ALIBABA CLOUD

阿里云

配置审计

资源合规审计

文档版本：20200925

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，请参见使用函数计算新建规则。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。

2.规则管理

2.1. 规则列表

本文为您介绍规则列表中规则的合规评估情况和运行状态。

当您初次进入**管理合规规则**页面时，规则列表为空。当您新建规则之后，可在列表中查看所有规则。在规则列表中您可以查看规则的基本信息，请重点关注**合规评估情况**和**运行状态**。

合规评估情况

规则合规评估情况如下表所示。

状态值	描述
合规	表示该规则的历史评估结果均为合规。
不合规	表示该规则的历史评估中有N个资源出现不合规。您需要进入规则详情，查看具体不合规资源。
无数据	表示该规则未评估资源。

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	配置审计支持您删除某规则的评估结果，方便您在正式的合规监控开始前，清空测试数据。
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，但永远不会被触发执行。
删除中	表示规则被执行删除操作后，配置审计正在删除处理中。

2.2. 新建规则

规则的本质是放在函数计算的函数中的逻辑判断代码，您可以引用配置审计为您准备的托管规则，也可以在函数计算中自定义规则函数。您还可以将需求通过工单提交给阿里云售后工程师，评估后有机会实现为托管规则。

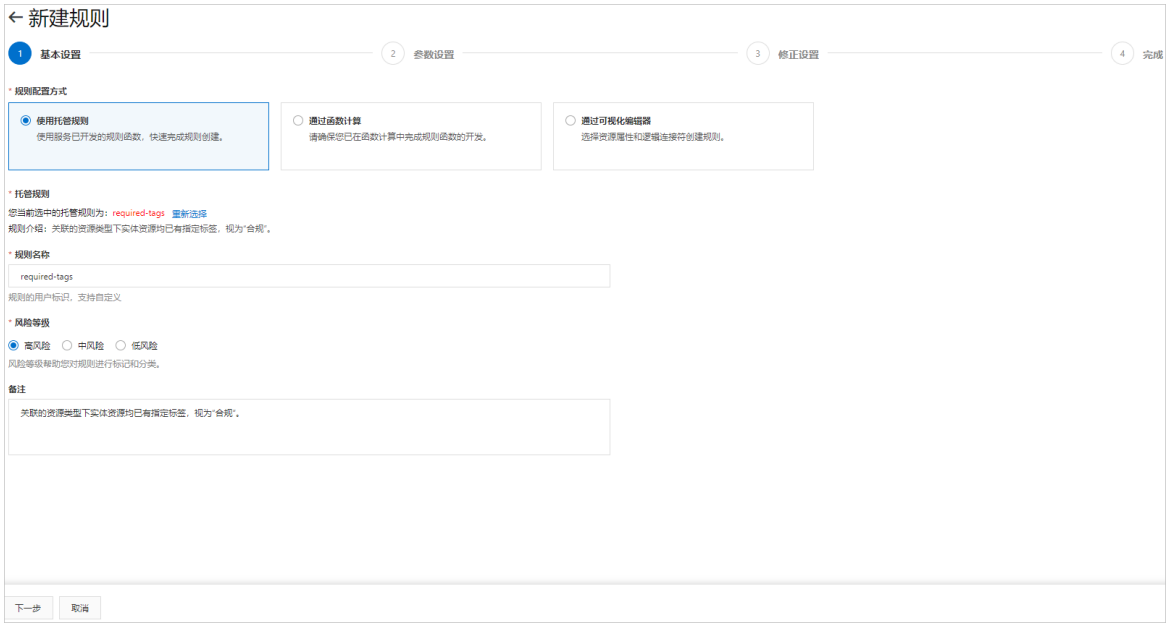
背景信息

在新建规则之前，请您先了解规则的定义及运行原理。

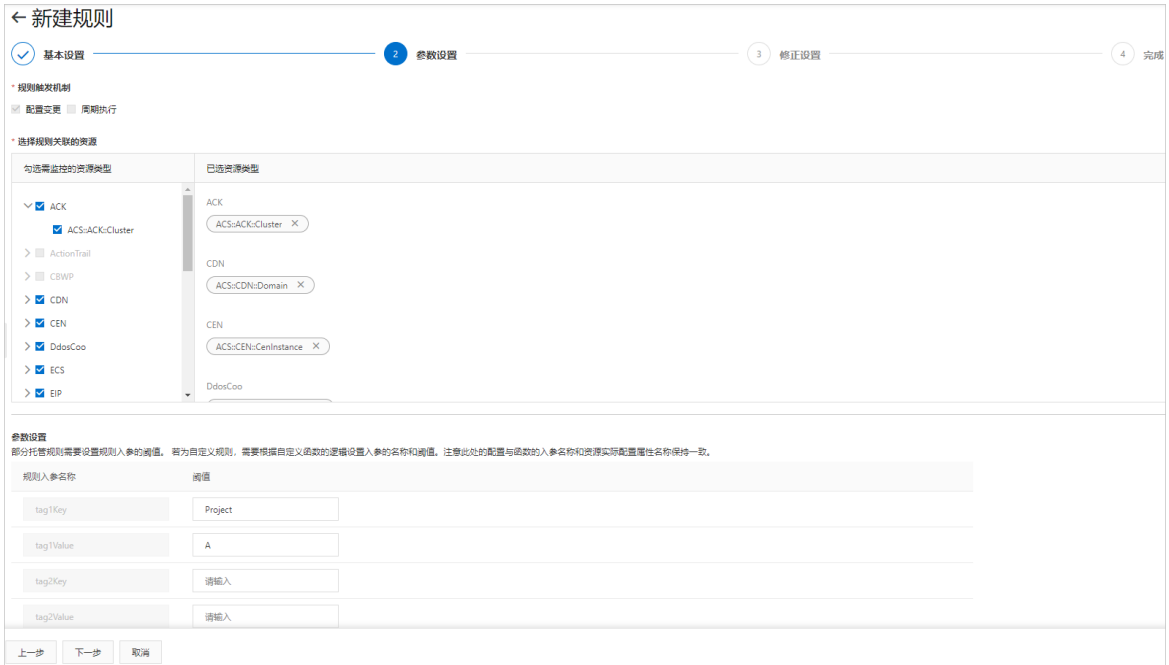
通过托管规则新建规则

使用函数计算已开发的规则函数，快速新建规则，请参见托管规则列表。

1. 登录配置审计控制台。
2. 在左侧导航栏，选择管理合规规则。
3. 在管理合规规则页面，单击新建规则。
4. 在基本设置页面，选择规则配置方式为使用托管规则，选择托管规则和风险等级，单击下一步。



5. 在参数设置页面，输入规则入参的阈值，单击下一步。



> **说明** 规则触发机制、关联资源和入参名称均采用默认值。

6. 在修正设置页面，修正执行方式默认为不执行修正，单击提交。

   如果您需要为当前规则绑定修正模板，请参见设置自动修正或设置手动修正。

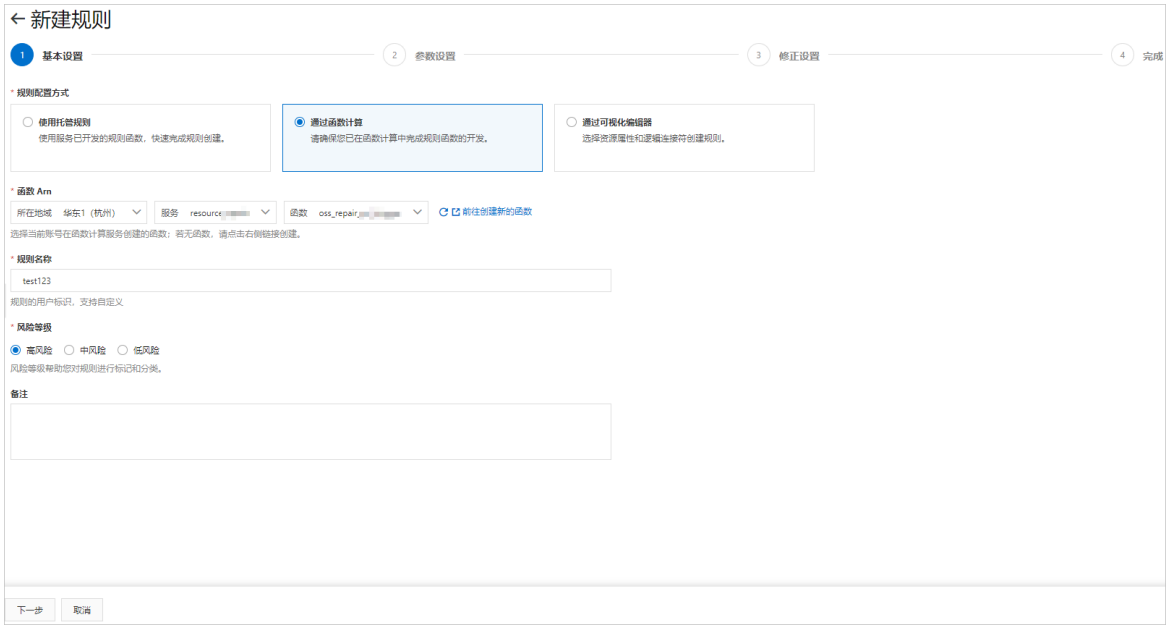
7. 查看规则新建结果。在完成页面，您可以查看规则新建结果。

- 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**修正详情**。
- 单击**返回规则列表**，您可以在**管理合规规则**列表中查看该规则，规则状态为**应用中**。

通过函数计算新建规则

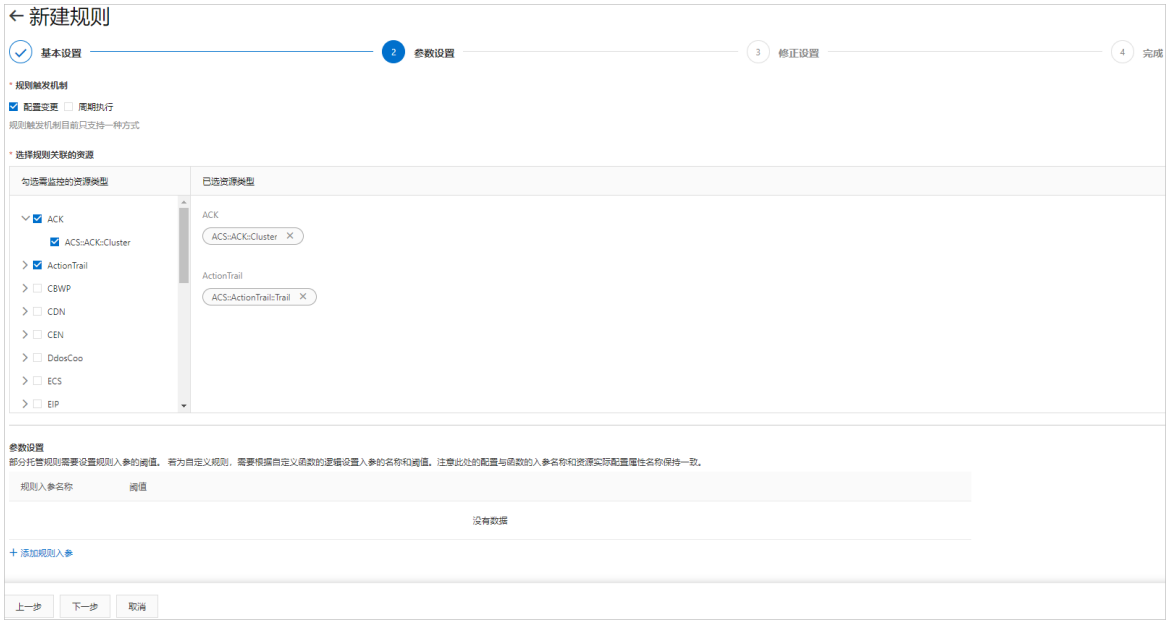
您可以在函数计算服务中自定义规则函数，请参见使用函数计算新建规则。

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**页面，单击**新建规则**。
4. 在**基本设置**页面，选择**规则配置方式**为**通过函数计算**，输入**规则名称**，选择**函数Arn**和**风险等级**，单击**下一步**。



请确保您已在函数计算中新建函数，才能直接选择函数，否则请单击**前往创建新的函数**链接，在函数计算控制台上新建函数，操作方法请参见新建函数。

5. 在**参数设置**页面，选择规则触发机制和规则关联资源，根据所需设置规则参数，单击**下一步**。



- 选择规则关联的资源后，规则将监听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。
- 输入规则入参名称和阈值，入参名称需要与资源实际的配置名称一致。

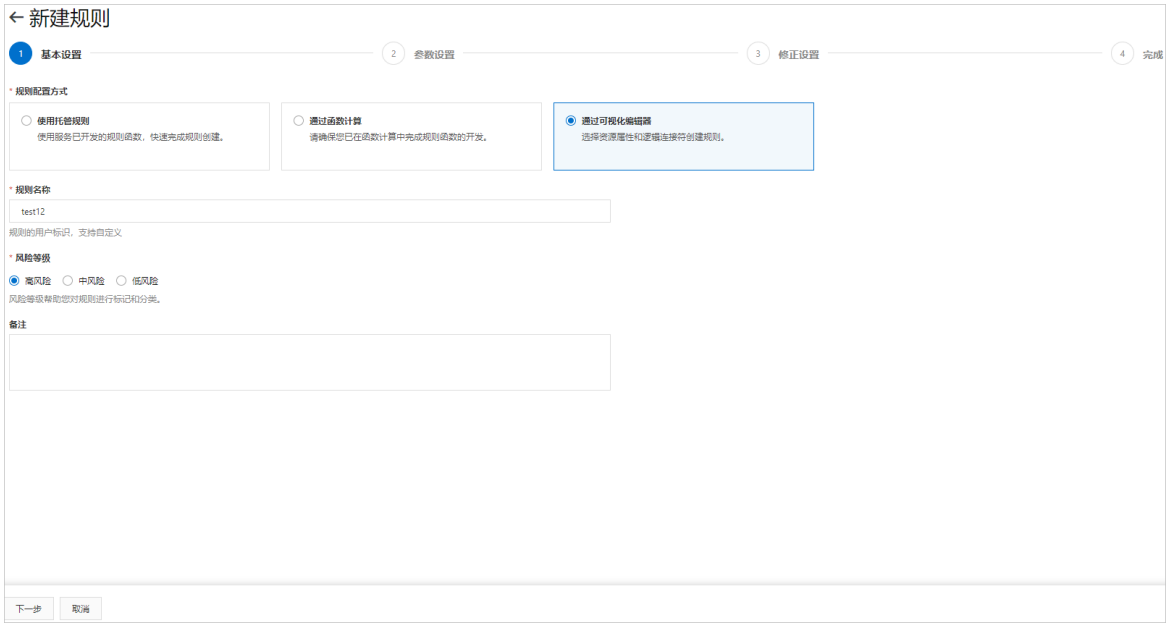
6. 在修正设置页面，修正执行方式默认为不执行修正，单击提交。

   如果您需要为当前规则绑定修正模板，请参见设置自动修正或设置手动修正。

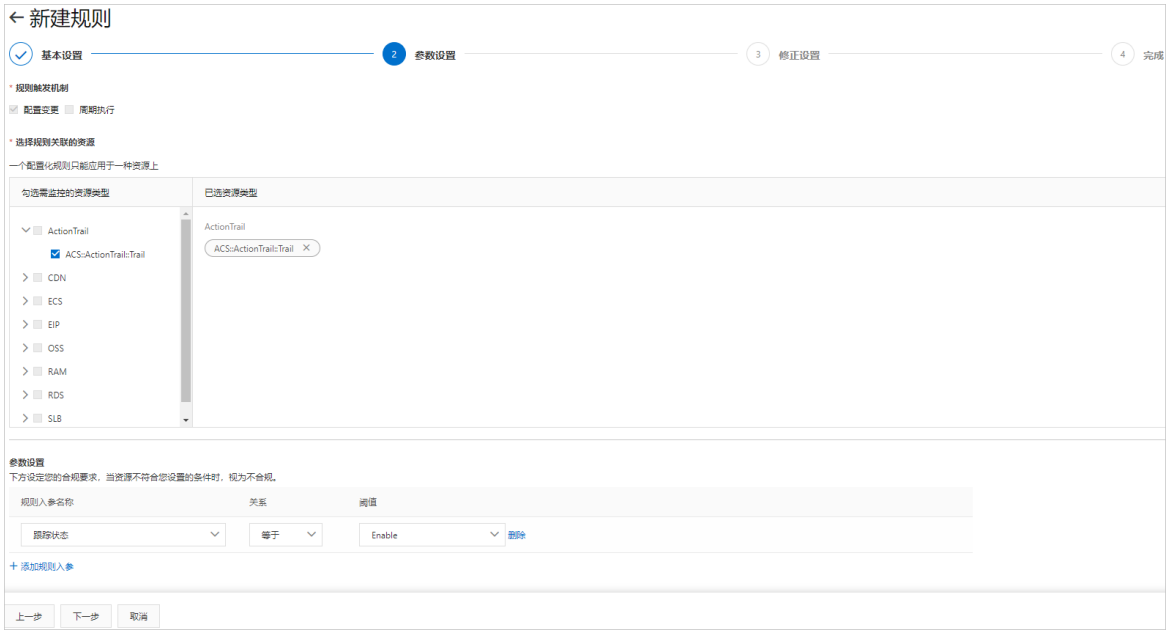
7. 查看规则新建结果。在完成页面，您可以查看规则新建结果。
   - 单击查看规则详情，您可以查看当前规则的规则详情和修正详情。
   - 单击返回规则列表，您可以在管理合规规则列表中查看该规则，规则状态为应用中。

通过可视化编辑器新建规则

1. 登录配置审计控制台。
2. 在左侧导航栏，选择管理合规规则。
3. 在管理合规规则页面，单击新建规则。
4. 在基本设置页面，选择规则配置方式为通过可视化编辑器，输入规则名称，选择风险等级，单击下一步。



5. 在**参数设置**页面，选择规则触发机制、规则关联资源和规则入参，单击**下一步**。



   - 选择规则关联的资源后，规则将监听您账号下该资源类型的所有实体资源。一条规则可以关联一个资源类型。
   - 选择**规则入参名称**、**关系**和**阈值**。

6. 在**修正设置**页面，**修正执行方式**默认为**不执行修正**，单击**提交**。

   如果您需要为当前规则绑定修正模板，请参见设置自动修正或设置手动修正。

7. 查看规则新建结果。在**完成**页面，您可以查看规则新建结果。
   - 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**修正详情**。
   - 单击**返回规则列表**，您可以在**管理合规规则**列表中查看该规则，规则状态为**应用中**。

2.3. 修改规则

当已有规则不能满足您资源审计的要求时，您可以修改规则中参数的阈值。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**页面，单击目标规则对应**操作**列的**编辑**。
4. 在**基本设置**页面，修改规则的备注信息，单击**下一步**。
5. 在**参数设置**页面，您可以根据页面提示修改相应配置信息，单击**下一步**。
   - 当目标规则**基本设置**页面的**规则配置方式**为**使用托管规则**，且存在参数时，您可以修改规则入参的阈值。
   - 当目标规则**基本设置**页面的**规则配置方式**为**通过函数计算**时，您可以修改资源类型和添加规则入参。
   - 当目标规则**基本设置**页面的**规则配置方式**为**通过可视化编辑器**时，您可以修改规则入参的阈值。
6. 在**修正设置**页面，选择修正设置的执行方式为**不执行修正**，单击**提交**。

   当您需要为预设规则**required-tags**绑定模板时，选择**修正执行方式**为**自动执行**或**手动执行**，在**修正模板**的下拉列表中选择对应的默认官方模板，根据界面引导完成服务授权，单击**提交**。
7. 查看规则修改结果。在**完成**页面，您可以查看规则修改结果。
   - 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**修正详情**。
   - 单击**返回规则列表**，您可以在**管理合规规则**列表中查看该规则，规则状态为**应用中**。

2.4. 停用规则

当您暂时无需检测指定规则时，可以对其执行停止操作。

前提条件

请您确保规则的**运行状态**为**应用中**。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**页面，单击目标规则对应**操作**列的

   ，选择**停用规则**。
4. 在**确定停用规则？**对话框中，单击**确定**。
5. 在**手机验证**对话框中，单击**点击获取**。阿里云会向您绑定的手机发送一个校验码。
6. 输入**校验码**，单击**确定**。
7. 查看规则状态。在**管理合规规则**页面，您可以通过筛选功能查看**已停用**的规则。

后续步骤

处于**已停用**状态的规则，您可以单击其对应**操作**列的

，选择**启用规则**，使规则重新处于**应用中**状态。

2.5. 删除规则

您只能删除当前账号新建的规则，不能删除以level3为前缀的规则。删除规则后，其配置信息不再保留。

前提条件

请确保您已停用规则，操作方法请参见停用规则。

背景信息

当您开启等保预检时，配置审计自动为您新建多条以level3为前缀的等保规则，该规则不允许删除。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**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？**对话框中，单击**停用并删除**。
     c. 在**手机验证**对话框中，单击**点击获取**。
     阿里云会向您绑定的手机发送一个校验码。
     d. 输入**校验码**，单击**确定**。
   - 批量删除
     a. 选中目标规则对应复选框，单击  。
     b. 在**批量删除**对话框中，单击**确定**。
     c. 在**手机验证**对话框中，单击**点击获取**。
     阿里云会向您绑定的手机发送一个校验码。
     d. 输入**校验码**，单击**确定**。
5. 查看删除规则。在**管理合规规则**页面，规则已被删除。

2.6. 手动执行审计

当您修改规则后，如需立刻看到审计结果，可以手动执行审计。如果不执行手动审计，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**。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**页面，通过筛选功能找到指定规则。
4. 单击目标规则的**规则名称/规则Id**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**页面，单击右上角的**重新审计**按钮。

2.7. 查看规则详情

您可以在目标规则详情页面，查看当前规则的统计数据、基本信息、触发机制和关联资源的合规结果。

规则评估统计

在指定规则详情页面，您可以查看其执行结果统计数据。

数据项	描述
累计审计资源数	该规则从启用至今，累计评估过的资源数，包括您已经释放的资源。
当前关联资源数	该规则当前有效账号下关联的资源数，不包括已经释放的资源。
合规资源数	当前关联的资源中，上次评估结果为**合规**的资源数量。
不合规资源数	当前关联的资源中，上次评估结果为**不合规**的资源数量。

> **说明** 资源数指真实的实体资源，而非资源类型数。

基本信息

您可以查看规则名称、备注、规则创建时间、规则状态、规则ARN和最近触发时间等。

规则触发机制

您可以查看规则的触发器类型、更改范围、监控范围和规则参数列表。

关联资源的合规结果

规则的监控范围以资源类型作为维度，该列表是资源实体列表。例如：某规则关联到云服务器ECS的实例上，如果该账号下有20个ECS实例，则列表显示20个ECS实例。

在**关联资源的合规结果**列表中，您可以查看实体资源ID，以及最近一次评估结果。您可以通过**操作**列执行如下操作：

- 单击**详情**，查看该资源详情。
- 单击**配置时间线**，查看该资源的配置时间线。
- 单击**合规时间线**，查看该资源的合规时间线。
- 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。

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服务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。

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。修正设置的使用方法如下：

- 执行修正设置

  当**修正执行方式**选择**自动执行**或**手动执行**时，您需要选择修正模板，根据提示授权，完成修正设置。您也可以在完成修正设置后，选择**不执行修正**，达到保留修正设置但不执行修正的目的。当您需要为该规则设置修正时，只需选择修正执行方式即可完成修正设置。

- 不执行修正设置

  当**修正执行方式**选择**不执行修正**时，可以跳过修正设置。

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

- 目前仅规则required-tags支持设置修正模板，配置审计将逐步支持其他规则。
- 目前仅支持选择官方提供的修正器模板，不支持选择自定义的修正模板。
- 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。
- 目前规则required-tags的修正器模板仅支持ECS实例、VPC实例、SLB实例、RDS实例、ECS磁盘五种资源类型的不合规修正。

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。

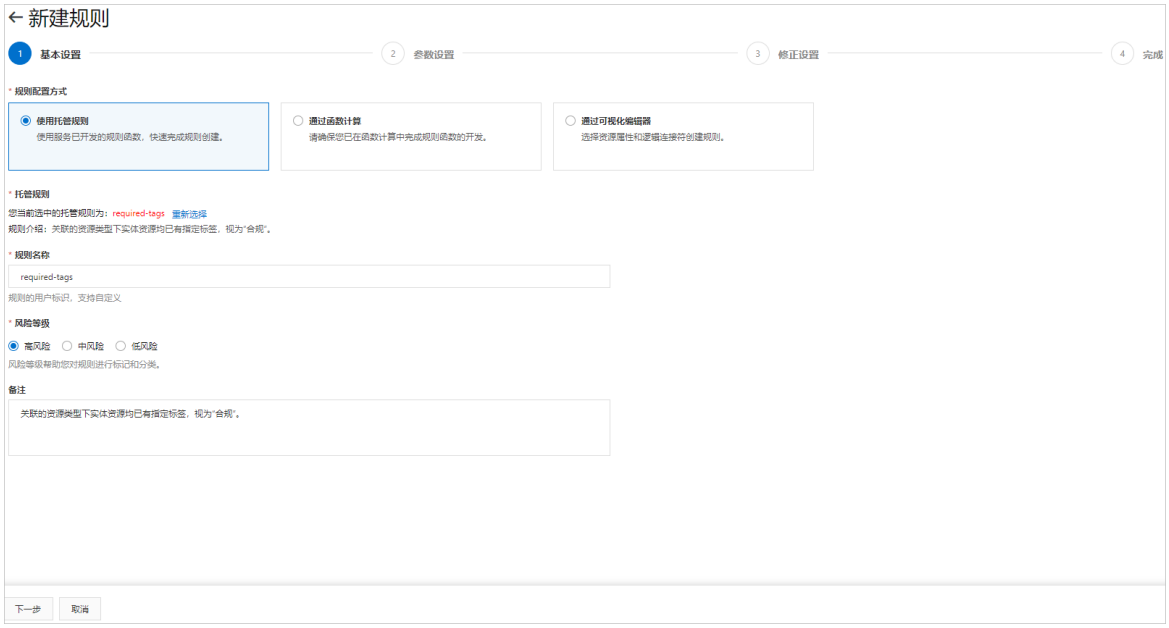
背景信息

本文以新建托管规则required-tags为例，为您介绍设置自动修正的操作方法。

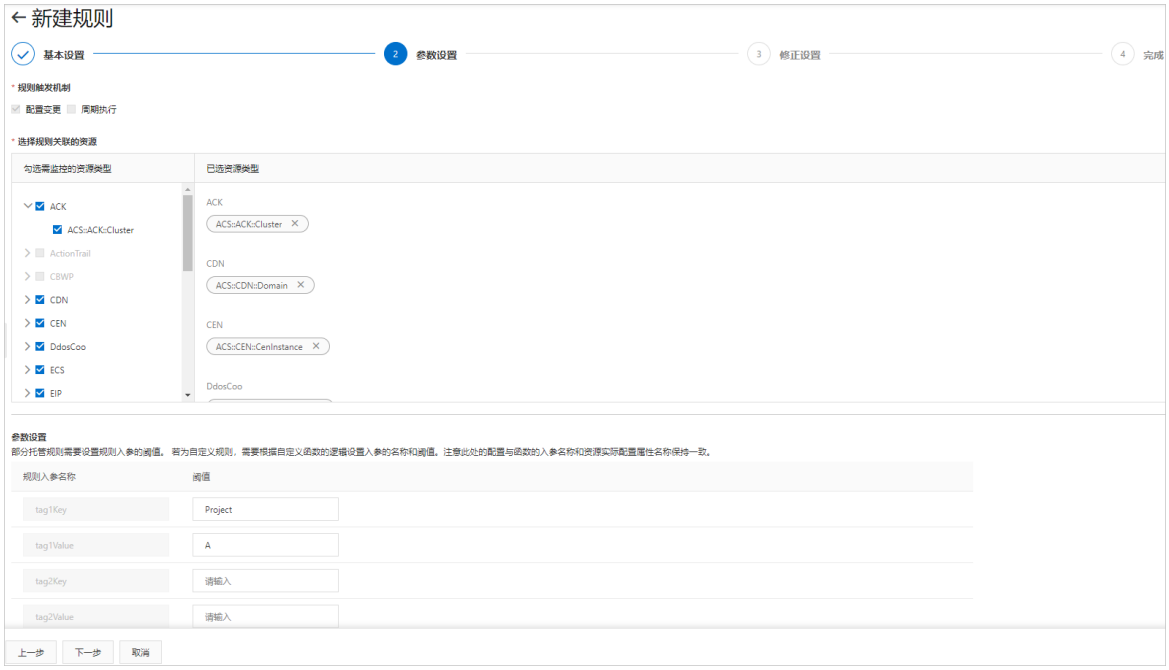
托管规则required-tags用于检测关联资源是否绑定指定标签。例如，您需要所有ECS实例均绑定标签“Project=A”，您可以通过required-tags规则监控所有ECS实例，当配置审计发现有ECS实例未绑定该标签时，该规则评估结果为不合规。如果您订阅了资源合规事件，则配置审计会向您指定的MNS Topic发送不合规告警，操作方法请参见发送资源事件到消息服务MNS。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择管理合规规则。
3. 在管理合规规则页面，单击新建规则。
4. 在管理合规规则页面，选择规则配置方式为使用托管规则，搜索并选中required-tags，选择该规则的风险等级，单击下一步。



5. 在参数设置页面，输入标签Key和Value的阈值，单击下一步。

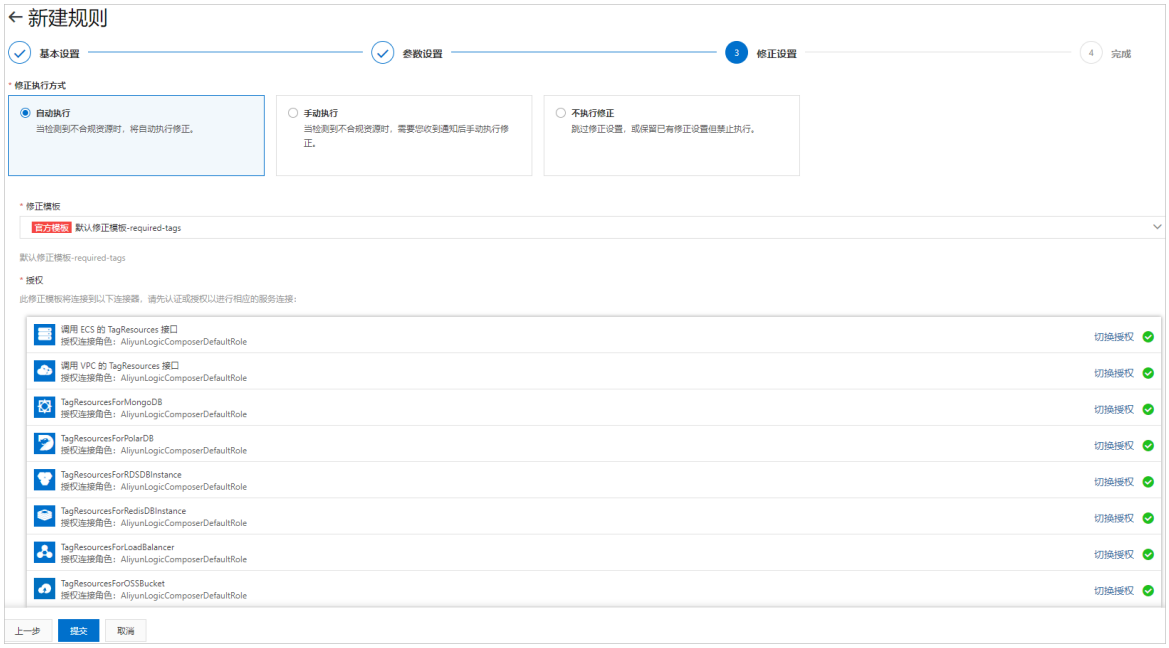


如果您需要检测多组标签，则可以依次填写Key和Value的阈值，最多支持检测6组标签。多组标签之间是与的关系，只有当目标资源同时绑定您配置的标签时，规则评估结果为**合规**。如果您需要实现或的关系，则请多次使用该托管规则新建多条规则。

例如，您需要账号下所有资源均绑定标签“Project=A”，可以使用**required-tags**规则检测资源，当配置审计检测到资源未绑定该标签时，该规则评估结果为**不合规**。

> **说明** 规则触发机制、关联资源和入参名称均采用默认值。

6. 在**修正设置**页面，选择修正设置的执行方式为**自动执行**，在**修正模板**的下拉列表中选择对应的默认官方模板，根据界面引导完成服务授权，并填写资源属性的期望值，单击**提交**。



7. 查看修正结果。当该条规则被评估为**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预设的期望值。

- 在管理合规规则列表中查看
  a. 在管理合规规则页面，筛选出合规评估情况为不合规的规则。
  b. 单击目标规则对应操作列的详情或规则名称/规则Id链接。
  c. 单击修正详情页签，您可以查看具体的修正设置和修正历史。
- 在查看全局资源中查看
  a. 在资源列表页面，通过筛选或搜索功能找到不合规的资源。
  b. 单击资源ID/资源名称链接，在资源信息页签，查看资源的最新审计结果。
  c. 在最新审计结果区域，单击目标规则的规则名称链接，跳转到目标规则的规则详情页签。
  d. 单击修正详情页签，您可以查看具体的修正设置和修正历史。

> 说明
> - 如果修改修正模板的参数后重新保存，则执行结果和历史记录会被清零。
> - 修改修正模板的执行方式不影响执行结果和历史记录。

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

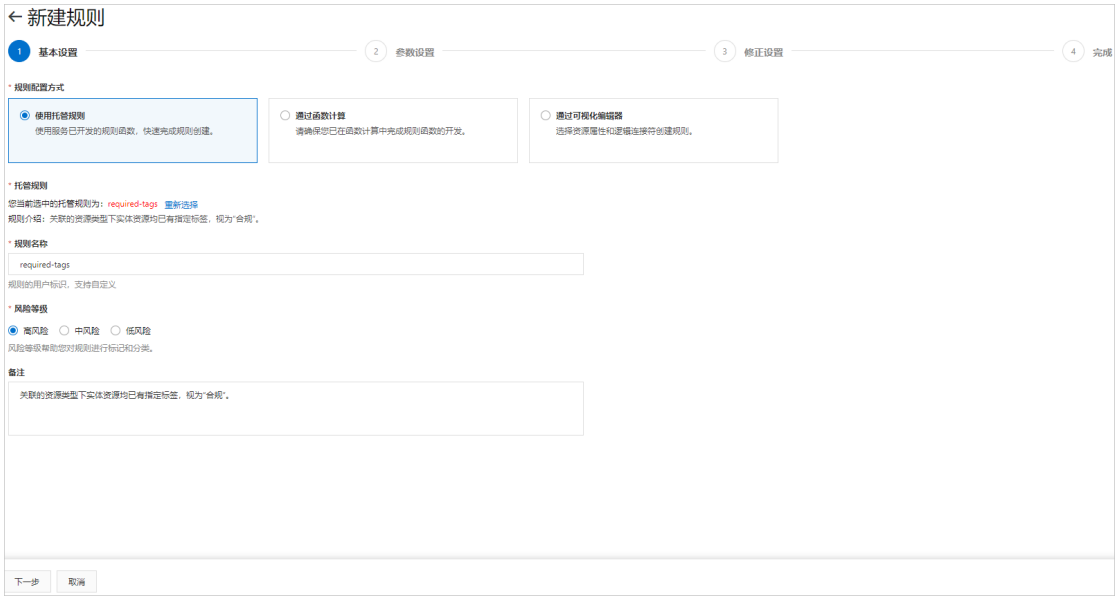
本文以新建托管规则required-tags为例，为您介绍设置手动修正的操作方法。

托管规则required-tags用于检测关联资源是否绑定指定标签。例如，您需要所有ECS实例均绑定标签“Project=A”，您可以通过required-tags规则监控所有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MNS Topic发送不合规告警，操作方法请参见发送资源事件到消息服务MNS。

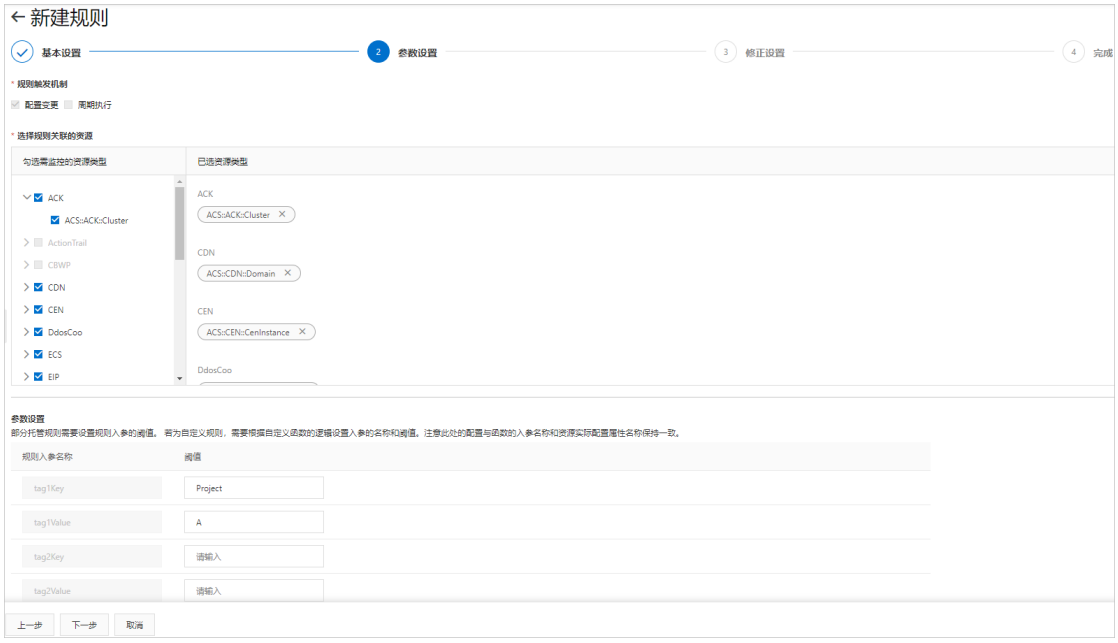
操作步骤

1. 设置修正。
   i. 登录配置审计控制台。
   ii. 在左侧导航栏，选择管理合规规则。
   iii. 在管理合规规则页面，单击新建规则。

iv. 在**基本设置**页面，选择**规则配置方式**为**使用托管规则**，搜索并选中**required-tags**，选择该规则的**风险等级**，单击**下一步**。



v. 在**参数设置**页面，规则触发机制、关联资源和入参均为默认值，输入标签Key和Value的阈值，单击**下一步**。

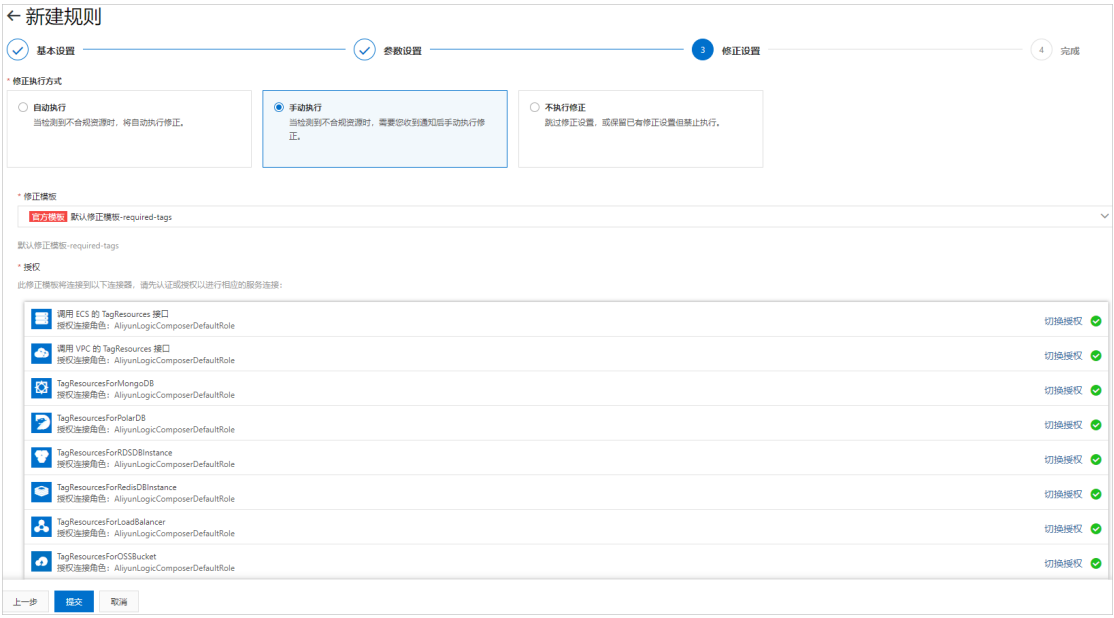


如果您需要检测多组标签，则可以依次填写Key和Value的阈值，最多支持检测6组标签。多组标签之间是与的关系，只有当目标资源同时绑定您配置的标签时，规则评估结果为**合规**。如果您需要实现或的关系，则请多次使用该托管规则新建多条规则。

例如，您需要账号下所有资源均绑定标签“Project=A”，可以使用**required-tags**规则检测资源，当配置审计检测到资源未绑定该标签时，该规则评估结果为**不合规**。

> **说明** 规则触发机制、关联资源和入参名称均采用默认值。

vi. 在**修正设置**页面，选择修正设置的执行方式为**手动执行**，在**修正模板**的下拉列表中选择对应的默认官方模板，根据界面引导完成服务授权，并填写资源属性的期望值，单击**提交**。



vii. 查看规则新建结果。在**完成**页面，您可以查看规则新建结果和修正详情。

- 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**修正详情**。
- 单击**返回规则列表**，您可以在**管理合规规则**列表中查看该规则，规则状态为**应用中**。

2. 执行修正。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，将资源配置修改为您预设的期望值。手动执行修正的操作方法如下：

   i. 在**管理合规规则**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。

   ii. 在目标规则的管理页面，单击**修正详情**页签。

   iii. 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. 查看修正结果。当该条规则被评估为**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预设的期望值。

   - 在**管理合规规则**列表中查看
     a. 在**管理合规规则**页面，筛选出**合规评估情况**为**不合规**的规则。
     b. 单击目标规则对应**操作**列的**详情**或**规则名称/规则Id**链接。
     c. 单击**修正详情**页签，您可以查看具体的修正设置和修正历史。
   - 在**查看全局资源**中查看
     a. 在**资源列表**页面，通过筛选或搜索功能找到不合规的资源。
     b. 单击**资源ID/资源名称**链接，在**资源信息**页签，查看资源的最新审计结果。
     c. 在**最新审计结果**区域，单击目标规则的**规则名称**链接，跳转到目标规则的**规则详情**页签。
     d. 单击**修正详情**页签，您可以查看具体的修正设置和修正历史。

> **说明**
>
> - 如果修改修正模板的参数后重新保存，则执行结果和历史记录会被清零。
> - 修改修正模板的执行方式不影响执行结果和历史记录。

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。

前提条件

请确保您已新建规则，且已设置修正，操作方法请参见设置手动修正或设置自动修正。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**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**。

4.查看合规结果

4.1. 查看规则评估结果

您可以通过以下三种方式查看资源的规则评估结果：

- 方法一：在**概览**页面的**合规审计统计**区域查看。
- 方法二：在**管理合规规则**列表的**合规评估情况**中查看。
- 方法三：在指定规则详情页面，查看该规则的评估结果，请参见查看规则详情。

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记录。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

资源的合规时间线包括如下要素：

- 合规时间线上的点
  - 起点：资源第一次被规则评估的时间。资源被规则评估可能是定时周期评估、手动执行评估或实时的配置变更触发评估。
  - 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：不同于资源的配置时间线，资源的规则评估根据实时的配置变更情况触发，并不具备连续性，也就不存在断点。
- 合规时间线的内容

  合规时间线是资源的一组合规评估记录。
  - 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，包括手动执行、周期执行、变更触发。
  - 合规评估结果：在合规时间线的左侧，每个节点会标注本次评估的结果**合规**或**不合规**，方便您快速找到需要关注的节点。
  - 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实时变更触发，则会显示**本次变更细节**，以便您快速查看**不合规**资源的配置变更详情。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**查看全局资源**。
3. 通过筛选或搜索功能找到指定资源。
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**，查看资源的合规时间线详情。

5.托管规则

5.1. 托管规则列表

当您在配置审计控制台新建规则时，可以直接选用托管规则。

如果您需要其他托管规则，可以提交工单。阿里云评估后会酌情支持，并将具备普遍适用性的规则实现为托管规则。

配置审计支持的托管规则和不合规规则的修复方法如下：

- ActionTrail
- CDN
- DDH
- ECS
- EIP
- OSS
- RAM
- RDS
- TAG
- SLB

5.2. ActionTrail

本文介绍配置审计为操作审计提供的托管规则详情，以及当规则不合规时的修复方法。

actiontrail-enabled

检测您账号是否在操作审计中创建了跟踪，如果未创建，则视为不合规。

触发机制：配置更改

资源：ACS::ActionTrail::Trail

参数：无

修复指南：当跟踪状态为关闭时，会导致该规则不合规。打开**是否开启日志记录**开关。配置审计会在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台
  i. 登录操作审计控制台。
  ii. 在左侧导航栏，单击**操作审计 > 跟踪列表**。
  iii. 在**跟踪列表**页面，单击目标跟踪名称链接，打开**是否开启日志记录**开关。
  iv. 单击**确定**。
- API

  调用StartLogging接口启动跟踪，请参见StartLogging。

5.3. CDN

本文介绍配置审计为CDN提供的托管规则详情，以及当规则不合规时的修复方法。

cdn-domain-https-enabled

检测CDN域名是否启用HTTPS加速，如果开启，则视为合规。

触发机制：配置更改

资源：ACS::CDN::Domain

参数：无

修复指南：当您账号下的CDN域名未启用HTTPS时，会导致该规则不合规。打开**HTTPS安全加速**开关。配置审计会在10分钟内感知到您的修改并自动启动审计。

控制台操作：

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**HTTPS配置**。
5. 在**HTTPS证书**区域，单击**修改配置**。
6. 在**HTTPS设置**页面，打开**HTTPS安全加速**开关，配置证书相关参数。
7. 单击**确定**。

5.4. DDH

本文介绍配置审计为专有宿主机（DDH）提供的托管规则详情，以及当规则不合规时的修复方法。

ddh-cpu-min-count-limit

您账号下的DDH实例的vCPU总量大于等于您设置的阈值，视为合规。

触发机制：配置更改

资源：ACS:ECS:DedicatedHost

参数：cpuCount（vCPU总量）

修复指南：当您账号下的DDH实例的vCPU总量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 方法一：DDH实例创建后无法更改其规格，需要重新创建符合规则的DDH实例。配置审计会在10分钟内感知到您的修改并自动启动审计。

  不合规DDH实例处理方法：释放该DDH实例（仅支持按量付费的DDH）。包年包月的DDH实例无法手动释放。

  风险：DDH实例被释放后，对应的所有资源都不再可用。DDH中的ECS实例所有数据丢失后，不可恢复。您可以根据业务需要，在DDH实例释放前，在您账号下的不同DDH之间迁移ECS实例。

  在不同DDH之间迁移ECS实例的操作方法，请参见在不同DDH之间迁移ECS实例。
- 方法二：修改规则参数的阈值，单击重新审计后刷新页面进行验证。

  查看DDH实例的vCPU总量的操作方法，请参见查看DDH资源。

ddh-memory-min-size-limit

您账号下的DDH实例的内存总量大于等于您设置的阈值，视为合规。

触发机制： 配置更改

资源：ACS:ECS:DedicatedHost

参数：memorySize（内存总量/GiB）

修复指南：当您账号下的DDH实例的内存总量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 方法一：DDH实例创建后无法更改其规格，重新创建符合规则的DDH实例。配置审计会在10分钟内感知到您的修改并自动启动审计。

  不合规DDH实例的处理方法：释放该DDH实例。

  > 说明 仅支持释放按量付费的DDH实例，不支持释放包年包月的DDH实例

  风险：DDH实例被释放后，对应的所有资源不可用。DDH中的ECS实例所有数据丢失，不可恢复。

  您可以根据业务所需，在DDH实例释放前，在您账号下的不同DDH之间迁移ECS实例。

  在不同DDH之间迁移ECS实例的操作方法，请参见在不同DDH之间迁移ECS实例。
- 方法二：修改规则参数的阈值，单击重新审计后刷新页面进行验证。

  查看DDH实例的内存总量的操作方法，请参见查看DDH资源。

ddh-socket-min-count-limit

您账号下的DDH实例的Socket数量等于您设置的阈值，视为合规。

触发机制：配置更改

资源：ACS:ECS:DedicatedHost

参数：socketCount

修复指南：当您账号下的DDH实例的Socket数量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 方法一：DDH实例创建后无法更改其规格，重新创建符合规则的DDH实例。配置审计会在10分钟内感知到您的修改并自动启动审计。

  不合规的DDH实例处理方法：释放该DDH实例。（仅支持按量付费的DDH实例）。包年包月DDH实例无法手动释放。

  风险：DDH实例被释放后，对应的所有资源都不再可用。DDH中的ECS实例所有数据丢失，不可恢复。

  您可以根据业务需要，在DDH释放前，在您账号下的不同DDH之间迁移ECS实例。

  在不同DDH之间迁移ECS实例的操作方法，请参见在不同DDH之间迁移ECS实例。
- 方法二：修改规则参数的阈值，单击重新审计后刷新页面进行验证。

  查看DDH实例的Socket数的操作方法，请参见查看DDH资源。

5.5. ECS

本文介绍配置审计为云服务器ECS提供的托管规则详情，以及当规则不合规时的修复方法。

ecs-cpu-min-count-limit

检查ECS实例的CPU数量最小限制。

触发机制：配置更改

资源：ACS::ECS::Instance

参数：cpuCount（CPU最小核数）

修复指南：当您账号下的ECS实例CPU核数小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 方法一：更改ECS实例规格（停止状态的实例才能更改实例规格），使更改后的ECS实例的CPU核数大于等于您设置的规则参数阈值。配置审计会在10分钟内感知到您的修改并自动启动审计。操作方法如下：
  - 控制台

    更改ECS实例规格的方法：在ECS控制台的实例列表中，单击**更改实例规格**。
  - API

    调用ModifyInstanceSpec接口，修改实例规格InstanceType的值，请参见ModifyInstanceSpec。
- 方法二：修改规则参数阈值，将ECS实例的实例规格添加到规则参数阈值中。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-desired-instance-type

检查ECS实例是否具有指定的实例类型。

资源：ACS::ECS::Instance

触发机制：配置更改

参数：instanceTypes（ECS实例类型列表，多个以英文逗号（,）分隔，例如：`t2.small, m4.large, i2.xlarge` 。）

修复指南：您账号下ECS实例规格族未在规则参数阈值中列举出，则会导致该规则不合规。规则参数阈值列表中包含ECS实例的实例规格，该实例即为合规。修复方法如下：

- 方法一：更改ECS实例规格（停止状态的实例才能更改实例规格），更改成规则参数阈值中列出的实例规格中的某一个。配置审计会在10分钟内感知到您的修改并自动启动审计。操作方法如下：
  - 控制台

    更改ECS实例规格的方法：在ECS控制台的实例列表中，单击**更改实例规格**。
  - API

    调用ModifyInstanceSpec接口，修改实例规格InstanceType的值，请参见ModifyInstanceSpec。
- 方法二：编辑规则参数阈值，将ECS实例的实例规格添加到规则参数阈值中。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-disk-encrypted

检查处于连接状态的磁盘是否已加密。如果使用KMSKeyId参数为加密指定了KMS密钥ID，则该规则将检查连接状态中的磁盘是否使用该KMS密钥进行加密。

资源：ACS::ECS::Disk

触发机制：配置更改

参数：kmsKeyIds（用于加密卷的KMS密钥的ID。）

修复指南：

- 如果您账号下所有处于关联状态的云盘若未加密，则会导致该规则不合规。
- 如果加密云盘的KMSKeyId不在规则参数阈值中，则会导致该规则不合规。

加密云盘的KMSKeyId存在于规则参数阈值中，该云盘即为合规。目前云盘加密功能只支持数据盘，解决方法只针对于数据盘。修复方法如下：

- 方法一：重新创建加密云盘，并用规则参数KMSKeyId中的阈值对云盘进行加密。配置审计会在10分钟内感知到您的修改并自动启动审计。

  不合规的云盘处理方法：释放云盘。

  风险：释放云盘会导致云盘数据丢失。释放云盘风险及操作步骤，请参见释放云盘。
- 方法二：将加密云盘的KMSKeyId添加到规则参数的阈值中。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-disk-in-use

检查磁盘是否在使用中。

资源：ACS::ECS::Disk

触发机制：配置更改

参数：无

修复指南：您账号下的ECS云盘处于待挂载状态中，会导致该规则不合规。将云盘挂载到实例上，使其状态变为**使用中**，既为合规。修复方法如下：

- 控制台

  进入云服务器ECS控制台，通过云盘列表，单击**更多 > 挂载**，将云盘挂载到实例上。
- API

  调用AttachDisk接口为一台ECS实例挂载一块按量付费的数据盘，请参见AttachDisk。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-gpu-min-count-limit

检查ECS实例的GPU数量最小限制。

触发机制：配置更改

资源：ACS::ECS::Instance

参数：gpuCount（ECS实例包含的最小GPU数量。）

修复指南：当您账号下的ECS实例GPU数量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 方法一：更改ECS实例规格（停止状态的实例才能更改实例规格），使更改后的ECS实例的GPU数量大于等于您设置的规则参数阈值。配置审计会在10分钟内感知到您的修改并自动启动审计。操作方法如下：
  - 控制台

    更改ECS实例规格的方法：在ECS控制台的实例列表中，单击**更改实例规格**。
  - API

    调用ModifyInstanceSpec接口，修改实例规格InstanceType的值，请参见ModifyInstanceSpec。

  若不合规实例为本地存储的实例，需要重新购买符合规则要求的ECS实例。

不合规的旧ECS实例处理方法：释放ECS实例（仅支持按量付费的ECS实例）。对于包年包月实例，计费周期到期后，您可以手动释放；如果15天内未续费，实例也会自动释放。实例到期前，您可以申请退款提前释放实例，也可以将计费方式转为按量付费后释放实例。

风险：释放ECS实例后会丢失所有数据，释放前，请做好备份。

释放实例风险及操作步骤，请参见释放实例。

- 方法二：编辑规则参数阈值，将ECS实例的实例规格添加到规则参数阈值中。

合规验证方法：在配置审计的规则详情页面，单击重新审计进行验证，或等10分钟配置审计自动启动验证。

ecs-instance-attached-security-group

检测ECS实例是否附加到特定安全组，已开通视为合规。

触发机制：配置更改

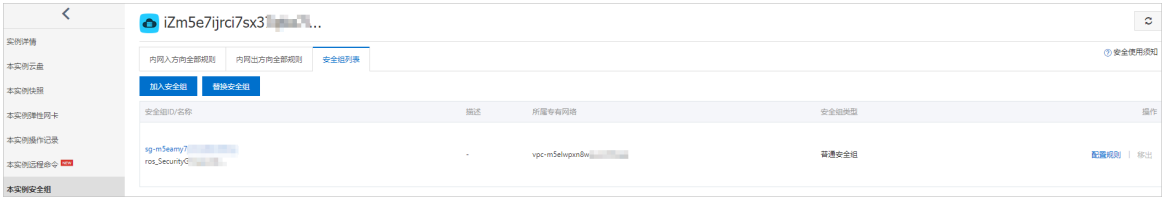
资源：ACS::ECS::Instance

参数：securityGroupIds（安全组ID列表，多个以英文逗号（,）分隔，例如：`sg-hp3ebbv7ir****,sg-hp3ebbv****`。）

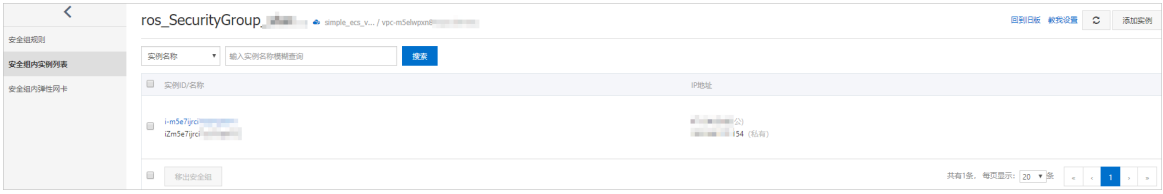
修复指南：您账号下的ECS实例加入的安全组ID未在规则参数阈值中列举出，则会导致该规则不合规。规则参数阈值列表中包含实例加入的任何一个安全组ID，该实例合规。修复方法如下：

- 方法一：将ECS实例加入到规则参数阈值中列出的安全组中。配置审计会在10分钟内感知到您的修改并自动启动审计。
- 方法二：将ECS实例加入的安全组ID添加到规则参数阈值中。绑定ECS实例与安全组的方法如下：
  - 控制台

    方法一：在ECS控制台的**本实例安全组**的**安全组列表**页签下，单击**加入安全组**。

    方法二：在ECS控制台的**安全组内实例列表**页面，单击右上角的**添加实例**。

  - API

    调用JoinSecurityGroup接口将一台ECS实例加入到指定的安全组，请参见JoinSecurityGroup。

合规验证方法：在配置审计的规则详情页面，单击重新审计进行验证，或等10分钟配置审计自动启动验证。

ecs-instance-deletion-protection-enabled

检测您账号ECS实例是否开启释放保护开关（仅支持按量付费支付类型），已开通视为合规。

触发机制：配置更改

资源：ACS::ECS::Instance

参数：无

修复指南：检测您账号ECS实例是否开启释放保护开关（仅支持按量付费支付类型），未开启会导致该规则不合规。修复方法如下：

- 控制台

  在ECS控制台的实例列表中，单击目标实例对应的**更多 > 实例设置 > 修改实例释放保护**，打开**实例释放保护**开关。配置审计会在10分钟内感知到您的修改并自动启动审计。

- API

  通过ModifyInstanceAttribute接口将DeletionProtection的值设为true，请参见ModifyInstanceAttribute。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-instances-in-vpc

检查您的ECS实例是否属于某个VPC。您可以指定待关联实例的VPC ID，如果ECS实例属于指定VPC ID返回合规；ECS实例不属于指定VPC ID返回不合规；ECS实例无VPC信息，返回不适用。

触发机制：配置更改

资源：ACS::ECS::Instance

参数：vpcIds（ECS实例的VPC ID，多个以英文逗号（,）分隔，例如：`vpc-25vk5****,vpc-6wesmaymqkgiuru5x****,vpc-8vbc16loavvujlzli****`。）

修复指南：您账号下ECS实例绑定的VPC ID未在规则参数阈值中列举出，则会导致该规则不合规。修复方法如下：

- 方法一：重新创建ECS实例，并将实例的VPC ID绑定到规则参数阈值中。配置审计会在10分钟内感知到您的修改并自动启动审计。

  不合规ECS实例处理方法：释放ECS实例（仅支持按量付费的ECS实例）。对于包年包月实例，计费周期到期后，您可以手动释放；如果15天内未续费，实例也会自动释放。实例到期前，您可以申请退款提前释放实例，也可以将计费方式转为按量付费后释放实例。

  风险：释放ECS实例后会丢失所有数据，释放前，请做好备份。

  释放实例风险及操作方法，请参见释放实例。

  当您购买ECS实例时，在**网络与安全**页面选择专有网络。

- 方法二：编辑规则参数阈值，将ECS实例绑定的VPC ID添加到规则参数阈值中。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-instance-no-public-ip

ECS实例未直接绑定公网IP，视为合规。该规则仅适用于IPv4协议。

触发机制：配置更改

资源：ACS::ECS::Instance

参数：无

修复指南：您账号下的ECS实例绑定公网IP，会导致该规则不合规。当ECS实例只有私有地址时，资源评估结果为合规。修复方法如下：

- 方法一：如果ECS绑定了弹性公网IP，则将弹性公网IP进行解绑。配置审计会在10分钟内感知到您的修改并自动启动审计。

在ECS控制台的实例列表中，单击目标实例对应的**更多 > 网络和安全 > 解绑弹性IP**，解绑弹性IP。

- 方法二：如果ECS绑定了公网IP，则将公网IP转换成弹性公网IP，在将弹性公网IP进行解绑。配置审计会在10分钟内感知到您的修改并自动启动审计。

  在ECS控制台的实例列表中，单击目标实例对应的**更多 > 网络和安全 > 公网IP转换为弹性公网IP**，将公网IP转换成弹性公网IP。配置审计会在10分钟内感知到您的修改并自动启动审计。

- 方法三：当您购买新ECS实例时，在**网络和安全组**页面，不勾选**公网IP**中的**分配公网IPv4地址**。配置审计会在10分钟内感知到您的修改并自动启动审计。

  不合规的ECS实例处理方法：释放ECS实例（仅支持按量付费的ECS实例）。对于包年包月实例，计费周期到期后，您可以手动释放；如果15天内未续费，实例也会自动释放。实例到期前，您可以申请退款提前释放实例，也可以将计费方式转为按量付费后释放实例。

  风险：释放ECS实例后会丢失所有数据，释放前，请做好备份。

  释放实例风险及操作方法，请参见释放实例。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

ecs-memory-min-size-limit

检查ECS实例内存最小容量限制。

触发机制：配置更改

资源：ACS::ECS::Instance

参数：memorySize（ECS实例内存最小容量）

修复指南：当您账号下的ECS实例内存容量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 方法一：更改ECS实例规格（停止状态的实例才能更改实例规格），使更改后ECS实例的内存大于等于您设置的规则参数阈值。操作方法如下：
  - 控制台

    更改ECS实例规格的方法：在ECS控制台的实例列表中，单击**更改实例规格**。

  - API

    调用ModifyInstanceSpec接口，修改实例规格InstanceType的值，请参见ModifyInstanceSpec。

- 方法二：修改规则参数的阈值，将ECS实例的实例规格添加到规则参数的阈值中。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

sg-public-access-check

安全组检测是否匹配0.0.0.0/0。

触发机制：配置更改

资源：ACS::ECS::SecurityGroup

参数：无

修复指南：ECS安全组入方向规则，授权策略为允许，授权对象为0.0.0.0/0，会导致该规则不合规。修复方法如下：

- 方法一：将授权对象为0.0.0.0/0的安全组入方向规则的授权策略调整为拒绝或者修改授权对象。
- 方法二：删除授权策略为允许，授权对象为0.0.0.0/0安全组入方向规则。

- 控制台

  调整授权策略和修改授权对象：在ECS控制台的**安全组规则**的**入方向**页签，编辑安全组规则，将授权策略设置为拒绝，或者修改授权对象。

  删除安全组规则：在ECS控制台的**安全组规则**的**入方向**页签，删除授权策略为允许，授权对象为0.0.0.0/0的规则。

- API

  调用ModifySecurityGroupRule修改安全组入方向规则Policy（访问权限）或者SourceCidrIp（授权对象）的值，请参见ModifySecurityGroupRule。

  调用RevokeSecurityGroup删除一条安全组入方向规则，请参见RevokeSecurityGroup。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

sg-risky-ports-check

检测安全组是否开启风险端口。

触发机制：配置更改

资源：ACS::ECS::SecurityGroup

参数：ports（风险端口）

修复指南：ECS安全组规则（包含出方向和入方向）开启的端口号出现在规则参数阈值中时，会导致该规则不合规。“-1/-1”代表不限制端口，若在安全组规则中设置了“-1/-1”，会导致该规则不合规。修复方法如下：

- 方法一：关闭ECS安全组规则中，规则参数阈值中列出的端口，即将对应端口的授权策略设置为拒绝。
- 方法二：删除开启了规则参数阈值中列出端口的安全组规则。
- 方法三：修改对应安全组规则的端口范围。
- 方法四：编辑规则参数阈值，将对应的端口号从阈值中删除。
  - 控制台

    在**入方向**的**快速添加**页面，将**授权策略**设置为拒绝或修改端口范围。

    在**入方向**列表中，单击目标授权策略对应的**删除**，删除已开启规则参数阈值中列出端口的安全组规则。

- API
  - 调用ModifySecurityGroupRule（入方向）和ModifySecurityGroupEgressRule（出方向）修改Policy（访问权限）或PortRange（端口范围）的值，请参见ModifySecurityGroupRule和ModifySecurityGroupEgressRule。
  - 调用RevokeSecurityGroup（入方向）和RevokeSecurityGroupEgress（出方向）删除一条安全组规则，请参见RevokeSecurityGroup。

合规验证方法：在配置审计的规则详情页面，单击**重新审计**进行验证，或等10分钟配置审计自动启动验证。

5.6. EIP

本文介绍配置审计为弹性公网IP（EIP）提供的托管规则详情，以及当规则不合规时的修复方法。

eip_attached

您可以使用该规则监控弹性公网IP的生效状态合规。

触发机制：配置更改

资源：ACS::EIP::EipAddress

参数：无

修复指南：查看您的弹性公网IP是否绑定实例，如果未绑定，则会导致该规则不合规。将弹性公网IP绑定到实例上，绑定的实例类型有NAT网关，ECS实例，SLB实例，辅助弹性网卡。配置审计会在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台
  - 绑定ECS实例，请参见绑定ECS实例。
  - 绑定NAT网关，请参见绑定NAT网关。
  - 绑定SLB实例，请参见绑定SLB实例。
  - 绑定辅助弹性网卡，请参见绑定辅助弹性网卡。
- API

  调用AssociateEipAddress接口将弹性公网IP绑定到同地域的云资源上，请参见AssociateEipAddress。

5.7. OSS

本文介绍配置审计为对象存储（OSS）提供的托管规则详情，以及当规则不合规时的修复方法。

oss-bucket-public-read-prohibited

查看您的OSS Bucket是否不允许公开读取访问权限。如果某个OSS Bucket策略或Bucket ACL允许公开读取访问权限，则该Bucket不合规。

触发机制：配置更改

资源：ACS::OSS::Bucket

参数：无

修复指南：查看您的OSS Bucket是否不允许公开读取访问权限。OSS Bucket的读写权限设置为公共读或公共读写时，会导致该规则不合规。对OSS Bucket读写权限进行设置，将OSS Bucket的读写权限设置为私有。配置审计会在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台

- 登录OSS管理控制台。
- 在左侧导航栏，单击Bucket列表。
- 在Bucket列表中，单击目标Bucket名称。
- 在目标Bucket概览页面，单击权限管理。
- 在读写权限区域，将Bucket ACL修改为私有。
- 单击保存。

- API

  调用PutBucketACL接口修改存储空间（Bucket）的访问权限，将其设置为private（私有），请参见PutBucketACL。

oss-bucket-public-write-prohibited

查看OSS Bucket是否不允许公开写入访问权限。如果某个OSS Bucket策略或BucketACL允许公开写入访问权限，则该Bucket不合规。

触发机制：配置更改

资源：ACS::OSS::Bucket

参数：无

修复指南：查看您的OSS Bucket是否不允许公开写入访问权限。OSS Bucket的读写权限设置为公共读写时，会导致该规则不合规。对OSS Bucket读写权限进行设置，将OSS Bucket的读写权限设置为私有或者公共读。配置审计会在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台
  - 登录OSS管理控制台。
  - 在左侧导航栏，单击Bucket列表。
  - 在Bucket列表中，单击目标Bucket名称。
  - 在目标Bucket概览页面，单击权限管理。
  - 在读写权限区域，将Bucket ACL修改为私有或公共读。
  - 单击保存。

- API

  调用PutBucketACL接口修改存储空间（Bucket）的访问权限，将其设置为private（私有）或public-read（公共读），请参见PutBucketACL。

oss-bucket-referer-limit

检测OSS Bucket是否开启防盗链开关，已开通视为合规。

触发机制：配置更改

资源：ACS::OSS::Bucket

参数：allowReferers（允许的防盗链列表，多个Referer以英文逗号隔开。）

修复指南：

- 情况一：规则入参的阈值非空，Bucket的防盗链开关允许空Referer处于开启状态，且设置的Referer白名单（白名单非空）未在阈值列表中，会导致规则不合规。
  i. 在OSS管理控制台上，关闭Bucket的防盗链开关允许空Referer。

     操作方法请参见设置防盗链。

ii. 在配置审计控制台上，将全部Referer白名单添加到规则参数allowReferers的阈值中。

操作方法请参见修改规则。

- 情况二：规则入参的阈值非空，Bucket的防盗链开关允许空Referer处于关闭状态，但设置的Referer白名单未在阈值列表中，会导致规则不合规。

i. 在OSS管理控制台上，查看Referer白名单。

操作方法请参见设置防盗链。

ii. 在配置审计控制台上，将全部Referer白名单添加到规则参数allowReferers的阈值中。

操作方法请参见修改规则。

- 情况三：规则入参的阈值为空，Bucket的防盗链开关允许空Referer处于关闭状态，会导致规则不合规。

在OSS管理控制台上，开启Bucket的防盗链允许空Referer，操作方法请参见设置防盗链。

oss-bucket-server-side-encryption-enabled

查看并确认您的OSS Bucket开启了服务器端加密功能。

触发机制：配置更改

资源：ACS::OSS::Bucket

参数：无

修复指南：查看您账号下的OSS Bucket是否启用了加密，若未加密，会导致该规则不合规。

将OSS Bucket服务器端加密设置成AES256或者KMS。配置审计会在10分钟内感知到您的修改并自动启动审计。

在OSS管理控制台上，开启服务器端加密功能，操作方法请参见设置服务器端加密。

5.8. RAM

本文介绍配置审计为访问控制（RAM）提供的托管规则详情，以及当规则不合规时的修复方法。

ram-user-mfa-check

检测RAM用户是否开启多因素认证MFA（Multi-factor authentication）。

触发机制：配置更改

资源：ACS::RAM::User

参数：无

修复指南：检测RAM用户是否开通MFA二次验证登录。若未开通，会导致该规则不合规。开启多因素认证后，配置审计在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台

在RAM控制台，为RAM用户开启MFA。操作方法请参见为RAM用户设置多因素认证。

- API

调用UpdateLoginProfile接口修改用户的登录配置，将MFABindRequired的值设置为true（是），请参见UpdateLoginProfile。

5.9. RDS

本文介绍配置审计为云数据库RDS提供的托管规则详情，以及当规则不合规时的修复方法。

rds-cpu-min-count-limit

检查RDS实例的CPU数量最小限制。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：cpuCount（RDS实例包含的最小CPU数量）

修复指南：当您账号下的RDS实例CPU数量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 控制台
  - 方法一：修改RDS实例的CPU核数，使其大于等于您设置的规则入参的阈值。

    在云数据库RDS管理控制台上，修改CPU核数，操作方法请参见变更配置。
  - 方法二：将规则入参的阈值修改为小于等于RDS实例的CPU核数。
    a. 在云数据库RDS管理控制台上，查看RDS实例的CPU核数。
       a. 在**实例列表**中，单击目标实例ID的链接。
       b. 在**基本信息**的**基本信息**区域，您可以查看实例的CPU核数。
    b. 在配置审计控制台上，修改cpuCount的阈值。

       操作方法请参见修改规则。
- API

  调用ModifyDBInstanceSpec接口修改DBInstanceClass的值，请参见变更实例。

rds-desired-instance-type

检查 RDS 实例是否具有指定的实例类型。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：instanceTypes（实例类型，多个以英文逗号（,）分隔，例如：`rds.mysql.s2.large,mysql.n1.micro.1` 。）

修复指南：您账号下RDS实例规格未在规则参数阈值中列举出，则会导致该规则不合规。规则参数阈值列表中包含RDS实例的实例规格，该实例即为合规。修复方法如下：

- 控制台
  - 方法一：修改RDS实例规格，使其为规则入参阈值中的某个值。

    在云数据库RDS管理控制台上，修改RDS实例规格，操作方法请参见变更配置。
  - 方法二：修改规则入参阈值，将RDS实例规格添加到规则入参的阈值中。
    a. 在云数据库RDS管理控制台上，查看RDS实例规格。
       a. 在**实例列表**中，单击目标实例ID的链接。
       b. 在**基本信息**的**配置信息**区域，您可以查看RDS实例规格。
    b. 在配置审计控制台上，将RDS实例规格添加到规则入参的阈值中。

       操作方法请参见修改规则。

- API

  调用ModifyDBInstanceSpec接口修改DBInstanceClass的值，请参见变更实例。

rds-high-availability-category

检查RDS实例是否具备高可用能力。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：无

修复指南：您账号下RDS实例不具备高可用能力，会导致该规则不合规。修复方法如下：

- 控制台
  - 方法一：针对无法升级版本的RDS实例，您需要重新创建实例。

    > 说明 您可以手动释放按量付费实例或退订包年包月实例。
    > - 退订包年包月实例
    >
    >   您可以登录退订管理页面，退订详情请参见退款规则及退订流程。
    > - 释放按量付费实例
    >
    >   释放实例的风险和操作方法请参见释放实例。

    在云数据库RDS管理控制台上，购买RDS实例时，选择实例系列为高可用版，操作方法请参见创建RDS SQL Server实例。
  - 方法二：将SQL Server的基础版实例升级为高可用版实例。

    SQL Server基础版实例升级为高可用版实例，操作方法请参见基础版升级为高可用版。
- API

  调用CreateDBInstance接口创建RDS实例时，将Category设置为HighAvailability（高可用版），请参见创建RDS实例。

rds-instance-enabled-security-ip-list

检测您账号下RDS数据库实例是否启用安全白名单功能，已开通视为合规。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：无

修复指南：您账号下RDS数据库实例在白名单中设置了0.0.0.0/0会导致该规则不合规。修改RDS数据库实例在白名单中的值，值不为0.0.0.0/0。配置审计会在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台

  在云数据库RDS管理控制台上，修改RDS实例白名单中的值，使其不为0.0.0.0/0。操作方法请参见设置白名单。
- API

调用ModifySecurityIps接口设置RDS实例的IP白名单，修改SecurityIps的值使其不为0.0.0.0/0，请参见修改IP白名单。

rds-instance-storage-min-size-limit

检查RDS实例最小存储空间限制。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：storageSize（RDS实例最小存储空间）

修复指南：您账号下的RDS实例存储空间小于您设置的阈值，会导致该规则不合规。修复方法如下：

- 控制台
  - 方法一：修改RDS实例的存储空间，使其大于等于您设置的规则入参的阈值。

    在云数据库RDS管理控制台上，修改存储空间，操作方法请参见变更配置。
  - 方法二：将规则入参的阈值修改为小于等于RDS实例的存储空间。
    a. 在云数据库RDS管理控制台上，查看RDS实例的存储空间。
       a. 在**实例列表**中，单击目标实例ID的链接。
       b. 在**基本信息**的**使用量统计**区域，您可以查看实例的存储空间。
    b. 在配置审计控制台上，修改storageSize的阈值。

       操作方法请参见修改规则。
- API

  调用ModifyDBInstanceSpec接口修改DBInstanceClass的值，请参见变更实例。

rds-instances-in-vpc

检查您的RDS实例的网络类型是否为专有网络。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：vpcIds（包含RDS实例的VPC ID，多个以英文逗号（,）分隔，例如：`vpc-25vk5****,vpc-6wesmaymqkgiuru5x****,vpc-8vbc16loavvujlzli****`。）

修复指南：您账号下RDS实例绑定的VPC ID未在规则参数阈值中列举出，则会导致该规则不合规。修复方法如下：

- 方法一：重新创建RDS实例并选择网络类型为专有网络，将VPC ID配置到规则入参的阈值中。

  > **说明** 您可以手动释放按量付费实例或退订包年包月实例。
  > - 退订包年包月实例
  >
  >   您可以登录退订管理页面，退订详情请参见退款规则及退订流程。
  > - 释放按量付费实例
  >
  >   释放实例的风险和操作方法请参见释放实例。

  i. 在云数据库RDS管理控制台上，创建实例。

操作方法请参见创建RDS SQL Server实例。

ii. 在云数据库RDS管理控制台上，查看RDS实例的VPC ID。

a. 在**实例列表**中，单击目标实例ID的链接。

b. 在**基本信息**的**基本信息**区域，您可以查看实例的VPC ID。

iii. 在配置审计控制台上，将RDS实例的VPC ID添加到规则入参的阈值中。

操作方法请参见修改规则。

- 方法二：修改规则入参阈值，将RDS实例的VPC ID添加到规则入参的阈值中。

i. 在云数据库RDS管理控制台上，查看RDS实例的VPC ID。

a. 在**实例列表**中，单击目标实例ID的链接。

b. 在**基本信息**的**基本信息**区域，您可以查看实例的VPC ID。

ii. 在配置审计控制台上，将RDS实例的VPC ID添加到规则入参的阈值中。

操作方法请参见修改规则。

rds-memory-min-size-limit

检查RDS实例内存最小容量限制。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：memorySize（RDS实例内容最小容量）

修复指南：当您账号下的RDS实例内存容量小于您设置的规则参数阈值，会导致该规则不合规。修复方法如下：

- 控制台
  - 方法一：修改RDS实例的数据库内存，使其大于等于您设置的规则入参的阈值。

    在云数据库RDS管理控制台上，修改数据库内存，操作方法请参见变更配置。
  - 方法二：将规则入参的阈值修改为小于等于RDS实例的数据库内存。

    a. 在云数据库RDS管理控制台上，查看RDS实例的数据库内存。

    a. 在**实例列表**中，单击目标实例ID的链接。

    b. 在**基本信息**的**配置信息**区域，您可以查看实例的数据库内存。

    b. 在配置审计控制台上，修改memorySize的阈值。

    操作方法请参见修改规则。
- API

  调用ModifyDBInstanceSpec接口修改DBInstanceClass的值，请参见变更实例。

rds-multi-az-support

检查您的 RDS 数据库实例是否支持多可用区。

资源：ACS::RDS::DBInstance

触发机制：配置更改

参数：无

修复指南：您账号下RDS实例不支持多可用区时，会导致该规则不合规。修复方法如下：

- 控制台
  - 方法一：迁移MySQL 、SQL Server、PPAS数据库实例的可用区。

    在云数据库RDS管理控制台上，迁移数据库实例的可用区，操作方法如下：

    a. RDS for MySQL：迁移可用区

    b. RDS for SQL Server：迁移可用区

    c. RDS for PPAS：迁移可用区
  - 方法二：对于不支持迁移的数据库实例，需要重新创建实例。

    > 说明 您可以手动释放按量付费实例或退订包年包月实例。
    >
    > - 退订包年包月实例
    >
    >   您可以登录退订管理页面，退订详情请参见退款规则及退订流程。
    > - 释放按量付费实例
    >
    >   释放实例的风险和操作方法请参见释放实例。

    在云数据库RDS管理控制台上，创建RDS实例时，选择**部署方案**为**多可用区部署**，操作方法请参见创建RDS SQL Server实例。
- API
  - 调用MigrateToOtherZone接口迁移RDS实例时，将ZoneId设置为多可用区，请参见迁移可用区。
  - 调用CreateDBInstance接口创建RDS实例时，将ZoneId设置为多可用区，请参见创建RDS SQL Server实例。

rds-public-access-check

检测RDS实例是否允许公网访问。

触发机制：配置更改

资源：ACS::RDS::DBInstance

参数：无

修复指南：您账号下RDS数据库实例在白名单中设置了0.0.0.0/0会导致该规则不合规。修改RDS数据库实例在白名单中的值，值不为0.0.0.0/0。配置审计会在10分钟内感知到您的修改并自动启动审计。修复方法如下：

- 控制台

  在云数据库RDS管理控制台上，修改RDS实例白名单中的值，使其不为0.0.0.0/0。操作方法请参见设置白名单。
- API

  调用ModifySecurityIps接口设置RDS实例的IP白名单，修改SecurityIps的值使其不为0.0.0.0/0，请参见修改IP白名单。

5.10. TAG

本文介绍配置审计为标签提供的托管规则详情，以及当规则不合规时的修复方法。

required-tags

配置审计能够检查您的资源是否绑定指定标签，并在发现不合规资源时向您发送告警。required-tags支持所有阿里云基础设施，例如：ECS实例、容器服务Kubernetes版、RDS实例、ECS磁盘和存储、文件存储NAS、文件存储HDFS、专有网络VPC、ECS安全组、负载均衡、OSS Bucket、ECS快照、ECS专有宿主机、云数据库PolarDB集群、云数据库MongoDB实例等。

触发机制：配置更改

参数：

tag1Key（所需标签的键）

tag1Value（所需标签的可选值）

修复指南：关联的资源未具有规则参数阈值中所有指定标签，则资源评估结果为不合规。修复方法如下：

- 方法一：为关联的资源绑定规则入参的阈值。

  以ECS实例为例，为您介绍绑定标签的操作方法，请参见创建或绑定标签。
- 方法二：修改规则入参的阈值，使其包含资源的所有标签。

  以RDS实例为例，为您介绍查看标签的操作方法。

  i. 在RDS管理控制台上，查看实例绑定的标签。

  a. 登录RDS管理控制台。

  b. 在左侧导航栏，单击**实例列表**。

  在**实例列表**中，即可查看目标实例绑定的所有标签。

  ii. 在配置审计控制台上，绑定RDS实例的所有标签。

  操作方法请参见修改规则。

5.11. SLB

本文介绍配置审计为负载均衡（SLB）提供的托管规则详情，以及当规则不合规时的修复方法。

slb-delete-protection-enabled

检测您账号负载均衡实例是否开启释放保护开关，已开通视为合规。

触发机制：配置更改

资源：ACS::SLB::LoadBalancer

参数：无

修复指南：检测您账号负载均衡实例是否开启释放保护开关，未开启会导致该规则不合规。修复方法如下：

- 控制台

  在负载均衡管理控制台上，开启删除保护开关的操作方法，请参见实例删除保护。
- API

  调用SetLoadBalancerDeleteProtection接口开启实例删除保护开关，将DeletionProtection的值设为on，请参见SetLoadBalancerDeleteProtection。

slb-listener-https-enabled

检测SLB是否开通HTTPS。

触发机制：配置更改

资源：ACS::SLB::LoadBalancer

参数：无

修复指南：负载均衡实例未开启HTTPS监听，会导致该规则不合规。修复方法如下：

- 控制台

  在负载均衡管理控制台上，添加HTTPS监听的操作方法，请参见添加HTTPS监听。

- API

  调用CreateLoadBalancerHTTPSListener接口新建HTTPS监听，请参见CreateLoadBalancerHTTPSListener。

slb-loadbalancer-in-vpc

检测负载均衡实例是否已关联到VPC。若您配置阈值，则关联的VpcId需存在您列出的阈值中，视为合规。若未设置阈值，网络类型为VPC网络的实例均为合规。

触发机制：配置更改

资源：ACS::SLB::LoadBalancer

参数：vpcIds（SLB实例的VPC ID，多个以英文逗号（,）分隔，例如：`vpc-25vk5****,vpc-6wesmaymqkgiuru5x****,vpc-8vbc16loavvujlzli****`。）

修复指南：您账号下SLB实例绑定的VPC ID未在规则参数阈值中列举出，则会导致该规则不合规。修复方法如下：

- 方法一：新建负载均衡实例并关联VPC，将VPC ID配置到规则入参的阈值中。

  > 说明
  > - 由于负载均衡实例创建后无法更改其网络类型，因此需要您重新创建符合规则的负载均衡实例。
  > - 您可以释放旧的负载均衡实例，释放实例的风险和操作方法请参见释放实例。
  > - 您只能释放按量付费的负载均衡实例，不能释放包年包月的负载均衡实例。如果您需要释放，请提交工单申请退款，负载均衡支持5天无理由退款。

  i. 在负载均衡管理控制台上，新建负载均衡实例。

     操作方法请参见创建负载均衡实例。

  ii. 在负载均衡管理控制台上，查看负载均衡实例管理的VPC ID。

     在**实例管理**列表中，在目标实例的**服务器地址**列，您可以查看VPC ID。

  iii. 在配置审计控制台上，将负载均衡实例关联的VPC ID添加到规则入参的阈值中。

     操作方法请参见修改规则。

- 方法二：修改规则入参阈值，将负载均衡实例关联的VPC ID添加到规则入参的阈值中。

  i. 在负载均衡管理控制台上，查看负载均衡实例管理的VPC ID。

     在**实例管理**列表中，在目标实例的**服务器地址**列，您可以查看VPC ID。

  ii. 在配置审计控制台上，将负载均衡实例关联的VPC ID添加到规则入参的阈值中。

     操作方法请参见修改规则。

slb-no-public-ip

负载均衡实例未直接绑定公网IP，视为合规。该规则仅适用于IPv4协议。

触发机制：配置更改

资源：ACS::SLB::LoadBalancer

参数：无

修复指南：您账号下的负载均衡实例绑定公网IP，会导致该规则不合规。修复方法如下：

- 控制台

  在负载均衡管理控制台上，新建负载均衡实例，选择**实例类型为私网**，操作方法请参见创建负载均衡实例。

  > 说明
  > - 由于负载均衡实例创建后无法更改其实例类型，因此需要您重新创建符合规则的负载均衡实例。
  > - 您可以释放旧的负载均衡实例，释放实例的风险和操作方法请参见释放实例。
  > - 您只能释放按量付费的负载均衡实例，不能释放包年包月的负载均衡实例。如果您需要释放，请提交工单申请退款，负载均衡支持5天无理由退款。

- API

  调用CreateLoadBalancer接口创建负载均衡实例，将AddressType的值设置为intranet，请参见CreateLoadBalancer。