Alibaba Cloud
漏洞扫描

User Guide

Issue: 20200703

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

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

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Overview

This topic describes the **Overview** page in the Cloud Security Scanner console. This page provides statistics of your assets that enable you to learn about the risk trends, security status, and asset information. This page displays the following information: the number of detected vulnerabilities, the numbers of unprocessed and processed risks, asset overview, task overview, scan target overview, task instance overview, and product updates.

On the Overview page, you can view and manage risks and vulnerabilities in your assets.

The Overview page consists of the following modules:

- **Risk and asset overview**: displays the numbers of risks at different levels (high, medium, low, and information), the number of high risk vulnerabilities, the total number of vulnerabilities, the number of assets that do not have a scan task configured, the number of assets that are periodically scanned, and the number of assets that are not periodically scanned.

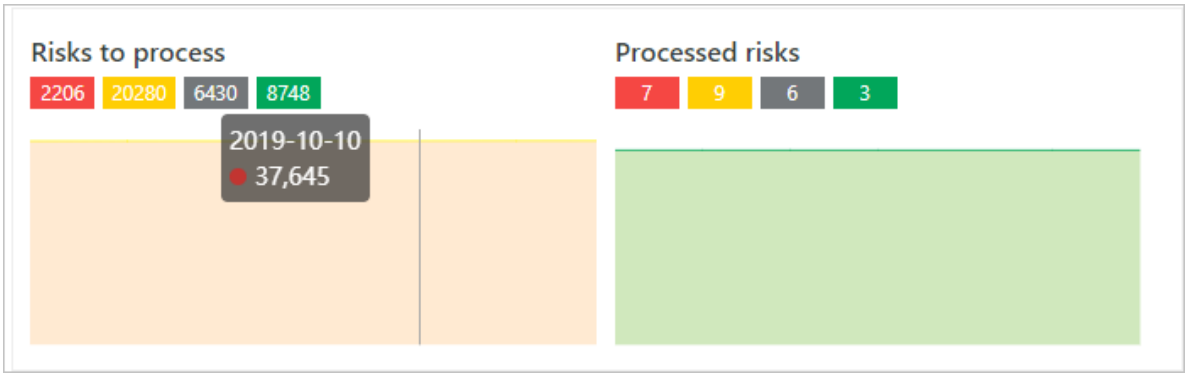
  - You can place the pointer over a legend key in the plot area to view the number of risks at a specific level.
  - Click **Process** or the number under **Total Vulnerabilities** to go to the Risks page. You can view vulnerability and risk details and manage the vulnerabilities and risks on this page.
  - Click a number under **Not Scanned**, **Periodically Scanned**, or **Not Periodically Scanned** to go to the **Scan Targets** > **Not Scanned**, **Periodically Scanned**, or **Not Periodically Scanned** page to view the asset information.

    - **Not Scanned**: displays the assets that do not have a scan task. We recommend that you create scan tasks for your assets as soon as possible and start periodic scan tasks. Periodic scan tasks scan your assets as scheduled. This helps you detect and fix vulnerabilities in a timely manner.
    - **Periodically Scanned**: displays the assets that have periodic scan tasks started. Your assets are periodically scanned. You can view the scan results and risk trends.
    - **Not Periodically Scanned**: displays the assets that do have a periodic scan task. You can add a tag to the assets that do not have a periodic scan task and quickly create a periodic scan task for these assets.

- **Risk Overview**: displays the risk statistics of your assets in the past seven days, including the numbers of risks that you have and have not processed, and the numbers of risks at different levels.
  - **To be Processed**: displays the latest risks to be processed, the numbers of risks at different levels (high, medium, low, and information), and the risk trends in the past seven days. This helps you learn about the risk trends of your assets.

    You can click a number at a specific level under **To be Processed** to go to the **Risks** page to view risk details and manage the risks. For more information, see Risks.
  - **Processed**: displays the risks that you have already processed at different levels (high, medium, low, and information), and the security status of your assets in the past seven days. This helps you learn about the security status of your assets after you have processed the risks.

    You can click a number at a specific level under **Processed** to go to the **Risks** page to view the details of risks and vulnerabilities that you have already processed.



In the **To be Processed** or **Processed** section, you can move the pointer from the left side to the right side to view the trend of the risks that you have or have not processed in the past seven days.

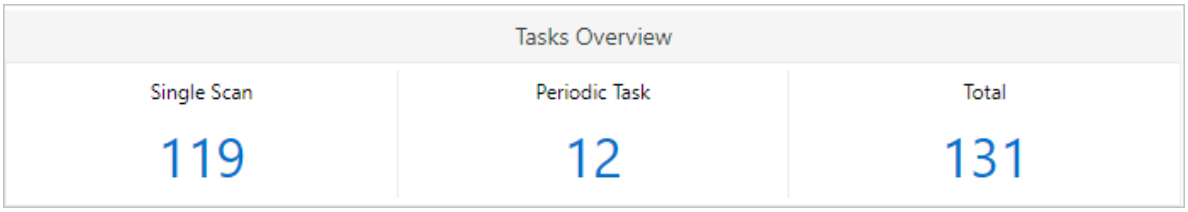
- **Asset Overview**: displays the number of assets that Cloud Security Scanner has the permission to scan, the number of Alibaba Cloud assets, and the number of discovered assets to be confirmed.

Click a number under **All Assets**, **Alibaba Cloud Assets**, or **To be Confirmed** to go to the **Scan Targets** > **All Assets**, **Alibaba Cloud Assets**, or **To be Confirmed** page to view the asset information.

Note:

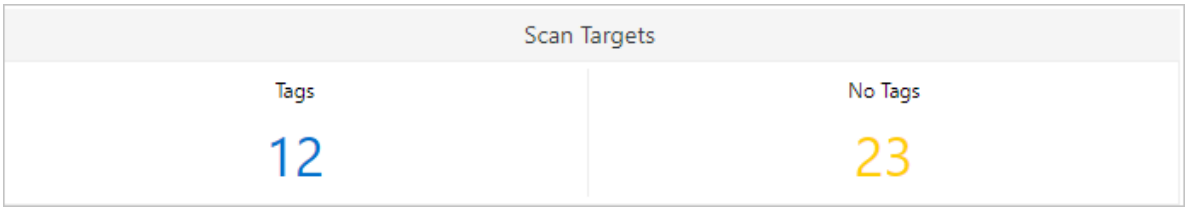
- After you activate Cloud Security Scanner, the asset discovery feature automatically discovers your Alibaba Cloud assets and newly added assets, and associates them with Cloud Security Scanner. The discovered assets are listed on the **To be Confirmed** page.
- You must confirm and group the discovered assets on the **To be Confirmed** page as soon as possible, and create and start scan tasks for them to avoid financial or data loss.

- **Task Overview**: displays the total number of scan tasks that you have created, and the numbers of two different types of scheduled tasks: one-time and periodic tasks.



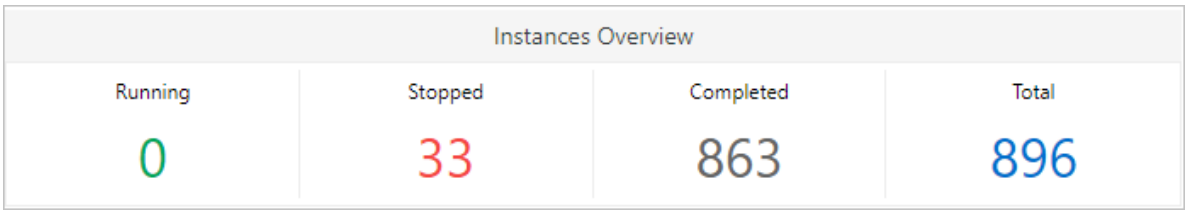
Click a number under **One-time Tasks**, **Periodic Tasks**, or **Total Tasks** to go to the Scan Tasks page to manage scan tasks.

- **Scan Targets**: displays the numbers of grouped and ungrouped assets.



  Click a number under **Tagged** or **Not Tagged** to go to the **Scan Targets** page. You can view assets grouped by tags on the **All Assets** page, or ungrouped assets on the **Not Tagged** page.

- **Instance Overview**: displays the total number of task instances and the numbers of instances in different states, including **Running**, **Stopped**, and **Completed**.



  Click a number under **Running**, **Stopped**, **Completed**, or **Total Instances** to go to the **Task Instances** page to view the instance information. For more information, see Manage task instances.

- **Product Updates**: displays product updates, including new features and vulnerability detection plug-ins.

  Click an item to view the information summary and feature description.

Related topics

#unique_7

2 Scan targets

2.1 Add assets

After you activate Cloud Security Scanner, you need to add the IP addresses or domain names of your Internet assets to the scan target list. Cloud Security Scanner automatically associates with Alibaba Cloud assets. You need to manually add assets that are not provided by Alibaba Cloud.

Prerequisites

You have activated Cloud Security Scanner. For more information, see #unique_10.

Procedure

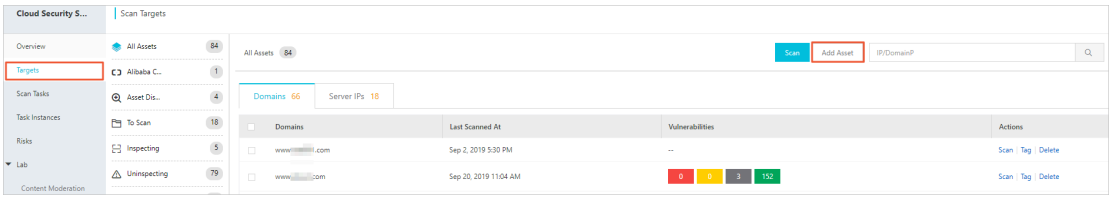
1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Scan Targets**.
3. Depending on whether your assets are provided by Alibaba Cloud, select a method to add assets. Assets can be manually or automatically added to Cloud Security Scanner.
   - **Add assets automatically**
     - In the dialog box that confirms whether you want to add assets automatically, click **OK**. Information about Elastic Compute Service (ECS), Server Load Balancer (SLB), and Elastic IP Address assets is synchronized with Cloud Security Scanner.
     - If you click **Cancel** in this step, you can change the **Asset Import Settings** on the **Settings** page.

        **Note:**

However, if you select the **I agree to have Cloud Security Scanner associate with the Elastic Compute Service, Server Load Balancer, and Elastic IP Address asset information under this UID.** check box, you cannot change the settings.

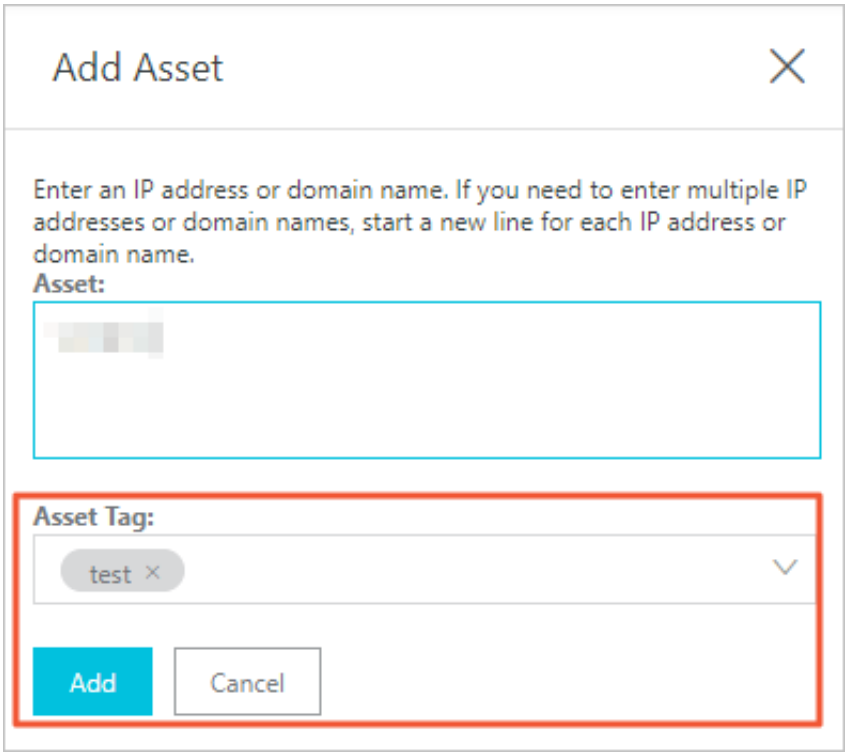
- **Add assets manually**

  a. On the **Scan Targets** page, click **Add Asset**.



  b. On the **Add Asset** page that appears, set the following parameters.

  - **Asset**: Enter the IP address or domain name that you want to add. You can enter multiple assets. Separate the assets with a line break.
  - **Asset Tag**: Select an existing tag from the drop-down list, or enter a new tag and press Enter.

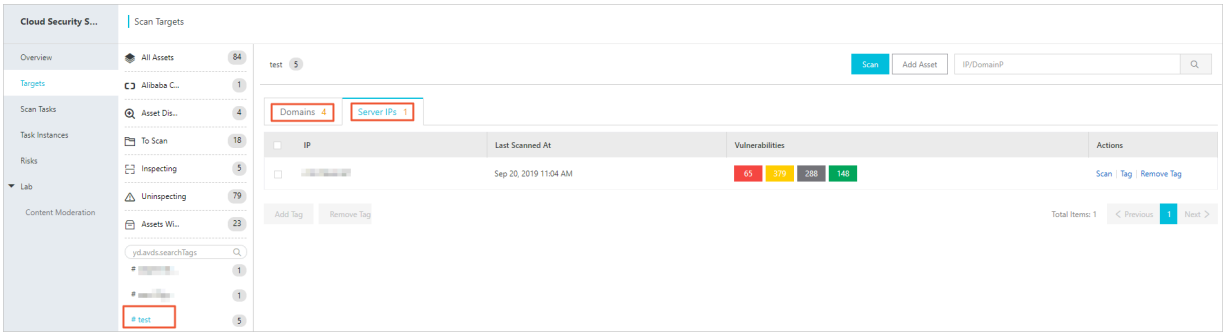


  c. Click **Add**.

Result

Assets that you have added are listed on the **Targets** page.

You can click the **Domains** or **Server IPs** tab to view domain names and IP addresses that you have added. You can also find a specific asset by specifying its tag.



What's next

Create scan tasks.

2.2 Manage assets

This topic describes how to manage assets that you have added to Cloud Security Scanner, for example, add tags, remove tags, or delete assets.

Prerequisites

You have added assets to Cloud Security Scanner. For more information, see Add assets.

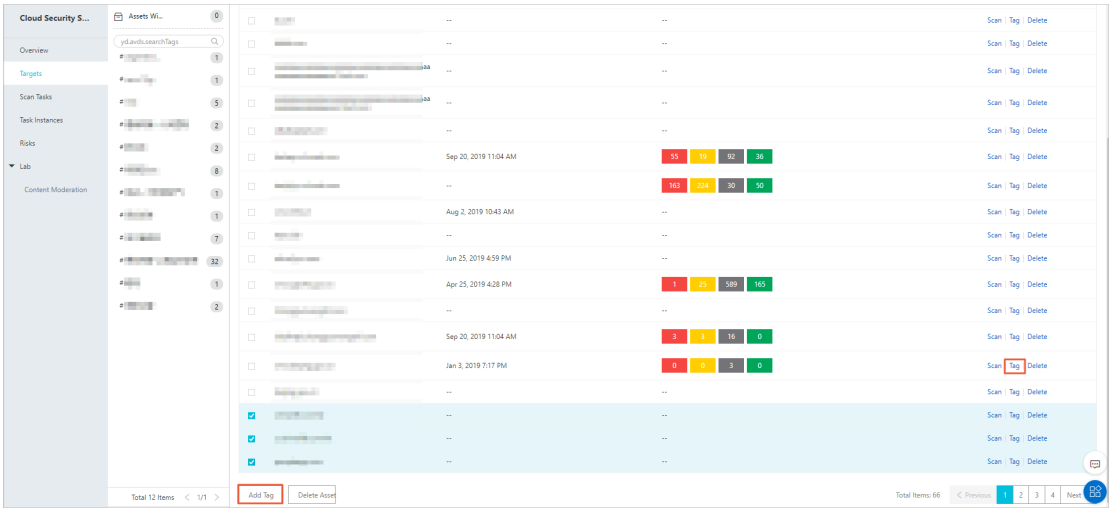
Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-navigation pane, click **Targets**.

3. On the **All Assets** page, find the target assets, and perform the following operations as needed.

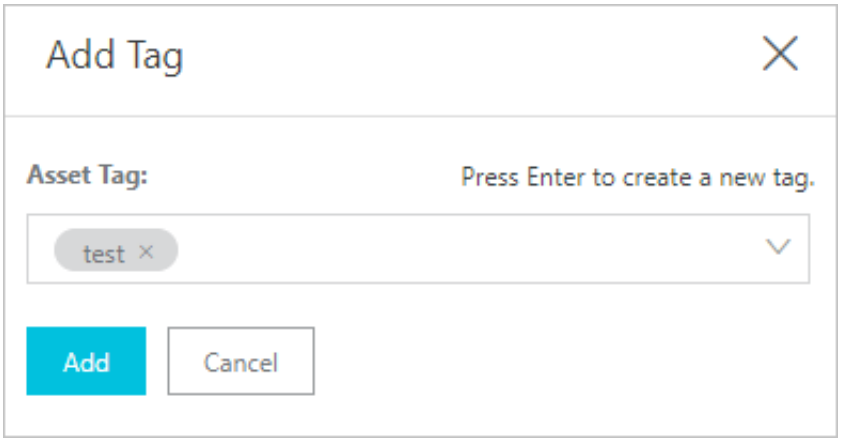
   - **Manage tags**

     a. Find the target asset and click **Tag** in the Actions column. You can also select multiple assets and click **Add Tag** in the lower-left corner to add a tag to multiple assets at the same time.

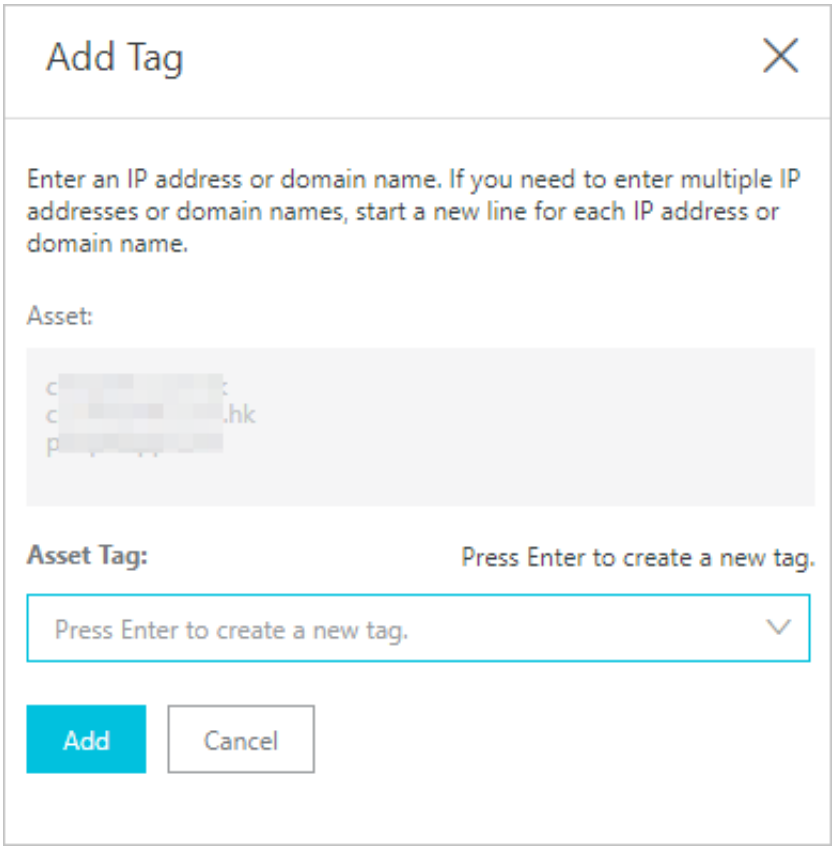


     b. On the **Add Tag** page that appears, add or remove the **Asset Tag**.

Manage individual tags



Manage multiple tags



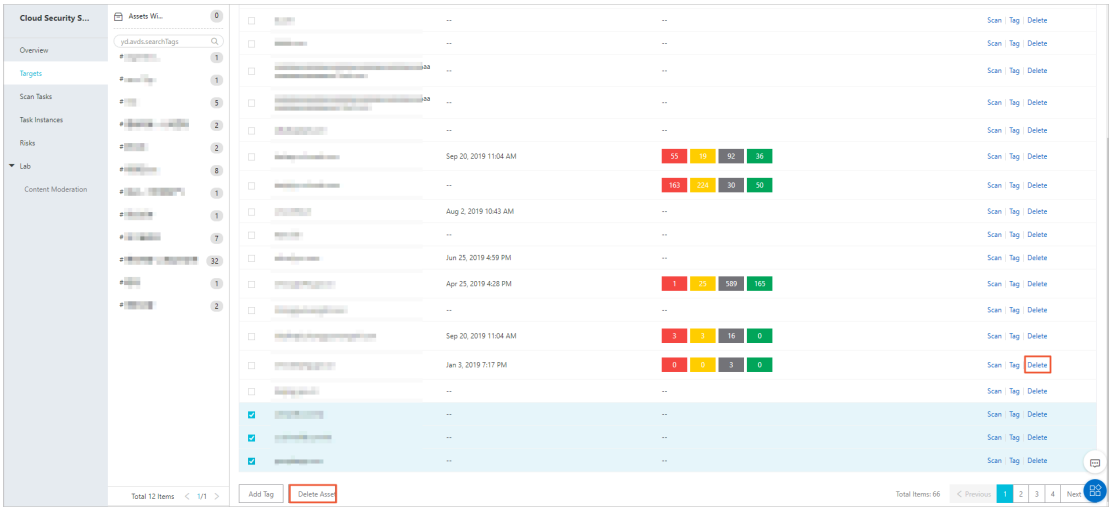
c. Click **Add**.

Note:

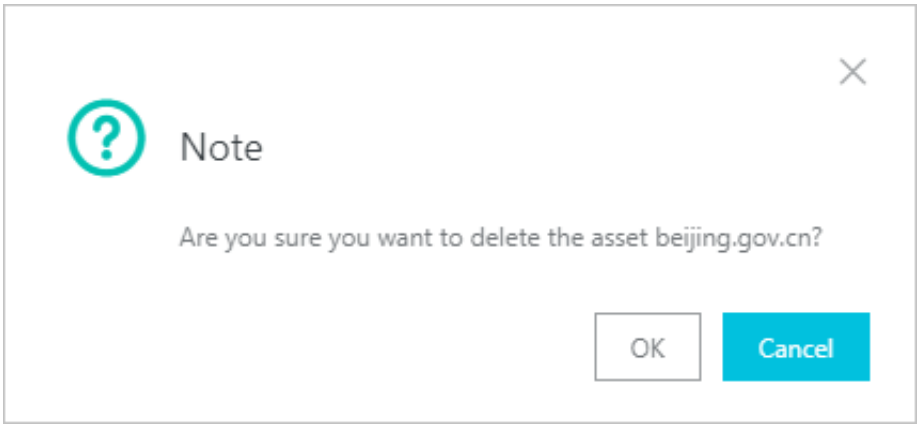
For more information about how to remove tags, see the **Remove tags from assets** and **Delete tags** sections in the Tags topic.

- **Delete assets**

  a. To delete an asset, click **Delete** in the Actions column.



  b. In the **Note** dialog box that appears, click **OK**.



Note:
You can also select multiple assets and click **Delete Asset** in the lower-left corner to delete multiple assets at the same time. This operation directly deletes all selected assets without any prompts. Proceed with caution.

2.3 Search for assets

This topic describes how to search for a specific domain or IP asset.

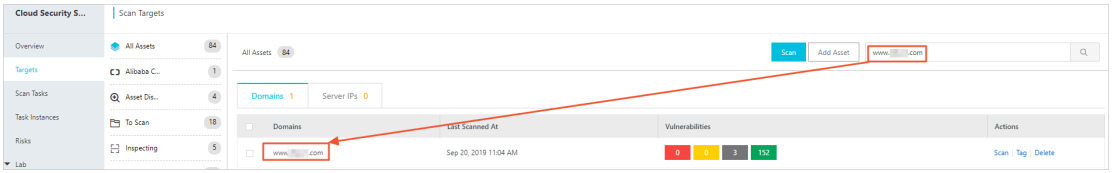
Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Scan Targets**.

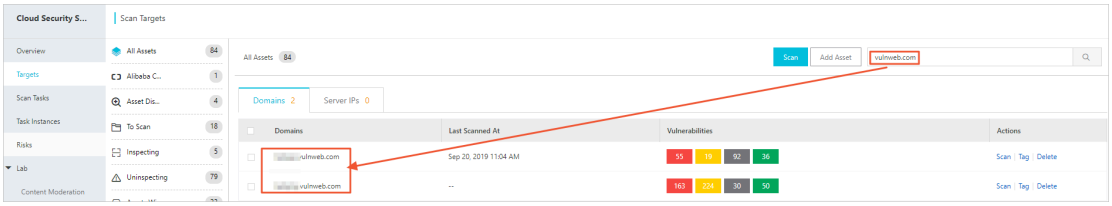
3. The following steps show how to search for a specific asset.

   - **Search by domain name**: You can specify a **specific domain name** or **root domain**.

     - Search for a **specific domain name**: Enter the full domain name into the search box and click the search icon. The domain asset information is displayed.

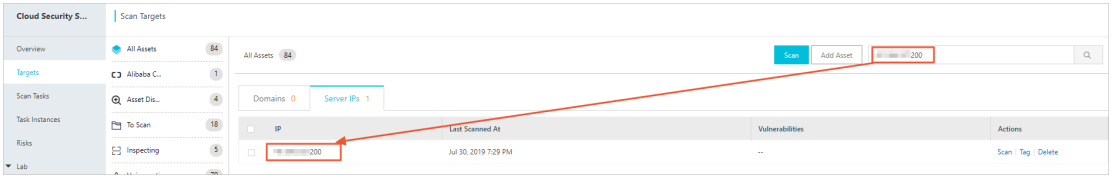


     - Search by **root domain**: Enter the root domain into the search box and click the search icon. All the domains that use the root domain are displayed.

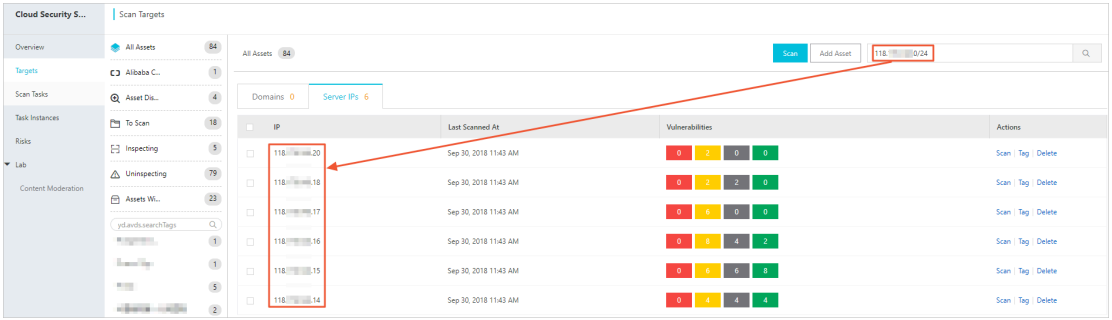


   - **Search by IP address**: You can specify a **specific IP address** or **CIDR block**.

     - Search for a **specific IP address**: Enter the full IP address into the search box and click the search icon. The IP asset information is displayed.



     - Search by **CIDR block**: Enter a CIDR block into the search box and click the search icon. The IP assets attached to the CIDR block are displayed.



2.4 Asset discovery

This topic describes how to confirm and delete associated assets that are discovered by Cloud Security Scanner.

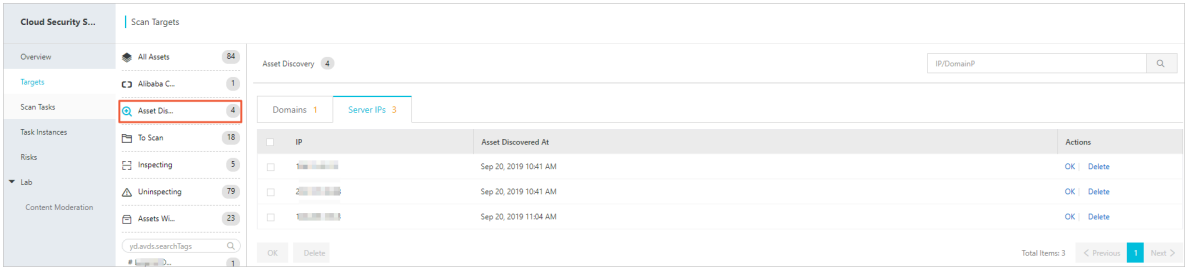
Context

When you enable Cloud Security Scanner for an asset, Cloud Security Scanner automatically starts an asset discovery task. Based on the assets that are manually and automatically associated with Cloud Security Scanner, the task uses an asset discovery model to periodically scan for assets that are associated with Cloud Security Scanner, and synchronizes the asset information to the **Scan Targets** > **Asset Discovery** page.

Note:
Currently, the asset discovery task runs once every seven days.

Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, choose **Scan Targets** > **Asset Discovery** to view assets that are associated with Cloud Security Scanner by asset discovery.

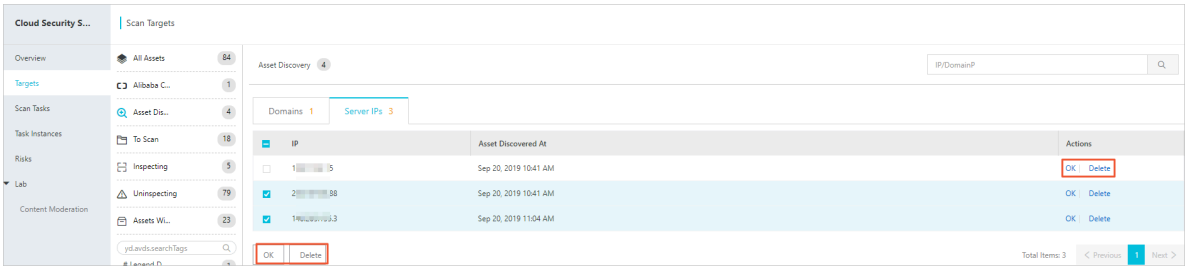


3. On the **Asset Discovery** page, you can **Confirm** or **Delete** the associated assets.
   - **OK**: Add discovered assets to the **Assets Without Tags** page.

Note:

You can delete assets that you do not need on the **Assets Without Tags** page.

- **Delete**: Remove discovered assets from the Asset Discovery page.



2.5 Tags

This topic describes how to use tags to group your assets.

Context

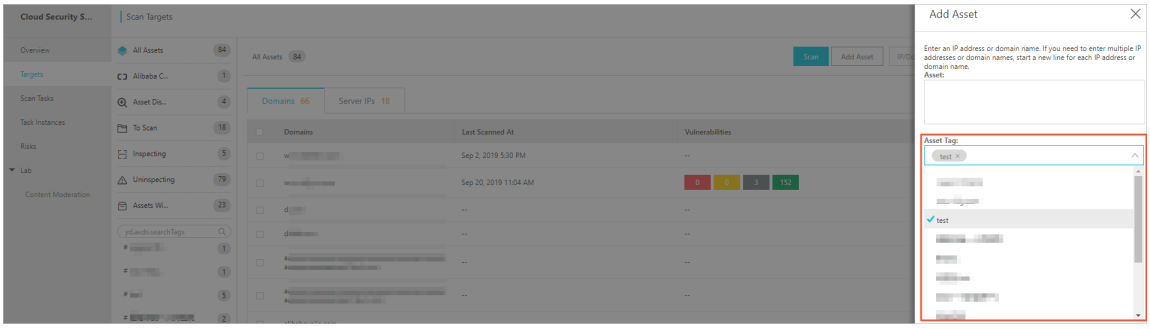
Cloud Security Scanner allows you to use tags to group your assets. You can add one tag to multiple assets or label an asset with multiple tags. This helps you detect risks in different types of assets and manage your assets properly.

Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Scan Targets**.

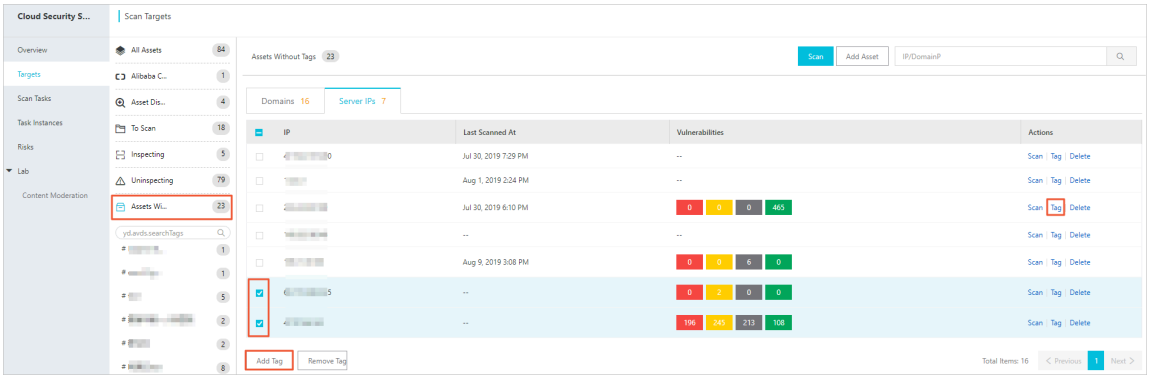
3. Perform the following steps to manage asset tags.

   - **Add tags to newly added assets**: On the **Scan Targets** page, choose **All Assets** > **Add Asset**. The **Add Asset** page appears. You can add tags to the asset on this page.



   - **Add tags to existing assets without tags**: On the **Scan Targets** page, click **Assets Without Tags** to go to the **Assets Without Tags** page. You can add tags to one or more assets on this page.

     After you add a tag to an asset, the asset is moved from the **Assets Without Tags** list to the list with the specified tag.

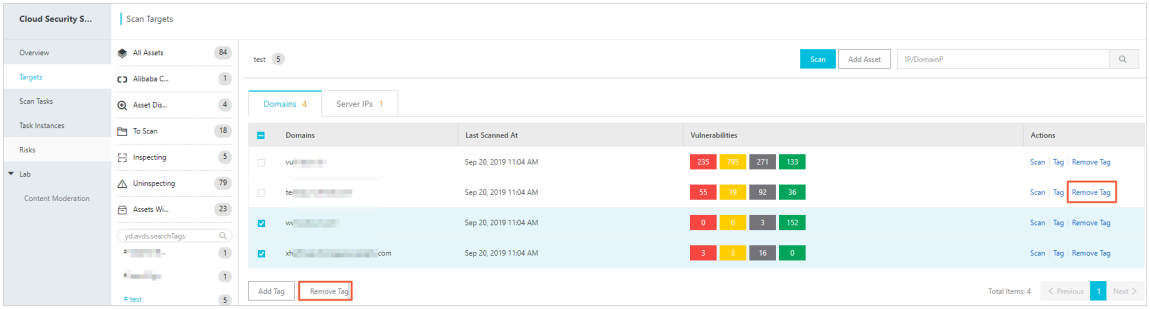


   - **Remove tags from assets**: On the **Scan Targets** page, click the target tag in the **tag list**. Find the target asset in the group and click **Remove Tag** in the Actions column to remove the tag. You can then add another tag to the asset.

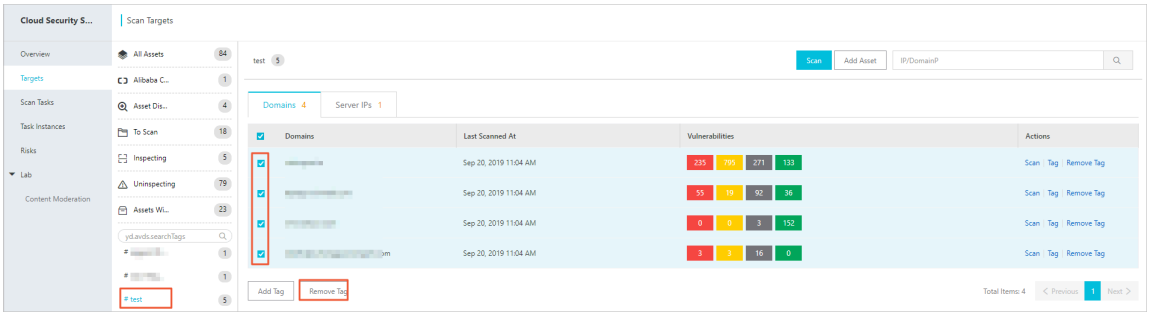
     You can also select multiple assets under the same tag and click **Remove Tag** in the lower-left corner to remove the tag from these assets.

Note:

After the tag is removed, the assets are removed from the group. If you remove the tag from all the assets in the group, the tag is deleted.



- **Delete tags**: On the **Scan Targets** page, click the target tag in the **tag list**, select all the assets, and then click **Remove Tag** in the lower-left corner to remove the tag from all the assets. After the tag is removed from all the assets, the tag is deleted.

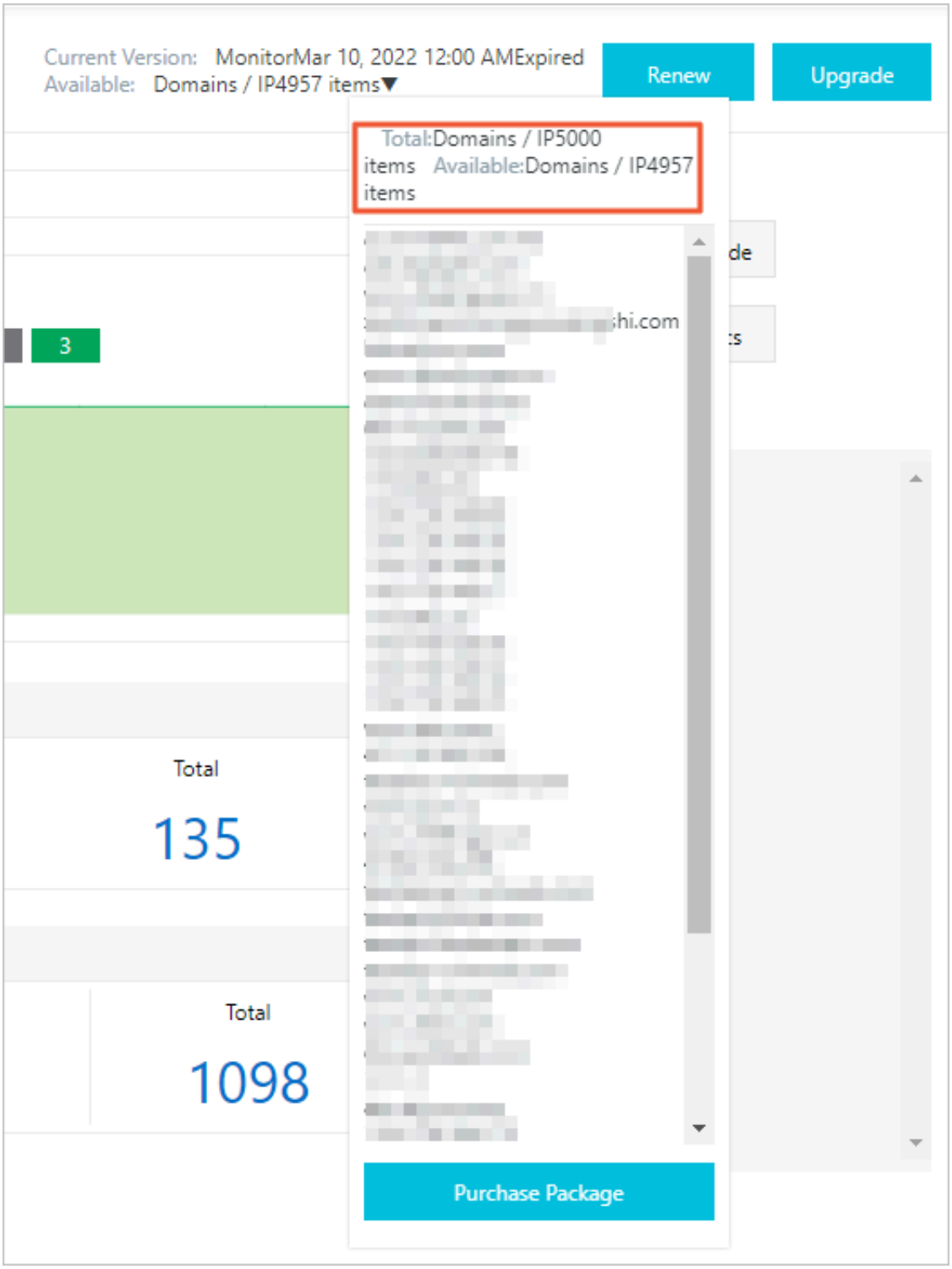


3 Scan tasks

3.1 Limits

Before you create a scan task in Cloud Security Scanner, check your **Available Quotas** and arrange the quotas properly.

On the **Overview** page, click the **Available Quotas** drop-down list icon in the upper-right corner to view your **Available Quotas** and **All Quotas**.



Note:

When your available quota drops to zero, you cannot run any scan tasks. Click **More Quotas** to purchase quotas. For more information, see #unique_7.

3.2 Create scan tasks

After you add your website assets to Cloud Security Scanner as scan targets, you can create scan tasks to scan for vulnerabilities and risks in your assets.

Prerequisites

You have added your assets to Cloud Security Scanner. For more information, see Add assets.

Context

When you create a scan task, you can use the following methods to specify target assets:

- Scan one or multiple assets.
- Scan assets specified by one or multiple tags.

When you create a scan task that scans multiple assets, we recommend that you use tags. Add the same tag to all the target assets, and then select the tag when you specify these assets for the scan task. For more information about how to set multiple tags at the same time, see Manage assets.

Note:
Before you create a scan task, check your **Available Quotas** and arrange your quotas properly. For more information, see Limits.

When you create a scan task, you can set the task as a one-time task, scheduled task, or periodic task.

Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Scan Targets**.
3. Add scan targets. Select assets based on your actual needs.
   - **Scan one or multiple assets**: In the asset list, select the target assets, and click **Scan** in the Actions column of any selected asset. A **Create Scan Task** page appears.
   - **Scan all assets in a specified group**: Click **Scan** in the upper-right corner of the asset list. The **Create Scan Task** page appears. Under **Scan Tasks**, select an existing tag.
4. On the **Create Scan Task** page, set the following parameters:

Parameter	Description
Task Name	Specify a name for the scan task.

Parameter	Description
Scan Targets	Specify the assets that you want to scan. You can select one or more tags in the drop-down list.
Effective Period	Specify the time period during which the scan task is allowed to scan the specified assets. The scan task scans assets only during the specified time period.  **Note:** We recommend that you set the effective period to off-peak hours.
Scan Type	Select a scan task type. You can set the task to one of the following types: • **Immediately**: After the scan task is created, it runs in the next **Effective Period**. • **Scheduled Task**: After the scan task is created, it is started at the specified **Start Time**, and scans the assets during the **Effective Period**. • **Periodic Task**: After the scan task is started at the specified **Start Time**, it scans the assets at the specified frequency (daily, weekly, or monthly) during the **Effective Period**.
Start time	When you set the **Scan Type** to **Scheduled Task** or **Periodic Task**, you must specify the start time of the scan task. The scan task is started at the specified start time, and scans the specified assets during the **Effective Period**.
Scan Frequency	When you set the **Scan Type** to **Periodic Task**, you must specify the scan frequency for the task. Valid values: • **Daily** • **Weekly** • **Monthly** After the scan task is started, it scans assets at the specified frequency.

5. Click **Create**.

Result

Scan tasks that you have created are listed on the **Scan Tasks** page.

What's next

Manage scan tasks.

3.3 Manage scan tasks

This topic describes how to manage scan tasks and periodic tasks.

Prerequisites

You have created scan tasks. For more information, see Create scan tasks.

Manage scan tasks and periodic tasks

Perform the following steps to manage scan tasks and periodic tasks.

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Scan Tasks** and perform the following operations as needed.
   - **View and search for tasks**
     - **View tasks**
     - **Search for tasks**

       Enter an **IP/Domain/Task Name** into the search box and click the search icon to search for a specific task. Tasks in the same type are listed on the current page according to their creation time.
   - **Filter tasks**

     Currently, Cloud Security Scanner allows you to filter tasks by task type. You can select a task type to filter tasks. Task types include **One-time Task** and **Periodic Task**. By default, **All** tasks are listed on the Scan Tasks page according to their creation time.
     - Select **One-time Task**. Tasks that are set to **Immediately** and **Scheduled Task** are filtered out.
     - Select **Periodic Task**. Tasks that are set to **Daily**, **Weekly**, and **Monthly** are filtered out.
   - **Edit and delete tasks**
     - **Edit a task**

       a. Find the target task and click **Edit** in the Actions column.

       b. On the **Edit Scan Task** page that appears, change the parameters.

       You can change the following parameters: **Task Name**, **Effective Period**, **Start Time**, and **Scan Frequency**. You can set Start Time to **Immediately** or **Scheduled**

Task, and set Scan Frequency to **Daily**, **Weekly**, or **Monthly**. You cannot change the **Scan Type** after the task is created.

c. Click **OK**.

- **Delete a task**

  Find the target task and click **Delete** in the Actions column. To delete multiple tasks at the same time, select the target tasks and click Delete in the lower-left corner.

- **View task instances**
  - On the **Task Instances** page, click an instance in the **Task Name/Scan Target** column to view the task instances. Task instance statuses include **Running, Completed, Stopped, and All**.
  - You can filter task instances by status. You can select **Waiting**, **Running**, **Paused**, **Completed**, and **Stopped**.
- **Enable and disable periodic tasks**

  You can **Enable** and **Disable** a periodic task in the **Status** column. Cloud Security Scanner determines whether to run the task and create task instances according to the task status.

3.4 Manage task instances

This topic describes how to manage task instances, vulnerabilities, and risks after you create a scan task.

Prerequisites

You have created a scan task. For more information, see Create scan tasks.

Procedure

1. Log on to the Cloud Security Scanner console.

2. In the left-side navigation pane, click **Task Instances** and perform the following operations as needed.

   - **View, search for, and filter task instances**

     - Task instances created by scan tasks and the relevant information are displayed on the **Task Instances** page.

       The numbers of vulnerabilities at different risk levels are displayed in the **Vulnerabilities** column. The following table lists the risk levels and descriptions.

Level	Description
High	Vulnerabilities that can be exploited directly and easily. Attacks that can cause severe impact on your websites or servers, or cause major financial and data loss.
Medium	Vulnerabilities that can affect your websites or servers, but are difficult to be directly exploited. Attacks that cannot be directly launched against your websites or servers, but can cause vulnerabilities for further attacks.
Low	Attacks that cannot be directly launched against your websites or servers, but can provide information for other attackers to find vulnerabilities.
Information	Vulnerabilities that do not directly cause website security issues, but may provide information for other attacks, or can be used in other attack methods, such as social applications.

     - You can enter an **IP/Domain/Task Name** into the search box to search for a specific task instance. Task instances are listed on the Tasks Instances page according to their start time.
     - You can also select a status from the status drop-down list to filter instances based on their status. Instance statuses include: **Waiting**, **Running**, **Stopped**, **Completed**,

and **Paused**. You can select a status and enter an **IP/Domain/Task Name** into the search box to search for instances.

- **View task instance details**

  a. On the **Task Instances** page, click the target instance in the **Instance Name/Scan Target** column to go to the Instance Details page.

  b. Instance details and scan results are listed on the **Instance Details** page.

  - **Instance Overview**: Displays the overall information about the instance, task status, and risk statistics.
  - **Attack Surfaces**: Displays the attack surfaces detected by the task instance, including domains, subdomains, ports, and Web applications.
  - **Risk Overview**: Displays the statistics of risks detected by the task instance.

- **View and export attack surface details**

  Attack surfaces are listed in the **Attack Surfaces** area on the Instance Details page. Attack surfaces include: **Domains**, **Subdomains**, **DNS Records**, **Hosts**, **Ports**, **Web Applications**, **Web Servers**, **Web Paths**, and **Crawler Requests**.

  To view attack surface details, click **Details** next to the attack surface.

  - Attack surface details - **domains**
  - Attack surface details - **subdomains**
  - Attack surface details - **ports**

    You can view the services provided through the ports of a host.
  - Attack surface details - **Web applications**

    You can view the information about the Web applications of a website, such as the content management system (CMS) and the framework.
  - **Other attack surfaces**

    You can view details of other attack surfaces as described in the proceeding examples.
  - **Export attack surface details**

    You can export attack surface details in the CVS format.

    a. Go to the details page of the target attack surface, and click **Export** in the upper-right corner. Export becomes **Exporting**

b. Refresh the current page and check the export status. After the export process is complete, Exporting becomes **Download**. Click **Download** to download the data.

Data is exported in the CSV format, as shown in the following figure. You can import the data to your data system for analysis.

- **View assets with risks**
  - Assets with risks are listed in the Risk Overview area on the **Instance Details** page. You can click an asset to go to the details page.

    The Risk Overview area lists the **domains and IP addresses** that are at risk. Assets are fully scanned for risks. You can view the vulnerability details to manage risks more accurately.
  - In the left-side list, click an **IP address** to go to the **Host Risk Details** page to view the risk details.

    The IP address and the attack surface details, including Web paths, ports, crawler requests, and Web applications are listed on the **Host Risk Details** page.
  - In the left-side list, click a **domain** to go to the **Domain Risk Details** page to view the risk details.

    The domain and attack surface details, including Web paths, Web servers, crawler requests, and Web applications are listed on the **Domain Risk Details** page.
- **View vulnerability details**

  You can redirect to the vulnerability details page from the **Instance Details** page or the **Host/Domain Risk Details** page and then manage the vulnerability.
  - **Redirect from the Instance Details page**

    a. On the **Instance Details** page, find the **Risk Overview** area, and click a **vulnerability name** to go to the details page.

    b. The details of the vulnerability, including the affected targets, status, and processing result are displayed on the **Vulnerability Details** page.

    c. You can click the left-side plus sign (+) to show the **Proof of Concept**. You can then verify and reproduce the vulnerability.
  - Redirect from the **Host/Domain Risk Details** page: Similar to redirecting from the Instance Details page, click a **vulnerability name** to view the details.

The details of the vulnerability, including the affected targets, status, and processing result are displayed on the details page.

- **View check items**

  a. On the **Instance Details** page, choose **Instance Overview** > **Instance Information** > **Checked Items** to go to the Check Results page. You can view details of the check items.

  b. All check items covered by the task instance are listed on the **Check Results** page. You can view the status of **check items** that you consider important, such as Redis, Hadoop, and MongoDB middleware.

- **View risk assessment reports**

  You can generate and download risk assessment reports to a local device for further analysis.

  a. On the **Task Instances** page, click **Generate** in the **Report** column to generate a risk assessment report.

  b. After the report is generated, click **Download**.

  c. Decompress the downloaded ZIP file and open the index.html file to view the report.

4 Content Moderation

Cloud Security Scanner allows you to create scan tasks for detecting content risks. This helps you detect risks in your website content, such as spams and website defacement. This topic describes how to create content scan tasks and query scan results.

Context

Content scan tasks can scan text and images that contain adult content, terrorism, advertisements, illicit content, profanity, and spams.

Create a content scan task

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, choose **Laboratory** > **Content Moderation**.
3. On the **Content Moderation** page, click **Create**.
4. On the **Create Task** page that appears, set the following parameters and click **OK**.

Parameter	Description
Task Name	Specify a name for the task.
Website URL	Enter the URL of the target website. **Note:** You can enter one website URL only.
Library	Select libraries used by the task. **Note:** After you specify libraries, the task also scans for content that contains keywords in the libraries and sends alerts to you when a risk is detected. For more information, see Manage libraries. If you do not specify a library, the system scans for risks based on the built-in libraries and sends you alerts when a risk is detected.
Full-site Scan Frequency	Select a frequency for the task to scan the entire website. Valid values: • Once a Day • Once Every 7 Days

Parameter	Description
Homepage Scan Frequency	Select a frequency for the task to scan the homepage. Valid values: • Every 5 Minutes • Every 30 Minutes • Every 60 Minutes

The content scan task is created. Tasks are automatically started.

View scan tasks

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, choose **Laboratory** > **Content Moderation**.
3. On the **Content Moderation** page, you can perform the following operations on the tasks:
   - Filter tasks by status.
   - You can search for specific tasks by task name or website URL.
   - To pause running tasks, select the target tasks and click **Pause**.
   - To resume tasks, select the target tasks and click **Continue**.
   - To edit a task, find the target task, click **Edit** in the Actions column, and edit the task on the **Edit Task** page that appears.
   - To delete a task, find the target task, click **Delete** in the Actions column, and then click **OK** in the **Delete Task** dialog box that appears.

View tasks

After a can task is completed, you can view the scan result. If risks are detected, you can check and manage the risks.

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, choose **Laboratory** > **Content Moderation**.
3. On the **Content Moderation** page, find the task that sent you the alert and click the alert in the **Risks** column.
   You are redirected to the **Risks** page. All risks detected by the task are listed on the **Risks** page.

4. On the **Risks** page, perform the following operations as needed.
   - Filter risks by status.
   - To manage a **Pending** risk, click the following actions in the Actions column. Supported actions are as follows:
     - **Mark as Processed**: You can perform this operation to set the **Risk Status** to **Processed**. This status indicates that the risk has been processed.
     - **Add to Whitelist**: You can perform this operation to set the **Risk Status** to **Whitelist**. This status indicates that you are aware of the risk and do not want it to be detected by Cloud Security Scanner again.
     - **False Positive**: If a risk is a false positive, you can set its status to **False Positive**.
   - To view risk details, find the target risk, click the link in the **Risk Type** column to go to the **Risk Details** page. You can view and manage the risk on this page.

Manage libraries

You can select libraries when you create or edit a content scan task. The task scans for content that contains keywords in the specified libraries and sends alerts to you when a risk is detected. You can create custom libraries and define the keywords based on your business requirements. The created libraries are available when you create scan tasks.

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, choose **Laboratory** > **Content Moderation**.
3. On the **Content Moderation** page, click **Manage Library**.
4. On the **Mange Library** page, perform the following operations as needed.
   - Create a library
     a. Click **Create Library**.
     b. On the **Create Library** page that appears, specify the **Library Name** and **Content**.

Note:

Separate keywords with commas (,).

c. Click **Create**.

The library is created.

- To edit a library, find the target library and click **Edit** in the Actions column. On the **Edit Library** page that appears, you can change the **Library Name** and **Content**.
- To delete a library, find the target library and click **Delete** in the Actions column. In the **Note** dialog box that appears, click **OK**.

5 Attack surfaces

5.1 Overview

The attack surfaces feature allows you to query and manage different types of attack surface data based on domain names, ports, hosts, and web applications. Thereby improving the management efficiency.

The attack surfaces feature allows you to query the following information of attack surfaces :

- Domain names
- Subdomains
- Hosts
- DNS records
- Ports
- Web applications
- Web paths

5.2 Query details of attack surfaces

The attack surfaces function provides a set of query syntax for you to set query conditions, helping you query details of attack surfaces.

Check the overview of attack surfaces

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Overview**.
3. On the **Overview** page, find the **Attack Surfaces** section to check the attack surface overview of your assets.

Query details of attack surfaces

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, choose **Laboratory** > **Attack Surfaces**.

3. On the **Attack Surfaces** page, click the tab corresponding to the data that you want to query.

   The attack surfaces feature allows you to query the following information of attack surfaces:

   - Domain names
   - Subdomains
   - Hosts
   - DNS records
   - Ports
   - Web applications
   - Web paths

4. On the tab that appears, check details of the attack surface, including Updated At and Actions detected by Cloud Security Scanner.

   You can query the details of attack surfaces by using one of the following methods:

   - **Fuzzy query**

     On the tab corresponding to a data source, enter a keyword in the search box. Then, Cloud Security Scanner performs a fuzzy search for the fields of the data source and displays query results.

     For example, on the **Subdomains** tab, if you enter aliyun or aliyun.com in the search box, subdomain and root domain of aliyun.com, as well as an overview of scanning performed for the subdomain, are displayed.

   - **Field-based query**

     On the tab corresponding to a data source, enter a field in the format of <Filed>:<Query content> in the search box to search for required information.

      **Note:**

DO NOT TRANSLATE For information of other query statements and examples, see Field query operators and Query fields and examples.

For example, on the **Ports** tab, if you enter ip:1.2.3.4 in the search box, the service port enabled on the server whose IP address is 1.2.3.4 is displayed.

Click **Save As Tags**. In the **Save As Tags** dialog box that appears, enter a tag name and save it as an asset tag. Then, you can select this tag as **Scan Target** when you Create scan tasks.

5.3 Field query operators

The attack surfaces feature provides a set of query syntax for you to query information. This topic describes the operators that may be used in field query in the attack surfaces feature.

Supported operators

Operator	Description	Remarks
AND	Indicates the "and" relationship. The query result must meet both query1 and query2. Format: query1 AND query2.	If no operator is used between multiple query conditions, the relationship is AND by default.
OR	Indicates the "or" relationship. The query result must meet either query1 or query2. Format:query1 OR query2.	N/A
NOT	Indicates the "not" relationship. The query result must not contain result that meets query1. Format:NOT query1. You can use this operator together with AND and OR.	N/A

Operator	Description	Remarks
""	Indicates exact match. The query result must exactly match query1. Format:<field>:"query1".	N/A
>	Queries the results that are greater than a specific number. Currently, this operator is supported only for port query in port service. For example, port > 80 is to query the ports whose ports number are greater than 80.	N/A
>=	Queries the results that are greater than or equal to a specific number. Currently, this operator is supported only for port query in port service. For example, port >= 80 is to query the ports whose ports number are greater than or equal to 80.	N/A
<	Queries the results that are less than a specific number. Currently, this operator is supported only for port query in port service. For example, port < 8080 is to query the ports whose ports number are less than 8080.	N/A
<=	Queries the results that are less than or equal to a specific number. Currently, this operator is supported only for port query in port service. For example, port <= 8080 is to query the ports whose ports number are less than or equal to 8080.	N/A

5.4 Query fields and examples

This topic describes the fields and examples for querying data sources on the Attack Surfaces page of the Cloud Security Scanner console. These examples help you quickly query the attack surface information of different data sources.

> **Note:**
> For more information about how to query details of attack surfaces, see Query details of attack surfaces.

Domain query

On the **Attack Surfaces** page, click the **Domains** tab. In the search box, enter aliyun to search for domain names that contain aliyun.

Subdomain query

The following table describes the fields for subdomain query.

Field	Description	Example
domain	The root domain that you want to query.	domain:aliyun.com
subdomain	The subdomain that you want to query.	subdomain:aliyun.com or subdomain:"1.aliyun.com"

For example, on the **Attack Surfaces** page, click the **Subdomains** tab. In the search box, enter domain:aliyun.com (for querying a root domain) or subdomain:aliyun.com (for querying a subdomain) to search for the domain or subdomain information about aliyun.

Host query

The following table describes the fields for host query.

Field	Description	Example
ip	The IP address of the host that you want to query.	ip:1.2.3.4: queries the information of the host whose IP address is 1.2.3.4.
cidr	The CIDR block of the host that you want to query.	cidr:1.2.3.4/24: queries the information about the host whose IP address falls into the CIDR block of 1.2.3.4/24.

Field	Description	Example
hostname	The name of the host that you want to query.	hostname:guest: queries hosts whose names contain the guest field.
state	The status of the host that you want to query.	• state:up: queries hosts that are in the **Up** state. • state:down: queries hosts that are in the **Down** state.
os	The operating system of the host that you want to query.	os:windows: queries hosts that run Windows OS.

For example, on the **Attack Surfaces** page, click the **Hosts** tab. In the search box, enter cidr:192.168.1.1/24 os:linux state:up to search for the host that runs Linux OS, falls into the CIDR block of 192.168.1.1/24, and is in the up state.

DNS record query

The following table describes the fields for DNS record query.

Field	Description	Example
domain	The root domain of the DNS record that you want to query.	domain:aliyun.com: queries the DNS record whose domain is aliyun.com.
subdomain	The subdomain that you want to query.	subdomain:1.aliyun.com: queries the DNS record whose subdomain is 1.aliyun.com.
record	The DNS record that you want to query.	record:"1.2.3.4": queries DNS records that contain 1.2.3.4.
type	The type of DNS records that you want to query.	• type:a: queries DNS records whose types are a. • type:cname: queries DNS records whose types are cname.

For example, on the **Attack Surfaces** page, click the **DNS Records** tab. In the search box, enter domain:aliyun.com type:a to search for the DNS records whose domain names are aliyun.com and types are **a**.

Port query

The following table describes the fields for port query.

Field	Description	Example
ip	The IP address of the host that you want to query.	ip:1.2.3.4: queries the host whose IP address is 1.2.3.4.
cidr	The CIDR block of the host that you want to query.	cidr:1.2.3.4/24: queries hosts whose IP addresses fall into the CIDR block of 1.2.3.4/24.
port	The port that has been enabled for a host.	port:80: queries hosts that have port 80 enabled.
protocol	The protocol used at the port that you want to query. Valid values: TCP and UDP.	protocol:tcp: queries TCP ports.
service	The port service that you want to query. Valid values: HTTP, HTTPS, HTTP-PROXY, MS-WBT-Server, and SSH.	service:http: queries HTTP services.
product	The product of the port that you want to query. Products (applications or devices providing port services) such as Apache and Nginx are supported. You can check all supported products on the **Port Service** page.	product:apache: queries hosts that have the Apache service deployed.
version	The version number of the product that you want to query.	version:1.0.2: queries products whose versions number are 1.0.2.

For example, on the **Attack Surfaces** page, click the **Ports** tab. In the search box, enter port:80 product:nginx to search for Nginx hosts that have port 80 enabled, or enter cidr:1.2.3.4/24 service:http to search for HTTP services of hosts whose IP addresses fall into the CIDR block of 1.2.3.4/24.

Web application query

The following table describes the fields for web application query.

Field	Description	Example
domain	The domain name of the web application that you want to query.	domain:aliyun.com: queries web applications whose domain names are aliyun.com.
name	The name of the web application that you want to query.	name:wordpress: queries websites that use WordPress.
title	The title of the web application that you want to query.	title:console: queries websites whose names contain console.
server	The server type of the web application that you want to query.	server:apache: queries websites that use the Apache server.
version	The version number of the web application that you want to query.	version:1.2.0: queries websites whose application versions are 1.2.0.

For example, on the **Attack Surfaces** page, click the **Web Applications** tab. In the search box, enter domain:aliyun.com name:wordpress to search for websites whose domain names are aliyun.com and that use WordPress.

Web path query

The following table describes the fields for web path query.

Field	Description	Example
hostname	The domain name of the web path that you want to query.	hostname:aliyun.com: queries web paths in the aliyun.com domain.
netloc	The name of the web path that you want to query.	netloc:"aliyun.com": queries path information.

For example, on the **Attack Surfaces** page, click the **Web Paths** tab. In the search box, enter hostname:abc.com to search for web paths in the abc.com domain.

6 Risks

This topic describes how to check and process detected vulnerabilities and risks on the **Risks** page.

Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click **Risks**.
3. On the **Risks** page, you can check and manage **vulnerabilities** and **content risks**. Perform the following operations as needed.
   - **Check and search for vulnerabilities**

     In the **vulnerability list**, you can search for specific vulnerabilities by **Status** (**Processed**, **Pending**, **False Positive**, and **Whitelist**), **Risk Level** (**High**, **Medium**, **Low**, and **Information**), **Vulnerability Type**, **Domain or IP**, or the time that the vulnerability was **Detected At**.
   - **View vulnerability details**

     You can click a vulnerability in the **Vulnerability Name** column to view the details, including the **Vulnerability Description**, **Proof of Concept**, **Impact**, **Suggestions**, and **Technical Reference**.
   - **Manage vulnerabilities**

     The following table lists the operations that you can perform to manage vulnerabilities.

Operation	Description
Mark as Processed	After you verify and fix a vulnerability, you can perform this operation to set the status of the vulnerability to **Processed**.
Add to Whitelist	If you do not want a vulnerability to be detected by Cloud Security Scanner again, you can perform this operation to set the status of the vulnerability to **Whitelist**. The system will not scan for this vulnerability again.

Operation	Description
Mark as False Positive	After you confirm that the vulnerability does not exist, you can perform this operation to set the status of the vulnerability to **False Positive**.

- **Manage one vulnerability at a time**: In the **vulnerability list**, click an action in the **Actions** column, or on the **Vulnerability Details**.
- **Manage multiple vulnerabilities at the same time**: In the **vulnerabilities list**, select the target vulnerabilities and click an action in the lower-left corner.

- **Check and search for content risks**
  - On the **Risks** page, you can search for specific risks by **Status** (**Processed**, **Pending**, **False Positive**, and **Whitelist**), **Risk Level** (**High**, **Medium**, **Low**, and **Information**), **Domain or IP**, and the time that the risk was **Detected At**.
  - In the **risk list**, find the target risk and click the **Source Code Risk** icon or the **Text Risk** icon in the **Risk Name** column to view the source code and content in text format.
- **Manage content risks**

  The following table lists the operations that you can perform to manage detected risks.

Operation	Description
Mark as Processed	After you verify and process a risk, you can perform this operation to set the status of the risk to **Processed**.
Add to Whitelist	If you do not want a risk to be detected by Cloud Security Scanner again, you can perform this operation to set the status of the risk to **Whitelist**.
Mark as False Positive	After you confirm that the risk does not exist, you can perform this operation to set the status of the risk to **False Positive**.

  - **Manage one risk at a time**: In the **risk list**, click an action in the **Actions** column.
  - **Manage multiple risks at the same time**: In the **risk list**, select the target risks and click an action in the lower-left corner.