ALIBABA CLOUD

阿里云

配置审计

常见问题

文档版本：20220624

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.启用配置审计 05
2.为什么启用配置审计时需要授权？ 06
3.为什么授权之后控制台概览页无数据？ 07
4.如何删除配置审计服务关联角色？ 08
5.资源 09
6.为什么部分资源未展示在资源列表中？ 10
7.为什么资源配置更改后在配置时间线中无记录？ 11
8.为什么配置发生不合规的变更未被检测到？ 12
9.规则 13
10.如何支持更多托管规则？ 14
11.为什么设置的规则未被评估？ 15
12.合规时间线和配置时间线是什么关系？ 16
13.自定义规则 17
14.如何配置自定义规则？ 18
15.自定义规则的数据结构是什么？ 19
16.为什么自定义规则函数未被触发？ 20
17.为什么执行自定义规则后评估结果仍然是无数据？ 22

1.启用配置审计

2.为什么启用配置审计时需要授权？

当您启用配置审计时，需要为当前账号授权，使配置审计可以通过调用云服务的OpenAPI接口查询您账号下的资源信息。只有获取到资源配置数据，配置审计才能形成资源列表，进而对资源进行审计。

3.为什么授权之后控制台概览页无数据？

授权配置审计服务之后，您首次登录控制台有一个初始化的过程，覆盖当前账号下各区域、服务、资源类型的资源列表，大约需要2~10分钟时间，请您耐心等待。关于如何授权配置审计，请参见授权服务。

4.如何删除配置审计服务关联角色？

本文为您介绍普通账号、管理账号、委派管理员账号和成员删除配置审计服务关联角色的方法。

配置审计服务关联角色涉及各账号的概念如下：

- 普通账号：未加入资源目录的独立的阿里云账号。
- 管理账号：开通资源目录并管理成员的阿里云账号。
- 委派管理员账号：关于委派管理员账号，请参见管理委派管理员账号。
- 成员：资源目录中的成员账号。

普通账号

删除配置审计服务关联角色。具体操作，请参见删除服务关联角色。

管理账号或委派管理员账号

1. 管理账号或委派管理账号将自己从账号组中移除。

   具体操作，请参见删除账号组。

2. 管理账号或委派管理员账号删除自己的配置审计服务关联角色。

   具体操作，请参见删除服务关联角色。

成员

1. 管理账号或委派管理员账号将成员从账号组中移除。

   具体操作，请参见更新账号组的配置。

2. 成员删除自己的配置审计服务关联角色。

   具体操作，请参见删除服务关联角色。

5.资源

6.为什么部分资源未展示在资源列表中？

- 如果全部资源都未出现，则因为配置审计目前不支持该资源类型。您可以提交工单反馈，我们将尽快安排支持。
- 如果部分资源未出现，则是数据问题，您可以提交工单反馈，我们将尽快为您排查。

7.为什么资源配置更改后在配置时间线中无记录？

您变更资源配置后，配置审计将在0~10分钟内监控到变更。因为配置审计对资源配置变更的感知有10分钟的窗口期。如果您在一个窗口期内，对资源进行变更后又恢复原样，则可能不会在配置审计中生成变更记录。

8.为什么配置发生不合规的变更未被检测到？

如果规则的触发机制设置为**配置变更**，其触发原理如下：

当处于窗口期头和尾的两个资源配置快照呈现出不同时，配置审计首先对比出详细的差异，再针对这个对比结果进行审计。如果资源配置的变更和修复恰好处于窗口期，则配置审计无法感知变更，就无法触发对应的规则。

9.规则

10.如何支持更多托管规则？

请您通过提交工单详细描述您的所需规则，格式请参见托管规则列表。配置审计将协同云服务一起评估，是否将您的需求实现为托管规则。

11.为什么设置的规则未被评估？

- 如果规则的触发机制为**周期执行**，则需要到固定的时间点才会评估。
- 如果规则的触发机制为**配置变更**，则您绑定规则后，被关联的资源需要发生配置变更才会触发规则。

您可以在规则详情页面，手动触发规则的**重新审计**，快速获得最新评估结果。

12.合规时间线和配置时间线是什么关系？

合规时间线的点是每一次合规评估的结果，合规评估可能是定时任务、实时变更触发或手动触发。配置时间线的点是每一次配置变更的记录。如果您的规则是通过配置变更来触发的，则合规时间线上规则评估的点跟配置时间线上配置变更的点是同一个时间点。

13.自定义规则

14.如何配置自定义规则？

关于如何配置自定义规则，请参见配置与开发自定义规则。

15.自定义规则的数据结构是什么？

当配置审计执行自定义规则中的函数时，默认传入函数计算的数据结构，请参见函数入参。

16.为什么自定义规则函数未被触发？

当您新建自定义规则或重新执行自定义规则时，为什么自定义规则中的函数未被触发？

操作步骤

1. 启用函数的日志功能，便于您查看函数的执行日志。

   关于如何启用函数的日志功能，请参见配置日志。

2. 在**调用日志**页签中，查看是否存在调用记录。
   - 是：说明自定义规则函数被成功触发。
   - 否：说明自定义规则函数未触发或触发失败，请执行步骤 3。
3. 调用GetConfigRule（普通账号）或GetAggregateConfigRule（管理账号或成员）接口，查看自定义规则函数是否触发。
   - 否：如果参数LastFailedEvaluationTimestamp的取值为空或在自定义规则执行评估之前，说明自定义规则函数未触发，请耐心等待几分钟后，重新查看。
   - 是：如果参数LastFailedEvaluationTimestamp的取值在自定义规则执行评估之后，请查看参数LastErrorCode和LastErrorMessage，获取错误原因和处理建议。

LastErrorCode	LastErrorMessage	错误原因	处理建议
ComponentClientException	InvalidArgument	函数的**请求处理程序类型**设置为**处理HTTP请求**。	a. 删除**请求处理程序类型**为**处理HTTP请求**的函数。 具体操作，请参见管理函数。 b. 重新创建**请求处理程序类型**为**处理事件请求**的函数。 具体操作，请参见创建函数。
	AccessDenied	账号权限不足。	请您确保创建自定义规则的账号已赋予访问函数计算的权限。
	ServiceNotFound	自定义规则中配置的服务不存在。	a. 删除函数ARN错误的自定义规则。 具体操作，请参见删除规则。 b. 重新创建函数ARN正确的自定义规则。 具体操作，请参见使用自定义规则新建规则。

LastErrorCode	LastErrorMessage	错误原因	处理建议
	FunctionNotFound	自定义规则中配置的函数不存在。	a. 删除函数ARN错误的自定义规则。 具体操作，请参见删除规则。 b. 重新创建函数ARN正确的自定义规则。 具体操作，请参见使用自定义规则新建规则。
ComponentServerException	InternalServerError	函数计算系统错误。	请您给函数计算提交工单。
	Timeout	触发函数评估超时。	请您重新对自定义规则手动执行审计。 具体操作，请参见手动执行审计。

17.为什么执行自定义规则后评估结果仍然是无数据？

自定义规则被触发后，函数计算中的函数对资源进行评估，并调用配置审计的PutEvaluations接口，将评估结果返回给配置审计。当您执行自定义规则后，评估结果仍然显示为“无数据”的排查方法如下：

- 通过操作审计排查

  通过操作审计控制台的**事件查询**功能，查看PutEvaluations接口的调用事件。

  当您执行自定义规则后，如果存在PutEvaluations接口的调用记录，则说明规则执行成功，该规则无匹配资源；反之，说明规则执行失败。

  > **说明** 地域选择华东2（上海）。

- 通过函数计算排查

  如果您已启用函数的日志功能，则可以查看PutEvaluations接口的调用记录。关于如何启用函数的日志功能，请参见配置日志。

  当您执行自定义规则后，请先在**函数代码**页签中打印日志，再在**调用日志**页签中查看PutEvaluations接口的调用记录。如果存在PutEvaluations接口的调用记录，则说明规则执行成功，该规则无匹配资源；反之，说明规则执行失败。