

Alibaba Cloud

CloudConfig Quick Start

Document Version: 20211229

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Quick start for ordinary accounts -----	05
2.Quick start for management accounts -----	11
3.Quick start for member accounts -----	19

1. Quick start for ordinary accounts

An ordinary account is an independent Alibaba Cloud account that is not included in a resource directory by a management account. This topic helps you get started with Cloud Config by using an ordinary account.

Procedure

The following figure shows the steps to get started with Cloud Config by using an ordinary account.

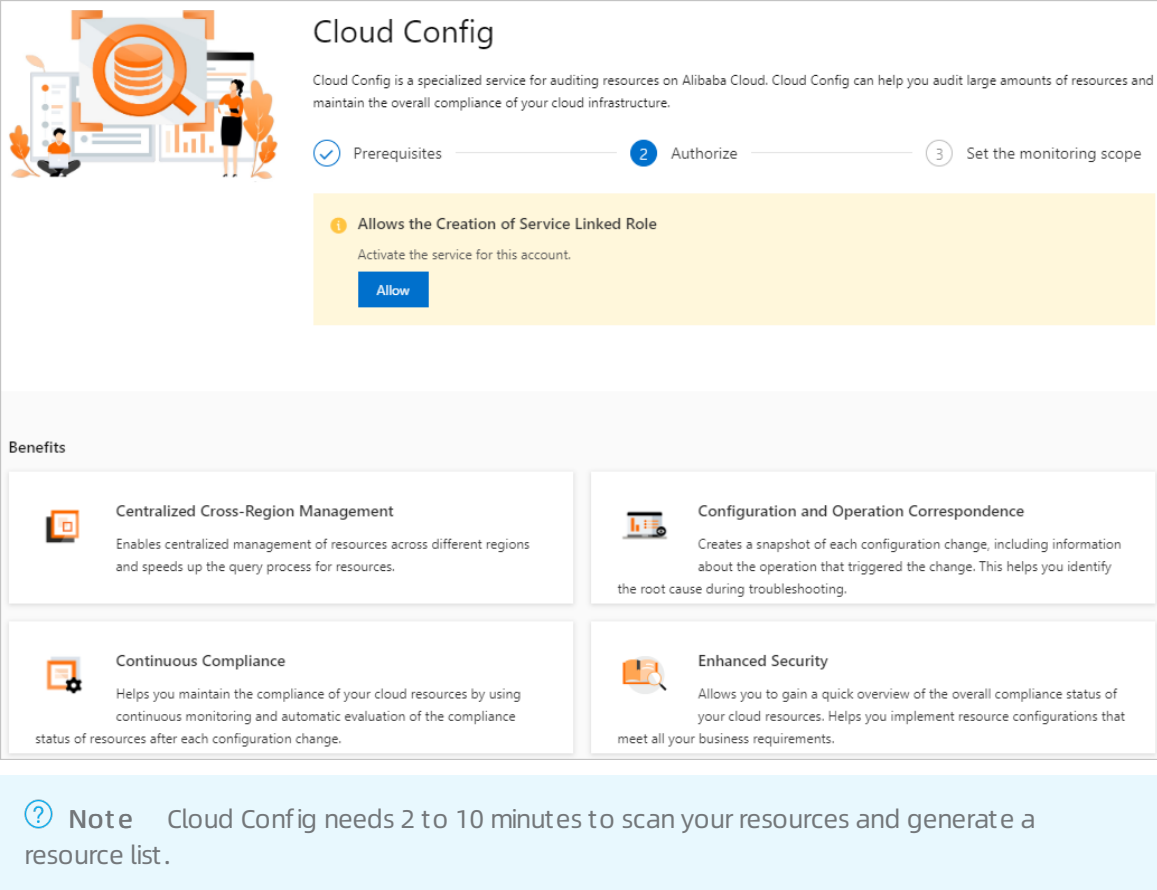


The following table describes the steps to get started with Cloud Config by using an ordinary account.

Category	Step	Description
Basic operations	Step 1: Authorize Cloud Config to access your resources	Before you use Cloud Config, you must authorize Cloud Config to access your resources.
	Step 2: View the resource list	You can view and manage the resources within your account.
	Step 3: Create a compliance package	You can create a compliance package based on a compliance package template. After you create a compliance package, you can view the compliance evaluation results of associated resources based on the specified rule.
Advanced operations	Step 4: Create a rule (Optional)	You can create rules by enabling managed rules provided by Cloud Config to audit specified resources.
	Step 5: Set the monitoring scope (Optional)	By default, Cloud Config monitors all supported types of resources. You can specify the types of resources to be monitored by Cloud Config.
	Step 6: Configure resource delivery (Optional)	You can specify an Object Storage Service (OSS) bucket to receive the scheduled resource snapshots and resource change logs within your account.
	Step 7: Subscribe to resource events (Optional)	You can specify a Message Service (MNS) topic to receive the resource non-compliance events and resource change logs within your account.

Step 1: Authorize Cloud Config to access your resources

1. Log on to the [Cloud Config console](#).
2. In the Authorize step, click **Allow** to create the service-linked role that authorizes Cloud Config to access your resources.



Cloud Config

Cloud Config is a specialized service for auditing resources on Alibaba Cloud. Cloud Config can help you audit large amounts of resources and maintain the overall compliance of your cloud infrastructure.

1 Prerequisites — 2 **Authorize** — 3 Set the monitoring scope

1 Allows the Creation of Service Linked Role

Activate the service for this account.

[Allow](#)

Benefits

- Centralized Cross-Region Management**
Enables centralized management of resources across different regions and speeds up the query process for resources.
- Configuration and Operation Correspondence**
Creates a snapshot of each configuration change, including information about the operation that triggered the change. This helps you identify the root cause during troubleshooting.
- Continuous Compliance**
Helps you maintain the compliance of your cloud resources by using continuous monitoring and automatic evaluation of the compliance status of resources after each configuration change.
- Enhanced Security**
Allows you to gain a quick overview of the overall compliance status of your cloud resources. Helps you implement resource configurations that meet all your business requirements.

Note Cloud Config needs 2 to 10 minutes to scan your resources and generate a resource list.

Step 2: View the resource list

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Resources > Global Resources**.
3. On the **Resources** page, enter a resource ID or set filter conditions to search for the specified resource.
 - You can enter a resource ID to search for the specified resource.
 - You can filter the resources based on the resource type, region, compliance status, and resource status to search for the specified resource with high efficiency.
4. Click the resource ID in the Resource ID / Resource Name column.
5. On the **Details** tab, view the basic information, core configurations, and latest compliance evaluation results of the resource.
 - In the **Basic Information** section, you can view the ID, name, type, and tags of the resource, the time when the resource was created, and the region and zone where the resource resides.
 - In the **Configuration Details** section, you can click **View JSON** to view the core configurations in the JSON format.
 - In the **Most Recent Evaluation** section, you can view the latest compliance evaluation result of the resource.

Step 3: Create a compliance package

1. Log on to the [Cloud Config console](#).

2. In the left-side navigation pane, click **Compliance Package**.
3. On the **Compliance Package** page, click **Enable Compliance Package** in the upper-right corner.
4. In the **Basic Information** step, specify the name and risk level of the compliance package. Then, click **Next**.
5. In the **Select a rule** step, select **Compliance Package Template**, **Rules**, or **Managed rule** from the drop-down list. After that, select one or more rules from the rule list. If you select **Compliance Package Template**, select a compliance package template from the drop-down list that appears. Then, click **Next**.
6. In the **Rule Settings** step, set the **Rule Name**, **Risk Level**, and **Description** parameters and click **Finish**.

Step 4: Create a rule (Optional)

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click **Create Rule**.
4. On the **Create Rule** page, search for a managed rule based on the rule name, tag, evaluation logic, or risk level.
5. Click **Apply Rule**.
6. In the **Properties** step, set the Rule Name, Risk Level, and Description parameters. Then, click **Next**.

The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.

7. In the **Assess Resource Scope** step, keep the default resource type and click **Next**.
8. In the **Parameters** step, click **Next**.

If the managed rule has an input parameter, you must set an expected value for the input parameter.

9. In the **Modify** step, click **Next**.

For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see [Configure automatic remediation](#) or [Configure manual remediation](#).

10. In the **Preview and Save** step, check the configurations and click **Submit**.
11. Verify that the rule is created.
 - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
 - Click **Return to Rule List**. In the Rules list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

Step 5: Set the monitoring scope (Optional)

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Settings > Monitoring Scope**.
3. On the **Monitoring Scope** page, click the **Edit** icon in the upper-right corner.
4. Specify the types of resources to be monitored.
 - If you select **All Supported Resource Types**, Cloud Config monitors all supported types of

resources that belong to your Alibaba Cloud account. If a new service is integrated with Cloud Config, the resource type of the service is automatically added to the monitoring scope.

- If you select **Custom Resource Types**, you can specify the types of resources to be monitored. In this case, Cloud Config monitors only the specified types of resources that belong to your Alibaba Cloud account.

5. Click **OK**.

6. In the **Email Verification** dialog box, click **Get Verification Code**.

Alibaba Cloud sends a verification code to the email address that is bound to your account.

7. Enter the verification code in the **Verification Code** field and click **OK**.

Step 6: Configure resource delivery (Optional)

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Delivery Services > Deliver Logs to OSS**.
3. On the **Deliver Logs to OSS** page, turn on **OSS Settings**.
4. Set the required parameters to specify an OSS bucket to store resource data.

The following table describes the parameters.

Parameter	Description
Select Acceptable Content	The type of resource data to be delivered to the OSS bucket. Valid values: <ul style="list-style-type: none">◦ Scheduled Snapshots: the scheduled resource snapshots. Cloud Config delivers scheduled resource snapshots to the OSS bucket at 00:00:00 and 12:00:00 every day.◦ Historical Configuration Changes: the resource change logs. Cloud Config delivers resource change logs to the OSS bucket when the configurations of resources change.
Region	The region where the OSS bucket resides.
Bucket	The name of the OSS bucket. The bucket name must be unique. <ul style="list-style-type: none">◦ If you select Create Bucket, you must specify a bucket name.◦ If you select Select Buckets, you must select an existing bucket from the Bucket drop-down list.
Server-side Encryption	Specifies whether and how to encrypt objects in the OSS bucket. This parameter must be set if you select Create Bucket . Valid values: <ul style="list-style-type: none">◦ No◦ AES256◦ KMS


5. Click **OK**.


Step 7: Subscribe to resource events (Optional)

1. Log on to the [Cloud Config console](#).

2. In the left-side navigation pane, choose **Delivery Services > Deliver Data to Message Service**.
3. On the **Deliver Data to Message Service** page, turn on **MNS Settings**.
4. Set the required parameters to specify an MNS topic to receive resource data.

The following table describes the parameters.

Parameter	Description
Select Acceptable Content	<p>The type of resource data to be delivered to the MNS topic. Valid values:</p> <ul style="list-style-type: none"> ◦ Historical Configuration Changes: the resource change logs. Cloud Config delivers resource change logs to the MNS topic when the configurations of resources change. ◦ Non-compliance Events: the resource non-compliance events. If a resource is evaluated as non-compliant, Cloud Config delivers the resource non-compliance event to the MNS topic.
MNS Region	The region where the MNS topic resides.
Topic Name	<p>The name of the MNS topic. The topic name must be unique within your Alibaba Cloud account in the specified region.</p> <ul style="list-style-type: none"> ◦ If you select Create a topic in the account, you must specify a topic name. ◦ If you select Select an existing topic from the account, you must select an existing topic from the Topic Name drop-down list.
Maximum Message Size (Byte)	<p>The maximum length of the message body that can be received by the topic. Unit: byte. Valid values: 1024 to 65536. Default value: 65536.</p> <div> <p> Note We recommend that you set this parameter to a value greater than or equal to 8192. Otherwise, the message delivery may fail due to the length limit.</p> </div>
Enable Logging	Specifies whether to store the operation logs of the MNS topic in the associated Log Service Logstore. Operation logs are generated when messages are received, forwarded, and deleted.
Minimum Risk Level of the Events to Subscribe	<p>The lowest risk level of the events to which you want to subscribe. Valid values:</p> <ul style="list-style-type: none"> ◦ All Risk Levels ◦ High Risk ◦ Medium Risk ◦ Low Risk <p>For example, if you select Medium Risk, Cloud Config delivers non-compliance events at the Medium Risk and High Risk levels. Non-compliance events at the Low Risk level are ignored.</p>

Parameter	Description
Resources to Subscribe	<p>The types of the resources whose events you want to subscribe to. Valid values:</p> <ul style="list-style-type: none">◦ All Supported Resource Types: subscribes to the events of all supported types of resources. If a new service is integrated with Cloud Config, the resource type of the service is automatically added to the monitoring scope.◦ Custom Resource Types: subscribes to the events of the specified types of resources.
Recipient Address for Large Files	<p>The OSS bucket that is used to receive the large messages that Cloud Config delivers to the MNS topic.</p> <ul style="list-style-type: none">◦ If you set this parameter, a message that Cloud Config delivers to the MNS topic is automatically transferred to the specified OSS bucket when the message size exceeds 64 KB.◦ If you leave this parameter empty, the excess part of a message that Cloud Config delivers to the MNS topic is automatically truncated when the message size exceeds 64 KB. <div><p> Note The Region and Account parameters are automatically set based on the settings in the Content and Recipient Address section. You need only to select the destination bucket.</p></div>

5. Click **OK**.

2.Quick start for management accounts

A management account is an Alibaba Cloud account that enables a resource directory and manages all member accounts. This topic helps you get started with Cloud Config by using a management account.

Procedure

The following figure shows the steps to get started with Cloud Config by using a management account.




The following table describes the steps to get started with Cloud Config by using a management account.

Category	Step	Description
Basic operations	Step 1: Authorize Cloud Config to access your resources	Before you use Cloud Config, you must authorize Cloud Config to access your resources.
	Step 2: Create an account group	You can use a management account to create an account group and add all or some member accounts in your resource directory to the account group. This way, you can manage the resources, compliance packages, and rules of multiple member accounts in an account group in a centralized manner.
	Step 3: View the resource list	You can use a management account to view the resources of all member accounts in a specified account group.
	Step 4: Create a compliance package	You can use a management account to create a compliance package based on a compliance package template for a specified account group. After you create a compliance package, you can view the compliance evaluation results of associated resources based on the specified account and rule.
Advanced operations	Step 5: (Optional) Create a rule	You can create rules based on the managed rules that are provided by Cloud Config and use the created rules to audit specified resources.
	Step 6: (Optional) Configure delivery settings	You can use a management account to specify an Object Storage Service (OSS) bucket to receive the scheduled resource snapshots and the logs of resource configuration changes of the management account and its member accounts. Only management accounts are authorized to configure the delivery settings of resource data. No member accounts have the relevant permissions.

Category	Step	Description
	Step 7: (Optional) Subscribe to resource events	You can use a management account to specify a Message Service (MNS) topic to receive the resource non-compliance events and the logs of resource configuration changes of the management account and its member accounts. Only management accounts are authorized to configure the delivery settings of resource data. No member accounts have the relevant permissions.

Step 1: Authorize Cloud Config to access your resources

1. Log on to the [Cloud Config console](#).
2. In the Authorize step, click **Allow** to create the service-linked role that authorizes Cloud Config to access your resources.



Cloud Config

Cloud Config is a specialized service for auditing resources on Alibaba Cloud. Cloud Config can help you audit large amounts of resources and maintain the overall compliance of your cloud infrastructure.


1 Prerequisites
2 Authorize
3 Set the monitoring scope

1 Allows the Creation of Service Linked Role

Activate the service for this account.


[Allow](#)

Benefits




Centralized Cross-Region Management

Enables centralized management of resources across different regions and speeds up the query process for resources.




Configuration and Operation Correspondence

Creates a snapshot of each configuration change, including information about the operation that triggered the change. This helps you identify the root cause during troubleshooting.



Continuous Compliance

Helps you maintain the compliance of your cloud resources by using continuous monitoring and automatic evaluation of the compliance status of resources after each configuration change.



Enhanced Security

Allows you to gain a quick overview of the overall compliance status of your cloud resources. Helps you implement resource configurations that meet all your business requirements.

Note Cloud Config needs 2 to 10 minutes to scan your resources and generate a resource list.

Step 2: Create an account group

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, click **Account Group**.
3. On the **Account Group** page, click **Create**.
4. On the **Create** page, configure a name and description for the account group, and then click **Add Member**.
5. Specify member accounts from the resource directory and click **OK**.

6. Click **Submit**.

In the **Account Group** list, find the account group that you created. If the status of the account group is **Created**, the account group is created. You can also view the name, description, member account quantity, type, and creation time of the account group.

Step 3: View the resource list

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Resources > Global Resources**.
3. On the **Global Resources** page, click the required account group tab.
4. On the account group tab, enter a resource ID or set filter conditions to search for the specified resource.
 - You can enter a resource ID to search for the specified resource.
 - You can filter the resources based on the resource type, region, compliance status, and resource status to search for the specified resource with high efficiency.
5. Click the resource ID in the **Resource ID / Resource Name** column.
6. On the **Details** tab, view the basic information, core configurations, and latest compliance evaluation results of the resource.
 - In the **Basic Information** section, you can view the ID, name, type, and tags of the resource, the time when the resource was created, and the region and zone where the resource resides.
 - In the **Configuration Details** section, you can click **View JSON** to view the core configurations in the JSON format.
 - In the **Most Recent Evaluation** section, you can view the latest compliance evaluation result of the resource.

Step 4: Create a compliance package

- 1.
- 2.
3. On the **Compliance Package** page, click the tab of the account group for which you want to enable a compliance package.
4. On the account group tab, click **Enable Compliance Package** in the upper-right corner.
- 5.
- 6.
7. In the **Rule Settings** step, set the **Rule Name**, **Risk Level**, and **Description** parameters and click **Finish**.

Step 5: (Optional) Create a rule

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, click **Create Rule**.
5. On the **Create Rule** page, search for a managed rule based on the rule name, tag, evaluation logic, or risk level.

6. Click **Apply Rule**.
7. In the **Properties** step, set the Rule Name, Risk Level, and Description parameters. Then, click **Next**.
The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.
8. In the **Assess Resource Scope** step, keep the default resource type and click **Next**.
9. In the **Parameters** step, click **Next**.
If the managed rule has an input parameter, you must set an expected value for the input parameter.
10. In the **Modify** step, click **Next**.
For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see [Configure automatic remediation](#) or [Configure manual remediation](#).
11. In the **Preview and Save** step, check the configurations and click **Submit**.
12. Verify that the rule is created.
 - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
 - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

Step 6: (Optional) Configure delivery settings

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Delivery Services > Deliver Logs to OSS**.
3. On the **Deliver Logs to OSS** page, turn on **OSS Settings**.
4. Set the required parameters to specify an OSS bucket to store resource data.

You can create an OSS bucket within the management account, or select an existing OSS bucket that belongs to the management account or a member account. The OSS bucket stores the resource data of the management account and member accounts of the relevant resource directory.

- To deliver resource data to an OSS bucket that belongs to the management account, select **Create Bucket** or **Select Buckets**, and then set the required parameters. The following table describes the parameters.

Parameter	Description
Select Acceptable Content	The type of resource data to be delivered to the OSS bucket. Valid values: <ul style="list-style-type: none">■
Region	The region where the OSS bucket resides.
Bucket	The name of the OSS bucket. The bucket name must be unique. <ul style="list-style-type: none">■ If you select Create Bucket, you must specify a bucket name.■ If you select Select Buckets, you must select an existing bucket from the Bucket drop-down list.

Parameter	Description
Server-side Encryption	<p>Specifies whether and how to encrypt objects in the OSS bucket. This parameter must be set if you select Create Bucket.</p> <p>Valid values:</p> <ul style="list-style-type: none"> ■ No ■ AES256 ■ KMS

- To deliver resource data to an OSS bucket that belongs to a member account, select **Select Buckets from Other Enterprise Management Accounts**, and then set the required parameters. Before you set the parameters, make sure that the member account has an available bucket. The following table describes the parameters.

Parameter	Description
Select Acceptable Content	<p>The type of resource data to be delivered to the OSS bucket. Valid values:</p> <ul style="list-style-type: none"> ■
The ARN of the bucket that belongs to the destination account	<p>The ARN of the bucket within the member account. The ARN consists of the following information: the ID of the region where the bucket resides, the ID of the member account, and the name of the bucket. You can select the region from the Region drop-down list, the member account from the Member Accounts drop-down list, and the bucket from the Bucket drop-down list.</p>
The role ARN that belongs to the destination account	<p>The ARN of the role to be assumed by the member account. The ARN consists of the following information: the ID of the member account and the service-linked role for Cloud Config. You can select the member account from the drop-down list and use the default service-linked role.</p>

5. Click **OK**.


Step 7: (Optional) Subscribe to resource events

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Delivery Services > Deliver Data to Message Service**.
3. On the **Deliver Data to Message Service** page, turn on **MNS Settings**.
4. Set the required parameters to specify an MNS topic to receive resource data.

You can create an MNS topic within the management account, or select an existing MNS topic that belongs to the management account or a member account. The specified MNS topic receives the resource data of the management account and member accounts of the relevant resource directory.

- To deliver resource data to a topic that belongs to the management account, select **Create a topic in the account** or **Select an existing topic from the account**, and then set the

required parameters. The following table describes the parameters.

Parameter	Description
Select Acceptable Content	
MNS Region	The region where the MNS topic resides.
Topic Name	<p>The name of the MNS topic. The topic name must be unique within your Alibaba Cloud account in the specified region.</p> <ul style="list-style-type: none">■ If you select Create a topic in the account, you must specify a topic name.■ If you select Select an existing topic from the account, you must select an existing topic from the Topic Name drop-down list.
Maximum Message Size (Byte)	<p>The maximum length of the message body that can be received by the topic. Unit: byte. Valid values: 1024 to 65536. Default value: 65536.</p> <div><p> Note We recommend that you set this parameter to a value greater than or equal to 8192. Otherwise, the message delivery may fail due to the length limit.</p></div>
Enable Logging	Specifies whether to store the operation logs of the MNS topic in the associated Log Service Logstore. Operation logs are generated when messages are received, forwarded, and deleted.
Minimum Risk Level of the Events to Subscribe	<p>The lowest risk level of the events to which you want to subscribe. Valid values:</p> <ul style="list-style-type: none">■ All Risk Levels■ High Risk■ Medium Risk■ Low Risk <p>For example, if you select Medium Risk, Cloud Config delivers non-compliance events at the Medium Risk and High Risk levels. Non-compliance events at the Low Risk level are ignored.</p>
Resources to Subscribe	<p>The types of the resources whose events you want to subscribe to. Valid values:</p> <ul style="list-style-type: none">■ All Supported Resource Types: subscribes to the events of all supported types of resources. If a new service is integrated with Cloud Config, the resource type of the service is automatically added to the monitoring scope.■ Custom Resource Types: subscribes to the events of the specified types of resources.

Parameter	Description
Recipient Address for Large Files	

- To deliver resource data to a topic that belongs to a member account, select **Select an existing topic from other enterprise management accounts**, and then set the required parameters. Before you set the parameters, make sure that the member account has available topics. The following table describes the parameters.

Parameter	Description
Select Acceptable Content	
The ARN of the topic that belongs to the destination account	The ARN of the topic within the member account. The ARN consists of the following information: the ID of the region where the topic resides, the ID of the member account, and the name of the topic. You can select the region from the Region drop-down list, the member account from the Member Accounts drop-down list, and the topic from the Topic Name drop-down list.
The role ARN that belongs to the destination account	The ARN of the role to be assumed by the member account. The ARN consists of the following information: the ID of the member account and the service-linked role for Cloud Config. You can select the member account from the drop-down list and use the default service-linked role.
Minimum Risk Level of the Events to Subscribe	<p>The lowest risk level of the events to which you want to subscribe. Valid values:</p> <ul style="list-style-type: none"> ■ All Risk Levels ■ High Risk ■ Medium Risk ■ Low Risk <p>For example, if you select Medium Risk, Cloud Config delivers non-compliance events at the Medium Risk and High Risk levels. Non-compliance events at the Low Risk level are ignored.</p>
Resources to Subscribe	<p>The types of the resources whose events you want to subscribe to. Valid values:</p> <ul style="list-style-type: none"> ■ All Supported Resource Types: subscribes to the events of all supported types of resources. If a new service is integrated with Cloud Config, the resource type of the service is automatically added to the monitoring scope. ■ Custom Resource Types: subscribes to the events of the specified types of resources.
Recipient Address for Large Files	

5. Click **OK**.

3.Quick start for member accounts

A member account is an Alibaba Cloud account in a resource directory. This topic helps you get started with Cloud Config by using a member account.

Procedure

The following figure shows the steps to get started with Cloud Config by using a member account.

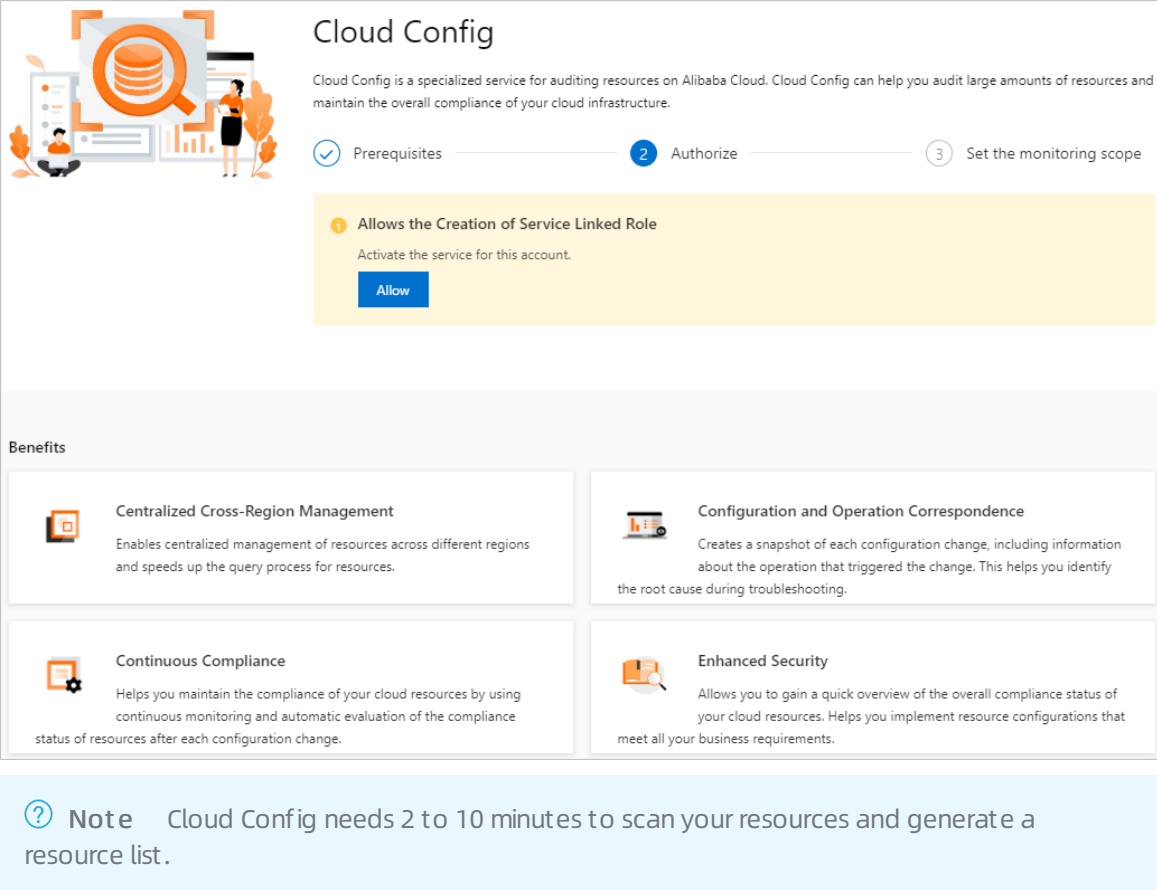


The following table describes the steps to get started with Cloud Config by using a member account.

Category	Step	Description
Basic operations	Step 1: Authorize Cloud Config to access your resources	Before you use Cloud Config, you must authorize Cloud Config to access your resources.
	Step 2: View the resource list	You can view and manage the resources within your account.
	Step 3: Create a compliance package	You can create a compliance package based on a compliance package template. After you create a compliance package, you can view the compliance evaluation results of associated resources based on the specified rule.
Advanced operations	Step 4: Create a rule (Optional)	You can create rules by enabling managed rules provided by Cloud Config to audit specified resources.

Step 1: Authorize Cloud Config to access your resources

1. Log on to the [Cloud Config console](#).
2. In the Authorize step, click **Allow** to create the service-linked role that authorizes Cloud Config to access your resources.



Cloud Config

Cloud Config is a specialized service for auditing resources on Alibaba Cloud. Cloud Config can help you audit large amounts of resources and maintain the overall compliance of your cloud infrastructure.

1 Prerequisites — 2 **Authorize** — 3 Set the monitoring scope

1 Allows the Creation of Service Linked Role
Activate the service for this account.
[Allow](#)

Benefits

- Centralized Cross-Region Management**
Enables centralized management of resources across different regions and speeds up the query process for resources.
- Configuration and Operation Correspondence**
Creates a snapshot of each configuration change, including information about the operation that triggered the change. This helps you identify the root cause during troubleshooting.
- Continuous Compliance**
Helps you maintain the compliance of your cloud resources by using continuous monitoring and automatic evaluation of the compliance status of resources after each configuration change.
- Enhanced Security**
Allows you to gain a quick overview of the overall compliance status of your cloud resources. Helps you implement resource configurations that meet all your business requirements.

Note Cloud Config needs 2 to 10 minutes to scan your resources and generate a resource list.

Step 2: View the resource list

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, choose **Resources > Global Resources**.
3. On the **Resources** page, enter a resource ID or set filter conditions to search for the specified resource.
 - You can enter a resource ID to search for the specified resource.
 - You can filter the resources based on the resource type, region, compliance status, and resource status to search for the specified resource with high efficiency.
4. Click the resource ID in the Resource ID / Resource Name column.
5. On the **Details** tab, view the basic information, core configurations, and latest compliance evaluation results of the resource.
 - In the **Basic Information** section, you can view the ID, name, type, and tags of the resource, the time when the resource was created, and the region and zone where the resource resides.
 - In the **Configuration Details** section, you can click **View JSON** to view the core configurations in the JSON format.
 - In the **Most Recent Evaluation** section, you can view the latest compliance evaluation result of the resource.

Step 3: Create a compliance package

1. Log on to the [Cloud Config console](#).

2. In the left-side navigation pane, click **Compliance Package**.
3. On the **Compliance Package** page, click **Enable Compliance Package** in the upper-right corner.
4. In the **Basic Information** step, specify the name and risk level of the compliance package. Then, click **Next**.
5. In the **Select a rule** step, select **Compliance Package Template**, **Rules**, or **Managed rule** from the drop-down list. After that, select one or more rules from the rule list. If you select **Compliance Package Template**, select a compliance package template from the drop-down list that appears. Then, click **Next**.
6. In the **Rule Settings** step, set the **Rule Name**, **Risk Level**, and **Description** parameters and click **Finish**.

Step 4: Create a rule (Optional)

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click **Create Rule**.
4. On the **Create Rule** page, search for a managed rule based on the rule name, tag, evaluation logic, or risk level.
5. Click **Apply Rule**.
6. In the **Properties** step, set the Rule Name, Risk Level, and Description parameters. Then, click **Next**.

The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.

7. In the **Assess Resource Scope** step, keep the default resource type and click **Next**.
8. In the **Parameters** step, click **Next**.

If the managed rule has an input parameter, you must set an expected value for the input parameter.

9. In the **Modify** step, click **Next**.

For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see [Configure automatic remediation](#) or [Configure manual remediation](#).

10. In the **Preview and Save** step, check the configurations and click **Submit**.
11. Verify that the rule is created.
 - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
 - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the **Status** column. In normal cases, the rule is in the **Active** state.