ALIBABA CLOUD

阿里云

配置审计

产品简介

文档版本：20200910

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

1.什么是配置审计

配置审计（Config）是一项资源审计服务，为您提供面向资源的配置历史追踪、配置合规审计等能力。面对大量资源，帮您轻松实现基础设施的自主监管，确保持续性合规。

产品架构

配置审计的实现原理如下图所示。

功能特性

功能	描述
管理资源监控范围	配置审计通过监控您账号下的资源变更，追踪配置变更历史，并实时地完成合规性审计。您可以通过简单配置来管理资源监控范围。如果您选择默认监控所有资源类型，当配置审计对接新产品时，新资源类型将自动纳入监控范围。如果您选择自定义资源类型，则不会自动纳入监控范围。
管理资源列表	授权配置审计服务后，您可以获得账号下跨区域聚合的资源清单，并通过筛选找到指定资源实体进而查询资源的配置详细。找到指定资源后，您可以快速跳转到该资源在云产品控制台的管理页面，管理该资源。
查看资源合规时间线	配置审计记录监控中资源的配置历史，并保存为配置时间线，即资源配置随时间推进的演变记录。您可以查询与配置变更相关的操作事件列表和事件详情。
资源合规审计	配置审计支持托管规则和自定义规则。规则配置成功后，您可以查看资源的评估结果和合规时间线，并对不合规的资源重新审计。您还可以对不合规的规则，执行修改、删除和停用操作。
订阅资源事件	您可以在配置审计中订阅资源的配置变更事件和不合规评估事件，并及时发送资源的变更和不合规通知。
不合规修正	您可以为规则设置修正模板。当规则被评估为不合规时，配置审计根据您的设置自动修正资源。
资源快照保存到OSS Bucket	如果您设置了OSS Bucket地址，则配置审计会将资源的配置变更快照以文件形式保存到指定地址。

功能	描述
资源日志保存到日志服务	如果您设置了日志项目，则配置审计会将资源的变更数据以日志形式保存到日志服务。
等保2.0预检	配置审计为您提供免费的等保2.0检测，动态且持续的为您监控云上信息系统的合规性，减少反复检测和整改流程，帮助您快速通过等保检测。

产品优势

配置审计的产品优势如下：

- 跨区域整合：将您各区域的资源整合为一份完整清单，并支持搜索资源。
- 配置变更与操作记录打通：为您记录每次配置变更的详情快照，同时记录下关联的操作记录，行为与结果相结合，更好地支持问题排查。
- 持续的合规监控：配置审计为您持续监控资源配置的变更，并在变更时自动触发合规评估，为您实现合规性的自主监管。
- 云上系统等保2.0预检：为您解读等保2.0条例在云上的实施方案，并支持您一键预检云上系统的合规现状。

使用须知

正式使用配置审计服务前，请您阅读如下使用须知：

- 请您确认已阅读并知晓配置审计服务条款。
- 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，您也可以将资源类型移出监控范围。
- 配置审计感知资源配置变更以10分钟为窗口期，如果您的资源恰好在窗口期内发生配置变更又重新变回原样，则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，如果您发现资源列表、配置详情、规则评估等数据不符合预期，或您有其他需求，例如：需要支持更多资源类型等，请您提交工单反馈。

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。

集中资源管理配置

管理跨区域部署的资源时非常不便，配置审计高效的管理资源各区域聚合的资源清单和快捷检索，并记录资源每次配置变更的详情快照。授权配置审计服务后，您可以获得当前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。

配置合规审计

授权配置审计服务后，您可以配置规则并绑定具体的资源类型。您可以使用托管规则，也可以自定义合规规则。

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。

等保2.0云上持续预检

配置审计解读等保2.0法规条例，并对应实现为云上资源配置的检测。您可以一键开启等保2.0云上预检功能，配置审计将持续为您监控资源的合规性。您还可以下载预检报告，呈递检测机构报备。

追溯历史，问题复盘

授权配置审计服务后，配置审计服务会每隔10分钟记录您的资源配置变更。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对应的操作记录。帮助您准确定位问题，快速复盘。

3.基本概念

通过本文您可以了解配置审计中用到的基本概念，帮助您正确理解和使用本产品。

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：

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

资源配置详情

配置审计通过云产品开放的资源查询接口可获取当前账号下所有资源。您可以在资源列表中查看各个资源的配置信息，也可以快速跳转到指定资源的云产品控制台，对其进行管理。

监控范围

监控范围指监控资源类型的范围，监控的粒度是资源类型。

- 当某个资源类型在监控范围内时，当前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。
- 当某个资源类型被移出监控范围时，当前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。

- 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。
- 对于您开通配置审计服务后新建的资源，配置时间线起点是资源新建时间。配置审计每10分钟记录资源配置变更，如果资源配置变更，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、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。配置审计服务使用函数计算服务的函数来承载规则代码。规则绑定资源类型后，当该资源类型中的资源发生配置变更时，自动触发规则评估，检测本次变更的合规性。您也可以设置规则定时触发，配置审计定时为您检测所有资源的合规性。配置审计支持的规则如下：

- 托管规则

  配置审计为您提供托管规则，请参见托管规则列表。

- 自定义规则

  自定义规则需要您先在函数计算控制台上新建函数，再在配置审计控制台上选择函数ARN，请参见自定义规则的开发。通过自定义规则可以更好的支持个性化的合规场景。

  您还可以使用可视化编辑器新建自定义规则，请参见使用可视化编辑器新建规则。

合规时间线

规则评估可以在变更发生时触发，对应的配置时间线会有一个对应的合规时间线，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。

- 如果规则为定时触发，则只包括定时评估的记录。

- 如果规则为变更触发，则只包括每次变更时评估的记录。
- 如果选择了两种触发方式，则包括上述两种评估记录。

等保预检

等保2.0预检为云上的合规检测规则，为您动态且持续的检测阿里云上资源的合规性，从而避免正式检测时多次反复整改，帮助您快速通过等保检测。关于等保2.0更多信息，请参见等保2.0解读。

4.使用限制

本文列举了配置审计的使用限制。

限制项	最大值
一个阿里云账号允许新建的规则数目	200条
一个阿里云账号允许设置的日志项目数目	1个
一个阿里云账号允许设置的存储桶数目	1个
一个阿里云账号允许设置的日志库数目	1个

说明 本文仅展示了各限制项的默认配额。对于可以调整配额的限制项，您可以前往配额中心申请提升配额。配额中心现已支持多个云产品，请参见配额中心支持的云产品。

5.支持配置审计的云服务

本文列举了支持配置审计的云服务。

服务	资源类型	资源代码
云服务器ECS	实例	ACS::ECS::Instance
	网络接口	ACS::ECS::NetworkInterface
	安全组	ACS::ECS::SecurityGroup
	磁盘	ACS::ECS::Disk
	快照	ACS::ECS::Snapshot
	自动快照策略	ACS::ECS::AutoSnapshotPolicy
	云助手命令	ACS::ECS::Command
	专用宿主机	ACS::ECS::DedicatedHost
	启动模板	ACS::ECS::LaunchTemplate
云数据库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
	路由表	ACS::VPC::RouteTable
	交换机	ACS::VPC::VSwitch
VPN网关	VPN网关	ACS::VPN::VpnGateway
	VPN连接	ACS::VPN::VpnConnection
	用户网关	ACS::VPN::CustomerGateway
弹性公网IP	弹性公网IP	ACS::EIP::EipAddress
访问控制	角色	ACS::RAM::Role
	策略	ACS::RAM::Policy
	用户	ACS::RAM::User
负载均衡	实例	ACS::SLB::LoadBalancer
	CA证书	ACS::SLB::CACertificate
	服务器证书	ACS::SLB::ServerCertificate

服务	资源类型	资源代码
	访问控制表	ACS::SLB::AccessControlList
CDN	域名	ACS::CDN::Domain
弹性伸缩	伸缩组	ACS::ESS::ScalingGroup
	伸缩规则	ACS::ESS::ScalingRule
	伸缩配置	ACS::ESS::ScalingConfiguration
对象存储OSS	Bucket	ACS::OSS::Bucket
云数据库Redis版	Redis实例	ACS::Redis::DBInstance
云数据库PolarDB	PolarDB集群	ACS::PolarDB::DBCluster
云数据库MongoDB版	MongoDB实例	ACS::MongoDB::DBInstance
CBWP	共享带宽包	ACS::CBWP::CommonBandwidthPackage
云企业网	实例	ACS::CEN::CenInstance
	带宽包	ACS::CEN::CenBandwidthPackage
	流日志	ACS::CEN::Flowlog
Web应用防火墙	实例	ACS::WAF::Instance
	域名	ACS::WAF::Domain
DDoS防护	实例	ACS::DdosCoo::Instance
文件存储	文件系统	ACS::NAS::FileSystem
云数据库HBase	集群	ACS::HBase::Cluster
容器服务Kubernetes版	集群	ACS::ACK::Cluster
NAT网关	文件系统	ACS::NAS::FileSystem