

# Alibaba Cloud CloudConfig

## User Guide

**Issue: 20200106**

## Legal disclaimer

---

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

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









ial, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document

.



## Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type.
<b>Bold</b>	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 Instance_ID</code>
[ ] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

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



# Contents

---

<b>Legal disclaimer.....</b>	<b>I</b>
<b>Document conventions.....</b>	<b>I</b>
<b>1 Resources.....</b>	<b>1</b>
1.1 View the resource list.....	1
1.2 Search for resources.....	2
1.3 View the current resource configuration.....	3
1.4 Manage resources.....	3
<b>2 Resource monitoring scope.....</b>	<b>5</b>
2.1 Manage resource monitoring scope.....	5
2.2 Unsupported resource type.....	6
<b>3 Resource configuration history.....</b>	<b>7</b>
3.1 View the resource configuration timeline.....	7
3.2 View resource change history.....	8
<b>4 Resource Compliance Audit.....</b>	<b>10</b>
4.1 Rule definition and Operation Principle.....	10
4.2 List of preset rules.....	12
4.3 Develop custom rules.....	20
4.4 Manage rules.....	26
4.4.1 Rule list.....	26
4.4.2 Create a rule.....	28
4.4.3 Modify and delete a rule.....	30
4.4.4 View rule details.....	31
4.5 View compliance results.....	32
4.5.1 View rule assessment results.....	32
4.5.2 Resource compliance timeline.....	33
<b>5 Preset rules.....</b>	<b>36</b>
5.1 ActionTrail.....	36
5.2 Alibaba Cloud CDN.....	36
5.3 DDH.....	37
5.4 ECS.....	39
5.5 EIP.....	49
5.6 OSS.....	50
5.7 RAM.....	53
5.8 RDS.....	53
5.9 TAG.....	60
5.10 SLB.....	61



# 1 Resources

---

## 1.1 View the resource list



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

After you activate the configuration audit service, you can obtain a list of resources for cross-region aggregation under your account, search for specific resource entities, and view the detailed configuration of resources.

**Note:** configuration audit only supports some Alibaba cloud products, so the resource list may only contain some of your resources. The configuration audit service is gradually expanding its coverage of Alibaba Cloud products, and is striving to provide you with a more complete resource list.

1. Log on [Configure the audit console](#).
2. In the left-side navigation pane, click resources to view the list of resources that are discovered within the service support scope under your account.

In the resource list, you can see general information such as resource Id, name, and creation time. Other information in the list is explained as follows:

1. The tags. The Tag information that you set for the resource when you manage the resource. This item is empty if you do not configure it.
2. Monitoring status. Configuration audit monitors your resource changes to help you record change history and automatically audit resource configuration compliance. This parameter indicates the current monitoring status of the resource based on the monitoring scope you have configured for audit. For more information about monitoring scope management, see [Manage resource monitoring scope](#).
3. The type of the resource. For more information about resource types, see [#unique\\_6](#), Configuration audit will continue to expand the scope of support for cloud products, please pay attention to [Unsupported resource type](#).

## 1.2 Search for resources



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

It is difficult to search for resources when you deploy resources in multiple Alibaba cloud regions. You must locate the correct region before you can find the target resource. The resource cross-region aggregation list can be used as a centralized portal for resource management.

You can filter resources by region, product, resource type, and monitoring status. You can also search for resources by resource Id or name, it helps you quickly find the resources in various regions under your account.

## 1.3 View the current resource configuration



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

You can view the current configuration information of a specified resource by filtering and searching the resource list.

1. Log on [Configure the audit console](#).
2. Click Trail list in the left-side navigation pane.
3. You can use a filter to retrieve resources or use a resource Id to find the specified resource.
4. Click resource Id to view key information about the resource, including the resource Id, name, creation time, and region. Click expand to view detailed and complete configuration information.

## 1.4 Manage resources



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

After finding a resource, you can quickly jump to the management page of the resource in the cloud product console to further operate the resource.

1. Log on [Configure the audit console](#).
2. In the left-side navigation pane, click resources.
3. Find the specified resource through the search, and then click manage resources in the actions column.

## 2 Resource monitoring scope

---

### 2.1 Manage resource monitoring scope

**Warning:**

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

Configuration audit records changes and real-time compliance audit by monitoring resource changes under your account. You can manage the scope of resource monitoring through simple configuration.

1. When you activate the configuration audit service, the resource types supported by all services are added to the monitoring scope by default.
2. If you set monitoring scope to "all types of resources supported by services", when new types of resources supported by audit are configured, they are added to the monitoring scope by default.
3. If you have other customized monitoring policies, you can go to [Management and monitoring scope](#) Page, follow the prompts on the page to set the type of monitored resource.

### Suspend a listener

1. When you remove a resource type from the monitoring scope, the real resources of this resource type under your account stop recording configuration changes until you move them back next time. Configuration change records during this period cannot be recovered.
2. For object resources of the resource type in the monitored scope, the monitoring status in the resource list is displayed as monitoring. For object resources of the resource type to be removed, in the resource list, "monitoring status" is displayed as "suspend listener".

### Restore a listener

1. On the [Management and monitoring scope](#) Page, and add the resource type back to the monitoring range, the status changes from "suspend listening" to "listening".
2. Configuration changes that occur when a listener is suspended cannot be recovered.

## 2.2 Unsupported resource type



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

See [#unique\\_12](#)

## 3 Resource configuration history

---

### 3.1 View the resource configuration timeline



#### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

Configuration audit records each configuration change details of the resources under monitoring, and organizes the results. That is, records of the evolution of resource configurations over time.

Configure a time line

- **Start point:** for the resources that are stored when you activate the configuration audit service, the starting point of the configuration timeline is the service activation time. For resources created after you activate the configuration audit service, the starting point of the configuration timeline is the resource creation time.
- **Node:** configuration audit refreshes the resource configuration snapshot every 10 minutes. If the snapshot is different from the one created 10 minutes ago, a configuration change record is displayed, which is a node on the configuration time line.

- **Breakpoint:** If you remove a resource type from the monitoring range, the monitoring of the related entity resources stops and the configuration timeline is not updated until you move the resource type back to the monitoring range, restart monitoring and tracking. The change history during monitoring stop cannot be traced.

Configure the content of the timeline

The configuration timeline belongs to a specific resource entity and is a set of historical resource configuration records.

- First, you can see the current configuration snapshot of the resource. Each node is a historical configuration snapshot.
- Each node includes the configuration details of the current change result, including the comparison details with the last change result.

[Note] configuration audit organizes resource changes every 10 minutes. If a resource configuration change occurs during the 10-minute window and is quickly restored before the change, the change cannot be perceived, therefore, the corresponding operation events cannot be displayed.

You can check the preceding information online or download it to your OSS bucket through APIs to facilitate offline integrated analysis. The OpenAPI and snapshot download capabilities are undergoing rapid iteration, so stay tuned.

## 3.2 View resource change history



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*



To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

The configuration audit service is connected to the actiontrail service. In addition to the configuration changes before and after the window period, you can also see the list of Operation events and event details for such changes, including the user, IP address, time, API name, and other operation information.

If you have not activated the actiontrail service, the content is empty. You can visit the [ActionTrail activation webpage](#).

## 4 Resource Compliance Audit

---

### 4.1 Rule definition and Operation Principle



#### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

Compliance is the code. Rules are a sample interpretation of the compliance requirements of enterprises. A compliance clause is a piece of Rule code. The essence of the code is the judgment logic of a resource configuration. The configuration audit service uses function compute functions to carry rule codes, which are called "rule functions". After the rule functions are referenced in the configuration audit service, after the associated resources and trigger mechanism are configured, the rules in the configuration audit service are formed.

In actual compliance monitoring, real-time resource configuration changes trigger the execution of rule functions to determine whether a resource configuration is compliant. By combining multiple rules, you can monitor the compliance of the entire resource configuration.

## Rule definition

**A rule is a judgment logic that determines whether a configuration item of a resource is compliant. It has the following features:**

- **The input parameters of a rule function are configuration items that can be obtained through the resource Query API, such as the resource type, Region, name, status, port/port switch status, and so on. The input parameter name must be consistent with the configuration item name.**
- **The logic of the rule function is to determine the input parameter value. The judgment logic is determined by your code. For example, if the HTTPS listening status of SLB is "on", it is considered "compliant ". The input parameter is the configuration field on the SLB resource that represents the HTTPS listener status . When this field value indicates "off", it is considered "non-compliance ".**
- **The output parameters of rule functions are compliant.**

## Resource type to which the rule points

**The rule functions defined in function compute do not have target direction, and do not indicate which resource type to point to. Configuration parameters with the same name may exist between different resources, an accurate compliance assessment cannot be implemented based on input parameters of rule functions.**

**Therefore, you must bind the created rule function to the specified resource type in configuration audit. When the configuration of this type of entity resource is changed, the system first finds the rules associated with the resource, and then determines which rule to trigger based on which configuration is changed.**

## Trigger a rule

**As mentioned above, when a resource configuration change occurs, configuration audit can accurately know which configuration has changed. The rule function with changed parameters as input parameters will be triggered to evaluate whether the change results are compliant. Therefore, the input parameter name of the rule function must be consistent with that of the actual resource configuration.**

**In addition, configuration audit allows you to set the rule to be triggered regularly to perform compliance assessment for you on a regular basis.**

## Compliance Assessment results

Configuration audit uses the obtained change results as input parameters and passes them to the rule function. The rule function returns the compliance results to the configuration audit, which presents and collects statistics in various ways in the configuration audit console. For more information, see [View rule assessment results](#).

You can customize rule functions in function Compute. For more information, see [Develop custom rules](#). You can also use the preset rules provided by configuration audit. For more information, see [List of preset rules](#).

## 4.2 List of preset rules



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

The following are the rules that have been configured by the Audit Service. You can select the following rules when creating rules in the console. The rule list can be updated.

If you need additional rules, submit them to us by submitting a ticket. After evaluation, we will provide proper support to implement rules with universal applicability as pre-configured rules by the system.

In the following rule list, "applicable resource types" are displayed as namespaces. You can choose [#unique\\_12](#) View the corresponding Chinese description in the list.

Check whether actiontrail is enabled for your account.

- Rule function name: actiontrail-enabled
- Applicable resource type: ACS::ActionTrail::Trail
- Rule input parameter: None
- Trigger mechanism: configuration change
- Rule compliance description: When an account enables the actiontrail service, it is considered compliance"
- Rule usage scenario: to meet the enterprise's internal compliance requirements, the operation audit service is generally required for the account to monitor and record the operation logs of the account's resources in real time. Use this rule to check whether operation audit is enabled for an account.

Check whether the number of CPUs in the ECS instance is below a threshold.

- Rule function name: ecs-you can use cpu-min-count-limit
- Applicable resource type: ACS::ECS::Instance
- Rule input parameter: cpuCount = threshold. cpuCount is the number of ECS instances. The threshold must be defined on the console.
- Trigger mechanism: configuration change
- Rule Compliance: When the cpuCount of an ECS instance under your account is greater than or equal to the threshold you set, it is considered as "compliance"
- Rule usage scenario: you can use the ECS instance type under the monitoring account of this rule, the number of CPU cannot be less than the threshold you set

Check whether the ECS instance under your account is of the specified instance type.

- Rule function name: ecs-desired-instance-type
- Applicable resource type: ACS::ECS::Instance
- According to the rule input parameter: instanceTypes = threshold. The threshold values are a list of ECS instance types separated by commas (,), for example, t2.small, m4.large, i2.xlarge. You must define the threshold value in the console.
- Trigger mechanism: configuration change
- Rule compliance description: all ECS instance types under your account have been listed in the threshold and are considered as "compliance"

- **Rule usage scenario:** you can use this rule to limit the number of ECS instances that can only be purchased under a certain account.

Check whether the ECS disk in connection status is encrypted.

- **Rule function name:** ecs-disk-encrypted
- **Applicable resource type:** ACS::ECS::Disk
- **Rule input parameter:** kmsimds = threshold value. If you do not set the threshold value, the rule only checks whether the disk is encrypted. If you set the threshold value, the rule checks whether the encrypted key Id is within the threshold you set. Separate multiple key IDs with commas (,).
- **Trigger mechanism:** configuration change
- **Rule compliance description:** all disks in the associated status under your account are encrypted. If you set a threshold value, the Id of the disk encryption must exist in the threshold you listed. This is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor the encryption status and encryption compliance of a disk.

Check whether the ECS disk is in use.

- **Rule function name:** ecs-disk-in-use
- **Applicable resource type:** ACS::ECS::Disk
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule compliance description:** all ECS disks under your account are in use and are considered "compliant"
- **Rule usage scenario:** you can use this rule to monitor disk usage.

Check whether the ECS instance is associated with a VPC instance.

- **Rule function name:** ecs-instances-in-vpc
- **Applicable resource type:** ACS::ECS::Instance
- **Rule input parameter:** vpcid = threshold. If you do not set the threshold, the rule only checks whether the ECS instance is associated with a VPC. If you set the threshold, the rule checks whether the VPC associated with the ECS instance is within the threshold you set. The VPC ids. Separate multiple VPC IDs with commas (,).
- **Trigger mechanism:** configuration change

- **Rule compliance description:** all ECS instances under your account are associated with VPCs. If you set a threshold, the associated VpcId must exist in the threshold you listed. This is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor whether all your ECS instances are mounted to a VPC or to a specified VPC.

Check whether the number of GPUs in the ECS instance is below a threshold.

- **Rule function name:** ecs-gpu-min-count-limit
- **Applicable resource type:** ACS::ECS::Instance
- **Rule input parameter:** gpuCount = threshold, gpuCount is the number of GPUs included in the ecs instance, and the threshold must be defined in the console
- **Trigger mechanism:** configuration change
- **Rule Compliance:** the number of GPUs of ecs instances under your account must be greater than or equal to the threshold you set"
- **Rule usage scenario:** you can use this rule to monitor the gpu usage compliance of ecs instances.

Check whether the memory capacity of the ECS instance is less than a threshold value.

- **Rule function name:** ecs-memory-min-size-limit
- **Applicable resource type:** ACS::ECS::Instance
- **Rule input:** memorySize = threshold, memorySize is the memory capacity of the ECS instance, you need to set the threshold on the console
- **Trigger mechanism:** configuration change
- **Rule compliance description:** if the memory capacity of the ECS instances under your account is greater than or equal to the threshold you set, it is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor ECS instance memory size compliance

Checks whether OSS buckets are accessible from the Internet.

- **Rule function name:** oss-bucket-public-acl-check
- **Applicable resource type:** ACS::OSS::Bucket
- **Rule input parameter:** None
- **Trigger mechanism:** Periodical execution

- **Rule compliance description:** OSS buckets under an account are not allowed to access the Internet"
- **Usage scenarios:** you can use this rule to check the internet access status of your OSS Bucket.

Check whether the number of CPUs of an RDS instance is less than a threshold.

- **Rule function name:** rds-cpu-min-count-limit
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** cpuCount = threshold, cpuCount is the number of CPUs of the RDS instance, you need to configure the threshold on the console
- **Trigger mechanism:** configuration change
- **Rule compliance description:** if the number of cpu cores of RDS instances under your account is greater than or equal to the threshold you set, it is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor the RDS instance cpu quantity compliance

Check whether the RDS instance under your account is of the specified instance type.

- **Rule function name:** rds-desired-instance-type
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** instanceTypes = threshold. The threshold values are a list of RDS instance types separated by commas (,), for example, "rds.mysql.s2.large,mysql.n1.micro.1"), you need to define this threshold in the console
- **Trigger mechanism:** configuration change
- **Rule compliance description:** all RDS instance types under your account have been listed in the threshold and are considered as "compliance"
- **Rule usage scenario:** you can use this rule to limit that only a certain type of RDS instances can be purchased under your account.

Check whether the RDS instance has high availability

- **Rule function name:** rds-high-availability-category
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change



- **Rule compliance description:** apsaradb for RDS instances under an account are considered as "compliant" because they have high availability"
- **Rule usage scenario:** you can use this rule to monitor the high availability configuration of RDS instances under your account.

Check whether the ECS instance is associated with a VPC instance.

- **Rule function name:** rds-instances-in-vpc
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** vpcid = threshold. If you do not set the threshold, the rule only checks whether the RDS instance is associated with a VPC. If you set the threshold, the rule checks whether the VPC associated with the RDS instance is within the threshold you set. The VPC ids. Separate multiple VPC IDs with commas (,).
- **Trigger mechanism:** configuration change
- **Rule compliance description:** The RDS instances under your account have been associated with VPCs. If you set the threshold, the associated VpcId must exist in the threshold you listed. This is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor whether all your RDS instances are mounted to a VPC, or whether they are mounted to a specified VPC.

Check whether the storage space of the RDS instance is not less than a threshold value.

- **Rule function name:** rds-instance-storage-min-size-limit
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** storageSize = threshold, storageSize is the storage space of the rds instance, you need to configure the threshold on the console
- **Trigger mechanism:** configuration change
- **Rule compliance description:** if the storage space of an RDS instance under your account is greater than or equal to the threshold you set, it is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor the RDS instance storage space size compliance

Check whether the memory capacity of the RDS instance is not less than a threshold value.

- **Rule function name:** rds-memory-min-size-limit
- **Applicable resource type:** ACS::RDS::DBInstance

- **Rule input:** memorySize = threshold, memorySize is the memory capacity of the RDS instance, you need to configure the threshold on the console
- **Trigger mechanism:** configuration change
- **Rule compliance description:** if the memory capacity of your RDS instances is greater than or equal to the threshold you set, it is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor the RDS instance memory size compliance

Checks whether the RDS instance supports multiple zones.

- **Rule function name:** rds-multi-az-support
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule compliance description:** apsaradb for RDS instances under an account support multiple zones, which is considered as compliance"
- **Rule usage scenario:** you can use this rule to monitor the RDS instance's support for multi-zone compliance

Check whether the RDS instance allows public network access.

- **Rule function name:** rds-public-access-check
- **Applicable resource type:** ACS::RDS::DBInstance
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule compliance description:** apsaradb for RDS instances under the account are considered as "compliant" because they are not allowed to access the Internet"
- **Rule usage scenario:** you can use this rule to monitor the public network access compliance of RDS instances

Check whether the specified resource has the specified tag.

- **Rule function name:** required-tags
- **Applicable resource types:** ACS::RDS::DBInstance; ACS::SLB::LoadBalancer; ACS::ECS::Disk; ACS::ECS::SecurityGroup; ACS::ECS::Instance; ACS::ECS::NetworkInterface
- **Rule input parameters:** tag1Key, specify the Key of the tag; tag1Value, specify the value of the tag.

- **Trigger mechanism:** configuration change
- **Rule compliance description:** all object resources under the associated resource type have specified tags, which are considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor whether your resources are tagged completely.

Check whether the security group is configured as 0.0.0.0/0.

- **Rule function name:** sg-public-accept-check
- **Applicable resource type:** ACS::ECS::SecurityGroup
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule compliance description:** the configuration of the ECS Security Group under the account is not "0.0.0.0/0", it is considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor whether the ECS Security Group is valid.

Check whether HTTPS listening is enabled for SLB

- **Rule function name:** slb-listener-https-enabled
- **Applicable resource type:** ACS::SLB::LoadBalancer
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule Compliance:** HTTPS listening is considered compliance"
- **Rule usage scenario:** you can use this rule to monitor the listener compliance

Check whether the EIP is bound to an ECS or SLB instance.

- **Rule function name:** eip-attached
- **Applicable resource type:** ACS::VPC::EipAddress
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule compliance description:** EIPs that are associated with ECS or SLB instances are considered as "compliance"
- **Rule usage scenario:** you can use this rule to monitor the effective status of an EIP.

Check whether the ECS instance is bound to a public Ip address.

- **Rule function name:** ecs-instance-no-public-ip
- **Applicable resource type:** ACS::ECS::Instance
- **Rule input parameter:** None
- **Trigger mechanism:** configuration change
- **Rule compliance description:** if an ECS instance is not directly bound to a public IP address, it is considered as "compliance ". This rule applies only to IPv4
- **Rule usage scenario:** you can use this rule to monitor the public network access compliance of ECS

## 4.3 Develop custom rules



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

**To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.**

Configure the audit service to provide you with dozens of preset rules. For more information, see [List of preset rules](#). You can also customize rules.

A custom rule runs in the same way as a predefined rule. The only difference is that the system preset rule is that the audit service has already built the rule function in function compute, you can directly select the function to be used in the configuration audit console. However, to customize rules, you must define rules in

function compute in advance, you need to enter the ARN of the rule function in the configuration audit console.

With custom rules, you can better support personalized compliance scenarios.

#### Create a custom rule

There are two steps. The first step is to create a function in function compute. The second step is to create a rule in configure audit service, just like preset rules. This article focuses on step 1. For step 2, see [Create a rule](#).

To create a custom rule, you must first create a function in the function compute console. Currently, function compute supports the following programming languages: Java8, Nodejs6, Nodejs8, Python2.7, Python3, PHP7.2, and dotnetcore2.1. Java 8 and dotnetcore support code package Upload (including oss upload). Other languages support code package Upload and online editing. For more information about function compute, see [Function Compute](#).

The following example shows how to customize a rule.

- Rule scenario: evaluate whether an ECS instance is started by a specific image
- Function languages use Python3

Create a rule function in function compute and reference it in configuration audit.

For more information about how to create function compute, see [Function Compute](#).

- After a rule function is created in function compute, an ARN function is automatically generated. The function ARN can be viewed on the overview page of the created function compute.

← demo Service Version: LATEST

Overview Code Triggers Log Function Metrics ARN - acs:fc:cn-shanghai:1208863178612953:services/ConfigDynamicRule.LATEST/function...

**Usage**

Resource Usage (This Month) 0 Times

Resource Usage (This Month) 0 CU-S

Usage data is updated hourly. For detailed usage report, go to [Billing Center](#).

**Function Properties** Configure Export

Function Name demo Region cn-shanghai

Code Size (Bytes) 1863 Byte Created Time Oct 8, 2019 1:57 PM

Last Modified Time Oct 8, 2019 3:19 PM Function Handler index.handler

Runtime python3 Memory 128 MB

Timeout 60 seconds Instance Concurrency 1

Code Checksum 8524551970455919842

- To reference the rule function in the configure audit service console, enter the ARN in the preceding figure.

← Create Rule

**Basic Information**

\* Rule Name

A rule name must start with a letter. It can contain letters and special characters such as en dash (-).

Description

\* Function ARN

[Create New Function](#)

After you have created a new function in Function Compute, you can view the function ARN in the function details.

**Monitoring Settings**

\* Trigger Type

☐ Configuration Changes ☐ Periodic

\* Select related resources.

## Rule Function Code construction

**The essence of a rule is a piece of logic judgment code, which is placed in the rule function you just created. In an actual continuous audit, the rule function is triggered to make an assessment.**

- **The following is the sample code of the rule. The code of this function mainly consists of two functions. handler is the entry function, that is, the function called When custom compliance is triggered. The handler must be configured when the function is being built.**

The screenshot displays the configuration interface for a function in the CloudConfig console. At the top, it shows 'Code Size (Bytes)' as 1.82 KB and 'Created Time' as Oct 8, 2019 1:57 PM. Below these are several configuration fields, each with a red asterisk indicating it is required:

- \* Function Handler:** A text input field containing 'index.handler'.
- \* Runtime:** A dropdown menu with 'python3' selected.
- \* Memory:** A dropdown menu with '128MB' selected.
- \* Timeout:** A text input field with '60' and a unit selector set to 'seconds'.
- \* Instance Concurrency:** A text input field with '1'. To its right is a help icon (?). Below this field, a message states: 'The python3 runtime environment does not support this feature.'
- Enable initializer:** A toggle switch that is currently turned off. Below it, the text 'Recommended' is displayed.
- Function Description:** A large text area with the placeholder text 'Enter the function description.'

- **The other function is put\_evaluations, which is called in the handler and returns the compliance result.**

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
'''
@ File: index.py
@ Time: 18:19:00
@ Author: wb510457
# Version: 1.0
@ License: (C) Copyright 2017-2018, Alibaba inc.
@ Desc: None
'''
```

```

# Put the import lib here
import logging
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkcore.request import CommonRequest

root = logging.getLogger()

# Function handler
Def handler (event, context ):
    """
    Processing functions
    : Param event: event
    : Param context: context
    : Return: assessment result
    """
    # Event data format conversion
    Evt = json. loads (event)
    If not evt:
        return None

# Input parameters
Rule_parameters = evt. get ('ruleparameters ')
# Input parameter -- image instance id
Image_id = rule_parameters.get (imageIds)
# Callback in function compute
Result_token = evt. get ('resulttoken ')
# Function execution parameter information
Blocking_event = evt. get ('blockingevent ')

# Initialize the return value.
Compliance_type = 'not _ applicable'
Annotation = None

# Obtain configuration items
Operation_item = updateking_event.get ('operationitem ')
If not operation_item:
    Logger. error ('configuration item is empty .')
    return None
# Assessment
If image_id in configuration_item
    Compliance_type = 'compute'
If not image_id in configuration_item
    Compliance_type = 'non _ compute'
# Start time of command execution
Ordering_timestamp = operation_item.get ('capturetime ')
# Resource id
Instance_id = destination_item.get ('instanceid ')
# Resource type
Instance_type = destination_item.get ('instancetype ')

# Evaluation results
Evicted = [
    {
        'Complanceresourceid': instance_id,
        'Complanceresourcetype ': instance_type,
        'Orderingtimestamp': ordering_timestamp,
        'Complancetype': compliance_type,
        'Annotation': annotation
    }
]

```



```

# Write back the evaluation result-write the evaluation result
data
    Put_evaluators (context, result_token, evaluators)
    Return evisibility
# Write back the evaluation result-write the evaluation result data
Def put_evaluations (context, result_token, evaluations ):
    """
    Callback Config Open API write back Evaluation Results
    : Param context: function compute context
    : Param result_token: the callback token.
    : Param evisibility: evaluation result
    : Return: None
    """
    # Create an AcsClient instance
    client = AcsClient(
        Context. credentials. access_key_id,
        Context. credentials. access_key_secret,
        Context. region,
    )

    # Create a request, and set required parameters.
    request = CommonRequest()
    Request. set_domain ('config domain ')
    request.set_version('2015-12-15')
    Request. set_action_name ('putevalue ')
    Request. add_body_params ('resulttoken', result_token)
    Request. add_body_params ('evaluate', evaluate)
    Request. set_method ('post ')

    try:
        response = client.do_action_with_exception(request)
        Logger.info ('putevaluedwith request: % s, response: % s' %
                      (Request, response ))
    except Exception as e:
        Logger. error ('putevaluederror: % s' % e)

```

Input parameters of a rule function

**Event parameter.** The input parameter information entered in the rule function is saved in the rule parameters, and other content is the event information automatically generated when the rule is triggered. The JSON format is as follows:

```

{
  version: "version ",
  orderingTimestamp: "command execution start time ",
  invokingEvent:{
    messageType: "Message Type ",
    configurationItem: {
      "accountId": "User ID ",
      "arn": "resource ARN ",
      "availabilityzone": "Available zone ",
      "regionId": "region id ",
      "configuration": "configuration information of resources
in string format, which varies with resources ",
      "configurationDiff": "configuration change content ",
      "relationship": "relationship ",
      "relationshipDiff": "Relationship content change ",
      "captureTime": "capture time ",
      "resourceCreationTime": "resource creation time ",
      "resourceStatus": "resource status ",

```

```

        "resourceId": "resource ID ",
        "resourceName": "Resource Name ",
        "resourceType": "c4",
        "supplementaryConfiguration": "supplemental configuration
",
        "tags": "tags"
    },
    notificationCreationTimestamp: "event message generation time"
},
ruleParameters: {
    {"key": "value"}
},
resultToken: "callback information of the user in function compute
"
}

```

**Context parameter.** The context information, which is automatically included when the rule is triggered.

- **context.credentials.access\_key\_id:** "accessKey value"
- **context.credentials.access\_key\_secret:** "accessSecret value"
- **context.region:** "region information"

After creating a custom rule in function compute, you can copy the ARN of the function and create the rule again after configuring the audit service.

## 4.4 Manage rules

### 4.4.1 Rule list



#### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. **HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.***

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

In the left-side navigation pane, click [Rule Management](#).

The first time you enter the page list is empty, after you have created a rule, you can see all your rules in this list. You can filter data based on the compliance status or running status of rules.

On the rule list page, you can view the basic information of the rule, including the "compliance assessment status" and "rule status".

#### Compliance Assessment

This column indicates the current execution status of the rule. It has four statuses:

Status value	Description
Regulatory compliance	Indicates that the historical evaluation results of this rule are "compliant".
Resource non-compliance (N)	It indicates that N resources in the historical evaluation of this rule are not compliant. Go to the rule details page to check which resources are not compliant.
Insufficient Data	It indicates that the rule has not been triggered yet, and therefore it cannot be judged whether it is compliant or not.
N/A	This status has a wide range. It means that the rule has been triggered and executed, but the configuration audit has not obtained the expected evaluation results. It can be considered as a mark indicating that the rule execution is abnormal.

#### Rule status

This column indicates the running status of the rule itself. There are five statuses:

Status value	Description
Application in progress	Indicates that the rule is currently listening and will be evaluated once the related configuration changes occur. If you want to retain the rule configuration while suspending the compliance audit , you can find the corresponding rule entry behind the rule entry on the rule management list page, choose More> stop rule to change the status of the rule to disabled.
Assessment in progress	Indicates that the rule has been triggered and is being evaluated.
Deleting evaluation results	With audit, you can delete the evaluation results of a rule so that you can clear test data before the formal compliance monitoring starts.
Disabled	Indicates that the rule is currently in the stopped listening state. Although the rule configuration still exists , it will never be triggered. On the rule management list page, find the corresponding rule entry and click More > Enable rule to re-enter the "application" status.
The instance is being deleted.	Indicates that the rule has been deleted and is being deleted.

#### 4.4.2 Create a rule



##### Warning:

*An official English-language version of the documentation is not available. For your convenience only , we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT,*

*INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

Rules are the logic judgment codes placed in functions of function compute. You can reference the preset rules prepared by configuration audit. For more information, see [List of preset rules](#). You can also customize rule functions in function Compute. For more information, see [Develop custom rules](#). You can also submit your requirements to us by submitting a ticket. After the assessment, you can implement pre-configured rules.

In [Rule Management](#) Page, click "Create rule ":

1. Select a rule creation method: you can select a system-preset rule or "custom rule ". Note: If you select custom rules, enter the name of the rule function that you have configured in function compute in the next step.
2. Basic information: you need to set a readable name for the rule, fill in the " remarks" that is, the description content, and then fill in the name of the rule function. ( (If rules are preset for the system, the function name is pre-filled .)
3. Trigger mechanism: Select the trigger method of the rule. Real-Time configuration change triggering and periodic execution are supported. When the configuration audit service detects a configuration change of the resource type associated with the rule and the actual content of the change is associated with the input parameters of the rule, the rule is triggered. Currently, rules can be periodically executed every 1, 3, 6, 12, and 24 hours.
4. Monitoring scope: configure the resource type associated with the rule. The rule will listen to all physical resources of this resource type under your account. A rule can be associated with multiple resource types.
5. Rule parameters: If you select a predefined rule, you must set a threshold value for the predefined rule parameters. If you select custom rules, you must set the Key and threshold of the rule input parameters. Note that the Key of a rule parameter is the input parameter name of the rule function. The input parameter name must be consistent with the actual configuration name of the resource.

6. Click OK. The rule is created and in the "application" state ".

### 4.4.3 Modify and delete a rule



#### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

This topic describes how to manage rules.

Modify/stop/start/manually evaluate/delete a rule

- **Rule modification:** Similar to rule creation, you can modify the basic information and running information of the rule. When you change a rule, the rule is executed according to the original configuration. After you save the changes, the rule is run with the new configuration.
- **Stop rule:** if you want to retain the rule configuration while suspending the compliance audit, you can find the action column next to the rule entry on the rule management list page, choose More> stop rule to change the status of the rule to disabled.
- **Start rule:** you can find the action column after the rule entry on the rule management list page, choose More> enable rules to re-enter the "applying" status.
- **Manual evaluation:** you can click re-evaluation in the upper-right corner of the rule list, re-evaluate in the upper-right corner of the rule details page, and click, perform a manual assessment of one or more rules at three locations.

- **Delete evaluation results:** configuration audit allows you to delete the evaluation results of a rule so that you can clear test data before the formal compliance monitoring starts. You can operate in the upper-right corner of "associated resources list" under Rule details.
- **Delete rule:** you must disable the rule before deleting it. The rule configuration will not be retained after deletion.

#### 4.4.4 View rule details



##### **Warning:**

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

**To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.**

**The details of a rule include the following information.**

##### Rule details

**Click details next to a rule on the rule list page to view all information about this rule.**

##### Rule evaluation statistics

**At the top of the rule details page, an overview of the rule execution is displayed: ( the "number of resources" in the statistics refers to the actual physical resources, not the number of resource types .)**

Data Item	Description
The total number of audit resources.	The number of resources that have been evaluated since the rule was enabled. Including the resources that you have released.
Number of currently associated resources	The number of resources under the currently associated account does not include the resources that have been released.
Number of compliant resources	The number of resources that were last evaluated as "compliant" in the current associated resources.
Number of non-compliant resources	The number of resources that were last evaluated as "non-compliant" in the associated resources.

#### Basic rule information

- The resource name, creation time, last evaluation time, and other basic information are not listed one by one, subject to the page content.
- Resource trigger mechanism, monitoring scope, and other operational configurations.

The list of resources currently associated with the rule.

The monitoring scope of a rule is based on the resource type. This list is a list of resource entities. For example, if a rule is associated with an ECS instance and there are 20 ECS instances under this account, the list contains 20 ECS instances.

This list displays the Id of the object resource and the last evaluation result. You can also quickly jump to the corresponding configuration timeline and compliance timeline of the resource through the quick operation to view the resource details. You can also quickly jump to the cloud product console, manage resources.

## 4.5 View compliance results

### 4.5.1 View rule assessment results



**Warning:**



*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.*

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

Currently [Configure the audit console](#), You can view the execution status of the rule in three aspects:

- [Overview page](#) Compliance statistics on the right-side bar ". Rules: Number of nonconforming rules/Number of compliant rules; resources: Number of nonconforming resources/Number of compliant resources.
- [Rule Management](#) The list page displays the current "compliance assessment" for each rule. For more information, see [Rule list](#) for an interpretation of compliance assessment.
- The evaluation statistics of the rule are displayed at the top of the rule details page. For more information, see [View rule details](#).

## 4.5.2 Resource compliance timeline



### Warning:

*An official English-language version of the documentation is not available. For your convenience only, we have introduced the use of machine-translation software capable of producing rough translations in various languages, including English. This machine-translated version of the documentation was produced using only machine-translation software and without any human intervention. We are making continuous efforts to improve the machine-translation software. HOWEVER, MACHINE TRANSLATIONS MAY CONTAIN ERRORS. ANY RELIANCE BY YOU UPON THIS MACHINE*

***TRANSLATION IS SOLELY AT YOUR OWN RISK, AND ALIBABA CLOUD SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTIES FOR ANY ADVERSE CONSEQUENCES (DIRECT, INDIRECT, CONSEQUENTIAL OR OTHERWISE) ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR ANY TRANSLATIONS THEREOF.***

To request a human-translated version of this article or to comment on the quality of machine translation, please use the "More suggestions" text area in the feedback form below to submit feedback.

In the configuration audit service, each resource entity has its own compliance timeline records. When a resource is evaluated by rules, a compliance assessment record is generated, and continuous compliance assessment forms a resource compliance timeline.

Point of compliance time line

- **Start point:** the time when the resource is evaluated by the rule for the first time . The time when the resource is evaluated by the rule may be the scheduled cycle evaluation, manual evaluation, or real-time configuration change trigger evaluation.
- **Node:** each rule assessment will form a node on the compliance time line, and each assessment may involve one or more rules.
- **Breakpoint:** Different from resource configuration timeline ([View the resource configuration timeline](#)), rule assessment is triggered based on real-time configuration changes. Since there is no continuity, there is no breakpoint.

Content of the compliant timeline

- The compliance timeline belongs to a specific resource entity and is a set of historical compliance assessment records.
- On the left side of the compliance timeline, in addition to the time, each node also clearly shows the triggering mechanism of the compliance assessment. This also shows the reason why resources are assessed, the options include manual execution, periodical execution, and change triggering.
- On the left side of the compliance timeline, each node also marks the evaluation result "compliance" or "non-compliance ". This allows you to quickly find the nodes that need attention.
- The details of each node include basic resource information and the list of associated rules (rules and evaluation results). If an evaluation is triggered by a

**real-time change, the details of this change will also be displayed, so that you can locate the "non-compliance" specific configuration as soon as possible.**

**You can check the preceding information online or download it to your OSS bucket through APIs to facilitate offline integrated analysis. The OpenAPI and snapshot download capabilities are undergoing rapid iteration, so stay tuned.**

## 5 Preset rules

---

### 5.1 ActionTrail

**The following rule indicates: Check whether ActionTrail is enabled in your configuration audit account.**

actiontrail-enabled

**Trigger type:** configuration change

**Resource:** ACS::ActionTrail::Trail

**Request parameters:** none

**Solution:** When a trail is disabled, the rule is not compliant. Open the trail enable logging switch. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** Enter the console, click Trail list, and click the name of the target trail enable logging switch.

**API operation:** call [#unique\\_30](#) interface to open the enable logging switch.

### 5.2 Alibaba Cloud CDN

**Checks whether HTTPS is enabled for the CDN domain name. If HTTPS is enabled, it is considered compliance.**

cdn-domain-https-enabled

**Trigger type:** configuration change

**Resource:** ACS::CDN::Domain

**Request parameters:** none

**Solution:** When HTTPS is not enabled for the CDN domain name under your account, this rule is not compliant. Open `Https secure accelerationSwitch`. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** Select Domain name > Management > Https configuration > Secure acceleration.

## 5.3 DDH

### ddh-cpu-min-count-limit

**If the number of VCPUs of an Alibaba Cloud DDH instance under your account is greater than or equal to the threshold you set, the ECS instance is deemed to be compliant.**

**Trigger type:** configuration change

**Resource:** ACS:: ECS:: DedicatedHost

**Request parameters:**

**CpuCount** (number of CPU cores)

**Solution:** when the total CPU usage of the DDH instance under your account is smaller than the threshold value you set, the rule is not compliant.

- **Method 1:** After a DDH is created, you cannot change its specification. You need to create a DDH that meets the rules. Config detects your changes within 10 minutes and automatically starts the audit.

**Solution to non-compliant old ddhs:** Release the DDH (only pay-as-you-go ddhs are supported). You cannot manually release a subscription DDH.

**Risk:** After a DDH is released, all its resources are no longer available. All data on ECS instances on a DDH is lost and cannot be recovered. You can migrate ECS instances between ddhs of your account before the DDH is released.

To migrate ECS instances between different ddhs, see [#unique\\_33](#).

- **Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

**View the CPU size when you create a host in the console:**

### ddh-memory-min-size-limit

**If the memory capacity of an Alibaba Cloud DDH instance under your account is greater than or equal to the threshold you set, it is deemed as compliance.**

**Trigger type:** configuration change

**Resource:** ACS::ECS::DedicatedHost

**Request parameters:**

**memorySize** (memory size/GB)

**Troubleshooting:** when the memory capacity of the DDH instance under your account is smaller than the threshold value you set, the rule is not compliant.

- **Method 1:** After a DDH is created, you cannot change its specification. Instead, you can create a DDH that meets the rules. Config detects your changes within 10 minutes and automatically starts the audit.

To troubleshoot an invalid DDH, release the DDH. ( Only pay-as-you-go ddhs are supported. You cannot manually release a subscription DDH.

**Risk:** After a DDH is released, all its resources are no longer available. All data on ECS instances on a DDH is lost and cannot be recovered.

You can migrate ECS instances between ddhs of your account before the DDH is released.

To migrate ECS instances between different ddhs, see [#unique\\_33](#).

- **Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

You can view the memory size when creating a DDH in the console as follows:

ddh-socket-min-count-limit

If the physical CPU of an Alibaba Cloud DDH instance under your account is equal to the threshold you set, it is considered compliance.

**Trigger type:** configuration change

**Resource:** ACS::ECS::DedicatedHost

**Request parameters:**

**socketCount** (physical CPU cores)

**Solution:** when the number of sockets in the DDH instance under your account is smaller than the threshold that you set, the rule is not compliant.

- **Method 1:** After a DDH is created, you cannot change its specification. Instead, you can create a DDH that meets the rules. Config detects your changes within 10 minutes and automatically starts the audit.

To troubleshoot an invalid DDH, release the DDH. ( Only pay-as-you-go ddhs are supported. You cannot manually release a subscription DDH.

**Risk:** After a DDH is released, all its resources are no longer available. All data on ECS instances on a DDH is lost and cannot be recovered.

You can migrate ECS instances between ddhs of your account before the DDH is released.

To migrate ECS instances between different ddhs, see [#unique\\_33](#).

- **Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

For more information about the number of sockets on a DDH, see:

## 5.4 ECS

ecs-cpu-min-count-limit

**Check the minimum number of CPUs for ECS instances.**

**Trigger type:** configuration change

**Resource:** ACS::ECS::Instance

**Request parameters:**

- **cpuCount**
- **Minimum number of CPUs for an ECS instance**

**Troubleshooting Guide:**

When the number of CPUs of the ECS instances under your account is smaller than the threshold that you set, the rule is not compliant.

**Method 1:** Change the ECS instance type. You can change the instance type only for stopped instances. Make sure that the number of CPUs of the new ECS instance is greater than or equal to the threshold you set. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

**Change the instance type in the console:**

**ModifyInstanceSpec:** call `ModifyInstanceSpec` to modify the value of `InstanceType`.

ecs-desired-instance-type

**Check whether the ECS instance has the specified instance type.**

**Resource:** `ACS::ECS::Instance`

**Trigger type:** configuration change

**Parameter:** `instanceTypes`

The list of ECS instance types separated by commas (,), such as `t2.small`, `m4.large`, and `i2.xlarge`.

**Troubleshooting Guide:**

The ECS instance type family under your account is not listed in the rule parameter threshold, it will cause the rule to be non-compliant. The rule parameter threshold list contains the instance types of the ECS instances, which are compliant.

**Method 1:** Change the ECS instance type to one of the instance types listed in the rule parameter threshold. Only stopped instances can be changed. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** Edit the rule parameter threshold and add the instance type of the ECS instance to the rule parameter threshold. Edit the content and click re-audit. Then, refresh the page for verification.

**Change the instance type in the console:**

**API to change the instance type:**

You can call this operation to modify the value of `InstanceType`.



## ecs-disk-encrypted

**Check whether the connected disk is encrypted. If you specify the KMS key ID for encryption by using the kmsKeyId parameter, this rule checks whether the disks in the connection status use the KMS key for encryption.**

**Resource:** ACS::ECS::Disk

**Trigger type:** configuration change

**Request parameters:**

**kmsIds**

**The ID of the KMS key used to encrypt the volume.**

**Troubleshooting Guide:**

- 1. If all cloud disks in the associated status under your account are not encrypted, this rule will be nonconforming.**
- 2. If the KMSKeyId of the encrypted cloud disk does not exist in the rule parameter threshold you listed, the rule is invalid.**

**The KMSKeyId of the encrypted cloud disk is included in the rule parameter threshold, which means the cloud disk is compliant. Currently, the disk encryption function only supports data disks. The solution is only applicable to data disks.**

**Method 1: re-create an encrypted cloud disk and encrypt it with the KMSKeyId listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.**

**Solution to non-compliant cloud disks: Release the cloud disks.**

**Risk: releasing a cloud disk may cause data loss.**

**For more information about how to release a cloud disk, see [#unique\\_35](#).**

**Method 2: Add the KMSKeyId of the encrypted cloud disk to the rule parameter threshold, click re-audit, and refresh the page for verification.**

## ecs-disk-in-use

**Check whether the disk is in use.**

**Resource:** ACS::ECS::Disk

**Trigger type:** configuration change

**Request parameters:** none

**Repair Guide:** If the ECS cloud disk under your account is in the not attached state, this rule is not compliant. Attach a cloud disk to an instance to change its status to In Use to be compliant.

**Console operation:** go to the cloud disk console, go to the cloud disk list, click More > Mount Attach a cloud disk to an instance.

**API operation:** call AttachDisk to attach a pay-as-you-go data disk to an ECS instance .

**Compliance verification method:** the Config will detect your changes within 10 minutes and automatically start the audit.

ecs-gpu-min-count-limit

**Check the minimum number of CPUs for ECS instances.**

**Trigger type:** configuration change

**Resource:** ACS::ECS::Instance

**Request parameters:**

**gpuCount**

The minimum number of CPUs for a gsc instance.

**Troubleshooting Guide:**

When the number of GPUs in your ECS instance is smaller than the threshold you set, this rule is not compliant.

**Method 1:** Change the ECS instance type (you can change the instance type only when the instance is stopped). Make sure that the number of GPUs in the ECS instance after modification is greater than or equal to the threshold value you set. Config detects your changes within 10 minutes and automatically starts the audit.

You cannot change the instance type of an instance that contains local storage.

If the non-compliant instance is a local storage instance, you need to re-purchase an ECS instance that meets the requirements of the rules.

**Processing of old ECS instances that do not comply with regulations:** release ECS instances (only pay-as-you-go ECS instances are supported). For a subscription

instance, you can manually release it after its billing cycle expires. If it is not renewed, the instance is automatically released. Before an instance expires, you can apply for a refund to release the instance in advance. You can also change the billing method to pay-as-you-go before releasing the instance.

**Risk:** All data will be lost after an ECS instance is released. Back up the data before release.

For more information about instance release risks and procedures, see [#unique\\_36](#).

**Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

**Change the instance type in the console:**

**API:** call `ModifyInstanceSpec` to modify the value of `InstanceType`.

ecs-instance-attached-security-group

**Checks whether an ECS instance is attached to a specific security group. Enabled ECS instances are considered compliance.**

**Trigger type:** configuration change

**Resource:** ACS::ECS::Instance

**Request parameters:**

**securityGroupIds**

The IDs of security groups separated by commas (,), such as sg-hp3ebbv7irjeg1 and sg-hp3ebbv7irj.

**Troubleshooting Guide:**

If the Id of the security group to which the ECS instances belong is not listed in the rule parameter threshold, the rule is invalid. The rule parameter threshold list contains the Id of any security group to which the instance is added.

**Method 1:** Add the ECS instances to the security group listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** add the security group Id that an ECS instance joins to the rule parameter threshold, click re-audit, and then refresh the page for verification.

**Console operation-bind instances and security groups:**

**Method 1:** go to Security group managementPage, in the Security GroupTab, click Join a security group.

**Method 2:** go to Security group managementPage, in the List of instances in a security groupTab, click Add an instance.

**API operation:**

**Bind instance with security group:** You can call JoinSecurityGroup to add an ECS instance to a specified security group.

ecs-instance-deletion-protection-enabled

**Check whether release protection is enabled for your ECS instances (only pay-as-you-go payment is supported). Enabled release protection is considered compliance .**

**Trigger type:** configuration change

**Resource:** ecs-instances-in-vpc

**Request parameters:** none

**Troubleshooting Guide:**

**Check whether release protection is enabled for your ECS instances (only pay-as-you-go is supported). Otherwise, this rule is not applicable.**

**Console operation:**

**Log on to the ECS console, choose more> instance settings> modify instance attributes, and select enable instance release protection. Config detects your changes within 10 minutes and automatically starts the audit.**

**API operation:**

**You can call the ModifyInstanceAttribute operation to set DeletionProtection to true.**

**Compliance verification method:**

After the window period, return to configuration audit-rule details and click re-audit to verify or view the audit results after the rule is automatically triggered.

ecs-instances-in-vpc

Check whether your ECS instance belongs to a Virtual Private Cloud (VPC). You can also specify the ID of the VPC to be associated with your instance. If an ECS instance belongs to a VPC with a specified ID, the return value is compliant. If an ECS instance does not belong to a VPC with a specified ID, the return value is not compliant. If an ECS instance does not have VPC information, the return value is not applicable.

Trigger type: configuration change

Resource: ACS::ECS::Instance

Parameter: vpcIds.

The ID of the VPC that contains these instances. Separate multiple VPC IDs with commas (,), for example, vpc-25vk5xwn8,vpc-6wesmaymqkgiuru5xmkvx,vpc-8vbc16loavvujlzi1yc8

Troubleshooting Guide:

If the VpcId of the ECS instance bound to your account is not listed in the rule parameter threshold, the rule is invalid.

Method 1: create a new ECS instance and bind the instance to one of the VpcId listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.

Processing of old ECS instances that do not comply with regulations: release ECS instances (only pay-as-you-go ECS instances are supported). For a subscription instance, you can manually release it after its billing cycle expires. If it is not renewed, the instance is automatically released. Before an instance expires, you can apply for a refund to release the instance in advance. You can also change the billing method to pay-as-you-go before releasing the instance.

Risk: All data will be lost after an ECS instance is released. Back up the data before release.

For more information about instance release risks and procedures, see [#unique\\_36](#).

**When you purchase an ECS instance, select VPC in network and security group-network.**

**Method 2: Edit the rule parameter threshold and add the VpcId bound to the ECS instance to the rule parameter threshold. Edit the content and click re-audit. Then, refresh the page for verification.**

ecs-instance-no-public-ip

**An ECS instance is deemed to be "compliant" if it is not directly bound to a public IP address. This rule applies only to IPv4.**

**Trigger type: configuration change**

**Resource: ACS::ECS::Instance**

**Request parameters: none**

**If the ECS instance under your account is bound to a public IP address, this rule is not compliant. If the ECS instance has only a private address, the resource assessment result is compliant.**

**Method 1: unbind the Elastic IP Address from the ECS instance if it is bound to a Elastic IP Address. Config detects your changes within 10 minutes and automatically starts the audit.**

**Method 2: If the ECS instance is bound with a public IP address, convert the public IP address to a Elastic IP Address, and unbind the Elastic IP Address. Config detects your changes within 10 minutes and automatically starts the audit.**

**Method 3: purchase a new ECS instance, and do not select allocate public ipv4 address in the network and security group. Config detects your changes within 10 minutes and automatically starts the audit.**

**Processing of old ECS instances that do not comply with regulations: release ECS instances (only pay-as-you-go ECS instances are supported). For a subscription instance, you can manually release it after its billing cycle expires. If it is not renewed, the instance is automatically released. Before an instance expires, you**

can apply for a refund to release the instance in advance. You can also change the billing method to pay-as-you-go before releasing the instance.

**Risk:** All data will be lost after an ECS instance is released. Back up the data before release.

For more information about instance release risks and procedures, see [#unique\\_36](#).

#### ecs-memory-min-size-limit

This metric checks the minimum memory capacity of an ECS instance.

**Trigger type:** configuration change

**Resource:** ACS::ECS::Instance

**Request parameters:**

**MemorySize** (minimum memory capacity of the ecs instance)

**Troubleshooting Guide:**

When the memory capacity of the ECS instances under your account is smaller than the threshold value specified by the rule, the rule is not compliant.

**Method 1:** Change the ECS instance type. You can change the instance type only for stopped instances. Make sure that the number of CPUs of the new ECS instance is greater than or equal to the threshold you set. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

**Change the instance type in the console:**

**ModifyInstanceSpec:** call ModifyInstanceSpec to modify the value of InstanceType.

#### sg-public-access-check

**Check whether the security group matches 0.0.0.0/0.**

**Trigger type:** configuration change

**Resource:** ACS::ECS::SecurityGroup

**Request parameters:** none

**Solution:** When an ECS Security Group rule is in the inbound direction, the authorization policy is "allow", and the authorized object is "0.0.0.0/0", this rule is not compliant.

**Method 1:** Change the authorization policy of the inbound rules of the security group whose authorization object is 0.0.0.0/0 to reject or modify the authorization object. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** delete the authorization policy as allow and the authorization object as 0.0.0.0/0 Security Group inbound rules. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:**

**Modify authorization policies and modify authorization objects:** log on to the security group console, edit security group rules-set authorization policies to block or modify authorization objects.

**Delete a security group rule:** log on to the security groups console. Choose security group rules> inbound. Delete the rule whose authorization policy is set to allow and whose authorization object is 0.0.0.0/0.

**API operation:**

- Modifies the values of the Policy (access permission) or SourceCidrIp (authorized object) of the inbound rules of a security group.
- Deletes an inbound rule from a security group.

sg-risky-ports-check

**This metric checks whether the security group has enabled risky ports.**

**Trigger type:** configuration change

**Resource:** ACS::ECS::SecurityGroup

**Request parameters:**

**Ports (risky ports)**

**Troubleshooting Guide:**



When the port number enabled by the ECS Security Group rule (including outbound and inbound) is in the rule parameter threshold, the rule is invalid. "-1/-1" indicates that no port limit is applied. If "-1/-1" is set in the security group rule, the rule is not applicable.

**Method 1:** disable the ports listed in the rule parameter threshold in the ECS Security Group rule, that is, set the corresponding port authorization policy to deny . Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** delete the security group rules that are enabled with the ports listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 3:** modify the port range of the security group rule. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 4:** Edit the rule parameter threshold and delete the corresponding port number from the threshold. Click re-audit and refresh the page for verification.

**Console operation:**

Log on to the security groups console, edit security group rules-set authorization policy to reject or modify the port range

**Delete security group rules:** log on to the security group console and choose security group rules from the left-side navigation pane. Delete the security group rules with the Ports specified in the rule parameter threshold enabled.

**API operation:**

- You can call this operation to modify the security group rule. Modify the Policy (access permission) or PortRange (Port range) values.
- Call `RevokeSecurityGroup` and `RevokeSecurityGroupEgress` to delete a security group rule.

## 5.5 EIP

eip\_attached

You can use this rule to monitor the effectiveness of Elastic IP Address.

**Trigger type:** configuration change

**Resource:** ACS::EIP::EipAddress

**Request parameters:** none

**Troubleshooting:** Check whether your Elastic IP Address is bound to an instance. If it is not bound to an instance, this rule may be nonconforming. Bind a Elastic IP Address to an instance. The instance types include NAT Gateway, ECS instances, SLB instances, and secondary ENIs. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** go to the Elastic IP Address console and choose Operations> bind.

**API operation:** call AssociateEipAddress to bind a Elastic IP Address to a cloud product instance in the same region.

## 5.6 OSS

oss-bucket-public-read-prohibited

Check whether your OSS bucket does not allow public read access. If an OSS bucket policy or bucket ACL allows the public read permission, the bucket is not compliant .

**Trigger type:** configuration change

**Resource:** ACS::OSS::Bucket

**Request parameters:** none

**Troubleshooting:** Check whether your OSS bucket does not allow public read access . If the ACL of the OSS bucket is set to public-read or public-read-write, this rule is not applicable. Set the OSS bucket ACL to private. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** log on to the OSS bucket console and choose bucket-basic settings to modify the bucket ACL.

**API operation:** you can call PutBucketACL to change the ACL of a Bucket to private.

#### oss-bucket-public-write-prohibited

**Check whether the OSS bucket does not allow public write access. If an OSS bucket policy or bucket ACL allows the public write access permission, the bucket is not compliant.**

**Trigger type: configuration change**

**Resource: ACS::OSS::Bucket**

**Request parameters: none**

**Fix: Check whether your OSS bucket does not allow public write access. If the ACL of the OSS bucket is set to public, this rule is not applicable. Set the OSS bucket ACL to private or public-read. Config detects your changes within 10 minutes and automatically starts the audit.**

**Console operation: log on to the OSS bucket console and choose bucket-basic settings to modify the bucket ACL.**

**API operation: you can call PutBucketACL to modify the ACL of a Bucket by setting the ACL to private or public-read.**

#### oss-bucket-referer-limit

**Check whether the anti-Leech function is enabled for the OSS bucket.**

**Trigger type: configuration change**

**Resource: ACS::OSS::Bucket**

**Request parameters:**

**allowReferers**

**The allowed anti-Leech list. Separate multiple referers with commas (,).**

**Troubleshooting Guide:**

**Scenario 1: The threshold of the rule parameter is not empty. The anti-Leech Referer whitelist configured in the OSS bucket (the whitelist is not empty) is not enabled in the threshold list or anti-LeechEmpty Referer allowedWill cause the rule to be non-compliant.**

**Case 2: The anti-Leech protection function is disabled because the threshold of rule parameters is not empty.** Empty Referer allowed If the Referer whitelist configured for the OSS bucket is empty, the rules are not compliant.

**Case 3: When the threshold of rule parameters is empty, anti-Leech is disabled.** Empty Referer allowed Will cause the rule to be non-compliant.

**Scenario 1:**

**Disable anti-Leech** Empty Referer allowed The referer whitelist values are listed in the rule parameter threshold of allowReferers. Config detects your changes within 10 minutes and automatically starts the audit.

**Scenario 2:**

**Set a referer whitelist and list all whitelist values in the rule parameter threshold of allowReferers.** Config detects your changes within 10 minutes and automatically starts the audit.

**Scenario 3:**

**Enable anti-Leech** Empty Referer allowed. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** Overview-basic settings-settings in anti-Leech

**API operation:** call PutBucketReferer to set the Referer access whitelist and whether to allow empty Referer fields.

oss-bucket-server-side-encryption-enabled

**Check that default encryption is enabled for your OSS bucket.**

**Trigger type:** configuration change

**Resource:** ACS::OSS::Bucket

**Request parameters:** none

**Troubleshooting Guide:**

**Check whether encryption is enabled for the OSS bucket under your account. If encryption is not enabled, this rule is not compliant.**

**Set the server-side encryption of the OSS bucket to AES256 or KMS. Config detects your changes within 10 minutes and automatically starts the audit.**

**Console operation:** log on to the OSS bucket console and choose bucket-basic settings to modify the server-side encryption mode of the bucket.

## 5.7 RAM

ram-user-mfa-check

**This metric checks whether RAM users have enabled MFA secondary logon.**

**Trigger type:** configuration change

**Resource:** ACS::RAM::User

**Request parameters:** none

**Fix:** Check whether RAM users enable MFA secondary logon. Otherwise, this rule is not compliant. On the console logon management page, set MFA to yes. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** Enter the RAM console, choose identities> users to enter the user details, and modify the value of "must enable MFA" in authentication management> console logon management.

**API operation:** Call the UpdateLoginProfile API to modify the logon configuration of the user and set MFABindRequired to true.

## 5.8 RDS

rds-cpu-min-count-limit

**Check the minimum number of CPUs for an RDS instance.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Parameter:** cpuCount (minimum number of CPUs in an RDS instance)

**Solution:** when the number of CPUs of an RDS instance under your account is smaller than the threshold that you set, the rule is not compliant.

**Method 1:** change the RDS instance specification so that the number of CPUs of the RDS instance after the change is greater than or equal to the threshold you set. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

Modify instance specifications by calling the `ModifyDBInstanceSpec` API.

rds-desired-instance-type

**Check whether the RDS instance has the specified instance type.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Parameter:** instanceTypes (list of RDS instance types separated by commas). For example: rds.mysql.s2.large and mysql.n1.micro.1.

**Troubleshooting:** if the RDS instance specifications under your account are not listed in the rule parameter threshold, the rule is not compliant. The rule parameter threshold list contains the instance type of the RDS instance, which is compliant.

**Method 1:** Change the RDS instance type to one of the instance types listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** Edit the rule parameter threshold and add the instance type of the RDS instance to the rule parameter threshold. Edit the content and click re-audit. Then, refresh the page for verification.

**Change the instance type in the RDS console:** log on to the RDS console, choose **more> change configuration** to change the instance type.

Modify instance specifications by calling the `ModifyDBInstanceSpec` API.

rds-high-availability-category

**Check whether the RDS instance has high availability.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Request parameters:** none

**Troubleshooting:** The RDS instances under your account do not have high availability, which causes the rule to be noncompliance.

**Method 1:** If you cannot upgrade the version of an ApsaraDB for RDS instance (instances other than SQL Server), you must purchase a new version. When purchasing an RDS instance, select the RDS instance series as High-availability editionSeries. Config detects your changes within 10 minutes and automatically starts the audit.

**Processing of non-compliant old RDS instances:** you can manually release a pay-as-you-go instance or unsubscribe from a subscription instance. You can log on [Unsubscribe page](#) To cancel the subscription.

After an instance is released, the instance data is immediately cleared. We recommend that you back up your data before you release an instance.

For more information about how to release an instance, see:

1. ApsaraDB RDS for MySQL [#unique\\_41](#)
2. RDS for SQL Server [#unique\\_42](#)
3. RDS for PostgreSQL [#unique\\_43](#)
4. RDS for PPAS [#unique\\_44](#)
5. RDS for MariaDB TX [#unique\\_45](#)

You can upgrade an ApsaraDB RDS for SQL Server instance from Basic Edition to High-availability Edition. During the upgrade, you can also upgrade the SQL Server version. Config detects your changes within 10 minutes and automatically starts the audit.

For more information, see [#unique\\_46](#).

**Console operation:** log on to the console purchase page, click Basic configuration > Series selection.

**Upgrade to SQL Server:** log on to the RDS console. On the basic information page, click Upgrade version.

The following table lists the upgrade rules.

**API operation:** When you call the CreateDBInstance API to create an RDS instance, set the value of Category to deleteavailability (high-availability edition).

rds-instance-enabled-security-ip-list

**Check whether the whitelist function is enabled for the RDS instances under your account. If it is enabled, it is considered compliance.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Request parameters:** none

**Troubleshooting:** if the whitelist of the RDS instances under your account is 0.0.0.0/0, this rule is not compliant. Modify the value of the RDS instance in the whitelist . The value is not 0.0.0.0/0. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** go to the RDS console, go to the RDS instance details page-data security, modify the whitelist value, and cancel the 0.0.0.0/0 setting.

**API operation:** call ModifySecurityIps to modify the values of SecurityIps in the whitelist.

rds-instance-storage-min-size-limit

**Check the minimum storage space limit of the RDS instance.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Parameter:** storageSize (minimum storage space of an RDS instance)

**If the storage space of an RDS instance under your account is smaller than the threshold you set, this rule will be invalid.**



**Method 1:** change the RDS instance specification so that the storage capacity of the RDS instance after the change is greater than or equal to the threshold value you set. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

**Modify instance specifications by calling the ModifyDBInstanceSpec API.**

rds-instances-in-vpc

Check whether your RDS instance belongs to a Virtual Private Cloud (VPC). You can also specify the ID of the VPC to be associated with your instance. The error message returned when the specified instance belongs to the specified vpc.

**Example**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Request parameters:**

**vpcIds**

The ID of the VPC that contains these instances. Separate multiple VPC IDs with commas (,), for example, vpc-25vk5xwn8, vpc-6wesmaymqkgiuru5xmkvx, vpc-8vbc16loavvujlzli1yc8.

**Troubleshooting:** if the VpcId bound to the RDS instance under your account is not listed in the rule parameter threshold, the rule is not compliant.

**Method 1:** create a new RDS instance and bind the instance to one of the VpcId listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.

**When purchasing RDS, select VPC in network and security group-VPC.**

**Method 2:** Edit the rule parameter threshold and add the VpcId bound to the RDS instance to the rule parameter threshold. Edit the content and click re-audit. Then, refresh the page for verification.

## rds-memory-min-size-limit

**This metric checks the minimum memory capacity of an RDS instance.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Parameter:** memorySize (minimum capacity of rds instance content)

**Solution:** when the memory capacity of your RDS instance is smaller than the threshold you set, the rule is not compliant.

**Method 1:** change the RDS instance specification so that the memory capacity of the RDS instance after the change is greater than or equal to the threshold you set. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** modify the threshold of rule parameters, and click re-audit. Then, refresh the page for verification.

To change the instance type, call `ModifyDBInstanceSpec` to change the instance type and change the value of `DBInstanceClass`.

## rds-multi-az-support

**Check whether your RDS instance supports multiple zones.**

**Resource:** ACS::RDS::DBInstance

**Trigger type:** configuration change

**Request parameters:** none

**Troubleshooting:** if the RDS instances under your account do not support multiple zones, this rule is not compliant.

**Method 1:** You can migrate MySQL, SQL Server, and PPAS instances across zones . After the RDS instance zone is migrated, Config detects your changes within 10 minutes and automatically starts the audit.

**For more information about the risks of zone migration and the procedure, see:**

1. ApsaraDB RDS for MySQL: [#unique\\_47](#)
2. RDS for SQL Server: [#unique\\_48](#)
3. RDS for PPAS: [#unique\\_49](#)

**Method 2:** If the RDS instance does not support zone migration, you need to purchase an RDS instance again. When purchasing an RDS instance, select the RDS zone as the multi-zone. Config detects your changes within 10 minutes and automatically starts the audit.

**Processing of non-compliant old RDS instances:** you can manually release a pay-as-you-go instance or unsubscribe from a subscription instance. You can log on [Unsubscribe page](#) To cancel the subscription.

After an instance is released, the instance data is immediately cleared. We recommend that you back up your data before you release an instance.

For more information about how to release an instance, see:

1. ApsaraDB RDS for MySQL: [#unique\\_41](#)
2. RDS for SQL Server: [#unique\\_42](#)
3. RDS for PostgreSQL: [#unique\\_43](#)
4. RDS for PPAS: [#unique\\_44](#)
5. RDS for MariaDB TX: [#unique\\_45](#)

**Console operation:** console purchase page-basic configuration-zone select multi-zone.

**API operation:**

When you call the CreateDBInstance API to create an RDS instance, enter the value of ZoneId in the multi-zone format.

You can call this operation to migrate an instance from one zone to another.

rds-public-access-check

**Checks whether the RDS instance allows public network access.**

**Trigger type:** configuration change

**Resource:** ACS::RDS::DBInstance

**Request parameters:** none

**Troubleshooting:** if the whitelist of the RDS instances under your account is 0.0.0.0/0, this rule is not compliant. Modify the value of the RDS instance in the whitelist

. The value is not 0.0.0.0/0. Config detects your changes within 10 minutes and automatically starts the audit.

**Console operation:** go to the RDS console, go to the RDS instance details page-data security, modify the whitelist value, and cancel the 0.0.0.0/0 setting.

**API operation:** call `ModifySecurityIps` to modify the values of `SecurityIps` in the whitelist.

## 5.9 TAG

required-tags

**Check whether your resource has the specified label.**

**This rule supports the following resource types:**

- ACS::RDS::DBInstance
- ACS::SLB::LoadBalancer
- ACS::ECS::Instance

**Trigger type:** configuration change

**Request parameters:**

**tag1Key** (required tag key)

**tag1Value** (optional value of the required tag)

**Solution:** If the associated resource does not contain all the specified tags in the rule parameter threshold, the resource assessment result is "non-compliance".

**Method 1:** add a tag specified in the rule parameter threshold for the associated resources. Config detects your changes within 10 minutes and automatically starts the audit.

**Method 2:** modify the rule parameter threshold so that the associated resources contain all the tags set by the threshold. Save the settings and click re-audit. Then, refresh the page for verification.

**Console operation:**

**ACS::RDS::DBInstance:** log on to the RDS console and select the edit resource tag.

**ACS::SLB::LoadBalancer:** log on to the server load balancer console and select edit resource tag.

**ACS::ECS::Instance:** go to the Instance console and select edit resource tag.

## 5.10 SLB

slb-delete-protection-enabled

**Check whether release protection is enabled for your SLB instance. Enabled release protection is considered compliance.**

**Trigger type:** configuration change

**Resource:** ACS::SLB::LoadBalancer

**Request parameters:** none

**Check whether release protection is enabled for your SLB instance. If release protection is disabled, this rule is not compliant.**

**Open Delete protection Switch. Config detects your changes within 10 minutes and automatically starts the audit.**

**Console operation:** Enter the server load balancer console, instance management> instance details> basic information, open Delete protection Switch.

**API operation:** Call the SetLoadBalancerDeleteProtection API to set the deletion protection status of the instance and set the DeletionProtection value to on.

slb-listener-https-enabled

**Check whether HTTPS is enabled for the SLB instance.**

**Trigger type:** configuration change

**Resource:** ACS::SLB::LoadBalancer

**Request parameters:** none

**Troubleshooting Guide:**

If HTTPS listening is enabled for an SLB instance, this rule is not compliant.

Configure an HTTPS listener for the server load balancer instance. Config detects your changes within 10 minutes and automatically starts the audit.

Console operation: go to the server load balancer console and configure an HTTPS listener through instance management-Port/health check/backend server configuration or operation-listener configuration wizard. Set the SLB protocol to HTTPS.

API operation: call `CreateLoadBalancerHTTPSListener` to create an HTTPS listener.

slb-loadbalancer-in-vpc

Check whether the SLB instance is associated with the VPC. If you set the threshold, the associated VpcId must exist in the threshold you listed. If no threshold value is set, all VPC-connected instances are compliant.

Trigger type: configuration change

Resource: ACS::SLB::LoadBalancer

Request parameters:

vpcIds

The ID of the VPC that contains these instances. Separate multiple VPC IDs with commas (,), for example, vpc-25vk5xwn8, vpc-6wesmaymqkgiuru5xmkvx, vpc-8vbc16loavvujlzi1yc8.

Troubleshooting: if the VpcId bound to the SLB instance under your account is not listed in the rule parameter threshold, the rule is not compliant.

Method 1: create a new SLB instance and bind the instance to one of the VpcId listed in the rule parameter threshold. Config detects your changes within 10 minutes and automatically starts the audit.

Solution to non-compliant old SLB instances: release SLB instances (only pay-as-you-go SLB instances are supported). You cannot manually release a subscription server load balancer instance. If you need to release a server load balancer instance, open a ticket to apply for a refund. The server load balancer instance can be refunded without reason within five days.

For more information about instance release risks and procedures, see [#unique\\_52](#).

When you purchase an SLB instance, select the VPC listed in the rule parameter threshold in network type.

**Method 2:** Edit the rule parameter threshold and add the VpcId bound to the SLB instance to the rule parameter threshold. Edit the content and click re-audit. Then, refresh the page for verification.

slb-no-public-ip

If the SLB instance is not directly bound to a public IP address, it is considered as compliance. This rule applies only to IPv4.

**Trigger type:** configuration change

**Resource:** ACS::SLB::LoadBalancer

**Request parameters:** none

If you bind a public IP address to an SLB instance under your account, this rule may be invalid.

The network type of the SLB instance cannot be changed. You can purchase a server load balancer instance again and select intranet as the instance type. Config detects your changes within 10 minutes and automatically starts the audit.

For non-compliant old server load balancer instances, release the server load balancer instance (for pay-as-you-go instances). You cannot manually release a subscription server load balancer instance. If you need to release a server load balancer instance, open a ticket to apply for a refund. The server load balancer instance can be refunded without reason within five days.

**Risk:** Your data will be cleared after the SLB instance is released.

For more information about instance release risks and procedures, see [#unique\\_52](#).

**Console operation:** Select intranet as the instance type on the purchase page.

**API operation:** call CreateLoadBalancer to create an SLB instance. Set AddressType to intranet.