## Access Cloud Security Center

Issue: 20190321

# 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:<br>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:<br>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:<br>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:<br>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 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 `AliYunDunU pdate`, 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`

# 2 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 AliAqsInst all_32 . sh && . / AliAqsInst all_32 . sh xxxxxx`
     - 64-bits Linux: `chmod + x AliAqsInst all_64 . sh && . / AliAqsInst all_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.

# 3 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.

# 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 `AliYunDunU pdate` ) 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 AliYunDunU pdate && / usr / local / aegis / aegis_clie nt / aegis_10_x x / 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:

- Domestic classic websites: `100 . 100 . 110 . 61  jsrv . aegis . aliyun . com`, `100 . 100 . 45 . 131  jsrv . aegis . aliyun . com`, `100 . 100 . 110 . 62  update . aegis . aliyun . com` and `100 . 100 . 45 . 29  update . aegis . aliyun . com`
- International classic websites: `100 . 100 . 103 . 52  jsrv . aegis . aliyun . com`, `100 . 100 . 30 . 54  jsrv . aegis . aliyun . com`, `100 . 100 . 30 . 55  update . aegis . aliyun . com` and `100 . 100 . 103 . 54  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_doma  in` and `h_srv_doma  in` in the `network_co  nfig` 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_co  nfig` 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.

# 5 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_clie nt`
  - Windows 64-bits: `C :\ Program Files ( x86 )\ Alibaba \ aegis \ aegis_clie nt`
  - 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_upda te`
  - **Windows 64-bits:** `C :\ Program Files ( x86 )\ Alibaba \ aegis \ aegis_upda te`
  - **Linux:** `/ usr / local / aegis / aegis_upda te`