ALIBABA CLOUD

Alibaba Cloud

配置审计

资源合规审计

文档版本：20210728

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.规则介绍

1.1. 规则的定义及运行原理

合规性即代码，规则是企业合规要求的代码式诠释。合规条款对应一段规则代码，代码的本质是对一条资源配置的判断逻辑。配置审计服务使用函数计算服务的函数来承载规则代码，称之为规则函数。在配置审计服务中引用规则函数，配置关联资源、触发机制、规则参数等信息后，就构成了配置审计服务中的规则。

在实际的合规监控中，就是通过实时的资源配置变更触发规则函数的执行，来判断某个资源配置是否合规。多个规则的组合就实现了对整个资源配置的合规监控。

规则的定义

规则的本质是一段判断逻辑，判断资源的某一个配置项是否合规，具备以下特点：

- 规则函数的入参是通过API查询资源获取的配置项，例如：资源的规格、所属地域、名称、状态、端口或网口开关状态等。入参名称与配置项名称保持一致。
- 规则函数的逻辑是对入参值的判断，判断逻辑由您的代码决定，例如：当负载均衡的HTTPS监听状态为开启时，视为合规。入参为负载均衡的资源上代表HTTPS监听状态的配置字段，而当该字段值表示关闭时，视为不合规。
- 规则函数的出参是合规结果。

规则指向的资源类型

在函数计算中定义的规则函数，此时还不具有目标指向性，因为该规则函数未指向具体的资源类型。不同资源之间可能存在同名的配置参数，仅仅根据规则函数的入参设置无法实现准确的合规评估。

因此需要您在配置审计中，将已经创建好的规则函数与确定的资源类型绑定。当该类型的实体资源发生配置变更时，配置审计先找到资源关联的规则，再根据具体配置的变更来判断待触发的规则。

规则的触发

当资源发生配置变更时，配置审计能够准确定位发生变更的配置，以变更参数作为入参的规则函数，自动触发规则执行，评估本次变更的结果是否合规。因此规则函数的入参名称要与实际资源配置的参数名称保持一致。

此外，配置审计还支持您将规则设置为周期触发，可定期为您执行合规评估。

合规评估的结果

配置审计将获取的变更结果作为入参传入规则函数，规则函数返回合规结果给配置审计，在配置审计控制台以各种方式为您呈现和统计，请参见查看资源的规则评估结果。

您可以在函数计算服务中自定义规则函数，请参见自定义规则函数介绍。您也可以使用配置审计为您准备的托管规则，请参见托管规则列表。

1.2. 规则列表介绍

本文为您介绍规则列表中规则的运行状态和合规评估情况。

规则列表中包括您新建的规则和配置审计提供的以合规包名称为前缀的规则。您可以查看规则的名称、风险等级、应用范围、运行状态、合规包、合规评估情况、修正执行方式和操作，请重点关注**运行状态**和**合规评估情况**。

运行状态

规则运行状态如下表所示。

状态值	描述
应用中	表示规则目前处于监听状态，一旦出现相关的配置变更，就会开始评估。
评估中	表示规则已被触发，正在进行评估。
删除评估结果中	表示规则对资源的评估结果正在被删除的过程中。
已停用	表示规则目前处于停止监听状态，虽然规则配置仍然存在，但不会被触发执行。
删除中	表示规则正在被删除的过程中。

合规评估情况

规则对资源的合规评估情况如下表所示。

状态值	描述
合规（N）	表示该规则的历史评估中有N个资源合规。
不合规（N）	表示该规则的历史评估中有N个资源不合规。您需要单击目标规则对应**操作**列的**详情**，在**检测结果**页签，查看不合规的资源。
无数据	表示该规则未评估资源。

1.3. 规则详情介绍

您可以在目标规则的详情页面，查看当前规则的详细信息、对资源的检测结果和修正详情。

规则详情

在**规则详情**页签，您可以查看规则的如下信息。

分类	描述
基本属性	您可以查看规则类型、规则名称、托管规则标识、函数ARN、创建时间、风险等级、触发机制、改进建议和备注。
评估资源范围	您可以查看规则对资源的评估范围，包括：资源类型、排除的资源ID、生效的资源组ID、生效地域和生效标签。
参数设置	您可以查看规则中设置的参数和值。

检测结果

在**检测结果**页签，您可以查看目标规则关联资源的统计数据和合规结果。

- 规则关联资源的统计数据

统计项	描述
累计审计资源数	目标规则从启用至今，累计评估过的资源数量，包括您已经释放的资源。
合规资源数	目标规则关联的资源中，上次评估结果为**合规**的资源数量。
不合规资源数	目标规则关联的资源中，上次评估结果为**不合规**的资源数量。

> **说明** 资源数指具有资源ID的资源数量，而非资源类型数。

- 规则关联资源的合规结果

  您可以查看目标规则关联资源的资源ID、资源类型和最近一次评估结果。您还可以对规则关联的资源执行如下操作。

分类	描述
详情	单击**详情**，查看该资源的基本信息、核心配置信息和最新审计结果。
配置时间线	单击**配置时间线**，查看该资源的配置时间线。
合规时间线	单击**合规时间线**，查看该资源的合规时间线。
管理资源	先单击  ，再单击**管理资源**，跳转到指定云服务的管理控制台，管理该资源。

修正详情

在**修正详情**页签，您可以查看规则的修正详情，并对其执行相关操作。具体如下表所示。

分类	描述
修正详情	您可以查看修正类型、修正模板、修正执行方式和修正参数。
修正执行历史	您可以查看已修正的资源ID、资源类型、修正执行时间、修正执行结果和修正原因。

1.4. 自定义规则函数介绍

当您通过函数计算新建自定义规则时，如果规则被触发，配置审计会运行对应的规则函数对资源进行检测，并提供资源合规评估结果。本文通过JSON示例为您介绍自定义规则函数的代码和入参。

函数代码

规则的本质是一段逻辑判断代码，这段代码存放在新建的函数中。在配置审计对资源的持续审计中，通过触发该函数的执行来实现对资源的评估。本函数代码主要有两个函数，具体如下：

- `handler`

  `handler` 为入口函数，即自定义规则触发时调用的函数。 `handler` 在新建函数时进行设置。
- `put_evaluations`

`put_evaluations` 在 `handler` 中调用，返回合规结果。

Python示例如下：

```
#!/usr/bin/env python
# -*- encoding: utf-8 -*-
import logging
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.auth.credentials import StsTokenCredential
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkcore.request import CommonRequest
logger = logging.getLogger()
# 合规类型
COMPLIACE_TYPE_COMPLIANT = 'COMPLIANT'
COMPLIACE_TYPE_NON_COMPLIANT = 'NON_COMPLIANT'
COMPLIACE_TYPE_NOT_APPLICABLE = 'NOT_APPLICABLE'
COMPLIACE_TYPE_INSUFFICIENT_DATA = 'INSUFFICIENT_DATA'
# 入口函数，完成业务逻辑编排和处理。
def handler(event, context):
  """
  处理函数
  :param event：事件
  :param context：上下文
  :return：评估结果
  """
  # 校验Event，代码可直接复制。
  evt = validate_event(event)
  if not evt:
    return None
  rule_parameters = evt.get('ruleParameters')
  result_token = evt.get('resultToken')
  invoking_event = evt.get('invokingEvent')
  ordering_timestamp = evt.get('orderingTimestamp')
  annotation = None
  # 初始化返回值，根据业务场景设置规则的默认合规结果。
  compliance_type = COMPLIACE_TYPE_NOT_APPLICABLE
  # 资源配置信息。当规则触发机制设置为配置变更时，该入参有效。当您新建规则或手动执行规则时，配置审计调用函数逐个评估资源，如果资源配置变更，配置审计根据变更的资源信息自动调用函数触发一次资源评估。
  # 当规则触发机制设置为周期执行时，该入参为空。请您根据API自行实现待评估资源的查询逻辑。
  configuration_item = invoking_event.get('configurationItem')
  account_id = configuration_item.get('accountId')
  resource_id = configuration_item.get('resourceId')
  resource_type = configuration_item.get('resourceType')
  region_id = configuration_item.get('regionId')
  # 对资源进行评估，需要根据实际业务自行实现评估逻辑，以下代码仅供参考。
  compliance_type, annotation = evaluate_configuration_item(
    rule_parameters, configuration_item)
  # 设置评估结果。格式符合以下示例即可。
  evaluations = [
    {
      'accountId': account_id,
      'complianceResourceId': resource_id,
      'complianceResourceType': resource_type,
```

```
        'complianceRegionId': region_id,
        'orderingTimestamp': ordering_timestamp,
        'complianceType': compliance_type,
        'annotation': annotation
      }
    ]
# 将评估结果返回并写入配置审计，代码可直接复制。
    put_evaluations(context, result_token, evaluations)
    return evaluations
# 根据入参和资源进行评估。需要根据实际业务自行实现评估逻辑，以下代码仅供参考。
def evaluate_configuration_item(rule_parameters, configuration_item):
    """
    评估逻辑
    :param rule_parameters：规则参数
    :param configuration_item：配置项
    :return：评估类型
    """
    # 初始化返回值
    compliance_type = COMPLIACE_TYPE_NOT_APPLICABLE
    annotation = None
    # 获取资源类型和资源ID
    resource_type = configuration_item['resourceType']
    full_configuration = configuration_item['configuration']
    # 判断配置信息
    if not full_configuration:
        annotation = 'Configuration is empty.'
        return compliance_type, annotation
    # 转换为JSON
    configuration = parse_json(full_configuration)
    if not configuration:
        annotation = 'Configuration:{} in invald.'.format(full_configuration)
        return compliance_type, annotation
    return compliance_type, annotation
def validate_event(event):
    """
    校验Event
    :param event：Event
    :return：JSON对象
    """
    if not event:
        logger.error('Event is empty.')
    evt = parse_json(event)
    logger.info('Loading event: %s .' % evt)
    if 'resultToken' not in evt:
        logger.error('ResultToken is empty.')
        return None
    if 'ruleParameters' not in evt:
        logger.error('RuleParameters is empty.')
        return None
    if 'invokingEvent' not in evt:
        logger.error('InvokingEvent is empty.')
        return None
    return evt
def parse_json(content):
```

```
    """
    JSON类型转换
    :param content：JSON字符串
    :return：JSON对象
    """
    try:
        return json.loads(content)
    except Exception as e:
        logger.error('Parse content:{} to json error:{}.'.format(content, e))
        return None
# 评估结果返回，并写入配置审计，代码可直接复制。
def put_evaluations(context, result_token, evaluations):
    """
    调用API返回并写入评估结果
    :param context：函数计算上下文
    :param result_token：回调令牌
    :param evaluations：评估结果
    :return: None
    """
    # 输入当前阿里云账号的AccessKey ID和AccessKey Secret，同时具备权限AliyunConfigFullAccess。
    client = AcsClient(
        'LTAI4FxbrTniVtqg1FZW****',
        'C0GXsd6UU6ECUmrsCgPXA6OEvy****',
        'ap-southeast-1',
    )
    # 新建Request，并设置参数，Domain为config.ap-southeast-1.aliyuncs.com。
    request = CommonRequest()
    request.set_domain('config.ap-southeast-1.aliyuncs.com')
    request.set_version('2019-01-08')
    request.set_action_name('PutEvaluations')
    request.add_body_params('ResultToken', result_token)
    request.add_body_params('Evaluations', evaluations)
    request.set_method('POST')
    try:
        response = client.do_action_with_exception(request)
        logger.info('PutEvaluations with request: {}, response: {}.'.format(request, response))
    except Exception as e:
        logger.error('PutEvaluations error: %s' % e)
```

函数入参

在函数中设置的入参信息保存在ruleParameters中，其他内容在规则触发时自动生成事件信息。JSON示例如下：

```
{
  "orderingTimestamp": "命令执行开始时间戳",
  "invokingEvent": {
    "messageType": "消息类型",
    "configurationItem": {
      "accountId": "阿里云账号ID",
      "arn": "资源ARN",
      "availabilityZone": "可用区",
      "regionId": "地域ID",
      "configuration": "资源的详细配置",
      "configurationDiff": "资源配置变更的具体变更项及变更前后信息",
      "relationship": "关联资源",
      "relationshipDiff": "关系内容变更",
      "captureTime": "配置审计发现资源变更事件并生成日志的时间戳",
      "resourceCreationTime": "新建资源的时间戳",
      "resourceStatus": "资源状态",
      "resourceId": "资源ID",
      "resourceName": "资源名称",
      "resourceType": "资源类型",
      "supplementaryConfiguration": "资源补充配置",
      "tags": "标签"
    }
  },
  "ruleParameters": {
    "key": "value"
  },
  "resultToken": "用户在函数计算中的回调信息"
}
```

Context参数是上下文信息，规则触发时自动带入。

- `context.credentials.access_key_id:"accessKey"`
- `context.credentials.access_key_secret:"accessSecret"`
- `context.region:"地域"`

2.管理规则

2.1. 新建托管规则

规则的本质是函数计算的函数中的一段逻辑判断代码，您可以使用配置审计提供的托管规则快速新建规则，对目标资源进行审计。

背景信息

在新建规则之前，请您先了解规则的定义及运行原理。

配置审计为您提供以下两种规则：

- 托管规则

  托管规则是配置审计已在函数计算中构建的规则函数，新建规则时直接从配置审计控制台选择目标托管规则。配置审计支持的托管规则，请参见托管规则列表。

- 自定义规则

  自定义规则是需要您提前在函数计算中定义的规则函数，新建规则时直接从配置审计控制台选择规则函数的ARN。自定义规则函数的代码和入参，请参见自定义规则函数介绍。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击**新建规则**。
4. 在**新建规则**页面，根据规则名称、标签、检测逻辑或风险等级筛选出目标托管规则。
5. 单击**应用规则**。
6. 在**基本属性**页面，设置规则名称、风险等级和备注，单击**下一步**。

   托管规则的名称、风险等级和触发机制均为系统默认。您可以根据所需修改规则名称和风险等级。
7. 在**评估资源范围**页面，资源类型保持默认，单击**下一步**。
8. 在**参数设置**页面，单击**下一步**。

   如果目标托管规则有规则入参，则需要设置其期望值。
9. 在**修正设置**页面，单击**下一步**。

   对于支持修正设置的托管规则，您可以选中**修正设置**前面的复选框，根据控制台提示，设置修正方式、修正类型和修正参数。具体操作，请参见设置自动修正或设置手动修正。
10. 在**预览并保存**页面，确认规则设置，单击**提交**。
11. 查看规则新建结果。
    - 单击**查看规则详情**，您可以查看当前规则的**规则详情**、**检测结果**和**修正详情**。
    - 单击**返回规则列表**，您可以在**规则**列表中查看新建的规则，其运行状态为**应用中**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。

4. 在目标账号组页签，单击**新建规则**。
5. 在**新建规则**页面，根据规则名称、标签、检测逻辑或风险等级筛选出目标托管规则。
6. 单击**应用规则**。
7. 在**基本属性**页面，设置规则名称、风险等级和备注，单击**下一步**。

   托管规则的名称、风险等级和触发机制均为系统默认。您可以根据所需修改规则名称和风险等级。
8. 在**评估资源范围**页面，资源类型保持默认，单击**下一步**。
9. 在**参数设置**页面，单击**下一步**。

   如果目标托管规则有规则入参，则需要设置其期望值。
10. 在**修正设置**页面，单击**下一步**。

    对于支持修正设置的托管规则，您可以选中**修正设置**前面的复选框，根据控制台提示，设置修正方式、修正类型和修正参数。具体操作，请参见设置自动修正或设置手动修正。
11. 在**预览并保存**页面，确认规则设置，单击**提交**。
12. 查看规则新建结果。
    - 单击**查看规则详情**，您可以查看当前规则的**规则详情**、**检测结果**和**修正详情**。
    - 单击**返回规则列表**，您可以在**规则**列表中查看新建的规则，其运行状态为**应用中**。

2.2. 新建自定义规则

当配置审计提供的托管规则不能满足您资源审计的需求时，您可以通过函数计算服务自定义规则，对目标资源进行审计。当规则被触发时，配置审计会运行对应的规则函数对资源进行检测，并给出资源合规评估结果。

前提条件

请确保您已开通函数计算服务。具体操作，请参见开通服务。

背景信息

在新建规则之前，请您先了解规则的定义及运行原理。

配置审计为您提供以下两种规则：

- 托管规则

  托管规则是配置审计已在函数计算中构建的规则函数，新建规则时直接从配置审计控制台选择目标托管规则。配置审计支持的托管规则，请参见托管规则列表。
- 自定义规则

  自定义规则是需要您提前在函数计算中定义的规则函数，新建规则时直接从配置审计控制台选择规则函数的ARN。自定义规则函数的代码和入参，请参见自定义规则函数介绍。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击**新建规则**。
4. 在**新建规则**页面，单击**新建自定义规则**。
5. 在**基本属性**页面，设置规则的函数ARN、规则名称、风险等级、触发机制和备注，单击**下一步**。

- 如果您已新建函数，直接选择函数的ARN。
- 如果您未新建函数，单击**前往创建新的函数**，在函数计算控制台上新建函数。具体操作，请参见新建函数。

  新建函数时，**创建方式**选择**事件函数**，**运行环境**选择python3，**函数入口**使用默认值**index.handler**，入口函数为handler。

6. 在**评估资源范围**页面，选择规则关联的资源类型，单击**下一步**。
7. 在**参数设置**页面，单击**添加规则入参**，设置规则入参名称和期望值，单击**下一步**。
   - 选择规则关联的资源后，规则将检测您账号下该资源类型的所有资源。一条规则可以关联多个资源类型。
   - 规则入参名称需要与资源实际配置名称保持一致。
8. 在**修正设置**页面，单击**下一步**。
9. 在**预览并保存**页面，确认规则设置，单击**提交**。
10. 查看规则新建结果。
    - 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**检测结果**。
    - 单击**返回规则列表**，您可以在**规则**列表中查看新建的规则，其运行状态为**应用中**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 在目标账号组页签，单击**新建规则**。
5. 在**新建规则**页面，单击**新建自定义规则**。
6. 在**基本属性**页面，设置规则的函数ARN、规则名称、风险等级、触发机制和备注，单击**下一步**。
   - 如果您已新建函数，直接选择函数的ARN。
   - 如果您未新建函数，单击**前往创建新的函数**，在函数计算控制台上新建函数。具体操作，请参见新建函数。

     新建函数时，**创建方式**选择**事件函数**，**运行环境**选择python3，**函数入口**使用默认值**index.handler**，入口函数为handler。
7. 在**评估资源范围**页面，选择规则关联的资源类型，单击**下一步**。
8. 在**参数设置**页面，单击**添加规则入参**，设置规则入参名称和期望值，单击**下一步**。
   - 选择规则关联的资源后，规则将检测您账号下该资源类型的所有资源。一条规则可以关联多个资源类型。
   - 规则入参名称需要与资源实际配置名称保持一致。
9. 在**修正设置**页面，单击**下一步**。
10. 在**预览并保存**页面，确认规则设置，单击**提交**。
11. 查看规则新建结果。
    - 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**检测结果**。
    - 单击**返回规则列表**，您可以在**规则**列表中查看新建的规则，其运行状态为**应用中**。

2.3. 修改规则

当已有规则不能满足您资源审计的需求时，您可以根据所需修改规则。您只能在规则列表中修改新建的规则，不能修改合规包中的规则。

背景信息

如果您启用了合规包，将在规则列表中自动生成以合规包名称为前缀的规则，这些规则不允许修改、删除、启用和停用。您可以在合规包中修改这些规则。具体操作，请参见修改合规包。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标规则对应**操作**列的**编辑**。
4. 在**基本属性**页面，设置规则的备注，单击**下一步**。
5. 在**评估资源范围**页面，单击**下一步**。

   对于自定义规则和标签类托管规则，您可以修改资源类型。
6. 在**参数设置**页面，设置规则入参的期望值，单击**下一步**。

   对于自定义规则，您可以同时设置规则入参名称和期望值。
7. 在**修正设置**页面，单击**下一步**。

   对于支持修正设置的托管规则，您可以选中**修正设置**前面的复选框，根据控制台提示，设置修正方式、修正类型和修正参数。具体操作，请参见设置自动修正或设置手动修正。
8. 在**预览并保存**页面，确认规则设置，单击**提交**。
9. 查看规则修改结果。
   - 单击**查看规则详情**，您可以查看当前规则的**规则详情**、**检测结果**和**修正详情**。
   - 单击**返回规则列表**，您可以在**规则**列表中查看修改后的规则，其运行状态为**应用中**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标规则对应**操作**列的**编辑**。
5. 在**基本属性**页面，设置规则的备注，单击**下一步**。
6. 在**评估资源范围**页面，单击**下一步**。

   对于自定义规则和标签类托管规则，您可以修改资源类型。
7. 在**参数设置**页面，设置规则入参的期望值，单击**下一步**。

   对于自定义规则，您可以同时设置规则入参名称和期望值。
8. 在**修正设置**页面，单击**下一步**。

   对于支持修正设置的托管规则，您可以选中**修正设置**前面的复选框，根据控制台提示，设置修正方式、修正类型和修正参数。具体操作，请参见设置自动修正或设置手动修正。
9. 在**预览并保存**页面，确认规则设置，单击**提交**。
10. 查看规则修改结果。
    - 单击**查看规则详情**，您可以查看当前规则的**规则详情**、**检测结果**和**修正详情**。

- 单击**返回规则列表**，您可以在**规则**列表中查看修改后的规则，其运行状态为**应用中**。

2.4. 停用规则

当您暂时无需使用某条规则时，可以对其执行停用操作。您只能在规则列表中停用新建的规则，不能停用合规包中的规则。

前提条件

请您确保规则的**运行状态**为**应用中**。

背景信息

如果您启用了合规包，将在规则列表中自动生成以合规包名称为前缀的规则，这些规则不能停用。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 停用规则。
   - 单个停用
     a. 在**规则**页面，单击目标规则对应**操作**列的
     
     图标，选择**停用规则**。
     b. 在**确定停用规则？**对话框，单击**确定**。
   - 批量停用
     a. 在**规则**页面，选中目标规则对应复选框，单击图标。
     b. 在**批量停用**对话框，单击**确定**。
4. 查看规则状态。
   在**规则**页面，您可以通过筛选功能查看**已停用**的规则。规则停用后，不再执行，且显示停用前的合规评估结果。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 停用规则。
   - 单个停用
     a. 在目标账号组页签，单击目标规则对应**操作**列的
     
     图标，选择**停用规则**。
     b. 在**确定停用规则？**对话框，单击**确定**。
   - 批量停用

a. 在目标账号组页签，选中目标规则对应复选框，单击图标。

b. 在**批量停用**对话框，单击**确定**。

5. 查看规则状态。

在目标账号组页签，您可以通过筛选功能查看**已停用**的规则。

相关操作

您可以启用处于**已停用**状态的规则，使其重新处于**应用中**状态。具体操作如下：

- 普通账号
  - 单个启用

    在**规则**页面，单击目标规则对应**操作**列的

    图标，选择**启用规则**。
  - 批量启用

    a. 在**规则**页面，选中目标规则对应复选框，单击图标。

    b. 在**批量启用**对话框，单击**确定**。
- 企业管理账号
  - 单个启用

    在目标账号组页签，单击目标规则对应**操作**列的

    图标，选择**启用规则**。
  - 批量启用

    a. 在目标账号组页签，选中目标规则对应复选框，单击图标。

    b. 在**批量启用**对话框，单击**确定**。

2.5. 删除规则

当您不再需要某条规则时，可以对其执行删除操作。删除规则后，其配置信息不再保留。您只能在规则列表中删除新建的规则，不能删除合规包中的规则。

前提条件

请确保您已停用规则。具体操作，请参见停用规则。

背景信息

如果您启用了合规包，将在规则列表中自动生成以合规包名称为前缀的规则，这些规则不允许删除。您可以在合规包中通过删除合规包或单击目标规则的，删除规则。关于如何删除合规包，请参见删除合规包。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，筛选出**已停用**的规则。
4. 删除规则。
   - 单个删除
     a. 单击目标规则对应**操作**列的
     
     ，选择**删除**。
     b. 在**确定删除规则？**对话框，单击**删除**。
   - 批量删除
     a. 选中目标规则对应复选框，单击  。
     b. 在**批量删除**对话框，单击**确定**。
5. 确认规则删除结果。
   在**规则**页面，规则已被删除。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 在目标账号组页签，筛选出**已停用**的规则。
5. 删除规则。
   - 单个删除
     a. 单击目标规则对应**操作**列的
     
     ，选择**删除**。
     b. 在**确定删除规则？**对话框，单击**删除**。
   - 批量删除
     a. 选中目标规则对应复选框，单击  。
     b. 在**批量删除**对话框，单击**确定**。
6. 确认规则删除结果。
   在目标账号组页签，规则已被删除。

2.6. 手动执行审计

当您修改规则或资源后，如需立刻看到审计结果，可以手动执行审计。如果不手动执行审计，只有当资源配置变更或达到规则触发周期时，您才能看到审计结果。

前提条件

请您确保规则的**运行状态**为**应用中**。

背景信息

您可以对新建的规则和合规包中以合规包名称为前缀的规则手动执行审计。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标规则的**规则名称**链接，或单击目标规则对应**操作**列的**详情**。
4. 在目标规则的**规则详情**页签，单击右上角的**重新审计**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标规则的**规则名称**链接，或单击目标规则对应**操作**列的**详情**。
5. 在目标规则的**规则详情**页签，单击右上角的**重新审计**。

3.修正设置

3.1. 概述

您可以在新建或修改规则时，为规则设置修正模板。修正模板本质是一个逻辑编排的工作流，当资源配置出现不合规时，可以快速自动或手动运行模板，修正资源配置。

修正模板的运行是由逻辑编排和运维编排代替您对资源进行修改操作，您需要授予相应权限。关于逻辑编排，请参见什么是逻辑编排。关于运维编排，请参见什么是运维编排服务。

当您新建或修改规则时，可以设置修正，也可跳过修正设置，只配置规则。设置自动修正和手动修正的差异如下：

- 如果您选择**自动执行**，当该条规则绑定的资源被判定为**不合规**时，将自动对资源进行修正。
- 如果您选择**手动执行**，当该条规则绑定的资源被判定为**不合规**时，不会自动对资源进行修正。您可以随时在规则的修正详情页面中，手动执行修正。

使用限制

- 目前部分托管规则支持设置修正模板，配置审计将逐步支持更多托管规则。
- 目前一个规则仅支持设置一个修正模板，且当前仅支持为配置审计中托管规则提供默认模板。

相关功能

修正设置相关功能如下表所示。

功能	描述
设置自动修正	您可以在新建规则时，为其绑定修正模板，且设置为自动执行。当资源配置出现不合规时，可以快速自动运行模板，修正资源配置。
设置手动修正	您可以在新建规则时，为其绑定修正模板，且设置为手动执行。当资源配置出现不合规时，您可以手动运行模板，修正资源配置。
删除修正设置	当您需要删除所有修正设置并收回授权时，您可以直接删除修正设置。

3.2. 设置自动修正

您可以在新建规则时，为其绑定修正模板，且设置为自动执行。当资源配置出现不合规时，可以快速自动运行模板，修正资源配置。

背景信息

本文以新建托管规则**存在所有指定标签**为例，为您介绍设置自动修正的操作方法。

托管规则**存在所有指定标签**用于检测关联资源是否绑定所有标签。例如，您需要所有ECS实例均绑定标签“Project=A”，您可以通过规则**存在所有指定标签**监控所有ECS实例，当配置审计发现有ECS实例未绑定该标签时，该规则评估结果为**不合规**。如果您订阅了资源合规事件，则配置审计会向您指定的消息服务MNS主题发送不合规通知。具体操作，请参见发送资源事件到消息服务MNS。

普通账号

1. 登录配置审计控制台。

2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击**新建规则**。
4. 在**新建规则**页面，根据托管规则名称筛选出目标托管规则。
5. 单击**应用规则**。
6. 在**基本属性**页面，设置规则名称和风险等级，单击**下一步**。

   托管规则的名称、风险等级和触发机制均为系统默认。您可以根据所需修改规则名称和风险等级。
7. 在**评估资源范围**页面，资源类型保持默认，单击**下一步**。
8. 在**参数设置**页面，输入标签Key和Value的期望值，单击**下一步**。

   如果您需要检测多组标签，则可以依次填写Key和Value的期望值，最多支持检测6组标签。多组标签之间是与的关系，只有当目标资源同时绑定您设置的标签时，规则对资源的评估结果为**合规**。如果您需要实现或的关系，则请多次使用该托管规则新建多条规则。

   例如，您需要账号下所有资源均绑定标签“Project=A”，可以使用托管规则**存在所有指定标签**检测资源，当配置审计检测到资源未绑定该标签时，该规则对资源的评估结果为**不合规**。
9. 在**修正设置**页面，单击**修正设置**对应的复选框，选择**自动执行**和**逻辑编排**，根据所需补充标签Key和Value的参数值，单击**下一步**。

   > **说明** 标签Key和Value的参数值，即为修正设置的目标值。
10. 在**预览并保存**页面，确认规则设置，单击**提交**。
11. 查看修正结果。

    当通过该条规则检测的资源被评估为**不合规**时，配置审计触发修正模板运行，自动将资源配置修改为您设置的目标值。

    i. 在左侧导航栏，单击**规则**。
    ii. 在**规则**页面，单击目标规则对应**操作**列的**详情**或**规则名称/规则ID**链接。
    iii. 在目标规则的详情页面，单击**修正详情**页签。
    iv. 在**修正详情**页签，您可以查看修正执行结果。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 在目标账号组页签，单击**新建规则**。
5. 在**新建规则**页面，根据托管规则名称筛选出目标托管规则。
6. 单击**应用规则**。
7. 在**基本属性**页面，设置规则名称和风险等级，单击**下一步**。

   托管规则的名称、风险等级和触发机制均为系统默认。您可以根据所需修改规则名称和风险等级。
8. 在**评估资源范围**页面，资源类型保持默认，单击**下一步**。
9. 在**参数设置**页面，输入标签Key和Value的期望值，单击**下一步**。

   如果您需要检测多组标签，则可以依次填写Key和Value的期望值，最多支持检测6组标签。多组标签之间是与的关系，只有当目标资源同时绑定您设置的标签时，规则对资源的评估结果为**合规**。如果您需要

实现或的关系，则请多次使用该托管规则新建多条规则。

例如，您需要账号下所有资源均绑定标签“Project=A”，可以使用托管规则**存在所有指定标签**检测资源，当配置审计检测到资源未绑定该标签时，该规则对资源的评估结果为**不合规**。

10. 在**修正设置**页面，单击**修正设置**对应的复选框，选择**自动执行**和**逻辑编排**，根据所需补充标签Key和Value的参数值，单击**下一步**。

> **说明** 标签Key和Value的参数值，即为修正设置的目标值。

11. 在**预览并保存**页面，确认规则设置，单击**提交**。
12. 查看修正结果。

    当通过该条规则检测的资源被评估为**不合规**时，配置审计触发修正模板运行，自动将资源配置修改为您设置的目标值。

    i. 在左侧导航栏，单击**规则**。
    ii. 在**规则**页面，单击目标规则对应**操作**列的**详情**或**规则名称/规则ID**链接。
    iii. 在目标规则的详情页面，单击**修正详情**页签。
    iv. 在**修正详情**页签，您可以查看修正执行结果。

相关功能

配置审计自动修正服务关联角色

3.3. 设置手动修正

您可以在新建规则时，为其绑定修正模板，且设置为手动执行。当资源配置出现不合规时，您可以手动运行模板，修正资源配置。

背景信息

本文以新建托管规则**检测资源是否已有必备标签**为例，为您介绍设置手动修正的操作方法。

托管规则**存在所有指定标签**用于检测关联资源是否绑定所有标签。例如，您需要所有ECS实例均绑定标签“Project=A”，您可以通过规则**存在所有指定标签**监控所有ECS实例，当配置审计发现有ECS实例未绑定该标签时，该规则评估结果为**不合规**。如果您订阅了资源合规事件，则配置审计会向您指定的消息服务MNS主题发送不合规通知。具体操作，请参见发送资源事件到消息服务MNS。

普通账号

1. 设置手动修正。

    i. 登录配置审计控制台。
    ii. 在左侧导航栏，单击**规则**。
    iii. 在**规则**页面，单击**新建规则**。
    iv. 在**新建规则**页面，根据托管规则名称筛选出目标托管规则。
    v. 单击**应用规则**。
    vi. 在**基本属性**页面，设置规则名称和风险等级，单击**下一步**。

    托管规则的名称、风险等级和触发机制均为系统默认。您可以根据所需修改规则名称和风险等级。

    vii. 在**评估资源范围**页面，资源类型保持默认，单击**下一步**。

viii. 在**参数设置**页面，输入标签Key和Value的期望值，单击**下一步**。

如果您需要检测多组标签，则可以依次填写Key和Value的期望值，最多支持检测6组标签。多组标签之间是与的关系，只有当目标资源同时绑定您设置的标签时，规则对资源的评估结果为**合规**。如果您需要实现或的关系，则请多次使用该托管规则新建多条规则。

例如，您需要账号下所有资源均绑定标签“Project=A”，可以使用托管规则**存在所有指定标签**检测资源，当配置审计检测到资源未绑定该标签时，该规则对资源的评估结果为**不合规**。

ix. 在**修正设置**页面，单击**修正设置**对应的复选框，选择**手动执行**和**逻辑编排**，根据所需补充标签Key和Value的参数值，单击**下一步**。

> **说明** 标签Key和Value的参数值，即为修正设置的目标值。

x. 在**预览并保存**页面，确认规则设置，单击**提交**。

2. 执行手动修正。

当您接收到资源不合规告警或主动发现资源不合规时，在规则的**修正详情**页签，手动触发模板运行，自动将资源配置修改为您设置的目标值。手动执行修正的操作方法如下：

i. 在左侧导航栏，单击**规则**。

ii. 在**规则**页面，单击目标规则对应**操作**列的**详情**或**规则名称/规则ID**链接。

iii. 在目标规则的详情页面，单击**修正详情**页签。

iv. 在**修正详情**页签，单击**修正执行方式**后面的**执行手动修正**。

3. 在**修正详情**页签，您可以查看修正执行结果。

企业管理账号

1. 设置手动修正。

i. 登录配置审计控制台。

ii. 在左侧导航栏，单击**规则**。

iii. 在**规则**页面，单击目标账号组页签。

iv. 在目标账号组页签，单击**新建规则**。

v. 在**新建规则**页面，根据托管规则名称筛选出目标托管规则。

vi. 单击**应用规则**。

vii. 在**基本属性**页面，设置规则名称和风险等级，单击**下一步**。

托管规则的名称、风险等级和触发机制均为系统默认。您可以根据所需修改规则名称和风险等级。

viii. 在**评估资源范围**页面，资源类型保持默认，单击**下一步**。

ix. 在**参数设置**页面，输入标签Key和Value的期望值，单击**下一步**。

如果您需要检测多组标签，则可以依次填写Key和Value的期望值，最多支持检测6组标签。多组标签之间是与的关系，只有当目标资源同时绑定您设置的标签时，规则对资源的评估结果为**合规**。如果您需要实现或的关系，则请多次使用该托管规则新建多条规则。

例如，您需要账号下所有资源均绑定标签“Project=A”，可以使用托管规则**存在所有指定标签**检测资源，当配置审计检测到资源未绑定该标签时，该规则对资源的评估结果为**不合规**。

x. 在**修正设置**页面，单击**修正设置**对应的复选框，选择**手动执行**和**逻辑编排**，根据所需补充标签Key和Value的参数值，单击**下一步**。

> **说明** 标签Key和Value的参数值，即为修正设置的目标值。

xi. 在**预览并保存**页面，确认规则设置，单击**提交**。

2. 执行手动修正。

当您接收到资源不合规告警或主动发现资源不合规时，在规则的**修正详情**页签，手动触发模板运行，自动将资源配置修改为您设置的目标值。手动执行修正的操作方法如下：

i. 在左侧导航栏，单击**规则**。

ii. 在**规则**页面，单击目标账号组页签。

iii. 在目标账号组页签，单击目标规则对应**操作**列的**详情**或**规则名称/规则ID**链接。

iv. 在目标规则的详情页面，单击**修正详情**页签。

v. 在**修正详情**页签，单击**修正执行方式**后面的**执行手动修正**。

3. 在**修正详情**页签，您可以查看修正执行结果。

相关功能

配置审计自动修正服务关联角色

3.4. 删除修正设置

当您需要删除所有修正设置并收回授权时，您可以直接删除修正设置。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标规则对应**操作**列的**详情**或**规则名称/规则ID**链接。
4. 在目标规则的管理页面，单击**修正详情**页签。
5. 在**修正详情**页签，单击**删除**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标规则对应**操作**列的**详情**或**规则名称/规则ID**链接。
5. 在目标规则的管理页面，单击**修正详情**页签。
6. 在**修正详情**页签，单击**删除**。

相关功能

配置审计自动修正服务关联角色

4.查看合规结果

4.1. 查看资源的规则评估结果

您可以通过以下两种方法查看资源的规则评估结果。

普通账号

- 方法一：在**规则**列表的**合规评估情况**列，查看目标规则对所有关联资源的评估结果。具体操作如下：
  i. 登录配置审计控制台。
  ii. 在左侧导航栏，单击**规则**。
- 方法二：在目标规则的**检测结果**页签，查看该规则对所有关联资源的评估结果。具体操作如下：
  i. 登录配置审计控制台。
  ii. 在左侧导航栏，单击**规则**。
  iii. 在**规则**页面，单击目标规则的**规则名称**链接，或单击目标规则对应**操作**列的**详情**。
  iv. 单击**检测结果**页签。

企业管理账号

- 方法一：在**规则**列表的**合规评估情况**列，查看目标规则对所有关联资源的评估结果。具体操作如下：
  i. 登录配置审计控制台。
  ii. 在左侧导航栏，单击**规则**。
  iii. 在**规则**页面，单击目标账号组页签。
- 方法二：在目标规则的**检测结果**页签，查看该规则对所有关联资源的评估结果。具体操作如下：
  i. 登录配置审计控制台。
  ii. 在左侧导航栏，单击**规则**。
  iii. 在**规则**页面，单击目标账号组页签。
  iv. 在目标账号组页签，单击目标规则的**规则名称**链接，或单击目标规则对应**操作**列的**详情**。
  v. 单击**检测结果**页签。

4.2. 查看资源合规时间线

在配置审计中，每个资源都有属于自己的合规时间线。当规则评估该资源时，产生合规评估记录，持续的合规评估形成了资源的合规时间线。

背景信息

合规时间线是资源的一组合规评估记录，包括的要素如下表所示。

要素	说明

要素	说明
合规时间线上的点	• 起点：资源第一次被规则评估的时间。合规评估可能是定时任务触发、实时变更触发或手动触发。 • 节点：资源每次的规则评估都会形成合规时间线上的一个节点，资源每次评估可能涉及一条或多条规则。 • 断点：如果您将指定资源类型移出监控范围，则配置审计停止监控该资源类型中的资源，也不会新增合规时间线。如果您将该资源类型移回监控范围，则配置审计重新监控该资源类型中的资源。资源停止监控期间的资源变更历史不可追溯。
合规时间线的内容	• 时间：合规评估发生的时间。 • 触发机制：本次合规评估时的触发机制，说明资源被评估的原因，包括定时任务触发、实时变更触发或手动触发。 • 合规评估结果：在**合规时间线**页签的左侧导航栏会显示每个节点的合规评估结果，便于您快速定位不合规资源。 • 每个节点的评估详情：包括**基本信息**和**本次审计结果**。如果本次评估由资源的配置变更触发或定时任务触发，则会显示**本次资源核心配置变更细节**，以便您快速查看不合规资源的配置变更详情。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**资源**。
3. 在**资源**页面，通过筛选或搜索功能找到目标资源。
4. 单击目标资源的**资源ID/资源名称**链接。
5. 单击**合规时间线**页签，查看资源的合规时间线详情。
   - 在**基本信息**区域，您可以查看该资源的资源ID、资源名称、资源类型、创建时间、标签、地域和可用区。
   - 在**本次审计结果**区域，您可以查看该资源的审计结果。
   - 在**本次资源核心配置变更细节**区域，您可以查看该资源配置项变更前和变更后JSON格式的代码。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**资源**。
3. 在**资源**页面，单击目标账号组页签。
4. 在目标账号组页签，通过筛选或搜索功能找到目标资源。
5. 单击目标资源的**资源ID/资源名称**链接。
6. 单击**合规时间线**页签，查看资源的合规时间线详情。
   - 在**基本信息**区域，您可以查看该资源的资源ID、资源名称、资源类型、创建时间、标签、地域和可用区。
   - 在**本次审计结果**区域，您可以查看该资源的审计结果。
   - 在**本次资源核心配置变更细节**区域，您可以查看该资源配置项变更前和变更后JSON格式的代码。