

Alibaba Cloud

Security Center Operation

Document Version: 20220613

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
 Danger	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.
 Warning	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.
 Notice	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.
 Note	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 <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.Create a security report ----- 05
- 2.Task management ----- 08
 - 2.1. Overview ----- 08
 - 2.2. Create a task ----- 09
 - 2.3. View the details of a task ----- 12
- 3.Use the container signature feature ----- 14
- 4.Use the multi-account control feature ----- 17

1. Create a security report

Security Center provides the security report feature. You can create security reports and specify the email addresses to which security reports are sent on a regular basis. This way, you can monitor the security status of your assets at the earliest opportunity. This topic describes how to create a security report.


Procedure


- 1.
- 2.
3. On the **Reports** page, click **Create Report**.

 **Notice** In addition to the existing default security report, you can create up to nine security reports.

4. On the **Add report** page, configure the parameters.

The following table describes the parameters.

Parameter	Description
Report Name	The name of the security report.
Report Type	<p>The type of the security report. Valid values:</p> <ul style="list-style-type: none">◦ Daily◦ Weekly◦ Monthly◦ Custom <p>If you set this parameter to Custom, you must set Data Collection Period to a time range in which the security statistics are collected for the report.</p>
Report Time	<p>The time range during which the security report is sent.</p> <p> Note The interval between the start time and the end time must be greater than or equal to 2 hours.</p>
Data Collection Period	The time range during which the security statistics are collected for the report. This parameter is required only if you set the Report Type parameter to Custom . You can set this parameter to a time range within last 30 days.
Language	The language of the content in the security report. Valid values: Simplified Chinese and English .

Parameter	Description
Recipient	<p>The email address that is used to receive the security report. If you want to enter multiple email addresses, press Enter after each input.</p> <div>  Note You must enter an email address that is verified. To verify an email address, perform the steps that are provided in the verification email. </div>

5. Click **Next** to go to the report details page.

6. In the left-side section of the report details page, select the items whose statistics you want to include in the security report.

The items include **Issue Resolved**, **Assets**, **Alerts**, **Vulnerabilities**, **Baseline check**, and **Attack**.

7. Click **Save**. The security report is created.


You can view the security report that you create on the **Reports** page. By default, a newly created report is enabled. Security Center sends the security report to the specified email addresses within the time range that you specified for the **Report Time** parameter.

What to do next


On the **Reports** page, you can perform the following operations based on your business requirements:

- **Immediately send a security report**

After you create a security report whose statistics are collected in a custom time range, you can click **Send Now**. Then, Security Center immediately sends the security report to the recipients that you specify.

 **Note** You cannot perform this operation on daily, weekly, and monthly security reports.


- **Stop sending a security report**

By default, a newly created report is enabled. Security Center sends the security report to the specified email addresses within the time range that you specified for the **Report Time** parameter. If you no longer require the security report, you can click the  icon below the report. The security report is no longer sent to the specified email addresses.

- **Modify, clone, or delete a security report**


You can modify, clone, or delete an existing security report.

- You can click **Edit** below a security report to modify the basic information and content of the security report.

 **Note** The **Report Type** parameter of the default security report is set to **Daily**. You cannot modify the **Report Type** parameter of the default security report.

- You can click **Clone** below a security report to clone the security report.

- You can click **Delete** below a security report to delete the security report. A deleted security report cannot be recovered. Proceed with caution.

 **Note** The default security report cannot be deleted.

- **Export a security report**

You can click **Export** below a security report to download the report. The report is saved as an HTML file.

2.Task management

2.1. Overview

Security Center provides automatic orchestration and response capabilities on the Playbook page. This allows you to orchestrate the logic of repetitive tasks in the response to security events into automatic processing policies and helps you reinforce the security of your system. After you create an automatic vulnerability fixing task, the task automatically runs on the assets that you select. This topic describes the operations that you can perform on the tabs such as Policy Center and Task Management.

Background information

You can create only automatic vulnerability fixing tasks on the Playbook page.

Operations on the Policy Center tab

The **Policy Center** tab displays the template policy named **Automatic batch vulnerability fixing policies** that is provided by Security Center. This template policy can be used to automatically fix vulnerabilities on multiple servers. To create policies by using this template policy, perform the following operations: In the Actions column, click **Clone**. A policy is created and is added to the **My Policy** tab.

Playbook				
<div>Policy Center My Policy Task Management</div>				
Policy Name	Policy Type	Mode	Creation/Last Update Time	Actions
Automatic batch vulnerability fixing policies Supports multiple hosts to automatically fix vulnerabilities in batches.	Vulnerability	Manual	Dec 23, 2019, 15:13:15 Jan 16, 2020, 13:58:06	Clone

Operations on the My Policy tab

The **My Policy** tab displays information about created policies. The information includes the names, types, modes, creation time, and last update time. On the tab, you can create tasks by using an existing policy. For more information, see [Create a task](#).

Playbook				
<div>Policy Center My Policy Task Management</div>				
Policy Name	Policy Type	Mode	Creation/Last Update Time	Actions
Automatic batch vulnerability fixing policies Supports multiple hosts to automatically fix vulnerabilities in batches.	Vulnerability	Manual	Jan 13, 2020, 15:01:21 Jan 13, 2020, 15:01:21	Create Delete
Automatic batch vulnerability fixing policies Supports multiple hosts to automatically fix vulnerabilities in batches.	Vulnerability	Manual	Jan 13, 2020, 14:29:56 Jan 13, 2020, 14:29:56	Create Delete

Operations on the Task Management tab



The **Task Management** tab displays the information about created tasks. The information includes the names, the number of times that the tasks have been executed, modes, creation time, end time, and task status. On the tab, you can view the details of the created tasks. For more information, see [View the details of a task](#).

Playbook

Policy Center

My Policy

Task Management

Task Name	Executed Num	Mode	Creation/Completion Time	Status	Actions
	1	Manual	Jan 19, 2020, 18:14:19 Jan 20, 2020, 18:15:02	Completed Total: 1; Success: 1; Failed: 0	Details
	1	Manual	Jan 10, 2020, 20:51:56 Jan 10, 2020, 20:51:56	Completed Total: 1; Success: 1; Failed: 0	Details

2.2. Create a task

You can quickly create an automatic vulnerability fixing task by using an existing policy on the My Policy tab of the Playbook page. After you create a task, the task automatically fixes the vulnerabilities that are detected on the selected servers from the specified start time. This helps you reinforce the security of your system. This topic describes how to create a task.

Prerequisites

-
- The policy that is used to create a task is added to the My Policy tab.

Context

The tasks that are created on the Playbook page can fix Linux software vulnerabilities, Windows system vulnerabilities, and Web-CMS vulnerabilities.

Procedure

- 1.
- 2.
- 3.
4. On the **My Policy** tab, find the required policy and click **Create** in the Actions column.
5. On the **Create** page, configure the following parameters.

← Create

How can I create tasks to automate risk handling? [view risks](#)

* Task Name:

Task01

Asset List

Asset Group

All Groups (513)

Default (166)

Assets 4 total 4

Search by asset name

☒

☒

☒

☒

☒

Select All

Linux software 166

Windows

Web-CMS

10 Items Selected

Enter the vulnerability name or CVE number.

<input checked="" type="checkbox"/> Vulnerability	Assets	Latest Scan Time
<input checked="" type="checkbox"/> RHSA-2019:2046-Moderate: polkit security and bug fix update		Mar 17, 2021, 07:01:36
<input checked="" type="checkbox"/> RHSA-2018:1200-Important: patch security update		Mar 16, 2021, 02:39:22
<input checked="" type="checkbox"/> RHSA-2018:3107-Moderate: wpa_supplicant security and bug fix update		Mar 17, 2021, 07:01:36
<input checked="" type="checkbox"/> RHSA-2018:1453-Critical: dhcp security update		Mar 16, 2021, 02:39:22
<input checked="" type="checkbox"/> RHSA-2019:2189-Moderate: procs-ng security and bug fix update		Mar 17, 2021, 07:01:41
<input checked="" type="checkbox"/> RHSA-2019:2060-Moderate: dhcp security and bug fix update		Mar 17, 2021, 07:01:36
<input checked="" type="checkbox"/> RHSA-2017:2450-Important: libvirt security update		Mar 16, 2021, 02:39:17

Total: 166 Items per Page 10 < Previous 1 2 3 4 ... 17 Next >

Notification

DingTalk robots

Email

Select DingTalk robot orAdd DingTalk Chatbot

☐

☐

☐

☐

☐

* Execution Time:

☒ Execute



☐ Custom Time

Create

Parameter	Description
Task Name	The name of the task.

10

> Document Version: 20220613

Parameter	Description
Asset List	<p>The assets on which you want to run the task. You can select an asset, asset groups, or multiple assets from asset groups. You can use one of the following methods to select the assets:</p> <ul style="list-style-type: none"> ◦ Select asset groups from the Asset Groups list. All assets in the selected groups are automatically selected. You can clear one or more selected assets in the Assets list on the right. ◦ Enter an asset name in the search box above the Assets list to search for specific assets. Fuzzy match is supported. Select the assets on which you want to run the automatic vulnerability fixing task from the search results. <p> Note The task runs only on the assets that you selected in the Assets list.</p>
Vulnerabilities on the Linux software, Windows, and Web-CMS tabs	<p>The vulnerabilities that are detected on the assets you selected. You can perform the following operations to select the vulnerabilities that you want to fix: Click the Linux software, Windows, or Web-CMS tab and select the vulnerabilities.</p> <p> Note You can select up to 200 vulnerabilities to fix.</p>
Notification	<p>The notification method. Valid values: DingTalk robots and Email. After the system runs the task, the system sends you notifications by using the notification method that you specify.</p> <ul style="list-style-type: none"> ◦ DingTalk robots: Select the DingTalk chatbots that are used to send notifications. You can also click Add DingTalk Chatbot to add a new DingTalk chatbot. For more information about how to add a DingTalk chatbot, see Add a DingTalk chatbot. ◦ Email: Enter the email addresses that are used to receive notifications. Separate multiple email addresses with commas (,).
Execution Time	<p>The time when the task automatically runs. Valid values:</p> <ul style="list-style-type: none"> ◦ Execute: After you create the task, the system immediately delivers the task to the Security Center agent. Then, the agent automatically runs the task. ◦ Custom Time: You must specify StartTime and EndTime to define a maintenance window. After you create the task, the system delivers the task to the Security Center agent and the agent automatically runs the task during the maintenance window. Vulnerabilities are fixed by using patches.

6. Click **Create**.

If you set **Execution Time** to **Execute**, the status of the task is **Progressing** after the task is created. If you set **Execution Time** to **Custom Time**, the status of the task is **Waiting** after the task is created.

Note You can cancel the tasks that are in the **Waiting** state on the Playbook page. To cancel a task, you must find the task and click **Cancel** in the Actions column.

Result

After you create a task, a **Created** message appears, and you are redirected to the **Task Management** tab.

What's next

After the task runs, you can view the task details on the **Task Management** tab. For more information about how to view task details, see [View task details](#).



2.3. View the details of a task

After you create a vulnerability fixing task, you can view the task details. The details include the servers on which the task runs and the notification settings.

Procedure

- 1.
- 2.
3. On the **Playbook** page, click the **Task Management** tab.
4. In the task list, find the required task and click **Details** in the Actions column.
5. On the task details page, view the details of the task on the **Asset List**, **Notification**, and **Others** tabs.

You can click the **Asset List**, **Notification**, or **Others** tab to view detailed information about the task. The following table describes the information displayed on each tab.

Tab	Description
Asset List	<p>Displays the following information about the task: Assets, Vulnerability Name, and Latest Scan Time.</p> 
Notification	<p>Displays the notification methods of the task. The methods include DingTalk Robots and Notification Email.</p> 

Tab	Description
Others	<p>Displays the Log and Policy Flow of the task.</p> <ul style="list-style-type: none"> ◦ Log: displays the task status, number of processes, numbers of failed and successful processes, and status of each step. ◦ Policy Flow: displays the flowchart of the task that fixes multiple vulnerabilities. <div data-bbox="552 495 1385 1234"> <div> Log <div> Status: Successful Total: 8; Success: 8; Failed: 0 </div> <ul style="list-style-type: none"> DescribeDisks 2020-01-06 19:36:01 filter_disk_error 2020-01-06 19:36:01 CreateSnapshot 2020-01-06 19:36:03 filter_snapshot 2020-01-06 19:36:03 vulFix 2020-01-06 19:36:04 wait10minute 2020-01-06 19:46:04 vulGroupBy 2020-01-06 19:46:04 checkFixResult 2020-01-06 19:46:04 outputResult 2020-01-06 19:46:04 notifyUser 2020-01-06 19:46:04 </div> <div> Policy Flow <pre> graph TD Start([Start]) --> CheckDiskSpace[Check Disk Space] CheckDiskSpace --> Filter[Filter out the abnormal hosts] Filter --> CreateSnapshot[Create Snapshot] CreateSnapshot --> CheckSnapshot[Check snapshot] CheckSnapshot --> StartFix[Start Fix] StartFix --> Fixing[Fixing] Fixing --> BatchVerification[Batch Verification] </pre> </div> </div>

3. Use the container signature feature

The container signature feature supports signing container images and verifying container image signatures. This feature ensures that only trusted container images are deployed and prevents unauthorized images from being started. This reinforces your asset security.

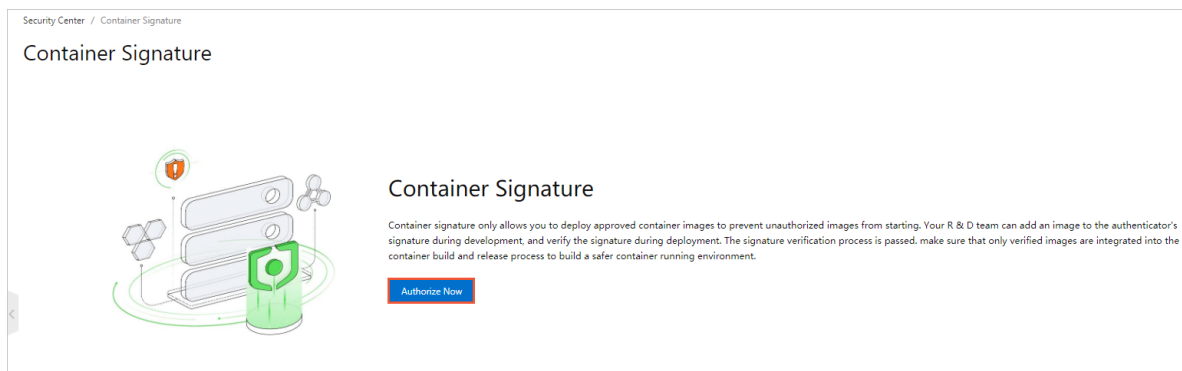
Prerequisites

You must complete the following operations before you can use the container signature feature:

- A customer master key (CMK) is created by using Key Management Service (KMS). The CMK is based on an asymmetric encryption algorithm.

Notice Only asymmetric key algorithms support the container signature feature. When you create a KMS CMK, set **Key Spec** to *RSA_2048* and **Purpose** to *Sign/Verify*. For more information about the key algorithms supported by KMS CMKs, see [Description of encryption algorithms supported by KMS](#).

- If this is the first time that you use the container signature feature, you must grant Security Center the required permissions to access relevant Alibaba Cloud services.



Procedure


- 1.
- 2.
3. (Optional) On the **Container Signature** page, click the **Witness** tab to create a witness.

If you have created a witness, skip this step and go to Step 4.

Otherwise, click **Create a witness** on the **Witness** tab. In the panel that appears, configure the parameters and click **OK**.

The following table describes the parameters.


Parameter	Description
-----------	-------------

Parameter	Description
Witness	Enter the name of the witness. When you configure a security policy, you must select a witness to enable the container signature feature for the required container. We recommend that you enter an informative name.
Select a certificate	<p>Select the KMS CMK that you created from the certificate list.</p> <div>  Note Only asymmetric key algorithms support the container signature feature. When you create a KMS CMK, set Key Spec to <i>RSA_2048</i> and Purpose to <i>Sign/Verify</i>. For more information about the key algorithms supported by KMS CMKs, see Description of encryption algorithms supported by KMS. </div>
Description	Enter the description of the witness.

4. Create a security policy.


On the **Security Policy** tab, click **Add Policy**. In the panel that appears, configure the parameters and click **OK**.

The following table describes the parameters.

Parameter	Description
Policy Name	<p>Enter the name of the security policy. When you configure a security policy, you must select a witness to enable the container feature for the required cluster.</p> <p>We recommend that you enter an informative name.</p>
Witness	<p>Select the witness that you created from the witness list.</p> <p>For more information about how to create a witness, see Step 3.</p>
Application Cluster	Select the cluster group for which you want to enable the container signature feature. Then, select the required Cluster Namespace .
Policy Enabled	<p>Turn on the switch. The policy is automatically enabled after it is created.</p> <div>  Note The switch is turned off by default. In this case, the policy does not take effect after it is created. </div>
Note	Enter the description of the security policy.

What's next

After you create and enable a security policy for a container, the container signature feature takes effect on the container that you select when you configure the security policy. The container image based on which the container is created is labeled as **Trusted Image**.

 **Note** The feature that displays trusted signature labels is not available.

4. Use the multi-account control feature

The multi-account control feature allows you to manage multiple cloud accounts and resource accounts of your enterprise in a centralized manner. You can configure protection settings for members of your enterprise and view the risks that are detected in the resources of the members in real time. This topic describes how to use the multi-account control feature.

Prerequisites

- A resource directory is enabled. For more information, see [Enable a resource directory](#).
- A member is created in the resource directory or joins the resource directory. For more information, see [Create a member](#) and [Invite an Alibaba Cloud account to join a resource directory](#).

Context

Security Center can be integrated with the Resource Directory service of Resource Management as a trusted service. Then, you can use Security Center to manage the members of your resource directory in a centralized and structured manner.

You can use the management account of your resource directory or a delegated administrator account to add other Alibaba Cloud accounts of your enterprise to your resource directory for centralized management.

After you specify a member as a **delegated administrator account**, the member is authorized by the management account of your resource directory to perform the following operations: access and manage the organization and the members of your resource directory from Security Center, and view the risks that are detected in the resources of the members. For more information, see [Management account](#) and [Manage a delegated administrator account](#).

Add a delegated administrator account

Before you can add members to your resource directory, you must specify a member as a delegated administrator account.

1. Log on to the [Resource Management console](#) by using the management account of your resource directory.
2. In the left-side navigation pane, choose **Resource Directory > Trusted Services**. On the page that appears, specify a member as a delegated administrator account for Security Center.

After you specify a delegated administrator account, the delegated administrator account can be used to perform management operations in a trusted service on behalf of the management account. In this topic, Security Center is the trusted service.

For more information, see [Add a delegated administrator account](#).

 **Note** You can add a maximum of five delegated administrator accounts for Security Center.

Add members

You can use the management account of your resource directory or a delegated administrator account to add members for centralized management.

- 1.
2. In the left-side navigation pane, choose **Operation > Multi-account Control**.
3. On the **Multi-account Control** page, click **Add**.
4. In the **Add** panel, select an account from the **Select account** drop-down list.

Note The members in the drop-down list are the same regardless of whether you use the management account of your resource directory or a delegated administrator account.

5. (Optional) Select **When a new account is created, the account is added to the list of managed accounts by default**. Newly created accounts are automatically added to the

member list.

6. Click **OK**.

You can view the added member in the member list of the **Multi-account Control** page.

Configure protection settings for a member

You can use the management account of your resource directory or a delegated administrator account to configure settings for a member without the need to log on to the Security Center console as the member. You can configure the Security Center agent installed on the assets that belong to the member, specify vulnerabilities for detection, and configure baseline check policies for the assets.

- 1.
2. In the left-side navigation pane, choose **Operation > Multi-account Control**.
3. In the member list of the **Multi-account Control** page, click **Settings** in the **Actions** column of an member.
4. In the **Settings** panel, configure parameters in the following steps for the member.

i. **Client management**

The following table describes the sections in the Client management step.

Section	Description	References
Proactive Defense	Proactive defense automatically intercepts common viruses, malicious network connections, and webshell connections. Proactive defense also allows you to use bait to capture ransomware.	Use proactive defense
Webshell Detection	Webshell detection scans servers and web directories for webshells and trojans at regular intervals. Security Center generates alerts for detected webshells and displays alerts only when webshell detection is enabled.	Use the webshell detection feature
K8s Threat Detection	The feature of threat detection on Kubernetes containers checks the security status of running container clusters and detects security threats and attacks in the container clusters at the earliest opportunity.	Use threat detection on Kubernetes containers
Dynamic adaptive threat detection capability	If a high-risk intrusion is detected on your server after the adaptive threat detection feature is enabled, the Security Center agent on your server automatically runs in Safeguard Mode For Major Activities mode. The mode enables all protection rules and security engines, which helps detect intrusions in a more comprehensive manner.	Use adaptive threat detection

Section	Description	References
Alarm aggregation switch	The feature of automatic alert correlation analysis automatically aggregates multiple alerts generated on the intrusions that may be launched by the same attacker. For example, alerts on attacks from the same IP address or service, or on the assets of the same user can be aggregated. After you enable the feature, you can handle alerts that have the same characteristics with a few clicks. The feature allows you to handle alerts in an efficient manner.	Enable automatic alert correlation analysis
Protection Mode	The Security Center agent is a local plug-in provided by Security Center. Before you can use Security Center to protect your servers, you must install the Security Center agent on your servers. Security Center provides multiple protection modes. This allows the Security Center agent to run in different modes to meet security requirements in different scenarios.	Manage protection modes
Client Protection	The client protection feature blocks malicious operations that attempt to uninstall the Security Center agent. The feature ensures that Security Center provides stable protection capabilities.	Use the client protection feature
Client engine	After you turn on the switch in the Client engine section, Security Center detects webshells and viruses only by using the engines of Alibaba Cloud. We recommend that you turn on the switch only when the network connections of your servers in data centers are limited.	None

ii. Click **Next**.

iii. **Vulnerability management**

You can enable or disable automatic scan for each type of vulnerabilities, and enable vulnerability scan for specific servers. In addition, you can configure the scan cycle and scan method, and specify the number of days after which a detected vulnerability is automatically deleted. For more information, see [Configure vulnerability settings](#).

iv. Click **Next**.

v. **Baseline inspection**

The baseline check feature allows you to configure baseline check policies for the member. You can use baseline check policies to check whether risks exist in the baseline configurations of the assets that belong to the member. For more information, see [Create baseline check policies](#).

5. After you complete the configurations, click **Determine**.

Security Center enables the features that are supported by the Security Center agent for the member, and performs baseline checks for the member, and scans the assets that belong to the

member for vulnerabilities based on the configurations.

View the risks detected in the resources of a member

You can view the risks detected in the resources of a member that is displayed in the member list of the **Multi-account Control** page and manage the member by using the management account of your resource directory or a delegated administrator account.

- 1.
2. In the left-side navigation pane, choose **Operation > Multi-account Control**.
3. In the account list of the **Multi-account Control** page, view the risks that are detected in the resources of a member and manage the member.
 - o View the risks detected in the resources of a member

You can view the information about a member. The information includes the security score of the assets that belong to the member, the details about the alerts that are generated on the assets, and the vulnerabilities and baseline risks that are detected on the assets.

<div><div><div></div><div>Search by account name</div></div></div>										
Account	Security Center	Security Score	Alerts	Vulnerabilities	Baseline Check	Config Assessment	Attacks	Actions		
1700000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000										

- o Manage a member
 - Click **View** to go to the **Resource Directory** page in the **Resource Management** console. On the **Resource Directory** page, you can view directory information about all assets, create members, invite members, or upgrade a resource account to a cloud account.
 - Click **Delete** to remove the member from the member list.