

ALIBABA CLOUD

# 阿里云

配置审计  
教程

文档版本：20201217

 阿里云

## 法律声明

阿里云提醒您在使用或阅读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。
<b>粗体</b>	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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[ ] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

---

# 目录


1.检测在操作审计是否存在活跃的跟踪	05
2.检测RDS实例是否为高可用实例	06
3.检测RDS实例是否允许公网访问	07
4.检测SLB实例是否开启HTTPS监听	08
5.检测资源是否绑定指定标签	09

# 1.检测在操作审计是否存在活跃的跟踪

您可以新建一条规则，检测在操作审计是否存在活跃的跟踪。

## 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，搜索并选中检测在操作审计是否存在活跃的跟踪，选择该规则的风险等级，单击下一步。

 **说明** 为满足企业内部合规，一般要求您的账号授权操作审计服务，实时监控并记录账号对资源进行操作的日志。使用该规则检测您的账号是否授权操作审计服务。

5. 在参数设置页面，规则触发机制和规则关联资源均为默认值，单击下一步。
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。
7. 在完成页面，您可以单击查看规则详情或返回规则列表，查看规则的评估结果。

## 2.检测RDS实例是否为高可用实例

您可以新建一条规则，检测云数据库RDS实例是否为高可用实例。

### 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**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**检测RDS实例是否为高可用实例**，选择该规则的风险等级，单击**下一步**。
5. 在**参数设置**页面，规则触发机制和规则关联资源均为默认值，单击**下一步**。
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**。
7. 查看规则的评估结果。在**完成**页面，您可以单击**查看规则详情**或**返回规则列表**，查看合规评估情况。

## 3.检测RDS实例是否允许公网访问

您可以新建一条规则，检测云数据库RDS实例是否允许公网访问。

### 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**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**检测RDS实例是否允许公网访问**，选择该规则的风险等级，单击**下一步**。
5. 在**参数设置**页面，规则触发机制和规则关联资源均为默认值，单击**下一步**。
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**。
7. 查看规则的评估结果。在**完成**页面，您可以单击**查看规则详情**或**返回规则列表**，查看合规评估情况。

## 4.检测SLB实例是否开启HTTPS监听

您可以新建一条规则，检测负载均衡（SLB）实例是否开启HTTPS监听。

### 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[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[检测SLB实例是否开启HTTPS监听](#)，选择该规则的风险等级，单击[下一步](#)。
5. 在[参数设置](#)页面，规则触发机制和规则关联资源均为默认值，单击[下一步](#)。
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](#)。
7. 查看规则的评估结果。在[完成](#)页面，您可以单击[查看规则详情](#)或[返回规则列表](#)，查看合规评估情况。



## 5.检测资源是否绑定指定标签


您可以新建一条规则，检测账号下资源是否绑定指定标签。

### 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**检测资源是否已有必备标签**，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”，可以使用规则**检测资源是否已有必备标签**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，**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. 在**完成**页面，您可以单击**查看规则详情**或**返回规则列表**，查看合规评估情况。