# 阿里云
# 配置审计

## 产品简介

文档版本：20190919

# 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 |
| --- | --- | --- |
|  | 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。 |  **禁止:**<br>重置操作将丢失用户配置数据。 |
|  | 该类警示信息可能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:**<br>重启操作将导致业务中断，恢复业务所需时间约10分钟。 |
|  | 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:**<br>您也可以通过按Ctrl + A选中全部文件。 |
| > | 多级菜单递进。 | 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。 | 单击 确定。 |
| `courier` 字体 | 命令。 | 执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。 |
| *## * | 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。 | `swich` *{stand \| slave}* |

# 目录

# 1 什么是配置审计

配置审计是一项面向资源的审计服务。在面对大量资源时，配置审计可以帮助您实现持续的基础设施的合规监管。

您可以使用配置审计服务进行以下操作：

1. 获得账号下资源清单，并可以通过简单的检索，获得每个资源当前的配置快照。请参见#unique_4。
2. 默认监控您账号下所有资源的配置变更，从开通服务起，记录资源配置变更的详细历史。若您将资源类型移出监控范围，则暂停记录。请参见#unique_5、#unique_6。
3. 查阅配置变更与操作事件的关系请参见#unique_7。
4. 配置合规规则，在资源配置变更时或定时的触发规则评估，自动监控资源合规性。请参见#unique_8。
5. 查看资源的合规情况，以及规则的评估情况。

正式使用配置审计服务前，请您阅读使用须知：

- 请您确认知晓并阅读配置审计#unique_9。
- 配置审计服务在逐步扩大对云产品的覆盖，您开通服务时由于受到支持的资源类型的限制，资源清单中会缺少部分资源。当配置审计支持新的资源类型时，会默认纳入监控范围，您可以后续自行移出。
- 配置审计感知资源配置变更以10分钟为窗口期，若您的资源恰好在窗口期内发生配置变更又重新变回原样，配置审计可能无法感知。
- 配置审计公测期间不承诺数据准确性，若您发现资源列表、配置详情、规则评估等数据不符合预期，烦请您通过工单反馈。若您有其他需求，如希望支持的资源类型等，烦请您工单反馈，感谢您的理解陪伴服务共同进步！

# 2 应用场景

当您在使用大规模资源时，配置审计服务可以帮助您自动监管资源配置的合规性。配置审计服务可以在以下场景帮助您监管资源：

### 资源管理

开通配置审计服务后，您可以获得账号下跨区域聚合的资源清单，并通过检索定位到具体资源，同时在线查看每个资源当前的配置快照。

说明：配置审计仅支持部分阿里云产品，由于受到资源类型的限制，资源清单中仅会存在部分资源。配置审计服务正在逐步扩大对阿里云产品的覆盖，为您提供更加完整的资源清单。

### 持续的合规审计

开通配置审计服务后，您可以配置规则并绑定具体的资源类型。

1. 您可以使用服务预设的规则，也可以自定义合规规则。
2. 当指定资源类型发生配置变更时，将会触发规则执行，评估配置的合规性。
3. 当资源配置不合规时，资源会被标记为不合规并向您发送通知。

### 追溯历史，问题复盘

开通配置审计服务后，配置审计服务会每隔10分钟记录您的资源配置变更快照。您可以看到每个资源的配置变更信息。

配置审计服务已与操作审计服务集成，可以为您列出每次配置变更记录对应的操作事件列表，方便您快速定位配置发生错误的初始位置以及当时的操作记录。帮助您准确定位问题，快速复盘。

# 3 基本概念

本文罗列了配置审计中用到的基本概念，帮助您正确理解和使用。

## 资源类型

配置审计是面向资源的审计服务。资源类型是一组实体资源的归类。例如云服务器ECS的实例资源类型为：ACS::ECS::Instance。资源可以分为以下几类：

1. 计算实例、存储实例等实体资源。
2. 工作组、工作流等应用级产品的管理概念。
3. 角色、策略等权限相关的管理资源。

## 资源配置详情

通过云产品开放的资源查询接口可获取的全部信息。

## 监控范围

监控范围指追踪的资源类型的范围，监控的粒度是资源类型。

1. 当选择某个资源类型在监控范围内，账号下所有该类型的实体资源都会被追踪，每10分钟记录配置变更快照。
2. 当某个资源类型移出监控范围，则账号下该类型的实体资源都将停止记录配置变更。

## 配置时间线

配置审计为您提供每个监控范围内的资源配置时间线。

1. 对于您开通配置审计服务时已保有的资源，配置时间线的起点是服务开通时间。
2. 对于您开通配置审计服务后新创建的资源，配置时间线起点是资源创建时间。配置审计每隔10分钟确认资源配置变更，若出现配置变更，则会在配置时间线出现一个节点，显示该时间点的资源配置详情、具体变更详情以及该变更涉及的操作事件。

## 规则

规则指用于判断资源配置是否合规的规则函数。配置审计依赖函数计算服务做规则开发，规则内容一般为某属性必须是/不是某个值。将规则绑定到资源类型后，资源类型发生配置变更时将自动触发规则评估，监督本次变更的合规性。您也可以设置为定时触发，配置审计定时为您校验所有资源的合规性。关于规则的管理，请参见#unique_8。配置审计中有2种规则：系统预设规则和自定义规则。

1. 系统预设规则：配置审计服务为您提供数十款系统预设规则，请参见#unique_12

2. #unique_13：自定义规则需要您登录函数计算服务自行创建规则函数，在配置审计控制台创建自定义规则时需要录入规则的函数ARN。通过自定义规则可以更好的支持个性化的合规场景。

合规时间线

规则评估可以是在变更发生时触发的，对应的配置时间线就会相应有一个合规时间线，是每次合规评估结果的历史记录。合规时间线的合规评估记录与规则触发方式有关。

1. 若规则为定时触发，则只包括定时评估的记录。
2. 若规则为变更触发，则包括每次变更时评估的记录。
3. 若选择了两种触发方式，则都会出现评估记录。

# 4 支持的资源类型

配置审计服务目前支持如下资源类型的配置追踪和审计，将持续增加覆盖。 您可以将此文档与 管理监控范围 页面的待选资源类型对照查阅，以页面内容为准。

| 产品 | 资源类型 | 资源Code |
| --- | --- | --- |
| 云服务器 ECS | 实例 | ACS::ECS::Instance |
| 云服务器 ECS | 网络接口 | ACS::ECS::NetworkInterface |
| 云服务器 ECS | 安全组 | ACS::ECS::SecurityGroup |
| 云服务器 ECS | 磁盘 | ACS::ECS::Disk |
| 云服务器 ECS | 快照 | ACS::ECS::Snapshot |
| 云服务器 ECS | 自动快照策略 | ACS::ECS::AutoSnapshotPolicy |
| 云服务器 ECS | 云助手命令 | ACS::ECS::Command |
| 云服务器 ECS | 专用宿主机 | ACS::ECS::DedicatedHost |
| 云服务器 ECS | 启动模板 | ACS::ECS::LaunchTemplate |
| 关系型数据库 RDS | 实例 | ACS::RDS::DBInstance |
| 操作审计 | 事件跟踪 | ACS::ActionTrail::Trail |
| 专有网络 VPC | VPC 实例 | ACS::VPC::VPC |
| 专有网络 VPC | 路由表 | ACS::VPC::RouteTable |
| 专有网络 VPC | 交换机 | ACS::VPC::VSwitch |
| VPN 网关 | VPN 网关 | ACS::VPN::VpnGateway |
| VPN 网关 | VPN 连接 | ACS::VPN::VpnConnection |
| 弹性公网 IP | 弹性公网 IP | ACS::EIP::EipAddress |
| VPN 网关 | 用户网关 | ACS::VPN::CustomerGateway |
| 访问控制 | 角色 | ACS::RAM::Role |
| 访问控制 | 策略 | ACS::RAM::Policy |
| 访问控制 | 用户 | ACS::RAM::User |
| 负载均衡 | 实例 | ACS::SLB::LoadBalancer |
| 负载均衡 | CA 证书 | ACS::SLB::CACertificate |

| 产品 | 资源类型 | 资源Code |
| --- | --- | --- |
| 负载均衡 | 服务器证书 | ACS::SLB::ServerCertificate |
| 内容分发 | 域名 | ACS::CDN::Domain |
| 弹性伸缩 | 伸缩组 | ACS::ESS::ScalingGroup |
| 弹性伸缩 | 伸缩规则 | ACS::ESS::ScalingRule |
| 弹性伸缩 | 伸缩配置 | ACS::ESS::ScalingConfiguration |
| 对象存储 OSS | Bucket | ACS::OSS::Bucket |