ALIBABA CLOUD

Alibaba Cloud

CloudConfig Tutorial

Document Version: 20200817

Alibaba Cloud

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

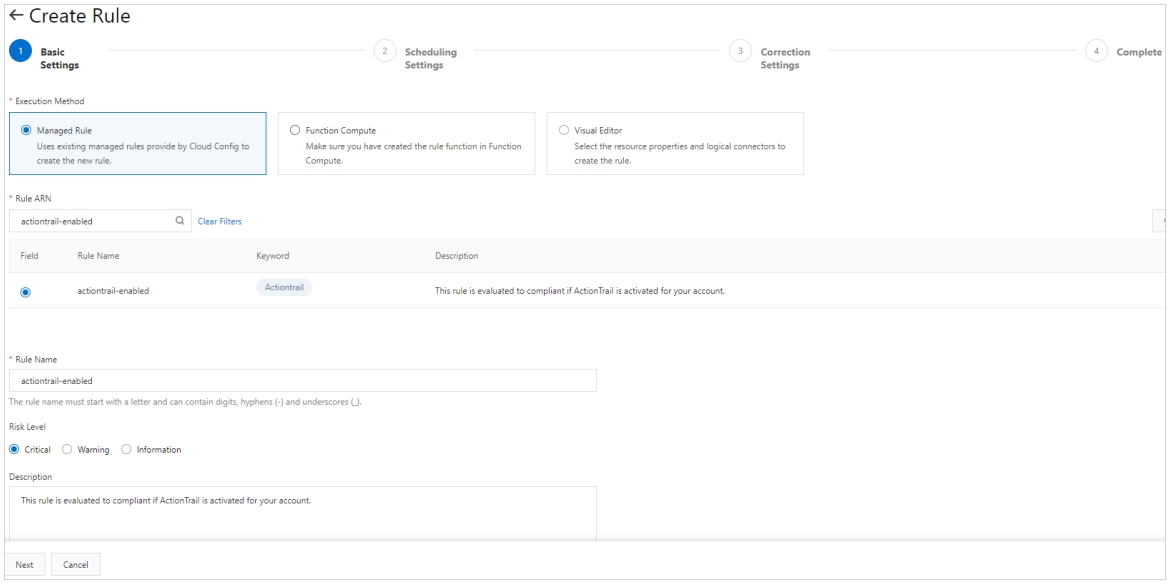
Table of Contents

1.Check whether the ActionTrail service is activated for your account

You can create a rule to check whether the ActionTrail service is activated for your account.

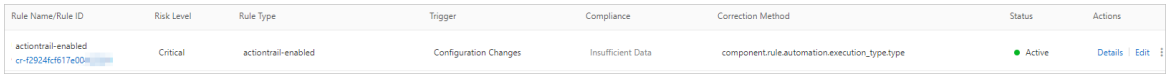
Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. Click **Create Rule**.
4. In the **Basic Settings** step of the **Create Rule** wizard, set **Method** to **Managed Rule**, search for and select the **actiontrail-enabled** rule, set the risk level of the rule, and then click **Next**.



> **Note** To meet internal compliance requirements, an enterprise must activate ActionTrail for an account to monitor the operations of the account on resources and record the operations in logs in real time. You can use the actiontrail-enabled rule to check whether the ActionTrail service is activated for your account.

5. In the **Parameter Settings** step of the **Create Rule** wizard, use the default values for the trigger type and related resources, and then click **Next**.
6. In the **Complete** step of the **Create Rule** wizard, set Correction Method to **Disable Correction** and click **Submit**.
7. Check the evaluation results of the rule. In the **Correction Settings** step of the **Create Rule** wizard, click **View Details** or **Return to Rule List** to view the compliance evaluation results.

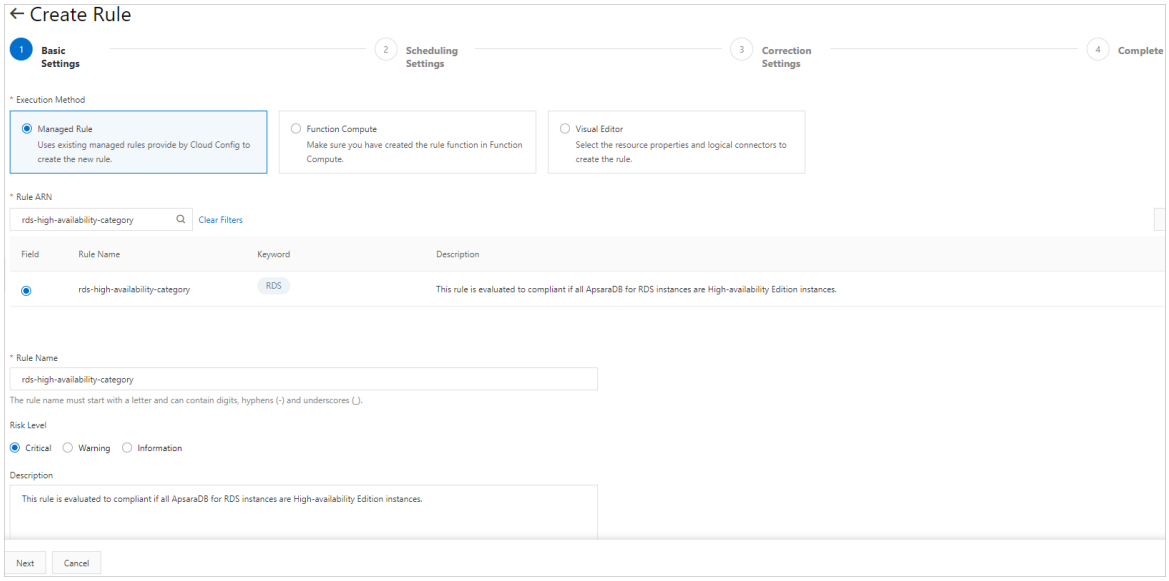


2.Check the high availability of RDS instances

You can create a rule to check whether Relational Database Service (RDS) instances are highly available.

Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. Click **Create Rule**.
4. In the **Basic Settings** step of the **Create Rule** wizard, set **Method** to **Managed Rule**, search for and select the **rds-high-availability-category** rule, set the risk level of the rule, and then click **Next**.



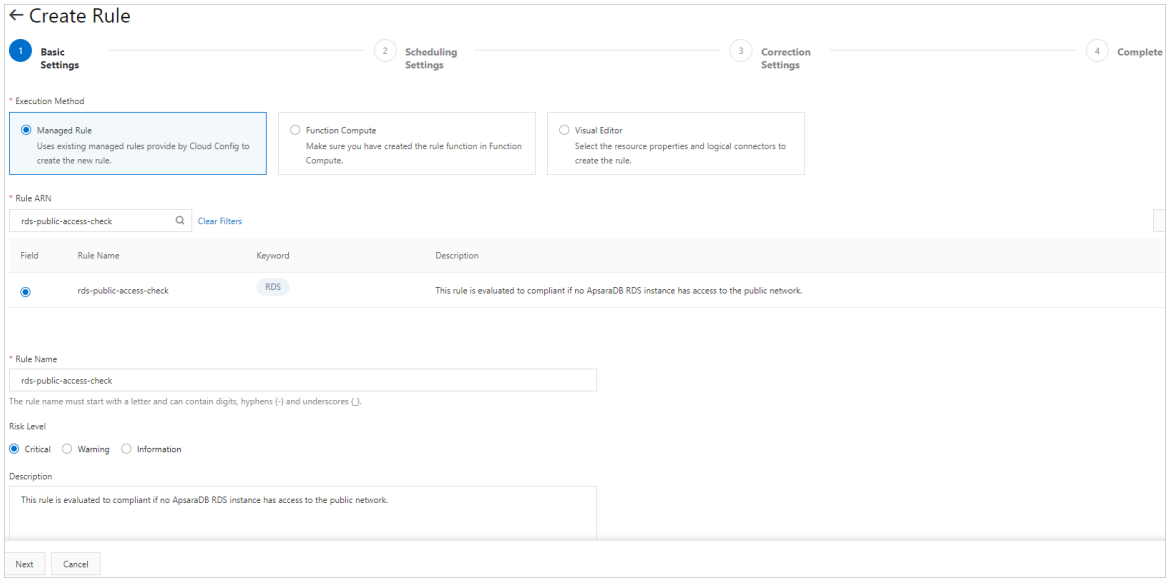
5. In the **Parameter Settings** step of the **Create Rule** wizard, use the default values for the trigger type and related resources, and then click **Next**.
6. In the **Complete** step of the **Create Rule** wizard, set Correction Method to **Disable Correction** and click **Submit**.
7. Check the evaluation results of the rule. In the **Correction Settings** step of the **Create Rule** wizard, click **View Details** or **Return to Rule List** to view the compliance evaluation results.

3.Check the compliance of public access to RDS instances

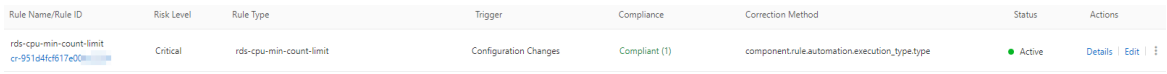
You can create a rule to monitor that Relational Database Service (RDS) instances do not allow access from the public network.

Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. Click **Create Rule**.
4. In the **Basic Settings** step of the **Create Rule** wizard, set **Method** to **Managed Rule**, search for and select the **rds-public-access-check** rule, set the risk level of the rule, and then click **Next**.



5. In the **Parameter Settings** step of the **Create Rule** wizard, use the default values for the trigger type and related resources, and then click **Next**.
6. In the **Complete** step of the **Create Rule** wizard, set Correction Method to **Disable Correction** and click **Submit**.
7. Check the evaluation results of the rule. In the **Correction Settings** step of the **Create Rule** wizard, click **View Details** or **Return to Rule List** to view the compliance evaluation results.

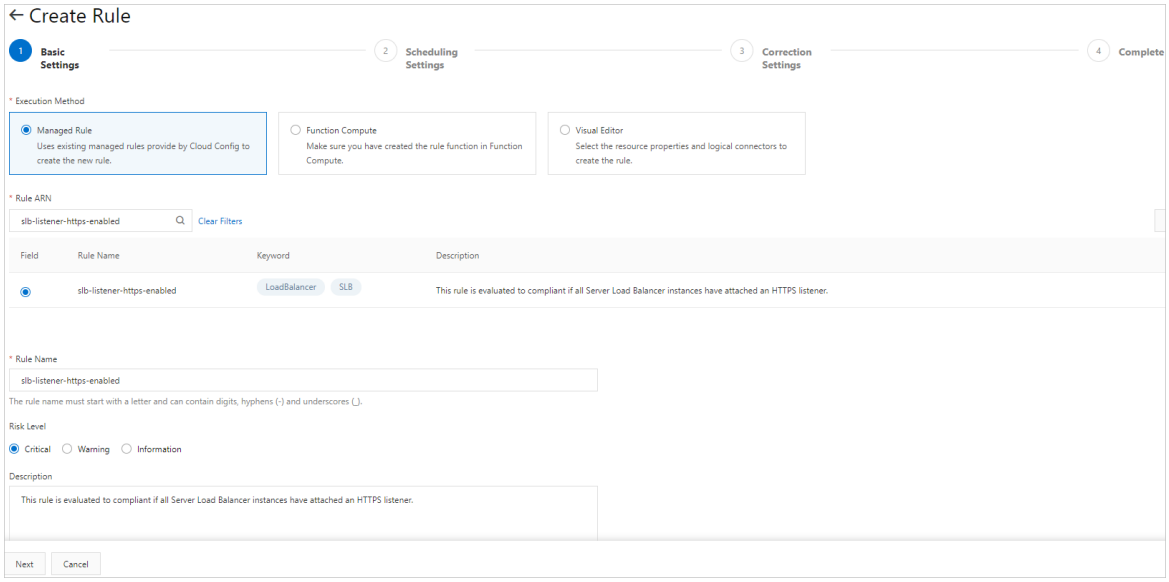


4.Check whether HTTPS listeners are enabled for SLB instances

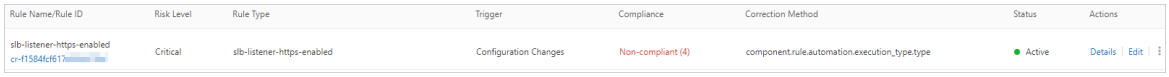
You can create a rule to check whether HTTPS listeners are enabled for Server Load Balancer (SLB) instances.

Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. Click **Create Rule**.
4. In the **Basic Settings** step of the **Create Rule** wizard, set **Method** to **Managed Rule**, search for and select the **slb-listener-https-enabled** rule, set the risk level of the rule, and then click **Next**.



5. In the **Parameter Settings** step of the **Create Rule** wizard, use the default values for the trigger type and related resources, and then click **Next**.
6. In the **Complete** step of the **Create Rule** wizard, set Correction Method to **Disable Correction** and click **Submit**.
7. Check the evaluation results of the rule. In the **Correction Settings** step of the **Create Rule** wizard, click **View Details** or **Return to Rule List** to view the compliance evaluation results.

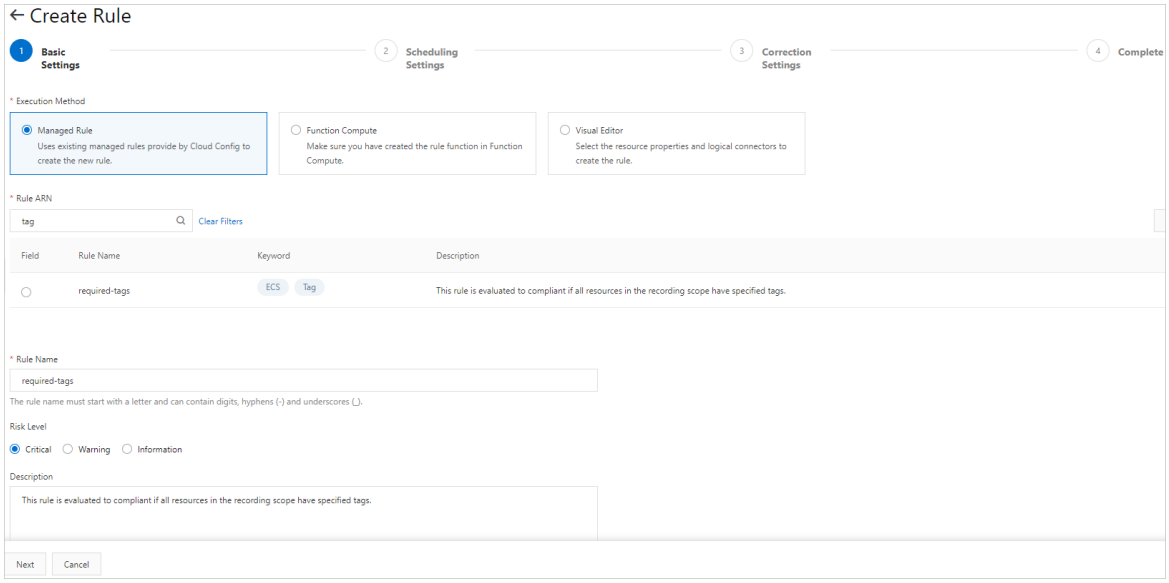


5.Check whether resources are bound to a specified tag

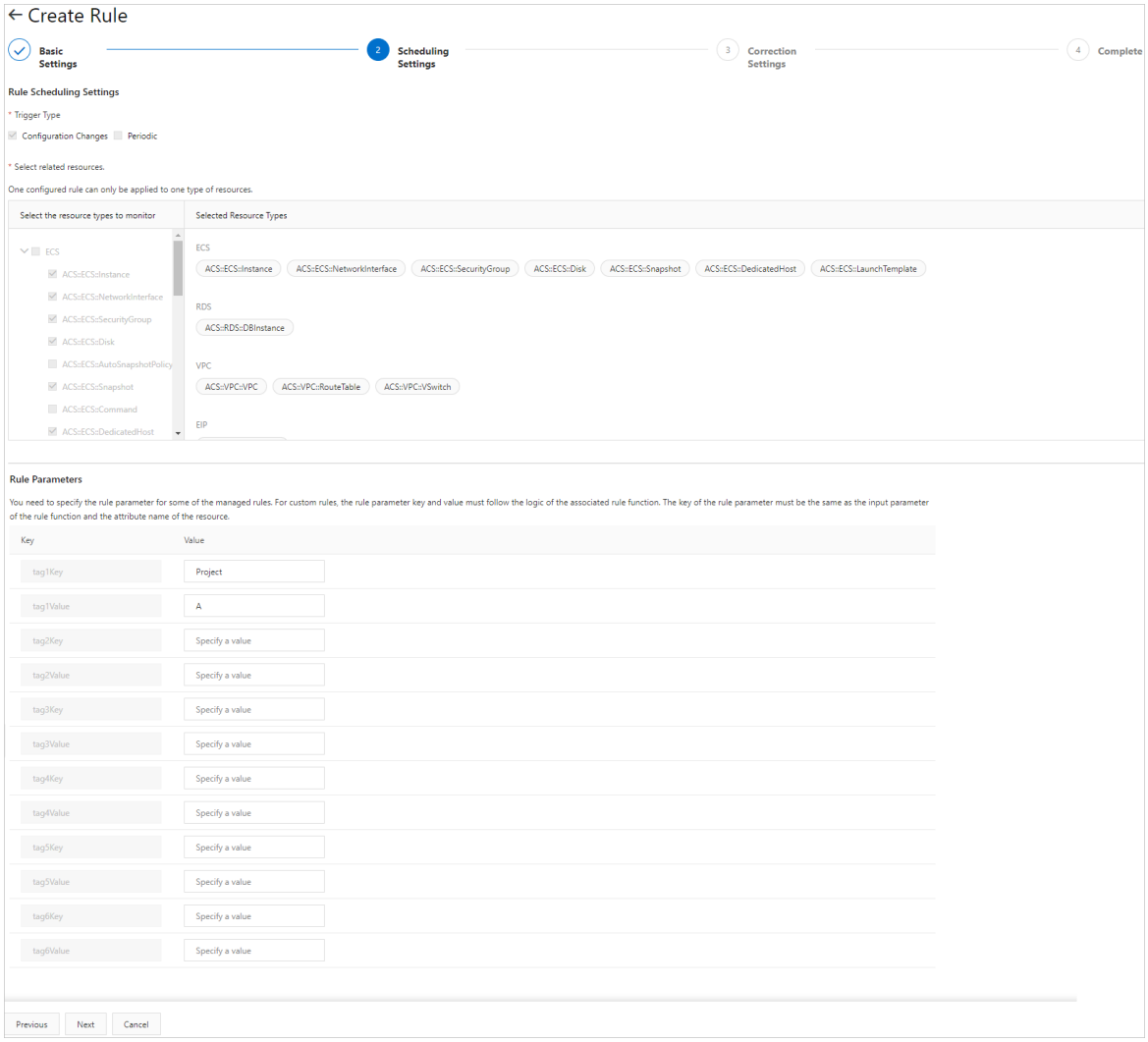
You can create a rule to check whether resources in your account are bound to a specified tag. Currently, you can configure such a rule for the following Alibaba Cloud services: Relational Database Service (RDS), Elastic Compute Service (ECS), Server Load Balancer (SLB), Object Storage Service (OSS), ApsaraDB for Redis, ApsaraDB for PolarDB, and ApsaraDB for MongoDB.

Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. Click **Create Rule**.
4. In the **Basic Settings** step of the **Create Rule** wizard, set **Execution Method** to **Managed Rule**, search for and select the **required-tags** rule, set the risk level of the rule, and then click **Next**.



5. In the **Scheduling Settings** step of the **Create Rule** wizard, enter the key and value of a tag and click **Next**.



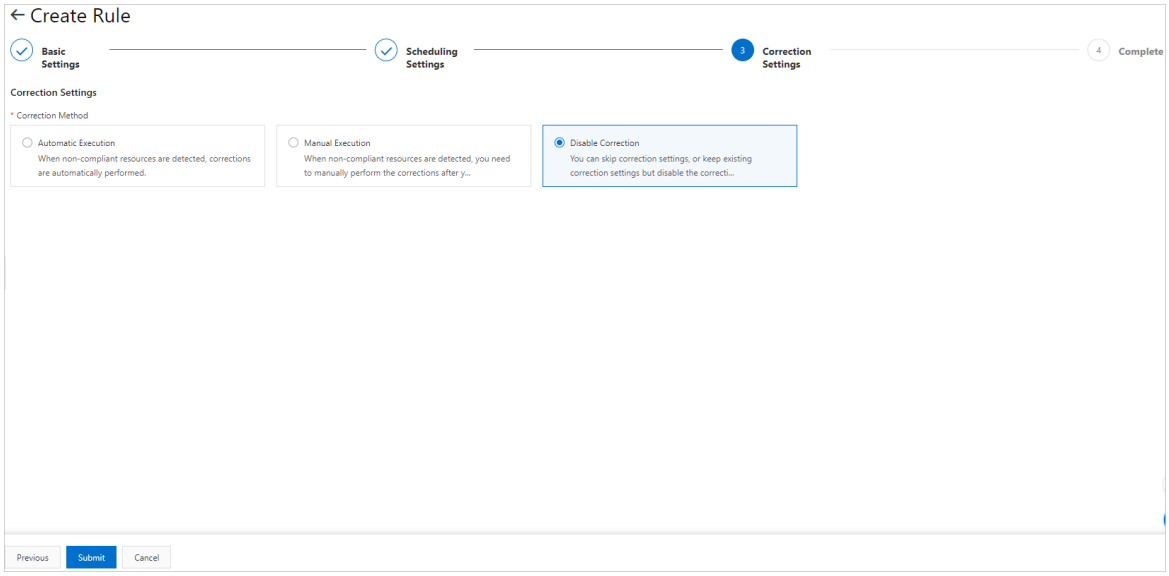
If you need to check multiple tags, you can set the keys and values of these tags one by one. Cloud Config allows you to check up to six tags. The rule is evaluated as **Compliant** only when the target resources are bound to all the tags that you have specified. If you want to check whether resources are bound to any tag in a group of tags, create a rule for each of the tags based on the required-tags rule.

For example, if you want all the resources in your account to be bound to the tag "Project=A", you can create a rule based on the **required-tags** rule to check the resources for this tag. When Cloud Config detects that some resources are not bound to the tag, the rule is evaluated as **Non-compliant**.

> **Note** Use the default values for the trigger type, related resources, and input parameters.

6. In the **Correction Settings** step of the **Create Rule** wizard, set Correction Method to **Disable Correction** and click **Submit**.

   You can bind a correction template to the current rule. For more information, see Set automatic correction or Set manual correction.



7. Check the evaluation results of the rule.In the **Correction Settings** step of the **Create Rule** wizard, click **View Details** or **Return to Rule List** to view the compliance evaluation results.