

# Alibaba Cloud

## Security Center Assets

Document Version: 20220707

# Legal disclaimer

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

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

# Document conventions

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

# Table of Contents

1. Overview	06
2. Asset exposure analysis	08
3. Manage servers	12
3.1. Overview	12
3.2. View the security status of a server	19
3.3. Enable or disable server protection	23
3.4. Collect asset fingerprints	24
3.5. Use the security check feature	28
3.6. View asset fingerprints	29
4. View container information	31
4.1. View security information about containers	31
4.2. Connect a self-managed Kubernetes cluster to Security Ce...	33
4.3. Use CI/CD-based container image scan	37
4.3.1. Overview	37
4.3.2. Obtain a token of the CI/CD plug-in	38
4.3.3. Install the CI/CD plug-in for a Jenkins Freestyle project	39
4.3.4. Install the CI/CD plug-in for a Jenkins Pipeline project	41
4.3.5. Install the CI/CD plug-in for GitHub Actions	43
4.3.6. View image scan results	46
5. View website status	47
6. View the security status of cloud services	51
7. View the details of an asset	54
8. Manage asset groups	57
9. Manage asset tags	61
10. Use the agent troubleshooting feature	65
11. Unbind a server not deployed on Alibaba Cloud from Security..	72

---

12.FAQ	74
--------	----

# 1. Overview

The Assets page in the Security Center console displays the statistics and security status of protected assets.

## Background information

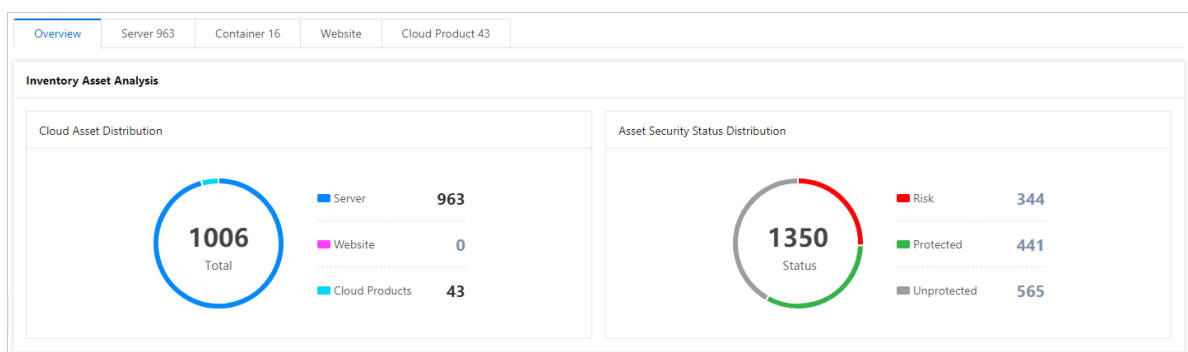
The Assets page displays asset information such as the asset type, regional distribution, protection status, and risk status.

Groups and tags are supported to classify your assets. This facilitates the management of your assets. You can group assets and view security events by asset group. You can also add a tag to the assets of the same attributes and search for specific assets by tag. For more information, see [Manage asset groups](#) and [Manage asset tags](#).

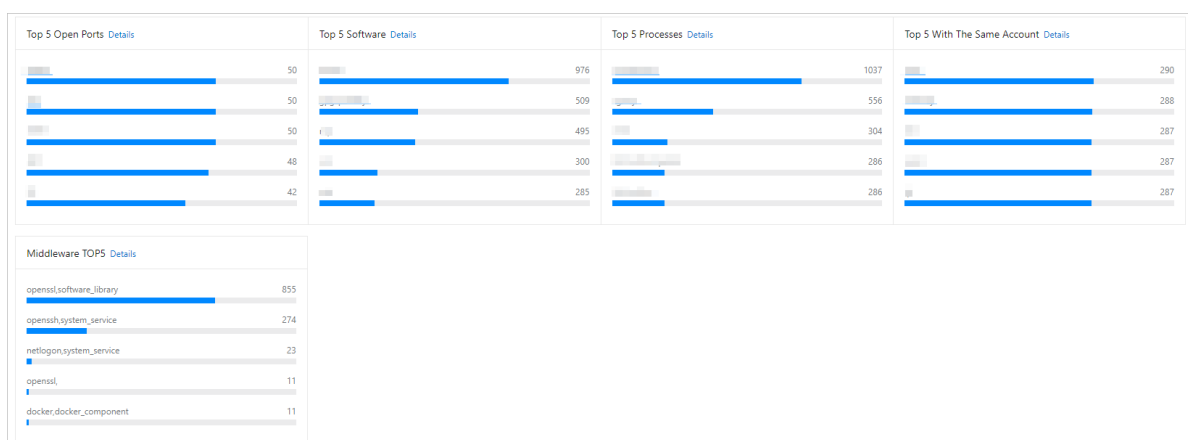
## Overview tab

The Overview tab on the Assets page in the [Security Center console](#) displays the following information:

- **Inventory Asset Analysis:** displays the numbers of your assets and their security statuses.



- **Server Asset Analysis:** displays information in a number of sections. The information includes the security status of your servers, status of the Security Center agent, regional distribution of your servers, operating systems that your servers run, top five open ports, top five software on your servers, top five processes on your servers, and top five assets that belong to the same Alibaba Cloud account.



- In the **Server Asset Analysis** section, you can click **Details** to go to the **Assets > Server(s)** tab where you can view the server details. For more information, see [View the security status of a server](#).

- You can click **Details** in the **Regional Distribution** section to go to the **Assets > Server(s) > Region** tab where you can view the regional distributions of your servers. For more information, see [View the security status of a server](#).
- You can click **Details** in the **Top 5 Open Ports**, **Top 5 Software**, **Top 5 Processes**, **Top 5 With The Same Account**, or **Middleware TOP5** section to go to the **Asset Fingerprints** page where you can view corresponding fingerprint details. For more information, see [Overview of asset fingerprints](#).
- **Cloud Product Risk Distribution**: displays the number of cloud services and their security statuses.



You can click the number next to **Risks** or **Security** to go to the **Assets > Cloud Product** tab. Then, you can view cloud services that are in the **At-risk** or **No risk** state. For more information, see [View the security status of cloud services](#).

**Note** If the number next to **Risks** or **Security** is 0, you cannot click the number to go the Cloud Product tab.

## 2.Asset exposure analysis

The feature of asset exposure analysis automatically analyzes the exposures of your Elastic Compute Service (ECS) instances on the Internet and visualizes the communication links between your ECS instances and the Internet. The feature also displays details about the vulnerabilities in the exposed ECS instances in a centralized manner. This way, you can identify the exposures of your assets on the Internet and fix the vulnerabilities based on the suggestions provided by the feature. This topic describes how to use asset exposure analysis of Security Center.

### Context

Asset exposure analysis depends on the middleware information that is collected in asset fingerprints. To collect the middleware information, perform the following operations: In the upper-right corner of the **Asset Fingerprints** page, click **Settings**. In the **Settings** dialog box, set **Middleware** to **Collected once an hour**, **Collected once 3 hours**, **Collected once 12 hours**, or **Collected once a day**. If you set **Middleware** to **Disable** or a value that indicates a long collection cycle such as **Collected once every 7 days**, asset exposure analysis does not refresh the analysis results on a daily basis. For more information, see [Automate periodic collection tasks](#).

The analysis results of asset exposures are automatically refreshed on a daily basis. You do not need to refresh the results.

### Limits

The analysis results of asset exposures involve only the exposures of your ECS instances on the Internet. The results do not contain the exposures of servers that are not deployed on Alibaba Cloud on the Internet.

### Statistics

The **Asset Exposure Analysis** page displays the exposure statistics of the assets on the Internet and the details of the exposures. The following table describes the details of the exposures.

Item	Description
Exposed Assets/Public IP	The total numbers of servers and IP addresses that are exposed on the Internet.
Gateways	The total number of gateway assets that are exposed on the Internet. The gateway assets include Network Address Translation (NAT) gateways and Server Load Balancer (SLB) instances. You can click the number below <b>Gateways</b> to go to the Gateways panel. In the panel, you can view the gateway assets that are exposed on the Internet. You can also click the name of an exposed gateway asset to go to the details page of the asset.
Exposed Ports	The total number of ports that are exposed on the Internet. You can click the number below <b>Exposed Ports</b> to go to the Exposed Ports panel. In the panel, you can view the ports that are exposed on the Internet. You can also click the name of an exposed port to view the assets that use this port.




Item	Description
Exposed Components	The total number of server components that are exposed on the Internet. The components include OpenSSL and OpenSSH. You can click the number below <b>Exposed Components</b> to go to the Exposed Components panel. In the panel, you can view the components that are exposed on the Internet. You can also click the name of an exposed component to view the assets that use this component.
Exploitable Vul	<p>The total number of vulnerabilities that can be exploited by attackers and the numbers of high-risk, medium-risk, and low-risk vulnerabilities. You can click the number of high-risk, medium-risk, or low-risk vulnerabilities to go to the <b>Vulnerabilities</b> page. The priorities of vulnerabilities are marked in different colors:</p> <ul style="list-style-type: none"><li>• High-risk vulnerabilities: red. These vulnerabilities pose major threats to your assets. We recommend that you take note of these vulnerabilities and fix them at the earliest opportunity.</li><li>• Medium-risk vulnerabilities: orange. These vulnerabilities cause damages to your assets. We recommend that you fix the vulnerabilities at the earliest opportunity.</li><li>• Low-risk vulnerabilities: gray. These vulnerabilities are less harmful to your assets than high-risk and medium-risk vulnerabilities. You can fix low-risk vulnerabilities at your convenience.</li></ul>
Weak Passwords	The total number of detected weak passwords on your servers that are exposed on the Internet. You can click the number below Weak Passwords to view the exposed servers on which weak passwords are detected.


## View the exposure details about an asset

The panel of asset exposure details shows the communication link between assets and the Internet. To view the exposure details about an asset, perform the following steps:

- 1.
- 2.
3. Specify filter conditions above the list of exposed assets to query the assets that you want to view.

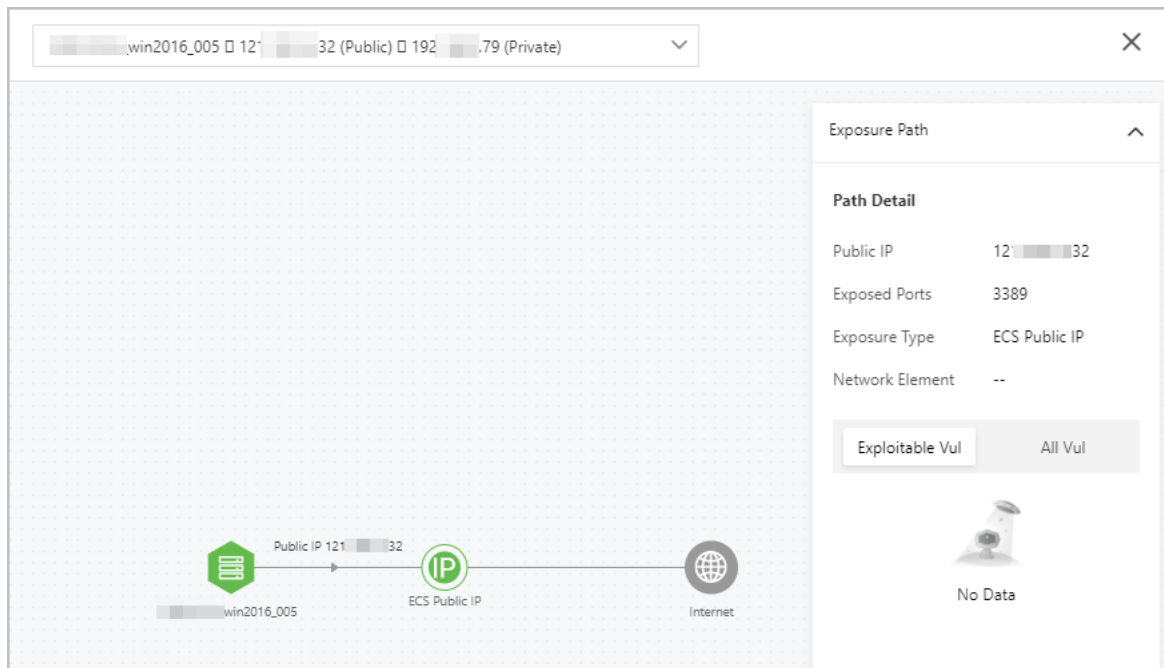
You can query the assets on which vulnerabilities are detected or no vulnerabilities are detected. You can also filter assets by asset group. Alternatively, you can enter a public IP address, port number, component name, name of your ECS instance, or ID of your ECS instance.

In the upper-right corner above the exposed asset list, you can click the  icon to export and save the exposure details of the assets to your computer. The exposure details of the assets are exported to an Excel file.

 **Note** The time required to export the exposure details varies based on the size of the exposure details data.

4. Find the asset that you want to view and click **Exposure Details** in the Operation column.

5. In the panel that appears, view the communication link topology between the asset and the Internet, the details of the link, the detected weak passwords, and the details of vulnerabilities.



If your server accesses the Internet by using multiple methods, the communication link topology shows multiple paths to access the Internet. For example, if your server accesses the Internet by using a NAT gateway and an SLB instance, the communication link topology shows two paths to access the Internet. You can click the asset on each access path to switch to the path and view the path details.

Different colors in a communication link topology indicate different severities of the vulnerabilities detected in each asset.

- Red: High-risk vulnerabilities are detected in your asset. These vulnerabilities can be exploited over the Internet by attackers.
- Orange: Medium-risk vulnerabilities are detected in your asset. These vulnerabilities can be exploited over the Internet by attackers.
- Gray: Low-risk vulnerabilities are detected in your asset. These vulnerabilities can be exploited over the Internet by attackers.
- Green: No vulnerabilities that can be exploited over the Internet by attackers or weak passwords are detected in your asset.

**Note** The mappings between the colors and severities of vulnerabilities apply only to your assets. The mappings do not apply to other components in the communication link topology, such as the Internet. By default, the icon that indicates the Internet is gray.

6. Click the name of a vulnerability. On the Application tab of the Vulnerabilities page, you can view the details of the application vulnerability.

In the vulnerability list that shows the application vulnerabilities detected in the asset, you can view the details of the vulnerabilities and manually fix the vulnerabilities based on the fix suggestions. We recommend that you fix high-risk vulnerabilities at the earliest opportunity. For more information, see [View and handle application vulnerabilities](#).

7. Click the **Weak Passwords** tab to view the details of detected weak passwords.

You can click the name of a weak password item to go to the details page of the asset. On the **Baseline Risks** tab, you can view all the baseline risks that are detected on the asset. Attackers may exploit the weak passwords of your servers to log on to your servers and steal data on your servers or compromise your servers. We recommend that you fix weak password vulnerabilities at the earliest opportunity.

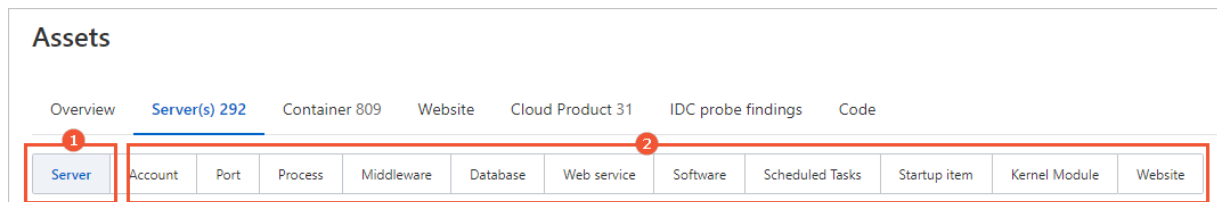
# 3. Manage servers

## 3.1. Overview

Security Center collects and records information including information about your servers and information about ports, software, processes, accounts, scheduled tasks, and middleware on the servers. This helps you monitor the status of your assets and trace the sources of security events.

### Background information

- You can view the information about all servers that are protected by Security Center on the **Server** tab. The Server tab is marked 1 in the following figure. For more information, see [View the security status of a server](#).
- You can also click a tab in the section that is marked 2 in the following figure to collect and view the asset fingerprints of your servers. The asset fingerprints include **Account**, **Port**, and **Process** fingerprints. For more information, see [Collect asset fingerprints](#) and [View asset fingerprints](#).



### Limits on the asset fingerprints feature

Only the Enterprise and Ultimate editions of Security Center support this feature. If you do not use these editions, you must upgrade Security Center to the Enterprise or Ultimate edition before you can use this feature. For more information about how to purchase and upgrade Security Center, see [Purchase Security Center](#) and [Upgrade and downgrade Security Center](#). For more information about the features that each edition supports, see [Features](#).

### Investigation of asset fingerprints

- You can collect asset fingerprints on the **Server(s)** tab of the **Assets** page. After you collect asset fingerprints, you can analyze them. You can collect the following types of asset fingerprints: **Account**, **Port**, **Process**, **Middleware**, **Database**, **Web service**, **Software**, **Scheduled Tasks**, **Startup item**, **Kernel Module**, and **Website**. For more information, see [Asset fingerprints](#).
- If you want to collect the asset fingerprints of a server, you can click the server name on the **Server(s)** tab of the **Assets** page to go to the server details page. On the **Asset Fingerprints** tab, you can manually run a task to collect asset fingerprints of the server. For more information, see [Collect the fingerprints of a specific asset with a few clicks](#).

### Asset fingerprints

Asset fingerprint type	Description
------------------------	-------------

Asset fingerprint type	Description
Account	<p>The information about the account of your server. Security Center periodically collects information about the account of your server. The information includes the following items:</p> <ul style="list-style-type: none"> <li>• <b>Server information:</b> the server in which the account is created.</li> <li>• <b>ROOT Permission:</b> whether the account is granted the root permissions.</li> <li>• <b>User Group:</b> the user group to which the account belongs.</li> <li>• <b>Expiration Time:</b> the time when the password of the account expires.</li> <li>• <b>Password Expired:</b> whether the password of the account expires.</li> <li>• <b>Password Locked:</b> whether the password of the account is locked.</li> <li>• <b>Account Expired:</b> whether the account expires.</li> <li>• <b>Sudo Account:</b> whether the account is granted the sudo permissions.</li> <li>• <b>Interactive Logon Account:</b> whether the account is granted the logon permissions.</li> <li>• <b>Last Login:</b> the last logon time of the account.</li> <li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the account.</li> </ul>
Port	<p>The information about the listener port of your server. Security Center periodically collects information about the listener port of your server. The information includes the following items:</p> <ul style="list-style-type: none"> <li>• <b>Server information:</b> the server to which the port belongs. This column displays the name and IP address of the server.</li> <li>• <b>Port:</b> the listener port number.</li> <li>• <b>Protocol:</b> the network protocol of the listener port.</li> <li>• <b>PID:</b> the ID of the server process that monitors the port.</li> <li>• <b>Process:</b> the server process that monitors the port.</li> <li>• <b>IP:</b> the IP address of the network interface controller (NIC) that is associated with the listener port.</li> <li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the listener port.</li> </ul>

Asset fingerprint type	Description
Process	<p>The information about the process that runs on your server. Security Center periodically collects information about the process that runs on your server. The information includes the following items:</p> <ul style="list-style-type: none"><li>• <b>Server information:</b> the server on which the process is running. This column displays the name and IP address of the server.</li><li>• <b>Process name:</b> the name of the process.</li><li>• <b>Process path:</b> the path from which the process is started.</li><li>• <b>Startup parameters:</b> the startup parameters of the process.</li><li>• <b>Start time:</b> the time when the process was started.</li><li>• <b>Running user:</b> the user who started the process.</li><li>• <b>Run permission:</b> the permissions of the user who started the process.</li><li>• <b>PID:</b> the ID of the process.</li><li>• <b>Parent process PID:</b> the ID of the parent process to which the process belongs.</li><li>• <b>File MD5:</b> the MD5 hash value of the process file.</li><li>• <b>Package Process Installation:</b> whether the process is installed by using a package.</li><li>• <b>Process Status:</b> the status of the process.</li><li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the process.</li></ul>

Asset fingerprint type	Description
Middleware	<p>The information about the middleware that runs on your server. Security Center periodically collects information about the middleware of your server. The middleware refers to system components that can independently run, such as MySQL databases and Docker. Docker is a container component. The information includes the following items:</p> <ul style="list-style-type: none"> <li>• <b>Server Information:</b> the server on which the middleware is run. This column displays the name and IP address of the server.</li> <li>• <b>Middleware:</b> the name of the middleware.</li> <li>• <b>Type:</b> the type of the middleware.</li> <li>• <b>Runtime Environment Version:</b> the runtime environment version of the middleware.</li> <li>• <b>Version:</b> the version of the middleware.</li> <li>• <b>PID:</b> the ID of the process that started the middleware.</li> <li>• <b>Version Verification:</b> the method that is used to obtain the version of the middleware.</li> <li>• <b>Parent Process PID:</b> the ID of the parent process that started the middleware.</li> <li>• <b>Enable User:</b> the user who started the middleware.</li> <li>• <b>Listening IP Address:</b> the listener IP address of the started middleware.</li> <li>• <b>Process Startup Path:</b> the path from which the process of the middleware is started.</li> <li>• <b>Listening Port:</b> the listener port of the started middleware.</li> <li>• <b>Listener Status:</b> the status of the listener.</li> <li>• <b>Listening Port Protocol:</b> the network protocol of the listener port for the middleware.</li> <li>• <b>Process Startup Time:</b> the time when the middleware was started.</li> <li>• <b>Process Startup Command:</b> the startup parameters of the middleware.</li> <li>• <b>Container Name:</b> the name of the container to which the middleware belongs.</li> <li>• <b>Image Name:</b> the name of the image to which the middleware belongs.</li> <li>• <b>Configure Path:</b> the absolute path of the startup configurations for the middleware.</li> <li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the middleware.</li> </ul>

Asset fingerprint type	Description
Database	<p>The information about the database that runs on your server. Security Center periodically collects information about the database that runs on your server. The information includes the following items:</p> <ul style="list-style-type: none"><li>• <b>Server Information:</b> the server on which the database is run. This column displays the name and IP address of the server.</li><li>• <b>Database Name:</b> the name of the database.</li><li>• <b>Type:</b> the type of the database.</li><li>• <b>Version:</b> the version of the database.</li><li>• <b>PID:</b> the ID of the process that started the database.</li><li>• <b>Version Verification:</b> the method that is used to obtain the version of the database.</li><li>• <b>Parent Process PID:</b> the ID of the parent process that started the database.</li><li>• <b>Enable User:</b> the user who started the database.</li><li>• <b>Listening IP Address:</b> the listener IP address of the started database.</li><li>• <b>Listening Port:</b> the listener port of the started database.</li><li>• <b>Listener Status:</b> the status of the listener.</li><li>• <b>Listening Port Protocol:</b> the network protocol of the listener port for the database.</li><li>• <b>Process Startup Time:</b> the time when the database was started.</li><li>• <b>Process Startup Command:</b> the startup parameters of the database.</li><li>• <b>Container Name:</b> the name of the container to which the database belongs.</li><li>• <b>Image Name:</b> the name of the image to which the database belongs.</li><li>• <b>Configure Path:</b> the absolute path of the startup configurations for the database.</li><li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the database.</li></ul>



Asset fingerprint type	Description
Web service	<p>The information about the web service of your server. Security Center periodically collects information about the web service of the server. The information includes the following items:</p> <ul style="list-style-type: none"> <li>• <b>Server Information:</b> the server on which the web service is run. This column displays the name and IP address of the server.</li> <li>• <b>Web Service Name:</b> the name of the web service.</li> <li>• <b>Type:</b> the type of the web service.</li> <li>• <b>Runtime Environment Version:</b> the Java Development Kit (JDK) version. JDK is the runtime of the web service.</li> <li>• <b>Version:</b> the version of the web service.</li> <li>• <b>PID:</b> the ID of the process that started the web service.</li> <li>• <b>Version Verification:</b> the method that is used to obtain the version of the web service.</li> <li>• <b>Parent Process PID:</b> the ID of the parent process that started the web service.</li> <li>• <b>Enable User:</b> the user who started the web service.</li> <li>• <b>Listening IP Address:</b> the listener IP address of the started web service.</li> <li>• <b>Listening Port:</b> the listener port of the started web service.</li> <li>• <b>Listener Status:</b> the status of the listener.</li> <li>• <b>Listening Port Protocol:</b> the network protocol of the listener port for the web service.</li> <li>• <b>Process Startup Time:</b> the time when the web service was started.</li> <li>• <b>Process Startup Command:</b> the startup parameters of the web service.</li> <li>• <b>Container Name:</b> the name of the container to which the web service belongs.</li> <li>• <b>Image Name:</b> the name of the image to which the web service belongs.</li> <li>• <b>Configure Path:</b> the absolute path of the startup configurations for the web service.</li> <li>• <b>Web Directory:</b> the path of the web configuration page.</li> <li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the web service.</li> </ul>
Software	<p>The information about the software that is installed on your server. Security Center periodically collects information about the software that is installed on your server. The information includes the following items:</p> <ul style="list-style-type: none"> <li>• <b>Server information:</b> the server on which the software is installed This column displays the name and IP address of the server.</li> <li>• <b>Version:</b> the version of the software.</li> <li>• <b>Software Update Time:</b> the time when the software version is updated.</li> <li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the software.</li> </ul>

Asset fingerprint type	Description
Scheduled Tasks	<p>The information about the scheduled task on your server. Security Center periodically collects information about the path of the scheduled task that is run on your server. The information includes the following items:</p> <ul style="list-style-type: none"><li>• <b>Server information:</b> the server on which the scheduled task is run. This column displays the name and IP address of the server.</li><li>• <b>Command:</b> the command in the scheduled task.</li><li>• <b>Task Cycle:</b> the interval at which the scheduled task is run.</li><li>• <b>MD5:</b> the MD5 hash value of the process for the schedule task.</li><li>• <b>Account Name:</b> the name of the account that is used to start the scheduled task.</li><li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the scheduled task.</li></ul>
Startup item	<p>The information about the startup item of your server. Security Center periodically collects information about the startup item of your server. The information includes the following items:</p> <ul style="list-style-type: none"><li>• <b>Server information:</b> the server on which the startup item is enabled. This column displays the name and IP address of the server.</li><li>• <b>Startup Item Path:</b> the path to the startup item.</li><li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the startup item.</li></ul>
Kernel Module	<p>The information about the kernel module of your server. Security Center periodically collects information about the kernel module of your server. The information includes the following items:</p> <ul style="list-style-type: none"><li>• <b>Server information:</b> the server to which the kernel module belongs. This column displays the name and IP address of the server.</li><li>• <b>Module Name:</b> the name of the kernel module.</li><li>• <b>Module Size:</b> the size of the kernel module file.</li><li>• <b>Module File Path:</b> the path to the kernel module file.</li><li>• <b>Total Submodules:</b> the number of dependent modules.</li><li>• <b>Last Scan Time:</b> the last time when Security Center collected the information about the kernel module.</li></ul>

Asset fingerprint type	Description
Website	<p>The information about the website on your server. Security Center periodically collects information about the website on your server. The information includes the following items:</p> <ul style="list-style-type: none"> <li>• <b>Server information:</b> the server on which the website is deployed. This column displays the name and IP address of the server.</li> <li>• <b>Domain Name:</b> the domain name of the website.</li> <li>• <b>Website Type:</b> the type of the software that is used by the website.</li> <li>• <b>Port:</b> the listener port of the website.</li> <li>• <b>Web Path:</b> the path to the home directory of the website.</li> <li>• <b>Web Root Path:</b> the path of the root directory in the web configuration.</li> <li>• <b>Enable User:</b> the user who started the website.</li> <li>• <b>Directory Permission:</b> the permissions on the web directory.</li> <li>• <b>Monitoring Protocol:</b> the listener protocol of the website.</li> <li>• <b>PID:</b> the ID of the process.</li> <li>• <b>Process Startup Time:</b> the time when the website was started.</li> <li>• <b>Image Name:</b> the name of the image to which the website belongs.</li> <li>• <b>Container Name:</b> the name of the container to which the website belongs.</li> <li>• <b>Latest Collection Time:</b> the last time when Security Center collected the information about the website.</li> </ul>

## 3.2. View the security status of a server

The Assets page in the Security Center console displays security information about all servers. The information includes the security status, the groups to which the servers belong, and the regions and virtual private cloud (VPCs) in which the servers reside. This topic describes how to search for servers to view the security status.

### Procedure

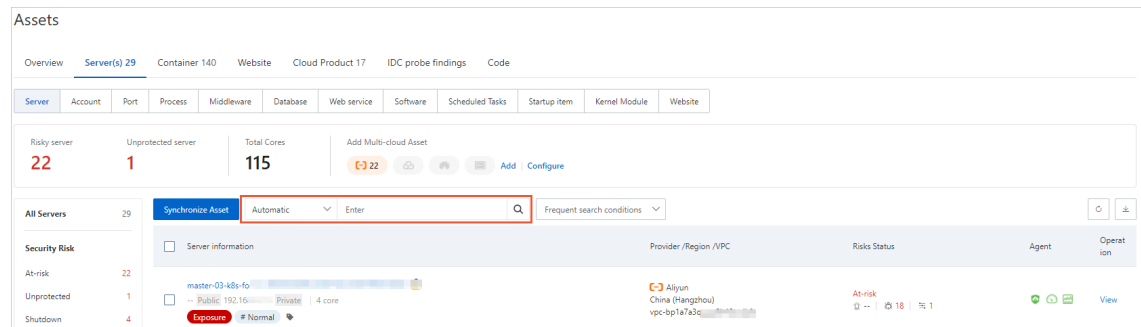
- 1.
- 2.
3. On the **Assets** page, click the **Server(s)** tab.
4. On the **Server(s)** tab, click the **Server** tab.
5. On the **Server** tab, view the security status of your servers.
  - Update the most recent information about servers
 

To update the most recent information about your servers and refresh the server list, click **Synchronize Asset** in the upper-left corner of the Server tab.
  - Collect the details of servers

To collect server details, select one or more servers and choose **More Operations > Asset Collection** below the server list. The details include the MAC address and kernel version of a server.

- View the security status of a server

To view the security status of a server, you can enter the server name, the public IP address, and the private IP address in the search box above the server list.






In the **Risks Status** column, you can view the security status of the server. In the **Operation** column, you can click **View** to go to the server details page. On the server details page, you can view information about the server on tabs such as **Basic Information**, **Vulnerabilities**, **Alerts**, **Baseline Risks**, and **Asset Fingerprints**. For more information, see [View the details of an asset](#).



- View the security status of servers by category

On the **Assets** page, servers are categorized to help you manage servers in an efficient manner. The categories include **At-risk**, **Unprotected**, and **Exposed**. You can view the security status of servers by category.

The following table describes servers by category.

Category	Description
<b>All Servers</b>	The servers that are protected by Security Center. The servers include Elastic Compute Service (ECS) instances and servers that are not deployed on Alibaba Cloud and have the Security Center agent installed.
<b>At-risk</b>	The servers on which vulnerabilities and baseline risks are detected, and servers on which alerts are generated.
<b>Unprotected</b>	<p>The servers on which the Security Center agent is in the <b>Close</b> or <b>Disable Protection</b> state.</p> <div>  <b>Notice</b> Security Center cannot protect the servers on which the agent is in the <b>Close</b> or <b>Disable Protection</b> state. You can configure Security Center to protect the servers. For more information, see <a href="#">Enable or disable server protection</a>. </div>
<b>Shutdown</b>	The servers that are shut down.

Category	Description
Exposed	<p>The servers that are exposed on the Internet. These servers are accessible over the Internet. For more information about the exposure details, see <a href="#">Asset exposure analysis</a>.</p> <div> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>Only the and editions support asset exposure analysis. If you do not use one of these editions, you must upgrade Security Center to the or edition before you can view the number and list of the servers that are exposed on the Internet.</li> <li>If <b>Unknown</b> is displayed on the right side of <b>Exposed Server</b>, the current edition of Security Center does not support asset exposure analysis. In this case, the number of exposed servers is not displayed in the Security Center console. To use asset exposure analysis, you must upgrade Security Center to the or edition. For more information, see <a href="#">Upgrade and downgrade Security Center</a>.</li> </ul> </div>
Add	The ECS instances that you purchased within the last 15 days.
Server Group	<p>The servers that are categorized based on server groups. You can find a server group and click the number in the <b>All Servers</b>, <b>At-risk</b>, or <b>Unprotected</b> column to view the security status of the servers that belong to the server group.</p> <div> <p> <b>Note</b> You can <b>manage</b> and <b>delete</b> a server group in the Security Center console. For more information, see <a href="#">Manage asset groups</a>.</p> </div>
Server Region	The servers that are categorized based on regions. You can find a region and click the number in the <b>All Servers</b> , <b>At-risk</b> , or <b>Unprotected</b> column to view the security status of the servers that are deployed in the region.
VPC	The servers that are categorized based on VPCs. You can find a VPC and click the number in the <b>All Servers</b> , <b>At-risk</b> , or <b>Unprotected</b> column to view the security status of the servers that reside in the VPC.


Category	Description
Importance	<p>The servers that are categorized based on asset importance levels. In the <b>Importance</b> section, you can click <b>Important</b>, <b>Normal</b>, or <b>Test</b> to view the security status of the related servers.</p> <p> <b>Note</b> Security Center allows you to classify your servers that belong to the current Alibaba Cloud account into three levels based on asset importance. You can determine the asset importance based on your business requirements. This way, you can manage multiple servers by asset importance level.</p>
Tag	<p>The servers that are categorized based on tags. You can click a tag in the <b>Tag</b> section to view the security status of the servers to which the tag is added.</p> <p> <b>Note</b> You can <b>manage</b> and <b>delete</b> a tag in the Security Center console. For more information, see <a href="#">Manage asset tags</a>.</p>

- View the security status of the servers that match one or more search conditions

After you click the **All Servers**, **At-risk**, **Unprotected**, **Shut down**, **Exposed**, or **Add** category, you can specify one or more search conditions to search for specific servers and view the security status.

This section provides an example on how to specify multiple search conditions to search for servers. In the example, servers that match the following search conditions are returned: Linux operating system, alerts generated, and the China (Hangzhou) region.

- On the **Server(s)** tab of the **Assets** page, click **Unprotected server**.
- In the drop-down list next to the search box, configure the **System Type**, **Alert problems**, and **Region** search conditions.
  - Select **Linux** for **System Type**.
  - Select **Yes** for **Alert problems**.
  - Select **China (Hangzhou)** for **Region**.

 **Note** If you cannot select a value for a search condition in the drop-down list, you can enter keywords for the search condition in the search box.

After you specify the search conditions, the search conditions are displayed in the **Search item** section above the server list.

- c. Click the switch on the left side of **Search item** to switch between the AND and OR Boolean operators.

- **AND**: specifies the **AND logical relation** between search conditions.
- **OR**: specifies the **OR logical relation** between search conditions.

After you specify the search conditions, servers that match all the specified search conditions are displayed in the server list.

- d. (Optional) If you want to specify the preceding search conditions as frequently used search conditions, click **Save** on the right side of **Search item**.

After you save frequently used search conditions, you can select the search conditions from the **Frequent search conditions** drop-down list to search for servers in an efficient manner.

## 3.3. Enable or disable server protection

After you install the Security Center agent on a server, Security Center can protect the server. You can modify the protection status of a server as needed. This topic describes how to enable or disable server protection.

### Prerequisites

The Security Center agent is installed on your server. You can enable or disable protection for your server only after the Security Center agent is installed on your server. For more information about how to install the Security Center agent, see [Install the Security Center agent](#).

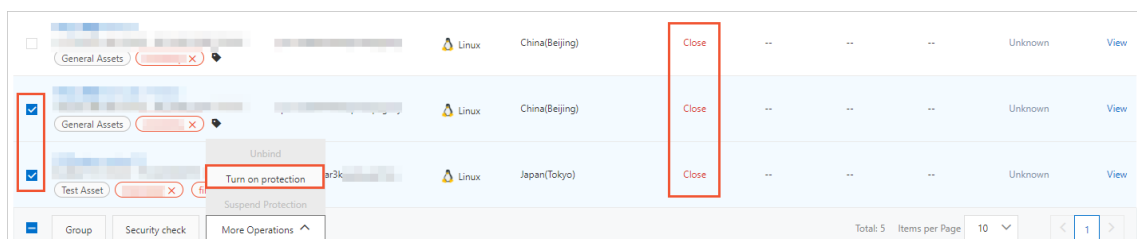
### Context

- The status in the **Agent** column changes to **Enable** on the **Assets** page.
- If the agent is not connected to Alibaba Cloud, the status changes to **Close**. To allow Security Center to protect a server, you must enable the Security Center agent for the server.

### Procedure

- 1.
- 2.
- 3.
4. On the **Server(s)** tab, you can enable or disable protection for a specific server.
  - **Enable protection**

To enable protection, select one or more servers whose status is **Close** in the **Agent** column, and choose **More Operations > Turn on protection**.

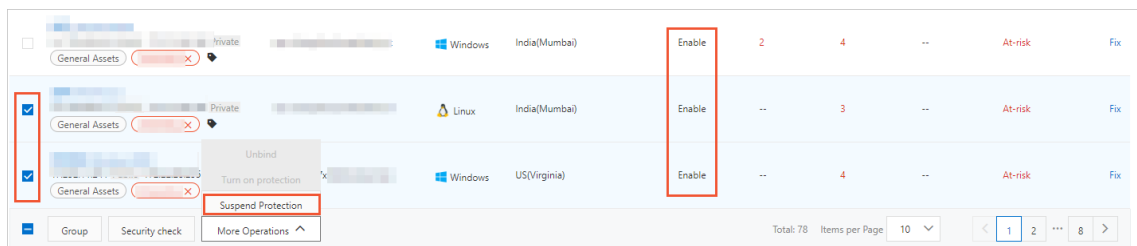


After server protection is enabled, the status in the Agent column changes to **Enable**.

- **Disable protection**

You can disable protection for a server as needed. To disable protection, select one or more servers whose status is **Enable** in the **Agent** column, and choose **More Operations > Suspend Protection**.

**Note** After protection is disabled, Security Center stops providing protection for your servers, including vulnerability detection and security event alerting. Proceed with caution.



After server protection is disabled, the status of the target servers changes to **Close** in the **Agent** column.

## 3.4. Collect asset fingerprints

The asset fingerprints feature can automatically collect asset fingerprints at specific intervals. The feature also allows you to manually collect asset fingerprints. This topic describes how to collect asset fingerprints.

### Context

After you purchase Security Center or , Security Center does not automatically collect asset fingerprints. You can use automatic or manual collection tasks to collect the latest fingerprints of specific assets.

You can select one of the following collection methods:

Collection methods	Description
Automate periodic collection tasks	You can configure fingerprint collection frequencies for assets, such as listener ports, software, processes, accounts, scheduled tasks, and middleware, to automate collection tasks that periodically run. For more information, see <a href="#">Automate periodic collection tasks</a> .
Collect the fingerprints of all assets with a few clicks	You can manually collect the latest fingerprints of all assets. On the <b>Server (s)</b> tab of the <b>Assets</b> page, click a subtab other than the <b>Server</b> subtab and click <b>Collect the latest data</b> to collect the latest fingerprints of all assets by running a collection task For more information, see <a href="#">Collect the fingerprints of all assets with a few clicks</a> .



Collection methods	Description
Collect the fingerprints of a specific asset with a few clicks	You can manually start a task to collect the fingerprints of an asset. On the <b>Assets</b> page, click the name of the asset whose fingerprints you want to collect. On the asset details page, click the <b>Asset Fingerprints</b> tab. In the upper-right corner of a subtab, click <b>Collect data now</b> to manually start a task to collect the fingerprints of the asset. For more information, see <a href="#">Collect the fingerprints of a specific asset with a few clicks</a> .

#### Note

- If you are a first-time user of the asset fingerprints feature, we recommend that you configure the fingerprint collection frequency for different assets to automate collection tasks. The automatic collection tasks collect the fingerprints of all assets.
- Collection tasks consume a small amount of CPU or memory resources of your server. Therefore, your business is not affected.

## Limits

Only the Enterprise and Ultimate editions of Security Center support this feature. If you do not use these editions, you must upgrade Security Center to the Enterprise or Ultimate edition before you can use this feature. For more information about how to purchase and upgrade Security Center, see [Purchase Security Center](#) and [Upgrade and downgrade Security Center](#). For more information about the features that each edition supports, see [Features](#).

## Automate periodic collection tasks

Security Center automatically collects the fingerprints of all your assets, such as ports, software, processes, accounts, scheduled tasks, and middleware. After you configure automatic collection, you can view the latest fingerprints that are collected within a specific time range on the **Server (s)** tab of the **Assets** page in the Security Center console.

- 1.
- 2.
3. On the **Assets** page, click the **Server(s)** tab.
4. On the **Server(s)** tab, click the **Account** subtab.

You can also click a subtab other than the **Server** subtab to configure collection tasks. You do not need to click all subtabs.

5. Click **Settings**.
6. In the **Settings** dialog box, configure the collection frequency for each asset type.

Settings

×

Port:

Collected once an hour

▼

Processes:

Disable

▼

Account:

Disable

▼

Software:

Disable

▼

Scheduled

Disable

▼

Tasks:

Middleware:

Disable

▼

?

Startup

Disable

▼

Item:

Kernel

Disable

▼

Module:

Website:


Disable

▼

OK

Cancel

Asset type	Frequency
------------	-----------

Asset type	Frequency
Port	Valid values: <ul style="list-style-type: none"> <li>◦ <b>Disable</b>: This is the default value. If you set Port to Disable, Security Center does not automatically collect the latest fingerprints.</li> <li>◦ <b>Collected once an hour</b></li> <li>◦ <b>Collected once every 3 hours</b></li> <li>◦ <b>Collected once every 12 hours</b></li> <li>◦ <b>Collected once a day</b></li> <li>◦ <b>Collected once every 7 days</b></li> </ul> <div style="background-color: #e1f5fe; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>◦ By default, the collection frequencies of all assets are <b>Disable</b>. You can configure different collection frequencies for the assets.</li> <li>◦ To configure a collection frequency for middleware, databases, and web services, you can configure the <b>Middleware</b> parameter.</li> <li>◦ If you use the <b>asset exposure analysis</b> feature, set the <b>Middleware</b> parameter to <b>Collected once an hour</b>, <b>Collected once every 3 hours</b>, <b>Collected once every 12 hours</b>, or <b>Collected once a day</b>. You cannot set the <b>Middleware</b> parameter to <b>Disable</b> or <b>Collected once every 7 days</b>.</li> </ul> </div>
Processes	
Account	
Software	
Scheduled Tasks	
Middleware	
Startup Item	
Kernel Module	
Website	

7. Click **OK**.

After the collection frequencies are configured, Security Center automatically runs collection tasks based on the collection frequencies. You can view the latest fingerprints of an asset on a subtab other than the **Server** on the **Assets** page. For more information, see [View asset fingerprints](#).

## Collect the fingerprints of all assets with a few clicks

If you want to view the latest fingerprints of all assets, you can perform the following steps:

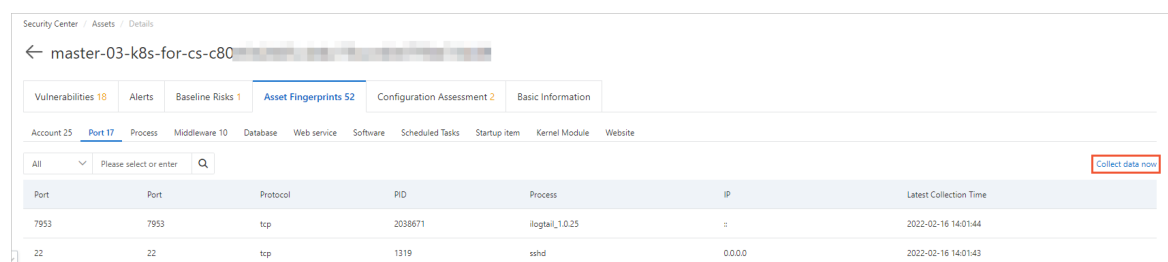
- 1.
- 2.
3. On the **Assets** page, click the **Server(s)** tab.
4. On the **Server(s)** tab, click the **Account** subtab.  
You can also click a subtab other than the **Server** subtab to configure collection tasks.
5. Click **Collect the latest data**.
6. In the **Collect the latest data** dialog box, select the assets whose fingerprints you want to collect.
7. Click **OK**.

The time required to collect the fingerprints is approximately 1 to 5 minutes.

## Collect the fingerprints of a specific asset with a few clicks

If you want to view the latest fingerprints of a specific server, you can find the server on the **Assets** page, navigate to the **Asset Fingerprints** tab of the server, and run a manual collection task. The task collects fingerprints of ports, processes, and software.

- 1.
2. In the left-side navigation pane, click **Assets**.
3. On the **Assets** page, click the **Server(s)** tab.
4. On the **Server(s)** tab, click the **Server** subtab.
5. In the server list, click the name of the server whose fingerprints you want to collect.
6. On the asset details page, click the **Asset Fingerprints** tab.
7. In the upper-right corner of a subtab on which you want to collect fingerprints, click **Collect data now** to start a collection task.



8. In the **Collect data** message, click **OK**.

The time required to collect the fingerprints is approximately 1 to 5 minutes.

## What's next

After you run the collection task, you can go to the **Server (s)** tab of the **Assets** page and click the subtab to view the latest fingerprints. For more information, see [View asset fingerprints](#).

## 3.5. Use the security check feature

On the **Server(s)** tab of the **Assets** page in the Security Center console, you can run security checks on a specific server to detect vulnerabilities, baseline risks, and webshells. You can also run security checks to collect asset fingerprints, such as information about ports, software, processes, accounts, and middleware. This topic describes how to run security checks on your servers.

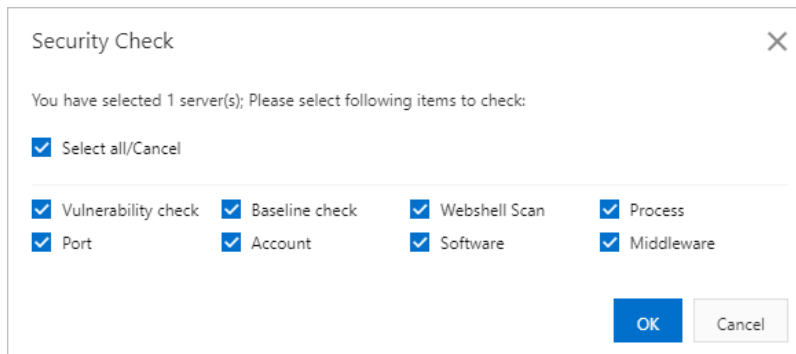
### Context

**Notice** If you run security checks on your server, Security Center detects vulnerabilities, baseline risks, and webshells, and collects asset fingerprints at the same time. In this case, the CPU utilization and memory usage of your server increase, which may affect your workloads. The security check may require 1 to 5 minutes. To prevent service interruptions, we recommend that you perform this operation during off-peak hours.

### Procedure

- 1.
- 2.
- 3.
4. In the server list, select one or more servers on which you want to run security checks.

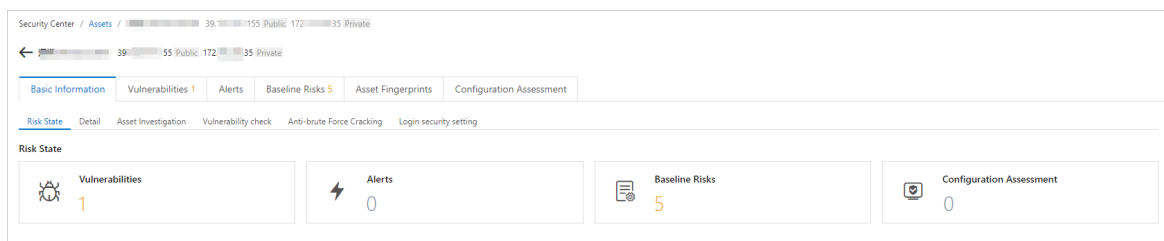
- Click **Security check** below the server list.
- In the **Security Check** dialog box, select check items.



- Click **OK** to start the check.
- In the message that appears, click **OK**.

The security check may require 1 to 5 minutes. You do not need to check again.

After the security check is complete, the results are displayed on the asset details page in the Security Center console.



## What's next

To view the check results, you can click the tab that corresponds to a specific check item.

- For more information about the detection results of each vulnerability type, see the following topics:
  - [View and handle Linux software vulnerabilities](#)
  - [View and handle Windows system vulnerabilities](#)
  - [View and handle Web-CMS vulnerabilities](#)
  - [View and handle application vulnerabilities](#)
  - [View and handle urgent vulnerabilities](#)
- For more information about the results of baseline checks, see [View baseline check results and handle baseline risks](#).
- For more information about the results of webshell detection, see [View and handle alerts](#).
- For more information about asset fingerprints, such as information about ports, software, processes, accounts, and middleware, see [View asset fingerprints](#).

## 3.6. View asset fingerprints

You can view asset fingerprints in the Security Center console. Asset fingerprints include the details and status of your assets. This topic describes how to view asset fingerprints.

### Prerequisites

- Security Center or is purchased or Security Center is upgraded to the Enterprise or Ultimate edition. For more information, see [Purchase Security Center](#) and [Upgrade and downgrade Security Center](#).
- Asset fingerprints are collected. For more information, see [Collect asset fingerprints](#).

## View the fingerprints of all assets

- 1.
- 2.
3. On the **Assets** page, click the **Server(s)** tab.
4. On the **Server(s)** tab, click a subtab to view the fingerprint.

The following list describes the sections on a subtab.

- The left-side section displays an asset fingerprint list. The list includes all asset fingerprints and the number of servers related to each fingerprint. The section is marked 1 in the preceding figure.
- The right-side section displays the fingerprint details. The section is marked 2 in the preceding figure. In the asset fingerprint list, you can click an asset such as a port number to view the asset fingerprint in this section.
- You can use the filter or enter search conditions in the search box above the section that is marked 2 in the preceding figure to search for an fingerprint. The filter and the search box are marked 3 in the preceding figure.

 **Note** Fuzzy match is supported for all types of assets.

# 4. View container information

## 4.1. View security information about containers

You can view information about all containers on the Container tab of the Assets page in the Security Center console.

### Context

Security Center Ultimate provides you with integrated capabilities to protect your containers, and prevents and detects threats to the runtime of containers in real time. The threats include vulnerabilities, configuration compliance risks, attacks, and intrusions. If you want to use Security Center to detect threats to Kubernetes clusters, you must manually enable the detection feature. For more information, see [Use threat detection on Kubernetes containers](#).

### View information about images

- 1.
- 2.
- 3.
4. On the **Container** tab, click the **Image** tab to view information about images. You can perform the following operations:
  - View overview information about images

In the section that displays overview information about images, you can view the following information: **At-risk Image Repository**, **Image Repository**, and **Remaining Quota**. You can click **Integrate** to add third-party image repositories to Security Center. You can also click **Settings** to specify images for image scans.

- Synchronize the most recent information about images to Security Center

You can click **Synchronize Asset** to synchronize the most recent information about images to Security Center.

- View the list of image repositories

The list of image repositories displays the information about all image repositories that are added to Security Center. The information includes names, regions, types, and security status of image repositories. You can perform the following operations:

- Search for an image repository

You can specify a search condition in the search box above the list to search for an image repository. The search conditions include the following information about an image repository: **Instance ID**, **Namespace**, and **Image Type**.

- View the information about an image repository

Find an image repository and click its name or **View** in the **Actions** column to go to the details page of the image repository. On the page, you can view the information about all images that belong to the image repository. The information includes the names, versions, sizes, and security status of the images.

Find an image and click **Scan** in the **Actions** column to scan the image. You can select multiple images and click **Batch Scan** below the list to scan the images at a time.

Find an image and click **Handle** in the **Actions** column to go to the image details page. You can view the information about the following risks that are detected in the image: image system vulnerabilities, image application vulnerabilities, image baseline risks, and malicious samples.

- View information in the Task management panel

On the details page of an image repository, click **Task management** in the upper-right corner. In the panel that appears, you can view the status of image scan tasks and fixing tasks for image risks.

## View information about clusters

- 1.
- 2.
- 3.
4. On the **Container** tab, click the **Cluster** tab to view the information about clusters. You can perform the following operations:

- View overview information about clusters

In the section that displays overview information about clusters, you can view **Total Clusters** and **At-risk Cluster**. You can click **Self-built cluster access** to add a self-managed Kubernetes cluster to Security Center. For more information about how to add self-managed Kubernetes clusters to Security Center, see [Connect a self-managed Kubernetes cluster to Security Center](#).

- Synchronize the most recent information about all clusters to Security Center

You can click **Synchronize Asset** to synchronize the most recent information about clusters to Security Center.

- View the list of clusters

The list of clusters displays information about all clusters. The information includes names, regions, types, and security status of clusters. You can perform the following operations:

- Search for a cluster

You can specify a search condition in the search box above the list to search for a cluster. The search conditions include **Cluster ID**, **Cluster Name**, and **Cluster Type**.

- View the information about a cluster

Find a cluster and click its name or **View** in the **Actions** column to go to the cluster details page. You can view the information about the cluster from different dimensions on the following tables: **Cluster**, **Node**, **Application**, and **Namespace**. You can view different information about the cluster and handle the risks that are detected on the cluster on the tabs.



## References


[Overview](#)[Container network topology](#)[Use threat detection on Kubernetes containers](#)[Use the container signature feature](#)[View image scan results](#)[Use the runtime security feature to monitor ACK clusters and configure alerts](#)

## 4.2. Connect a self-managed Kubernetes cluster to Security Center

Security Center allows you to handle the risks of containers on the Assets page of the Security Center console. You can connect a self-managed Kubernetes cluster to Security Center and manage your containers in the Security Center console in a centralized manner. This topic describes how to connect a self-managed Kubernetes cluster to Security Center.

### Limits

- You can connect a maximum of 10 self-managed Kubernetes clusters.
- If a self-managed Kubernetes cluster that you want to connect is deployed in a virtual private cloud (VPC), the cluster must reside in the China (Hangzhou), China (Beijing), China (Shanghai), China (Shenzhen), or China (Hong Kong) region.

 **Note** If a self-managed Kubernetes cluster that you want to connect is deployed on the Internet, no limits are imposed on the region of the cluster.

### Connect a self-managed Kubernetes cluster to Security Center

- 1.
- 2.
- 3.
4. In the upper-right corner of the **Container** tab, click **Self-built cluster access**.
5. In the **Self-built cluster management** panel, click **Self-built cluster access**.
6. In the **Access Self-built K8s cluster** panel, configure the parameters.

Parameter	Description
Cluster name	The name of the self-managed Kubernetes cluster. The name can contain letters, digits, underscores (_), and hyphens (-).

Parameter	Description
Self-built K8s cluster version	The version of the self-managed Kubernetes cluster. Valid values: <ul style="list-style-type: none"><li>◦ <b>V1.21</b></li><li>◦ <b>V1.20</b></li><li>◦ <b>V1.19</b></li><li>◦ <b>V1.18</b></li><li>◦ <b>V1.17</b></li><li>◦ <b>V1.16</b></li></ul>
Region of cluster	The region in which the self-managed Kubernetes cluster resides.
Network type	The network type of the self-managed Kubernetes cluster. Valid values: <ul style="list-style-type: none"><li>◦ <b>Public network</b></li><li>◦ <b>VPC</b></li></ul>
VPC where the cluster is located	The VPC in which the self-managed Kubernetes cluster is deployed.
ApiServerIp	The IP address of the API server for the self-managed Kubernetes cluster.
K8s configuration information	The configuration file of the self-managed Kubernetes cluster. You must generate a configuration file on your server before you upload the file. For more information about how to generate a configuration file for a Kubernetes cluster, see <a href="#">Generate a configuration file for a Kubernetes cluster</a> .

7. Click **OK**.

After you connect the Kubernetes cluster to Security Center, you can view the cluster information in the **Self-built cluster management** panel.

## Generate a configuration file for a Kubernetes cluster

To generate a configuration file, make sure that your server meets the following prerequisites:

- A Kubernetes cluster is created on your server.
- Docker is installed.
- If you create an access control policy for your cluster, make sure that the access control policy allows access from the region in which the container resides.

The following table describes the supported regions and the CIDR blocks of the address pools in the regions.

Region	City	Region ID	CIDR block
China (Hangzhou)	Hangzhou	cn-hangzhou	100.104.177.0/26
China (Shanghai)	Shanghai	cn-shanghai	100.104.7.192/26

Region	City	Region ID	CIDR block
China (Qingdao)	Qingdao	cn-qingdao	100.104.87.192/26
China (Beijing)	Beijing	cn-beijing	100.104.20.128/26
China (Zhangjiakou)	Zhangjiakou	cn-zhangjiakou	100.104.187.64/26
China (Hohhot)	Hohhot	cn-huhehaote	100.104.36.0/26
China (Shenzhen)	Shenzhen	cn-shenzhen	100.104.9.192/26
China (Chengdu)	Chengdu	cn-chengdu	100.104.69.0/26
China (Hong Kong)	Hong Kong	cn-hongkong	100.104.111.128/26
Japan (Tokyo)	Tokyo	ap-northeast-1	100.104.69.0/26
Singapore (Singapore)	Singapore	ap-southeast-1	100.104.41.128/26
Indonesia (Jakarta)	Jakarta	ap-southeast-5	100.104.193.128/26
US (Silicon Valley)	Silicon Valley	us-west-1	100.104.145.64/26
US (Virginia)	Virginia	us-east-1	100.104.36.0/26


1. Log on to the server where the Kubernetes cluster resides as the root user.
2. Create a user.
  - i. Run the following command to create ClusterRole:

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: ${userName}-cluster-reader
rules:
- apiGroups:
  - ""
  resources:
  - "*"
  verbs:
  - get
  - list
  - watch

```

- ii. Run the following command to create ClusterRoleBinding:

 **Notice** Before you run the command in this step and all the following steps, you must replace `<UserName>` with your username.

```
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRoleBinding
metadata:
  name: ${userName}-read-all
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ${userName}-cluster-reader
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: ${userName}
```

### 3. Create a certificate.

- i. Run the following command to create a private key for the user:

```
openssl genrsa -out <UserName>.key 2048
```

- ii. Run the following command to create a certificate signing request:

```
openssl req -new -key <UserName>.key -out <UserName>.csr -subj "/O=K8s/CN=<UserName>"
```

- iii. Run the following command to sign the certificate:

```
openssl x509 -req -in <UserName>.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out <UserName>.crt -days 365
```

### 4. Create a configuration file for the cluster.

- i. Run the following command to create the cluster configuration field:


```
kubectl config set-cluster k8s --server=https://192.168.XX.XX:6443 --certificate-authority=ca.crt --embed-certs=true --kubeconfig=/root/<UserName>.conf
```

- ii. Run the following command to create the user configuration field:

```
kubectl config set-credentials <UserName> --client-certificate=<UserName>.crt --client-key=<UserName>.key --embed-certs=true --kubeconfig=/root/<UserName>.conf
```

- iii. Run the following command to create the context configuration field:

```
kubectl config set-context <UserName>@<ClusterName> --cluster=k8s --user=<UserName> --kubeconfig=/root/<UserName>.conf
```

 **Notice** Before you run the command in this step and all the following steps, you must replace `<ClusterName>` with the name of your cluster.

iv. Run the following command to switch context:

```
kubectl config use-context <UserName>@<ClusterName> --kubeconfig=/root/<UserName>.conf
```

v. Run the following command to view the configuration file:

```
kubectl config view --kubeconfig=/root/<UserName>.conf
```

5. Run the following commands to check whether the *kubeconfig* file is available.

```
mkdir -p /home/<UserName>/.kube  
cp <UserName>.conf /home/<UserName>/.kube/config  
kubectl get pod -n kube-system
```

If the pod information is displayed in the command-line window after all the preceding commands are complete, the *kubeconfig* file is available, and Security Center can access the cluster. Otherwise, the *kubeconfig* file is unavailable.

## 4.3. Use CI/CD-based container image scan

### 4.3.1. Overview

Security Center provides the feature of CI/CD-based container image scan to detect image risks in an efficient manner. The feature is intended for the project building stage on Jenkins and GitHub. The feature can detect high-risk system vulnerabilities, application vulnerabilities, viruses, webshells, execution of malicious scripts, and configuration risks, and help you identify sensitive data on images. The feature also provides solutions to detected image risks.

#### Limits

Only the Advanced, Enterprise, Ultimate, and Value-added Plan editions of Security Center support the feature. If you do not use one of these editions, you must upgrade Security Center to the Advanced, Enterprise, Ultimate, or Value-added Plan edition before you can use the feature. For more information about how to purchase and upgrade Security Center, see [Purchase Security Center](#) and [Upgrade and downgrade Security Center](#). For more information about the features that each edition supports, see [Features](#).

#### Implementation

To use CI/CD-based container image scan, you need to only install the CI/CD plug-in on Jenkins or GitHub to allow Security Center to automatically scan images for risks when you build projects in Jenkins or GitHub. You do not need to synchronize your images to Security Center for risk scans. After the scan is complete, the scan result is displayed on the **CI/CD** tab of the **Assets** page in the Security Center console. The CI/CD plug-in is used to scan images. You can handle image risks based on the scan result.

#### Scenarios

The following list describes the scenarios in which you can use CI/CD-based container image scan:

- Jenkins Freestyle project
- Jenkins Pipeline project

- [GitHub Actions](#)

## Prerequisites

Your server meets the minimum configuration requirements. This prevents slow image scans.

- Minimum configuration settings
  - Number of CPU cores: 1.
  - Memory: 2 GB.
  - Storage capacity: 60 GB.
  - Network: The server is available over the Internet and can access the Alibaba Cloud service whose endpoint is `tds.ap-southeast-1.aliyuncs.com`.
- Optimal configuration settings
  - Number of CPU cores: 4.
  - Memory: 8 GB.
  - Storage capacity: 100 GB.
  - Network: The server is available over the Internet and can access the Alibaba Cloud service whose endpoint is `tds.ap-southeast-1.aliyuncs.com`. The upstream bandwidth is greater than 10 Mbit/s.

## 4.3.2. Obtain a token of the CI/CD plug-in


When you install the CI/CD plug-in of Security Center on Jenkins or GitHub, you must specify a token of the plug-in and the AccessKey pair of an Alibaba Cloud account or a Resource Access Management (RAM) user. This topic describes how to obtain a token of the CI/CD plug-in, create a RAM user, and grant the RAM user the permissions to use container image scan of Security Center.

### Obtain a token

- 1.
- 2.
- 3.
4. On the **Container** tab, click **CI/CD**.
5. Click **Integration Configuration**.
6. In the **Integration Configuration** panel, click **+ Add Token**.
7. Enter the name of the plug-in and click **OK**. The name can be up to 64 characters in length.  
The information about the plug-in is displayed in the list of the **Integration Configuration** panel.  
You can view and obtain a token of the plug-in in the **Token** column.

### Create a RAM user and grant permissions to the RAM user

1. Create a RAM user and grant the RAM user the permissions to use container image scan of Security Center. For more information, see [Create a RAM user](#).

 **Note** When you create the RAM user, you must select **Open API Access** in the **Access Mode** section.

2. Create a policy that defines the permissions to use container image scan of Security Center. For more information, see [Create a custom policy on the JSON tab](#).

Copy the following policy document to the code editor on the JSON tab:

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "yundun-sas:CreateJenkinsImageScanTask",
        "yundun-sas:ListImageAnalysisRuleProject",
        "yundun-sas:SubmitImageAnalysisOutput",
        "yundun-sas:UpdateJenkinsImageScanTaskStatus",
        "yundun-sas:UploadAnalyzerRuntimeLog",
        "yundun-sas:CreateBatchUploadURL"
      ],
      "Resource": "*"
    }
  ]
}
```

3. Attach the policy to the RAM user that you created. For more information, see [Grant permissions to a RAM user](#).

### 4.3.3. Install the CI/CD plug-in for a Jenkins Freestyle project

Security Center allows you to install the CI/CD plug-in for a Jenkins Freestyle project. After you install the CI/CD plug-in, Security Center scans images in the project when you build the project. This topic describes how to install the CI/CD plug-in for a Jenkins Freestyle project.

#### Limits

You can install the CI/CD plug-in only on Jenkins 1.625.3 or later.

#### Download the CI/CD plug-in


- 1.
- 2.
- 3.
4. On the **Container** tab, click **CI/CD**.
5. Click **Integration Configuration**.
6. In the **Integration Configuration** panel, click **Download Plug-in** in the upper-right corner.

The CI/CD plug-in in the HPI format is downloaded to your computer. The name of the plug-in is **sas-jenkins-plugin**.

#### Install the CI/CD plug-in on Jenkins

1. Log on to Jenkins.
2. In the left-side navigation pane, click **Manage Jenkins**.
3. On the **Manage Jenkins** page, click **Manage Plugins**.



4. On the **Manage Plugins** page, click the **Advanced** tab.
5. In the **Upload Plugin** section, click **Choose File**.  
Select the downloaded CI/CD plug-in named **sas-jenkins-plugin**.
6. Click **Upload**.

 **Notice** After you install the **sas-jenkins-plugin** plug-in, you must restart Jenkins for the plug-in to take effect.




## Configure image scans

1. Log on to Jenkins.
2. Find the Jenkins Freestyle project whose images you want to scan and click the name of the project.
3. In the left-side navigation pane, click **Configure**.
4. On the page that appears, find the **Build** section and select **Image vulnerability scan** from the drop-down list.
5. In the Image vulnerability scan section, configure the parameters. After you complete the configuration, the images in the Jenkins Freestyle project can be scanned.

The following table describes the parameters.

Parameter	Description
AccessKeyId	<p>The AccessKey ID of your Alibaba Cloud account or a RAM user of the Alibaba Cloud account.</p> <p> <b>Note</b> We recommend that you enter the AccessKey ID of a RAM user.</p>
AccessKeySecret	<p>The AccessKey secret of your Alibaba Cloud account or a RAM user of the Alibaba Cloud account.</p> <p> <b>Note</b> We recommend that you enter the AccessKey secret of a RAM user.</p>
Token	<p>A token of the CI/CD plug-in. For more information about how to obtain a token of the CI/CD plug-in, see <a href="#">Obtain a token of the CI/CD plug-in</a>.</p>
ImageId	<p>The IDs of the images that you want to scan or the tag of the image repository to which the images belong.</p>
Domain	<p>Set the value to <code>tds.ap-southeast-1.aliyuncs.com</code>.</p>



Parameter	Description
RegistryUrl	<p>The URL of the image repository.</p> <div> <b>Notice</b> If you want to scan the images in a remote image repository, you must configure this parameter.</div>
RegistryUsername	<p>The username used to log on to the image repository.</p> <div> <b>Notice</b> If you want to scan the images in a remote image repository, you must configure this parameter.</div>
RegistryPwd	<p>The password used to log on to the image repository.</p> <div> <b>Notice</b> If you want to scan the images in a remote image repository, you must configure this parameter.</div>

6. Click **Save**.

After you complete the configuration, Security Center scans images in the project for risks when you build the project.

## What to do next

You can view image scan results on the **Container** tab of the **Assets** page in the Security Center console. For more information, see [View image scan results](#).

## 4.3.4. Install the CI/CD plug-in for a Jenkins Pipeline project

Security Center allows you to install the CI/CD plug-in for a Jenkins Pipeline project. After you install the CI/CD plug-in, Security Center scans images in the project when you build the project. This topic describes how to install the CI/CD plug-in for a Jenkins Pipeline project.

### Limits

You can install the CI/CD plug-in only on Jenkins 1.625.3 or later.

### Download the CI/CD plug-in

- 1.
- 2.
- 3.
4. On the **Container** tab, click **CI/CD**.
5. Click **Integration Configuration**.
6. In the **Integration Configuration** panel, click **Download Plug-in** in the upper-right corner.


The CI/CD plug-in in the HPI format is downloaded to your computer. The name of the plug-in is **sas-jenkins-plugin**.

## Install the CI/CD plug-in on Jenkins

1. Log on to Jenkins.
2. In the left-side navigation pane, click **Manage Jenkins**.
3. On the **Manage Jenkins** page, click **Manage Plugins**.
4. On the **Manage Plugins** page, click the **Advanced** tab.
5. In the **Upload Plugin** section, click **Choose File**.

Select the downloaded CI/CD plug-in named **sas-jenkins-plugin**.

6. Click **Upload**.

 **Notice** After you install the **sas-jenkins-plugin** plug-in, you must restart Jenkins for the plug-in to take effect.

## Configure image scans

1. Log on to Jenkins.
2. Find the Jenkins Pipeline project whose images you want to scan and click the name of the project.
3. In the left-side navigation pane, click **Configure**.
4. In the Pipeline section, configure the parameters. After you complete the configuration, the images in the Jenkins Pipeline project can be scanned.

The following list provides examples of in declarative and scripted pipelines for Jenkinsfile. You can select an example to complete the configuration based on your business requirements.

- Scripted pipeline example

```
node {
    sas(accessKeyId: '$AK', accessKeySecret: '$SK', token: '$TOKEN', imageId: '$IMAGE',
    domain: '$DOMAIN', registryUrl: '$REGISTRY_URL', registryUsername: '$REGISTRY_USERNAME', registryPwd: '$REGISTRY_PWD')
}
```

- Declarative pipeline example

```
pipeline {
  agent any
  environment {
    ACCESS_KEY_ID = '$AK'
    ACCESS_KEY_SECRET = '$SK'
    IMAGE_ID = '$IMAGE'
    TOKEN = '$TOKEN'
    DOMAIN = '$DOMAIN'
    REGISTRY_URL = null
    REGISTRY_USERNAME = null
    REGISTRY_PWD = null
  }
  stages {
    stage('Build') {
      steps {
        sas(accessKeyId: env.ACCESS_KEY_ID, accessKeySecret: env.ACCESS_KEY_SECRET,
imageId: env.IMAGE_ID, token: env.TOKEN, domain: env.DOMAIN, registryUrl: env.REGISTRY_URL,
registryUsername: env.REGISTRY_USERNAME, registryPwd: env.REGISTRY_PWD)
      }
    }
  }
}
```

5. Click **Save**.

After you complete the configuration, Security Center scans images in the project for risks when you build the project.


## What to do next

You can view image scan results on the **Container** tab of the **Assets** page in the Security Center console. For more information, see [View image scan results](#).

## 4.3.5. Install the CI/CD plug-in for GitHub Actions

Security Center allows you to install the CI/CD plug-in on GitHub. After you install the CI/CD plug-in, Security Center scans images in GitHub when you build the images. This topic describes how to install the CI/CD plug-in on GitHub.

### Procedure


1. Log on to GitHub.
2. Click the profile picture in the upper-right corner and select **Your repositories** from the drop-down list that appears.
3. On the **Repositories** tab, click the **repository** for which you want to install the CI/CD plug-in.
4. Click the **Actions** tab.
5. In the **All workflows** section, find the workflows pipeline file for which you want to install the CI/CD plug-in and click the  icon in the **Actor** column.
6. In the drop-down list, select **View workflow file**.
7. In the **Workflow file for this run** section, configure the parameters based on the following example:




```


name: Docker build and scan security issue by sas-image-scanner
on:
  push:
    branches: [ main ]
  pull_request:
    branches: [ main ]
env:
  REPO_TAG: your_docker_image_repo:your_docker_image_tag
jobs:
  build:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v2
      - name: Build the Docker image
        run: docker build . --file Dockerfile --tag ${ env.REPO_TAG }
      - name: Scan image by sas-image-scanner
        run: >
          docker run --rm -v /var/run/docker.sock:/var/run/docker.sock --network=host
            sas-image-scanner-registry.cn-hangzhou.cr.aliyuncs.com/sas_public/sas-image-scanner:latest
            --accessKeyId=${ secrets.ACCESSKEYID } --accessKeySecret=${ secrets.ACCESSKEYSECRET }
            --token=${ secrets.SAS_TOKEN } --imageId=${ env.REPO_TAG }

```

The following table describes the parameters.

Parameter	Required	Description
accessKeyId	Yes	<p>The AccessKey ID of your Alibaba Cloud account or the RAM user of the Alibaba Cloud account.</p> <div>  <b>Notice</b> We recommend that you enter the AccessKey ID of a RAM user. The AccessKey pair of an Alibaba Cloud account is made up of the AccessKey ID and AccessKey secret. These credentials provide you full permissions on the resources within the account. You must keep the AccessKey pair confidential. To avoid security threats caused by malicious uses, do not disclose your AccessKey pair to external channels. We recommend that you follow the best practices of Alibaba Cloud and use the AccessKey pair of a RAM user to call API operations. </div>

Parameter	Required	Description
accessKeySecret	Yes	<p>The AccessKey secret of your Alibaba Cloud account or the RAM user of the Alibaba Cloud account.</p> <div>  <b>Notice</b> We recommend that you enter the AccessKey secret of a RAM user. The AccessKey pair of an Alibaba Cloud account is made up of the AccessKey ID and AccessKey secret. These credentials provide you full permissions on the resources within the account. You must keep the AccessKey pair confidential. To avoid security threats caused by malicious uses, do not disclose your AccessKey pair to external channels. We recommend that you follow the best practices of Alibaba Cloud and use the AccessKey pair of a RAM user to call API operations. </div>
token	Yes	<p>A token of the CI/CD plug-in. For more information about how to obtain a token of the CI/CD plug-in, see <a href="#">Obtain a token of the CI/CD plug-in</a>.</p>
imageId	Yes	<p>The ID of the image that you want to scan. By default, images are scanned locally.</p> <ul style="list-style-type: none"> <li>◦ If you want to scan a local image, you must set this parameter to the ID of the image or the tag of the image repository to which the image belongs.</li> <li>◦ If you want to scan remote images, you must configure the registryUrl parameter or set this parameter to the tag of the image repository to which the images belong.</li> </ul> <div>  <b>Notice</b> If you want to scan images in a remote image repository, you must configure the registryUrl, registryUsername, and registryPassword parameters. </div>
domain	No	<p>The endpoint of Security Center. Set the value to tds.ap-southeast-1.aliyuncs.com.</p>
registryUrl	No	<p>The URL of the image repository.</p> <div>  <b>Notice</b> If you want to scan the images in a remote image repository, you must configure this parameter. </div>
registryUsername	No	<p>The username used to log on to the image repository.</p> <div>  <b>Notice</b> If you want to scan the images in a remote image repository, you must configure this parameter. </div>

Parameter	Required	Description
registryPwd	No	<p>The password used to log on to the image repository.</p> <div> <b>Notice</b> If you want to scan the images in a remote image repository, you must configure this parameter.</div>

After you complete the configurations, Security Center scans images in the project for risks when you build the project.

## What to do next

You can view image scan results on the **Container** tab of the **Assets** page in the Security Center console. For more information, see [View image scan results](#).

### 4.3.6. View image scan results

After you install the CI/CD plug-in on Jenkins or GitHub, Security Center scans images in a Jenkins or GitHub project for risks when you build the project. You can view image scan results and handle risks based on the solutions that are provided by Security Center. This topic describes how to view image scan results.

#### Procedure

- 
- 
- 
- On the **Container** tab, click **CI/CD**.
- In the CI/CD plug-in list, find the plug-in that is used to scan images and click **View** in the **Actions** column.
- In the image list of the **Container** tab, view the image scan results.

You can view the recently scanned images in the image list. You can also search for an image by image ID or image tag.
- Find the image whose risks you want to handle and click **Handle** in the **Actions** column to go to the image details page.
  - On the image details page, you can view the following information: **Image System Vul**, **Image Application Vul**, **Image Baseline Check**, and **Image Malicious Sample**. In the upper-left corner of the vulnerability list, you can filter vulnerabilities by priority. You can also search for specific vulnerabilities.
  - If you want to view the details about a vulnerability, click **View** in the **Actions** column. The details page that appears provides the affected assets, the command that can be used to fix the vulnerability, and other details.

## 5. View website status

In the Security Center console, you can view the security status and security reports of your websites on the Assets page. In addition, you can run security checks on your websites. This topic describes how to view the security status of assets that are associated with your websites and security reports of your websites.

### View the security status of associated assets and the number of alerts

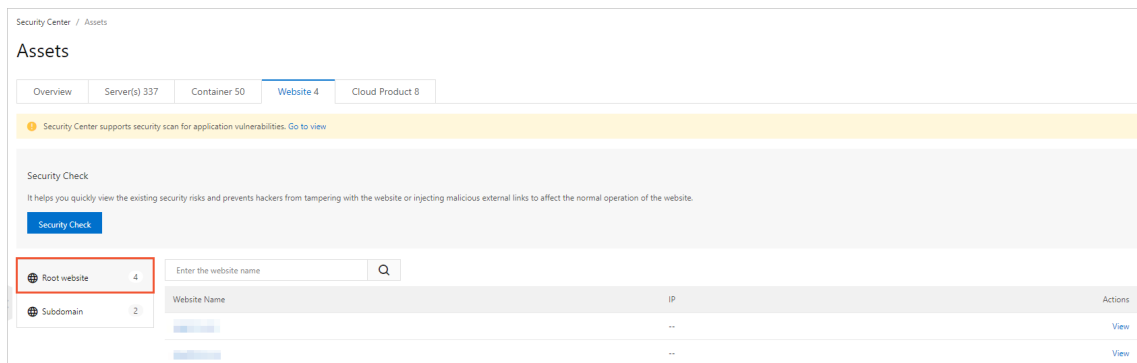
The Assets page displays security information about each website protected by Security Center. The information includes the root domain, subdomain, risk status of associated assets, and number of alerts. The following procedure describes how to view the security status of associated assets and the number of alerts.

- 
- 
- 
4. On the **Website** tab, view the information about each website protected by Security Center.

You can perform the following operations:

- **View root websites and associated assets**

You can click **Root website** to view information about all root websites, including **Website Name** and **IP**.

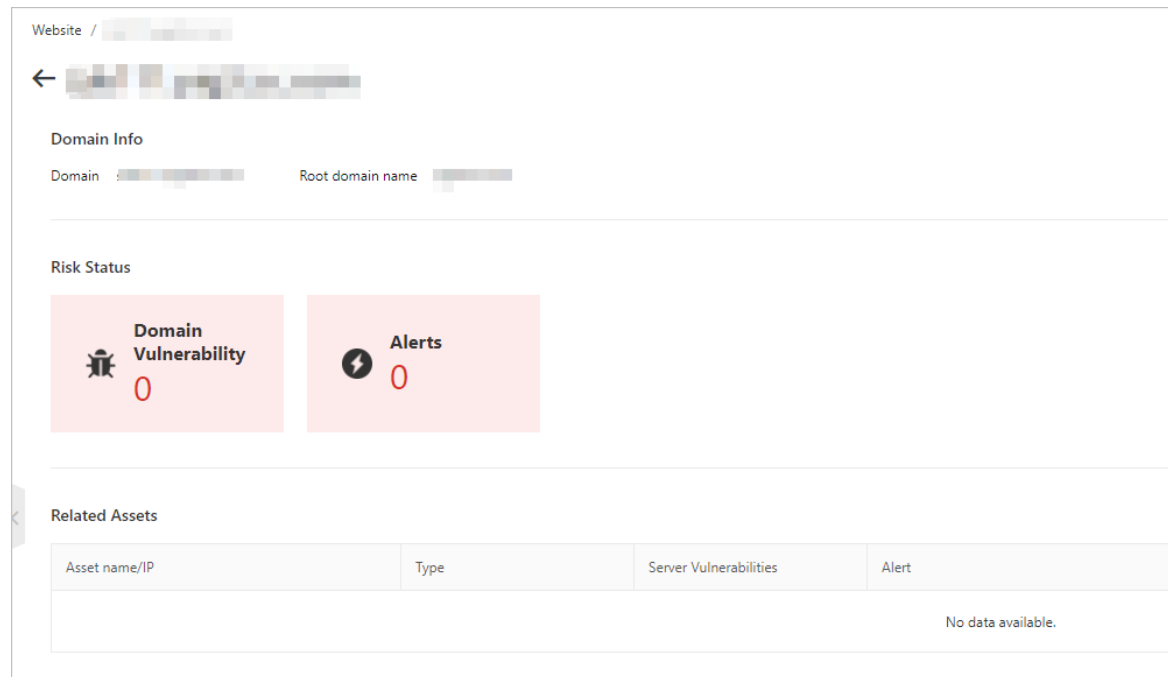


- **View subdomains and associated assets**

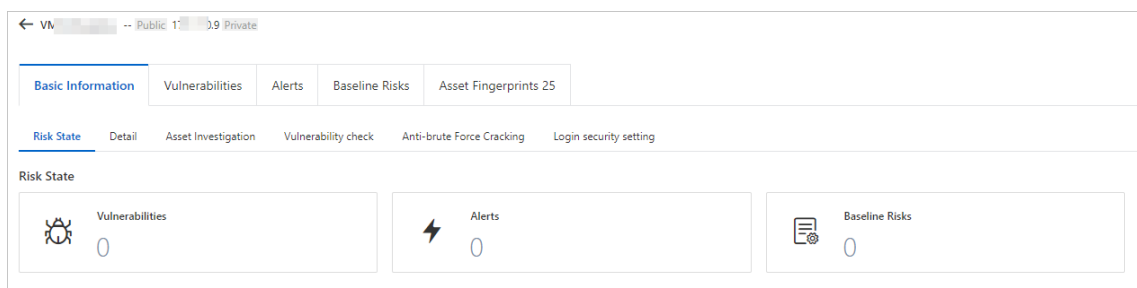
You can click **Subdomain** to view information about all subdomains, including **Website Name** and **IP**.

- 
- 
- 
- 
5. (Optional) View the security status of associated assets and the number of alerts.

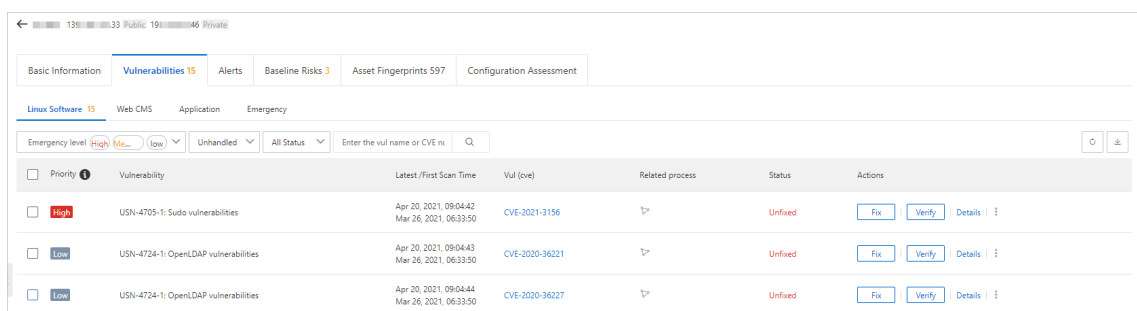
On the **Root website** or **Subdomain** tab, click a name in the **Website Name** column or **View** in the **Actions** column to view the details of a website.



- You can view **Domain**, **Root domain name**, **Risk Status**, and **Related Assets** of a website. The **Related Assets** section provides **Asset name/IP**, **Type**, **Server Vulnerabilities**, and **Alert**.
- You can click the name of an asset to go to the details page. On the **Basic Information** tab, you can view **Risk State** of the asset. For more information, see [View the details of an asset](#).



- You can click a number in the **Server Vulnerabilities** or **Alert** column to view the details. For more information about how to handle alerts, see [View and handle alerts](#).



## View website security reports



Security Center supports security checks for your websites and provides security reports based on the check results. The following procedure describes how to view a website security report.

- 1.
- 2.
- 3.
4. In the **Security Check** section, click **Security Check**.
5. On the **Website Security Report** page, view security suggestions and statistics, which include the numbers of risky websites, alerts, and vulnerabilities.

You can view the following information:

- **Overview**

In the **Overview** section, you can view the security score and the numbers of domains, risky websites, alerts, and vulnerabilities. Security Center calculates security scores based on the security status of websites. For more information about scoring, see [Penalty points for website security scoring](#). The following list describes the security scores to which each color corresponds:

- **Green:** 90 to 100 points. If the security score is displayed in green, your websites are in good security condition.
- **Yellow:** 70 to 89 points. If the security score is displayed in yellow, your websites have security risks. We recommend that you handle the risks based on the suggestions displayed on the page.
- **Red:** 10 to 69 points. If the security score is displayed in red, your websites have a large number of security risks and are vulnerable to attacks. We recommend that you reinforce the security of your websites at the earliest opportunity.

- **Risky Websites (TOP5)**

In the **Risky Websites (TOP5)** section, you can view a list of risky websites. The list provides website details, including the domains, SSL certificate configuration status, number of vulnerabilities, and number of alerts.

SSL certificates help encrypt website data by using HTTPS, which prevents data theft. If your website is not configured with SSL certificates, click **configure**.

If you want to handle the risks of a specific domain, click **Processing** in the Operation column. On the details page that appears, you can view the basic information about the domain, including the risk status and associated assets. In the **Related Assets** section, click a number in the **Server Vulnerabilities** or **Alerts** column. On the **Vulnerabilities** or **Alerts** page of the asset, fix the vulnerabilities or handle the alerts. For more information about how to fix vulnerabilities, see [View and handle Web-CMS vulnerabilities](#) and [View and handle application vulnerabilities](#). For more information about how to handle alerts, see [Handle alerts](#).

- **Alerts**

In the **Alerts** section, you can view the alerts generated on your website servers. You can view the alert names, risk levels, affected assets, and the last time when alerts were generated. If you want to handle a specific alert, click **Processing** in the Operation column. On the **Alerts** page, handle the alert as required. For more information, see [Handle alerts](#).

- **Vulnerabilities**

In the **Application vulnerability risks (top 5)** and **WebCMS Vul (TOP5)** sections, you can view the lists of vulnerabilities detected on your website servers. The lists provide vulnerability announcements, risk levels, and affected assets. If you want to handle a specific vulnerability, click **Repair** in the Operation column. On the **Vulnerabilities** page, handle the vulnerability as required.

- **Suggestions**

In the **Suggestions** section, you can view the security suggestions provided by Security Center based on the check results. When you receive a suggestion, such as **We recommend that you enable tamper protection to prevent malicious modification and avoid unnecessary losses**, click **Processing**. On the **Tamper Protection** page, you can enable tamper protection for your servers.

## Penalty points for website security scoring

Cause	Penalty point	Upper limit of penalty points
Security alerts are generated.	5 points for each security alert	A total of 30 points for all security alerts
Security vulnerabilities exist.	5 points for each security vulnerability	A total of 40 points for all security vulnerabilities
Domains are not configured with SSL certificates.	5 points for each domain	A total of 20 points for all domains

## 6. View the security status of cloud services

The Assets page displays the security information about cloud services. The information includes at-risk cloud services and their service types. The service types include Server Load Balancer (SLB), NAT Gateway, ApsaraDB RDS, and ApsaraDB for MongoDB. This topic describes how to search for specific cloud services to view their security statuses and how to specify search conditions.

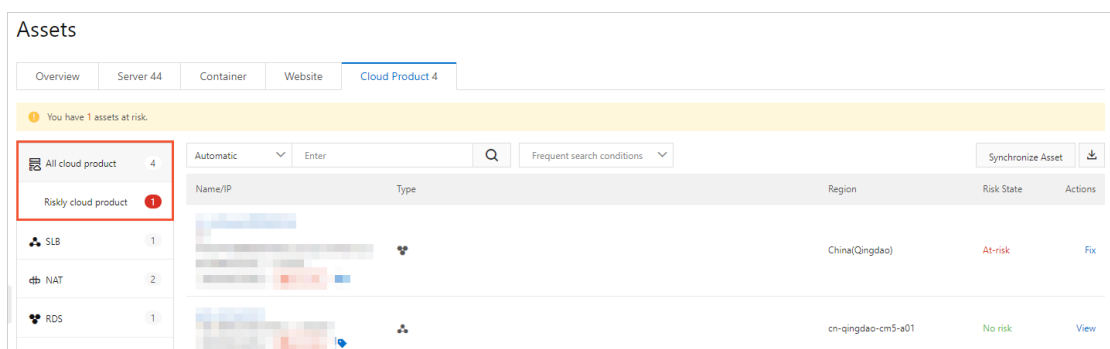
### Procedure

- 
- 
- 
- On the **Cloud Product** tab, view the security statuses of your cloud services.

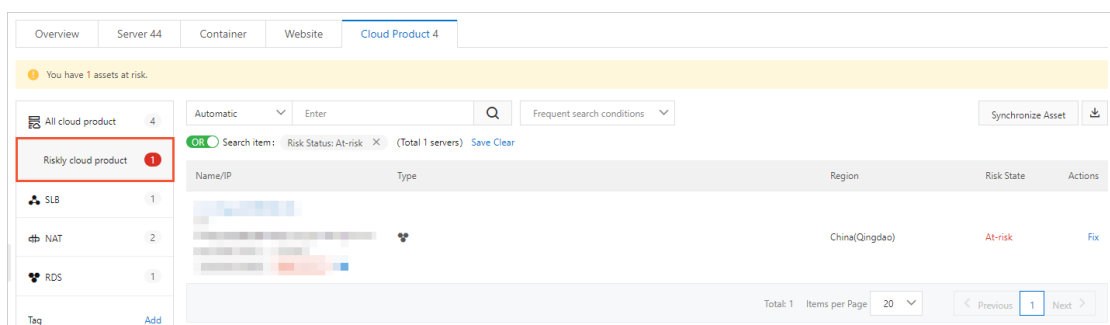
You can perform the following operations based on your requirements:

- Search for cloud services by asset status

- In the left-side pane of the Cloud Product tab, click **All cloud product** to view the number of all cloud services (**All cloud product**) and the number of at-risk cloud services (**Risky cloud product**). You can also view the security status of the cloud services.



- Click **Risky cloud product** to view the cloud services that are at risk.



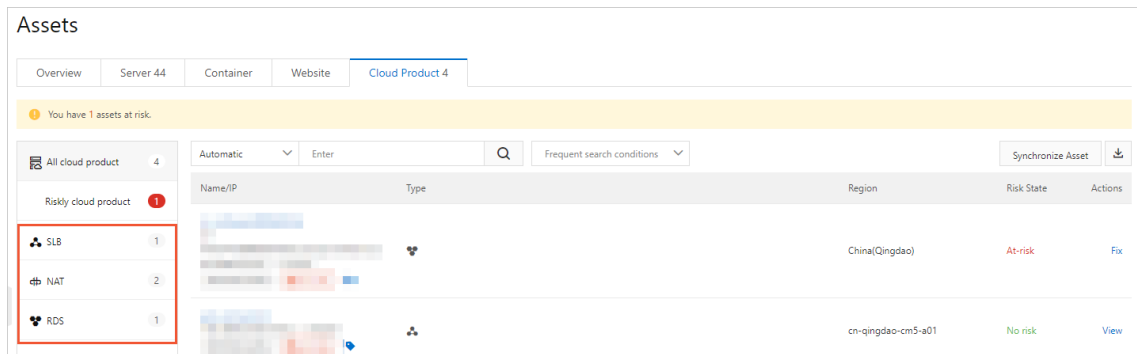
Click the name of a cloud service, or click **View** or **Fix** in the Actions column to view the details of a cloud service. For more information, see [View the details of an asset](#).

- Search for cloud services by service type

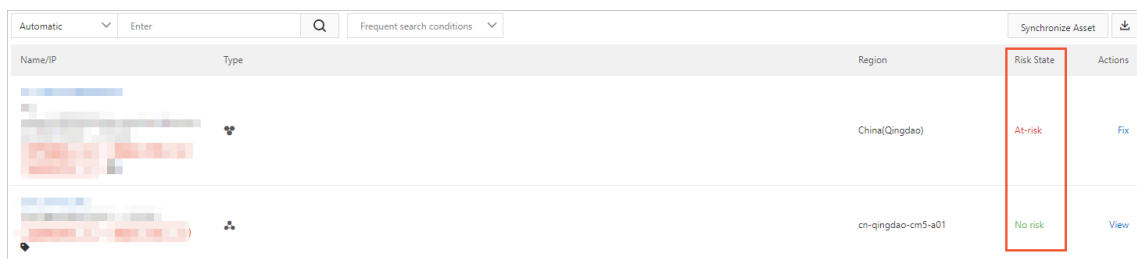
You can search for cloud services based on the following service types:

- SLB

- NAT Gateway
- ApsaraDB RDS
- ApsaraDB for MongoDB

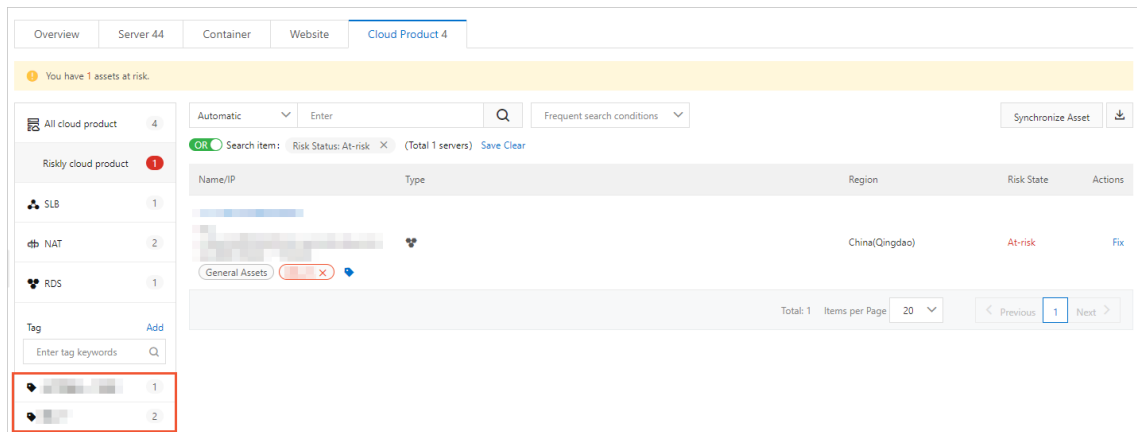


In the left-side pane of the Cloud Product tab, you can view the number of cloud services by service type. Click SLB, NAT, RDS, or MongoDB to view the security status of the assets.



#### ○ Search for cloud services by tag

In the Tag section in the left-side pane, you can view the number of assets that are bound to each tag. You can click a tag to view the security status of cloud services that are bound to the tag.



#### ○ Multi-conditional search

You can select All cloud product, SLB, NAT, RDS, or MongoDB in the left-side pane, and use the search box below Cloud Product to search for specific assets.

For example, you can select All cloud product and configure multiple search conditions to search for specific assets.

- Use multiple sub-conditions to search for specific assets:

You can select a condition from the drop-down list of the search box below **Cloud Product**, and select a sub-condition or enter a keyword in the search box to search for specific assets. Supported search conditions are **Internet IP**, **Instance name**, **Instance ID**, **Alert problems**, **Risk Status**, **Tag**, **Group name**, and **Region**.

#### Note

In this example, set the Boolean search operator to **OR**, select **Region** from the drop-down list, and then select **Region: China (Hangzhou)**. Select **Region** from the drop-down list again and select **Region: China (Qingdao)**. Consequently, assets that are deployed in the China (Hangzhou) and China (Qingdao) regions appear.

The screenshot shows the search interface with the following details:

- Search Box:** Boolean operator set to **OR**. Search items: **Region: China (Hangzhou)** and **Region: China (Qingdao)**. Total 0 servers.
- Table:**

Name/IP	Type	Region	Risk State	Actions
[Redacted]	db	China (Hangzhou)	No risk	<a href="#">View</a>
[Redacted]	db	China (Hangzhou)	No risk	<a href="#">View</a>
[Redacted]	db	China (Hangzhou)	No risk	<a href="#">View</a>
[Redacted]	db	China (Hangzhou)	No risk	<a href="#">View</a>

- Use multiple search conditions to search for specific assets:

Apply multiple search conditions to search for specific assets. In this example, select **Region** from the drop-down list, and select **Region: China (Hangzhou)**. Select **Risk Status** from the drop-down list and select **Risk Status: At-risk**. Set the Boolean search operator to **AND** or **OR**. Consequently, assets that are at risk in the China (Hangzhou) region appear.

The screenshot shows the search interface with the following details:

- Left Panel:** Filtered to 'Risky cloud product' with 1 item.
- Search Box:** Boolean operator set to **AND**. Search items: **Region: China (Hangzhou)** and **Risk Status: At-risk**. Total 0 servers.
- Table:** Empty, showing 'No Data'.

#### Note

- Select **SLB**, **NAT**, **RDS**, **MongoDB**, or **Tag** in the left-side pane, and use the search box below **Cloud Product** to search for specific assets.
- Select **All cloud product**, **SLB**, **NAT**, **RDS** or **MongoDB** in the left-side pane, and use the **Tag** feature to search for specific assets.

- Save frequently used search conditions

You can save applied search conditions as frequently used search conditions. Click **Save** below the search box. In the **Save condition** dialog box, specify a name for the search condition.

The screenshot shows the search interface with the following details:

- Search Box:** Boolean operator set to **AND**. Search items: **Region: China (Hangzhou)** and **Risk Status: At-risk**. Total 0 servers. The **Save** button is highlighted.

## 7. View the details of an asset

The Assets page in the Security Center console shows the details of all assets, including basic information, vulnerability information, alert management, baseline checks, and asset fingerprints. This topic describes how to view the details of a server or cloud service.

### Context

The Assets page in the Security Center console shows basic information about all assets.

The following table describes the features that Security Center provides for servers and cloud services.

- x: not supported
- √: supported

Feature	Description	Server	Cloud service
Basic Information	Risk State: shows the number of risks detected for an asset. The following types of risks can be detected: <ul style="list-style-type: none"><li>• Vulnerabilities</li><li>• Alerts</li><li>• Baseline Risks</li><li>• Configuration Assessment</li></ul>	√	√ (Only the risks of the Alerts and Configuration Assessment types can be detected.)
	Detail: shows the configurations and protection status of an asset. You can configure a tag and a group for the asset.	√	√ (Asset grouping is not supported.)
	Asset Investigation: shows the statistical information about asset fingerprints, including ports, software, processes, accounts, and middleware.	√	√
	Vulnerability check: shows the types of vulnerabilities that can be detected. You can specify the types of vulnerabilities that you want to detect for an asset.	√	x
	Anti-brute Force Cracking: shows the defense rule that is applied against brute-force attacks. You can modify the rule.	√	√
	Login security setting: shows the configured logon locations, IP addresses, time periods, and accounts. You can manage relevant alerts for an asset.	√	x

Feature	Description	Server	Cloud service
Vulnerabilities	Shows the results of vulnerability detection on an asset.	√	X
Alerts	Shows the alerts that are generated for an asset.	√	√
Baseline Risks	Shows the results of the baseline check on an asset.	√	X
Asset Fingerprints	Shows the details of asset fingerprints for an asset.	√	X
Configuration Assessment	Shows the results of configuration assessment on an asset.	√	√

## Procedure

- 1.
- 2.
3. On the **Assets** page, click the **Server(s)**, **Container**, **Website**, or **Cloud Product** tab.
4. Find the required asset and click its name.
5. View the details of the asset.

On the asset details page, click the **Basic Information**, **Vulnerabilities**, **Alerts**, **Baseline Risks**, **Asset Fingerprints**, or **Configuration Assessment** tab to view asset information.

This section describes the operations that you can perform on each tab:


- **Basic Information:** On this tab, you can click the required tab to view and manage asset details.


- **Risk State:** On this tab, you can view the numbers of vulnerabilities, alerts, and risk items detected in baseline checks. You can click the number in each section to view details.
- **Detail:** On this tab, you can view the configurations and protection status of the asset. You can also manage the asset tag and group.

- **Change the group**

Click **Group**. In the **Group** dialog box, select a new group and click **OK**.

- **Add a tag**

Click the  icon. In the **Add tag** dialog box, select a tag and click **OK**.

You can click the  icon on the right of a tag to delete the tag.

- **Asset Investigation:** On this tab, you can view statistical information about asset fingerprints. You can click the number below an item to go to the **Asset Fingerprints** tab on which you can view the details.
- **Vulnerability check:** On this tab, you can view the types of vulnerabilities for which you enable or disable the vulnerability detection feature. You can enable or disable this feature as needed. Supported types include Linux Software, Windows System, Web CMS, and Emergency.

- **Anti-brute Force Cracking:** On this tab, you can view the defense rule that is applied against brute-force attacks. You can modify and save the defense rule as needed. For more information about how to create defense rules, see [Configure alert settings](#).
- **Login security setting:** On this tab, you can set the **Login Location** parameter and turn on or turn off Uncommon IP Alert, Uncommon Time Alert, and Uncommon Account Alert. You can configure the logon locations, IP addresses, time periods, and accounts for the asset.
- **Vulnerabilities:** On this tab, you can view the results of vulnerability detection on the asset. For more information about how to fix vulnerabilities, see [Vulnerability fix](#).
- **Alerts:** On this tab, you can view the alerts that are generated for the asset. For more information about how to handle alerts, see [View and handle alerts](#).
- **Baseline Risks:** On this tab, you can view the results of the baseline check on the asset. For more information about how to handle baseline risks, see [Run a baseline check](#).
- **Asset Fingerprints:** On this tab, you can view and collect statistical information about asset fingerprints, including ports, software, processes, accounts, scheduled tasks, and middleware. You can manually run a task to collect the latest fingerprints of the asset.
  - a. Click the **Port**, **Software**, **Process**, **Account**, **Scheduled Tasks**, or **Middleware** tab. Then, click **Collect data now** in the upper-right corner of the list.
  - b. In the **Collect data** message, click OK.

It requires one to five minutes to complete the data collection task. After the task is completed, you can view the latest fingerprint data of the selected type of asset. For more information, see [Asset fingerprints](#).
- **Configuration Assessment:** On this tab, you can view the results of configuration assessment on the asset. For more information, see [View the check results of configuration assessment for your cloud services and handle the detected risks](#).



## 8. Manage asset groups

You can group assets on the Assets page in the Security Center console. To find or manage multiple assets at a time, we recommend that you add the same types of assets to an asset group. This topic describes how to create, modify, and delete an asset group. This topic also describes how to change the asset group for your servers.

### Create an asset group

- 1.
- 2.
- 3.
4. In the server list on the left, click **Server Group**.

All Servers	291	<div><div>Add group</div><div>Please input group name</div><div>Q</div></div>				
		Server Group	Servers	Risk	Unprotected	Actions
Risky server	236	Default	284	229	55	Manage
Unprotected server	55	<div></div>	6	6	0	Manage / Delete
Shutdown Server(s)	11	H <div></div>	1	1	0	Manage / Delete
Exposed Server	90	cases	0	0	0	Manage / Delete
New Server(s)	36	<div></div> <div></div>	0	0	0	Manage / Delete
<div>Server Group</div>	57	zh <div></div>	0	0	0	Manage / Delete
Region	9	pre <div></div>	0	0	0	Manage / Delete

 **Note** By default, the assets that are not grouped are in the **Default** group.

5. Click **Add group**.
6. In the **Add Group** dialog box, enter an asset group name and add servers to the asset group.

7. Click **OK**.

In the server group list, you can view the new asset group.

## Modify or delete an asset group

The following procedure describes how to modify or delete an asset group:

- 1.
- 2.
- 3.
4. In the server list on the left, click **Server Group**.
5. Find the asset group that you want to modify or delete and click **Manage** or **Delete**.

You can perform the following operations based on your business requirements:

- **Modify a group**
  - a. Find the asset group that you want to modify and click **Manage** in the Actions column.

b. In the **Group** dialog box, modify the asset group name or servers in the asset group.

c. Click **OK**.

o **Delete a group**

To delete an asset group, click **Delete** in the Actions column and click **OK**.

**Note** After you delete an asset group, the assets in the group are moved to the Default group.

## Change the asset group for your servers

You can add assets to an asset group to manage multiple assets at a time. We recommend that you add the same types of assets to an asset group. For example, when you configure a baseline check policy template, you can specify an asset group to apply the policy to all assets in the group. You can also filter and view assets based on asset groups in the asset list.

To add assets to a specific server group, perform the following steps:

- 1.
- 2.
- 3.
4. On the Server(s) tab, select one or more assets and click **Group**.

<input type="checkbox"/>	47.118.18 Public 192.168.1.1 Private	Exposure	vpc-uf6k3	Linux	China(Shanghai)	Enable	1	4	...	At-risk	Fix
	General Assets Internetip X										
<input checked="" type="checkbox"/>	47.118.18 Public 172.16.1.1 Private	Unexposed	vpc-14nkb	Linux	Singapore	Close	...	...	...	Unknc	View
	General Assets Internetip X										
<input checked="" type="checkbox"/>	161.157 Public 172.16.1.1 Private	Unexposed	vpc-14nkd	Linux	Singapore	Close	...	...	...	Unknc	View
	General Assets Internetip X										
<div><div>Group</div><div>Security check</div><div>More Operations</div></div>											
Total: 291 Items per Page 10 20 50 1 2 ... 15											

5. In the **Group** dialog box, select a new asset group.

Group

X

New group: 

Select

OK

Cancel

6. Click **OK**.

## 9. Manage asset tags


Security Center allows you to add asset importance tags and custom tags to your assets on the Assets page. This way, you can filter assets for those with the same attributes. This topic describes how to add asset importance tags to your assets and how to add, modify, and remove custom tags.

### Context

Security Center provides the asset importance tags described in the following table to classify assets. You can select appropriate importance tags for your assets.

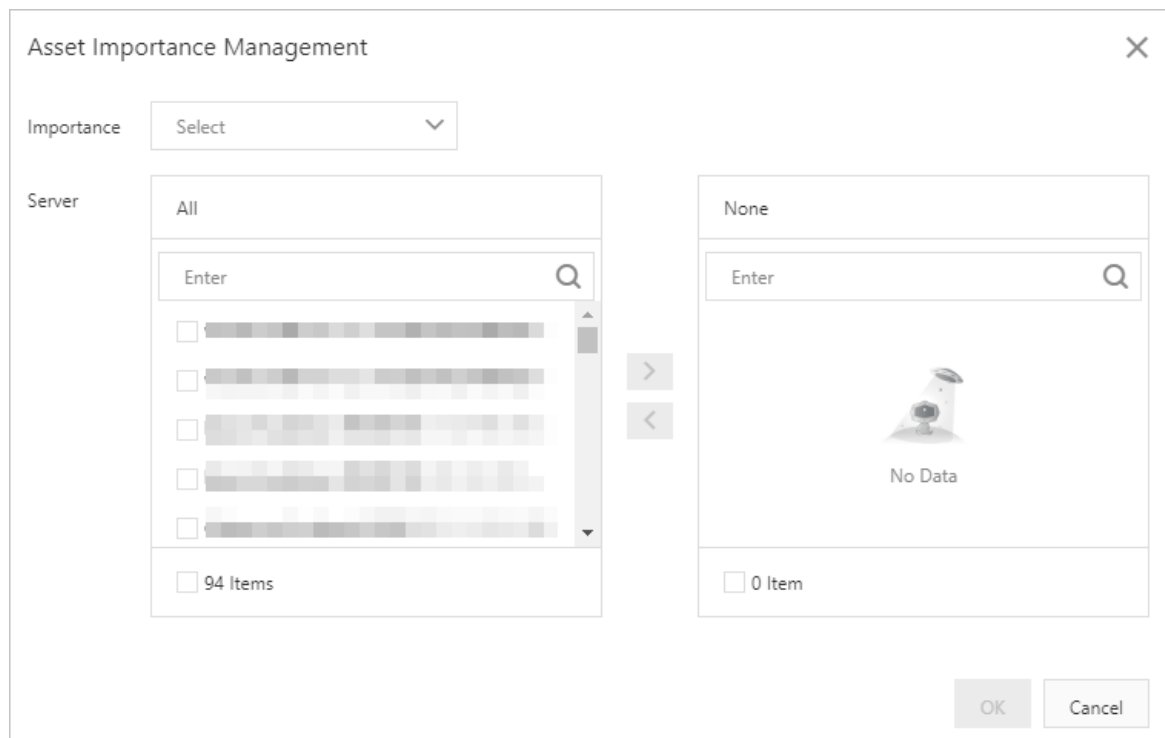
An asset importance tag is transformed to an **asset importance score**. An **asset importance score** is used to calculate the score of the urgency to fix a vulnerability. You can determine the priorities to handle vulnerabilities based on the score of the urgency to fix a vulnerability. We recommend that you add importance tags to your core assets. If you do so, Security Center prompts you to fix the vulnerabilities based on the priorities. The following table describes the relationships between asset importance tags and asset importance scores. For more information about the priorities to fix vulnerabilities, see [Priorities to fix vulnerabilities](#).

Asset importance tag	Asset importance score	Recommendation
Important Assets	1.5	Assets that run crucial workloads or store core data. Virus intrusions into these assets adversely affect the system and cause major loss.
General Assets	1	Assets that run non-crucial workloads and are highly replaceable. Virus intrusions into these assets cause less impact on the system.
Test Assets	0.5	Assets for functional or performance tests or assets that cannot cause major loss.

 **Note** If you do not add asset importance tags, the **General Assets** tag is added to each asset. This tag indicates that the asset importance score is 1.

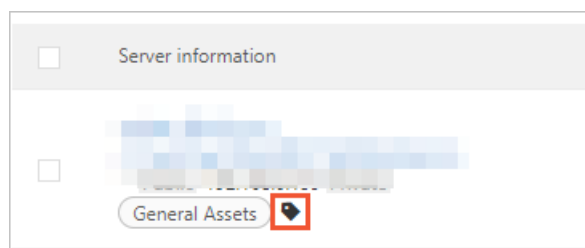
### Add an asset importance tag

- 1.
- 2.
- 3.
4. In the left-side navigation tree, click **Management** next to **Asset Importance**.
5. In the **Asset Importance Management** dialog box, select the required asset importance tag and the assets to which you want to add the tag.



**Note** You can add only one asset importance tag to an asset.

6. Click **OK**.

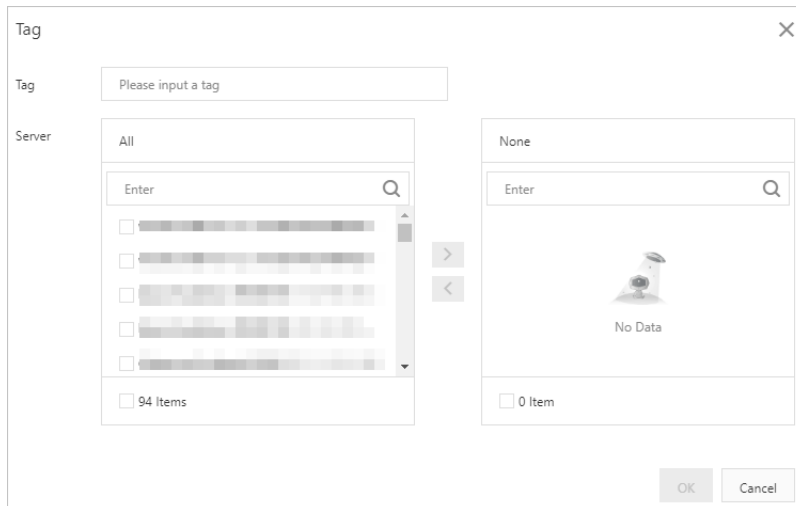


After you add an asset importance tag to an asset, the tag is displayed below the name of the asset.


If you want to modify the asset importance tag or custom tag of a single asset, you can click the icon of the asset. In the **Add tag** dialog box, select the required asset importance tag or custom tag. Then, click **OK**.


## Add a custom tag

- 1.
- 2.
3. Click the **Server(s)** or **Cloud Product** tab.
4. On the **Server(s)** or **Cloud Product** tab, click **Management** next to **Tag** in the left-side navigation tree.
5. In the **Tag** dialog box, enter the tag name and select the assets to which you want to add the tag.




6. Click **OK**.

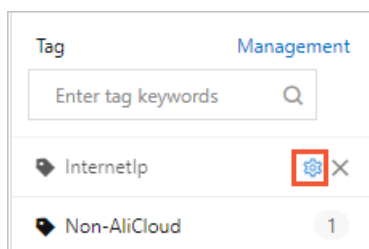
In the asset list, you can click the  icon in the **Tag** column to add the tag to an asset.

 **Note** You can add multiple tags to one asset. All tags of an asset are displayed in the **Tag** column.

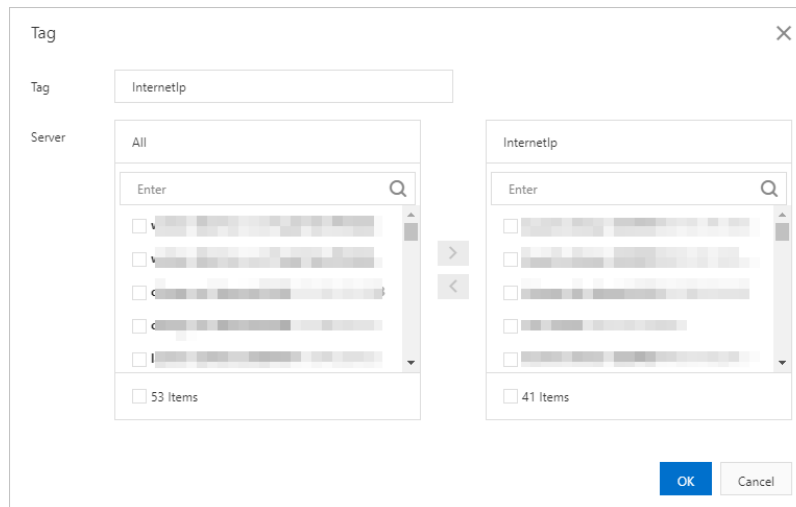
## Modify or remove a custom tag

The following procedure describes how to modify or remove a custom tag. To modify a tag, you can rename the tag or adjust the assets of the tag.

- 1.
- 2.
3. Click the **Server(s)** or **Cloud Product** tab.
4. On the **Server(s)** or **Cloud Product** tab, modify or remove a tag.
  - o **Modify a tag**
    - a. Find the tag that you want to modify and move the pointer over the tag. Then, click the  icon that appears.




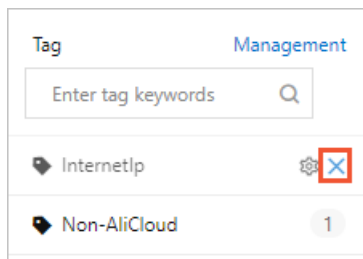
- b. In the **Tag** dialog box, enter a new name in the **Tag** field, add assets to the tag, or remove assets from the tag.



- c. Click **OK**.

o **Remove a tag**

Find the tag that you want to remove and move the pointer over the tag. Then, click the  icon that appears. In the message that appears, click **OK**.





# 10. Use the agent troubleshooting feature

If the Security Center agent becomes offline upon an exception, the agent fails to be installed or uninstalled, or the processes of the Security Center agent cause high CPU utilization, you can use the agent troubleshooting feature of Security Center to troubleshoot issues. This topic describes how to use the agent troubleshooting feature.

## Context

The troubleshooting results contain the issues and the suggestions on how to solve the issues. You can download diagnostic logs to verify and analyze the issues.

## Limits

The agent troubleshooting feature is available for the servers that run the following versions of operating systems:

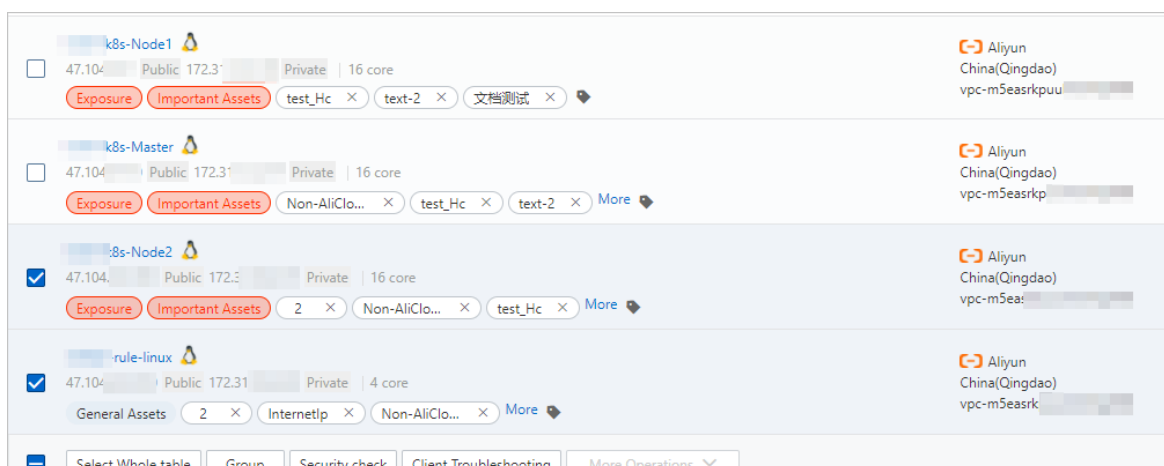
- Windows Server 2008 and later
- 64-bit Linux (versions later than CentOS 5)

## Scenarios

- If your servers are added to Security Center, you can click **Client Troubleshooting** on the **Server(s)** tab of the **Assets** page in the Security Center console to troubleshoot issues. For more information, see [Troubleshoot issues for servers that are added to Security Center](#).
- If your servers are not added to Security Center, you can run `aegis_checker` commands on the servers to troubleshoot issues. For more information, see [Troubleshoot issues for servers that are not added to Security Center](#).

## Troubleshoot issues for servers that are added to Security Center

- 1.
2. In the left-side navigation pane, click **Assets**.
3. On the **Assets** page, click the **Server(s)** tab.
4. On the **Server(s)** tab, select one or more servers for which you want to troubleshoot issues from the server list and click **Client Troubleshooting** below the server list.




5. In the **Troubleshoot Agent Issues** dialog box, configure the **Question type** and **Mode** parameters.

The following table describes the parameters.

Parameter	Description
<b>Question type</b>	The type of the issue that you want to troubleshoot. If you cannot identify the type, select <b>Overall Check (Unknown Issues)</b> .
<b>Mode</b>	<p>The mode that you want to use to troubleshoot issues. Valid values:</p> <ul style="list-style-type: none"><li>◦ <b>Standard</b>: In this mode, logs of the Security Center agent are collected and then reported to Security Center for analysis. The time required for troubleshooting is approximately 1 minute.</li><li>◦ <b>Strict</b>: In this mode, the information about the Security Center agent is collected and then reported to Security Center for analysis. The information includes network conditions, processes, and logs. The time required for troubleshooting is approximately 5 minutes.</li></ul>

6. Click **Start Check**.

 **Note** When you troubleshoot issues, the related diagnostic program collects information about the agent that is installed on the servers and reports the information to Security Center for analysis. The information includes the network conditions, the processes of the Security Center agent, and logs.

7. In the **Attention** message, click **OK**. In the **Task management** panel, view all troubleshooting tasks.

You can also click **Client Mission Management** in the upper-right corner of the **Assets** page to go to the **Task management** panel.

8. Find the task whose details you want to view and click **Details** in the **Operation** column. The **Execution log** panel appears.

The **Execution log** panel displays the details about the troubleshooting tasks for each server.

The following table describes the parameters in the **Execution log** panel.

Parameter	Description
<b>Start time/end time</b>	The time when the troubleshooting task starts and ends.
<b>Server information</b>	The name of the server on which the troubleshooting task is run.

Parameter	Description
Status	The status of the troubleshooting task. Valid values: <ul style="list-style-type: none"><li>◦ <b>Success</b>: The command that is used for troubleshooting is issued.</li><li>◦ <b>Timeout</b>: The command that is used for troubleshooting is issued for a while, but the troubleshooting result is not returned.</li><li>◦ <b>Failure</b>: The troubleshooting result is generated.</li></ul>
Problem	The issues that are found after the troubleshooting task is complete.
Results	The solutions to the issues.
Operation	The operation that you can perform on the diagnostic logs of the troubleshooting task. You can download the logs to verify and analyze the issues.

If the solutions to the issues are provided in the **Results** column, you can follow the solutions to solve the issues. If no solutions are provided in the **Results** column, click **Download Diagnostic Log** in the **Operation** column to download the diagnostic logs. Then, report the downloaded logs and the ID of your Alibaba Cloud account to Alibaba Cloud engineers for verification and analysis.

## Troubleshoot issues for servers that are not added to Security Center

If your servers are not added to Security Center, you can run commands on the servers based on the operating system of each server to troubleshoot issues.

1. Log on to the server for which you want to troubleshoot issues.


### Note



- You must log on to a Windows server as an administrator.
- You must log on to a Linux server as a root user.

2. Run the command on the server.


The command that you use to troubleshoot issues varies based on the operating system of an Elastic Compute Service (ECS) instance or a server that is not deployed on Alibaba Cloud. The following table describes the commands.

Server	Operating system	Mode	Command
--------	------------------	------	---------

Server	Operating system	Mode	Command
		Standard	<div>Run the following command on the ECS instance as a root user:</div> <div><pre>wget "http://update2.aegis.aliyun.com/download/aegis_client_self_check/linux64/aegis_checker.bin" &amp;&amp; chmod +x aegis_checker.bin &amp;&amp; ./aegis_checker.bin</pre></div> <div>If no network connection is established between the ECS instance and Security Center, you must download the <b>aegis_checker</b> program and install the program on the ECS instance. Then, run the following command on the instance:</div> <div><pre>chmod +x aegis_checker.bin ./aegis_checker.bin</pre></div> <div><div> <b>Note</b></div> In Standard mode, logs of the Security Center agent are collected and then reported to Security Center for analysis. The time required for troubleshooting is approximately 1 minute.</div>
	Linux		

Server	Operating system	Mode	Command
ECS instance		Strict	<p>Run the following command on the ECS instance as a root user:</p> <pre>wget "http://update2.aegis.aliyun.com/download/aegis_client_self_check/linux64/aegis_checker.bin" &amp;&amp; chmod +x aegis_checker.bin &amp;&amp; ./aegis_checker.bin -b "ew0KICAgICJldWlkIjogIiIsDQogICAgImNtZ F9pZHgiOiAiIiwNCiAgICAiaXNzdWUiOiAib3R oZXJfaXNzdWUiLA0KICAgICJtb2RlIjogMywNC iAgICAianNyd19kb21haW4iOiBbXSswNCiAgICA idXBkYXRlX2RvbWFnbiI6IFtdDQp9"</pre> <p> <b>Note</b> In Strict mode, the information about the Security Center agent is collected and then reported to Security Center for analysis. The information includes network conditions, processes, and logs. The time required for troubleshooting is approximately 5 minutes.</p>
	Windows	Standard	<p>Use one of the following methods for troubleshooting:</p> <ul style="list-style-type: none"> <li>Download the <b>aegis_checker</b> program and run the program as an administrator.</li> <li>Run the following command in Command Prompt as an administrator:</li> </ul> <pre>powershell -executionpolicy bypass - c "(New-Object Net.WebClient).DownloadFile('http:// update2.aegis.aliyun.com/download/ae gis_client_self_check/win32/aegis_ch ecker.exe', \$ExecutionContext.SessionState.Path. GetUnresolvedProviderPathFromPSPath( './aegis_checker.exe'))"; "./aegis_checker.exe"</pre> <p> <b>Note</b> Windows servers do not support the Strict mode.</p>

Server	Operating system	Mode	Command
Server that is not deployed on Alibaba Cloud	Linux	Standard	<p>Run the following command on the server as a root user:</p> <pre>wget "http://aegis.alicdn.com/download/aegis_client_self_check/linux64/aegis_checker.bin" &amp;&amp; chmod +x aegis_checker.bin &amp;&amp; ./aegis_checker.bin</pre>
		Strict	<p>Run the following command on the server as a root user:</p> <pre>wget "http://aegis.alicdn.com/download/aegis_client_self_check/linux64/aegis_checker.bin" &amp;&amp; chmod +x aegis_checker.bin &amp;&amp; ./aegis_checker.bin -b "ew0KICAgICJldWlkIjogIiIsDQogICAgImNtZF9pZHgiOiAiIiwNCiAgICAiaXNzdWUiOiAib3RoZXJfaXNzdWUiLA0KICAgICJtb2RlIjogMywNCiAgICAianNyd19kb21haW4iOiBbXSwnCiAgICAidXBkYXRlX2RvbWVpbiI6IFtdDQp9"</pre>

Server	Operating system	Mode	Command
	Windows	Standard	<p>Use one of the following methods for troubleshooting:</p> <ul style="list-style-type: none"> <li>Download the <a href="#">aegis_checker</a> program and run the program as an administrator.</li> <li>Run the following command in Command Prompt as an administrator:</li> </ul> <pre>powershell -executionpolicy bypass -c "(New-Object Net.WebClient).DownloadFile('http://aegis.alicdn.com/download/aegis_client_self_check/win32/aegis_checker.exe', \$ExecutionContext.SessionState.Path.GetUnresolvedProviderPathFromPSPath('.\aegis_checker.exe'))"; "./aegis_checker.exe"</pre> <p> <b>Note</b> Windows servers do not support the Strict mode.</p>

3. After the troubleshooting is complete, export the generated log package.

The directory in which the log package is stored varies based on the operating system of a server.

- Linux servers

The log package is stored in `/root/miniconda2/aegis_checker/output`.

- Windows servers

The log package is stored in `./miniconda2/aegis_checker/output` of the current directory.

In the extracted log file, logs prefixed with **[root cause]** include the issues that the `aegis_checker` program detects on the Security Center agent. If some issues are solved, you can view the details in the logs. If some issues are not solved, the program may provide solutions. You can follow the solutions to solve the issues. If the program does not provide a solution to an issue, take a screenshot of the troubleshooting result. Then, report the screenshot, the log package, and the ID of your Alibaba Cloud account to Alibaba Cloud engineers for verification and analysis.

# 11. Unbind a server not deployed on Alibaba Cloud from Security Center

Security Center protects servers that are not deployed on Alibaba Cloud and have the Security Center agent installed. If you do not require protection for these servers, you can unbind the servers from Security Center. This topic describes how to unbind a server that is not deployed on Alibaba Cloud from Security Center.

## Prerequisites

- The Security Center agent installed on the server that you want to unbind from Security Center is in the **Close** state. For more information, see [Enable or disable server protection](#) and [Uninstall the Security Center agent](#).
- The client protection feature is disabled on the server that you want to unbind from Security Center. For more information, see [Use the client protection feature](#).

## Context

If the server that is not deployed on Alibaba Cloud shuts down but still has unhandled vulnerabilities or alerts, you can unbind the server from Security Center on the Assets page. This prevents the unhandled vulnerabilities and alerts from affecting the security score of your assets. If you no longer want Security Center to protect the server, you can directly uninstall the Security Center agent. For more information about how to uninstall the Security Center agent, see [Uninstall the Security Center agent](#).

After you unbind a server from Security Center, the server is no longer displayed in the server list on the Assets page. Security Center no longer protects the server. However, all processes and files in the directory of the Security Center agent are retained on the server. If you want Security Center to protect the server again, start up the server. After the server connects to the Internet, the Security Center agent automatically runs on the server, and Security Center starts to protect the server.

If you uninstall the Security Center agent, all processes and files in the directory of the Security Center agent are deleted from the server.

### Note


- You can unbind only the servers that are not deployed on Alibaba Cloud from Security Center. If you use an Alibaba Cloud Elastic Compute Service (ECS) instance, you do not need to perform the unbinding operation. If you uninstall the Security Center agent from an ECS instance, the ECS instance is still displayed in the server list on the Assets page.
- After you unbind a server that is not deployed on Alibaba Cloud from Security Center, the server no longer consumes the quota of protected servers or protected server vCPUs. This way, you can install the Security Center agent on other servers based on your business requirements.

## Procedure

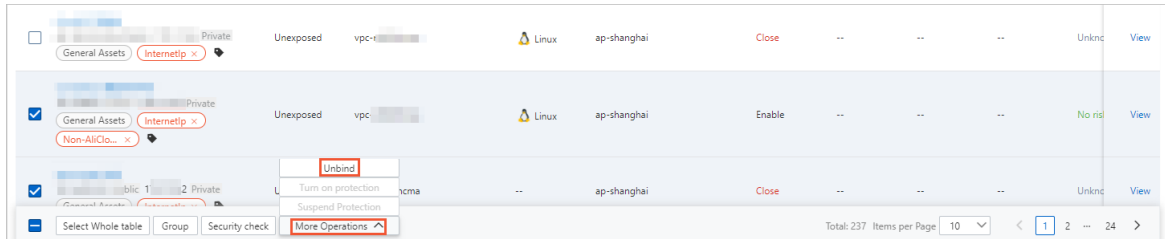
- 1.
- 2.



3.

4.  **Note** You can **unbind** only the server whose protection status is displayed as **Disable Protection** or **Close** in the Agent column. If the agent on the server is in the **Enable** state, you must select **Suspend Protection** below the server list on the Assets page. For more information, see [Enable or disable server protection](#).

In the server list, select the server that you want to unbind from Security Center and choose **More Operations > Unbind** below the server list.

5. Click **OK**.

After you unbind the server from Security Center, the server is no longer displayed in the server list.

# 12.FAQ


This topic answers the frequently asked questions about the Assets page of the Security Center console.

- [How do I unbind an external server from Security Center?](#)
- [How do I unbind an Elastic Compute Service \(ECS\) instance from Security Center?](#)

## How do I unbind an external server from Security Center?

If an external server no longer requires protection, you can manually unbind this server from Security Center in the Security Center console. For more information, see [Unbind a server not deployed on Alibaba Cloud from Security Center](#).

After the server is unbound from Security Center, the server is no longer protected by Security Center. You cannot view data related to the server in the Security Center console, such as alerts, vulnerabilities, or attack information.

 **Note** If you suspend or uninstall the Security Center agent instead of unbinding the server from Security Center, you can continue to view data related to the server in the Security Center console.

## How do I unbind an Elastic Compute Service (ECS) instance from Security Center?

You cannot unbind an ECS instance from Security Center in the Security Center console. If you uninstall the Security Center agent from an ECS instance, the status of the ECS instance changes to disconnected in the asset list of the Security Center console. The ECS instance is not removed from the asset list. Only after you log on to the [ECS console](#) and release the ECS instance, it is unbound from Security Center and removed from the asset list.