ALIBABA CLOUD

Alibaba Cloud

配置审计

产品简介

文档版本：20220211

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 ---- 05
2.应用场景 ---- 07
3.基本概念 ---- 08
4.使用限制 ---- 10
5.配置审计支持的资源类型和资源关系 ---- 11
6.普通账号、成员账号和企业管理账号的使用差异 ---- 20

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：

- 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。

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

本文解释了配置审计的基本概念，帮助您正确理解和使用配置审计。

概念	说明
资源类型	资源类型是一组实体资源的归类。例如：云服务器ECS实例的资源类型为ECS实例。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	配置审计通过云服务开放的资源查询接口可获取当前阿里云账号下的所有资源。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服务控制台，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，当前阿里云账号下该资源类型的所有资源都会被追踪，每10分钟记录一次配置变更。 • 当某个资源类型被移出监控范围时，当前阿里云账号下该资源类型的所有资源都停止记录配置变更。
规则	规则指用于判断资源配置是否合规的规则函数。配置审计使用函数计算中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，检查本次配置变更的合规性。您也可以设置规则定时触发，配置审计定时为您检查所有资源的合规性。配置审计支持的规则如下： • 托管规则 关于托管规则，请参见托管规则列表。 • 自定义规则 您需要先在函数计算控制台新建函数，再在配置审计控制台上选择函数ARN。关于使用函数计算新建规则的具体操作，请参见自定义规则函数。
配置时间线	配置审计为您提供每个监控范围内资源的配置时间线。 • 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，配置时间线的起点是资源新建时间。配置审计每10分钟记录一次资源配置变更，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。
合规时间线	规则评估在资源配置变更发生时触发，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。 • 如果规则为资源配置变更触发，则只包括配置变更时评估的记录。 • 如果规则同时为定时触发和资源配置变更触发，则同时包括定时和配置变更时评估的记录。
等保预检	等保2.0预检为云上的合规检测，为您动态且持续地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的更多信息，请参见什么是等保2.0。

概念	说明
CIS	CIS（Center for Internet Security）是互联网安全中心。CIS安全控制是企业为了实现基本网络安全而必须满足的前20个控制点或目标的列表。
资源目录	资源目录（Resource Directory）是阿里云面向企业客户提供的一套多级资源（账号）关系管理服务。
企业管理账号	企业管理账号是资源目录的超级管理员，也是开通资源目录的初始账号，对其创建的资源目录和成员账号拥有完全控制权限。只有通过企业实名认证的阿里云账号才能开通资源目录，每个资源目录有且只有一个企业管理账号。 **说明** 企业管理账号位于资源目录外部，不归属于资源目录，所以不受资源目录的任何管控策略影响。
成员账号	在资源目录内，成员账号作为资源容器，是一种资源分组单位。成员账号通常用于指代一个项目或应用，每个成员账号中的资源相对其他成员账号中的资源是物理隔离的。您可以通过企业管理账号授予RAM用户、RAM用户组或RAM角色对成员账号内资源的访问权限。 成员账号被企业管理账号邀请进入资源目录，或由企业管理账号在资源目录内直接创建。
账号组	账号组是一组成员账号的集合。在一个资源目录中，企业管理账号可以选择所有或部分成员账号形成一个管理单元进行集中的合规管理，这个管理单元就是账号组。从资源维度上讲，账号组是多个成员账号中的资源汇聚而成的资源池。 企业管理账号可以查看账号组中所有成员账号中的资源列表、资源详情、资源配置时间线、资源合规时间线和关联资源，还可以在账号组中新建规则与合规包。这些规则和合规包将对该账号组中所有成员账号下的资源生效，进行持续地合规评估。

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
一个普通账号或企业管理账号允许新建的规则数目	200条
一个普通账号或企业管理账号允许设置的日志项目数目	1个
一个普通账号或企业管理账号允许设置的日志库数目	1个
一个普通账号或企业管理账号允许设置的存储空间数目	1个
一个普通账号或企业管理账号允许设置的主题数目	1个
一个企业管理账号允许新建的账号组数目	5个
一个账号组内允许包含的成员账号数目	200个

说明

- RAM用户、用户组或RAM角色可以绑定的策略个数与授权范围无关，即单个资源组内授权与整个云账号内授权的策略额度是相同的，彼此独立，不会互相占用。
- 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.配置审计支持的资源类型和资源关系

本文列举了配置审计支持云服务的资源类型和资源关系。

云服务	资源类型	关系	相关资源
云服务器ECS	ECS实例（ACS::ECS::Instance）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
		关联	ECS安全组（ACS::ECS::SecurityGroup）
		挂载	ECS云盘（ACS::ECS::Disk）
		包含	ECS弹性网卡（ACS::ECS::NetworkInterface）
		挂载	EIP弹性公网IP（ACS::EIP::EipAddress）
		被包含	ECS专用宿主机DDH（ACS::ECS::DedicatedHost）
	ECS弹性网卡（ACS::ECS::NetworkInterface）	被包含	ECS实例（ACS::ECS::Instance）
		关联	ECS安全组（ACS::ECS::SecurityGroup）
		被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
		挂载	EIP弹性公网IP（ACS::EIP::EipAddress）
	ECS安全组（ACS::ECS::SecurityGroup）	挂载	VPC专有网络（ACS::VPC::VPC）
		关联	ESS伸缩配置（ACS::ESS::ScalingConfiguration）
		关联	ECS实例（ACS::ECS::Instance）
		关联	ECS弹性网卡（ACS::ECS::NetworkInterface）
		关联	ACK集群（ACS::ACK::Cluster）
		关联	堡垒机实例（ACS::Bastionhost::Instance）
		关联	终端节点（ACS::PrivateLink::VpcEndpoint）

云服务	资源类型	关系	相关资源
	ECS云盘（ACS::ECS::Disk）	挂载	ECS实例（ACS::ECS::Instance）
		挂载	ECS自动快照策略（ACS::ECS::AutoSnapshotPolicy）
		关联	KMS主密钥（ACS::KMS::Key）
	ECS自动快照策略（ACS::ECS::AutoSnapshotPolicy）	挂载	ECS云盘（ACS::ECS::Disk）
		挂载	NAS文件系统（ACS::NAS::FileSystem）
	ECS专用宿主机 DDH（ACS::ECS::DedicatedHost）	包含	ECS实例（ACS::ECS::Instance）
	ECS云助手命令（ACS::ECS::Command）	无	无
	ECS实例启动模板（ACS::ECS::LaunchTemplate）	无	无
	VPC专有网络（ACS::VPC::VPC）	包含	ESS伸缩组（ACS::ESS::ScalingGroup）
		挂载	VPN网关（ACS::VPN::VpnGateway）
		包含	ECS实例（ACS::ECS::Instance）
		挂载	ECS安全组（ACS::ECS::SecurityGroup）
		包含	ECS弹性网卡（ACS::ECS::NetworkInterface）
		包含	ACK集群（ACS::ACK::Cluster）
		包含	Elasticsearch Logstash实例（ACS::Elasticsearch::Logstash）
		包含	Elasticsearch实例（ACS::Elasticsearch::Instance）
		包含	堡垒机实例（ACS::Bastionhost::Instance）
		包含	终端节点（ACS::PrivateLink::VpcEndpoint）
		包含	TSDB实例（ACS::TSDB::Instance）
		包含	RDS实例（ACS::RDS::DBInstance）

云服务	资源类型	关系	相关资源
专有网络VPC		包含	SLB负载均衡（ACS::SLB::LoadBalancer）
		包含	PolarDB集群（ACS::PolarDB::DBCluster）
		包含	Redis实例（ACS::Redis::DBInstance）
		包含	MongoDB实例（ACS::MongoDB::DBInstance）
		包含	HBase集群（ACS::HBase::Cluster）
		包含	VPC路由表（ACS::VPC::RouteTable）
		包含	NAT网关（ACS::NAT::NATGateway）
		包含	VPC交换机（ACS::VPC::Vswitch）
	VPC交换机（ACS::VPC::Vswitch）	挂载	VPC路由表（ACS::VPC::RouteTable）
		被包含	VPC专有网络（ACS::VPC::VPC）
		包含	ACK集群（ACS::ACK::Cluster）
		包含	Elasticsearch Logstash实例（ACS::Elasticsearch::Logstash）
		包含	Elasticsearch实例（ACS::Elasticsearch::Instance）
		包含	堡垒机实例（ACS::Bastionhost::Instance）
		包含	TSDB实例（ACS::TSDB::Instance）
		包含	ESS伸缩组（ACS::ESS::ScalingGroup）
		挂载	VPN网关（ACS::VPN::VpnGateway）
		包含	MongoDB实例（ACS::MongoDB::DBInstance）
		包含	HBase集群（ACS::HBase::Cluster）

云服务	资源类型	关系	相关资源
		包含	Redis实例（ACS::Redis::DBInstance）
		包含	PolarDB集群（ACS::PolarDB::DBCluster）
		包含	RDS实例（ACS::RDS::DBInstance）
		包含	SLB负载均衡（ACS::SLB::LoadBalancer）
		包含	ECS弹性网卡（ACS::ECS::NetworkInterface）
		包含	ECS实例（ACS::ECS::Instance）
	VPC路由表（ACS::VPC::RouteTable）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
云数据库RDS	RDS实例（ACS::RDS::DBInstance）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
		被包含	ESS伸缩组（ACS::ESS::ScalingGroup）
负载均衡SLB	SLB负载均衡（ACS::SLB::LoadBalancer）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
		挂载	EIP弹性公网IP（ACS::EIP::EipAddress）
		被包含	ESS伸缩组（ACS::ESS::ScalingGroup）
	SLB客户端证书（ACS::SLB::CACertificate）	无	无
	SLB服务端证书（ACS::SLB::ServerCertificate）	无	无
	SLB访问控制列表（ACS::SLB::AccessControlList）	无	无
云数据库PolarDB	PolarDB集群（ACS::PolarDB::DBCluster）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
云数据库	Redis实例	被包含	VPC专有网络（ACS::VPC::VPC）

云服务	资源类型	关系	相关资源
Redis版	（ACS::Redis::DBInstance）		
		被包含	VPC交换机（ACS::VPC::Vswitch）
云数据库MongoDB版	MongoDB实例（ACS::MongoDB::DBInstance）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
云数据库Hbase	HBase集群（ACS::HBase::Cluster）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
弹性公网IP	EIP弹性公网IP（ACS::EIP::EipAddress）	挂载	CBWP共享带宽包（ACS::CBWP::CommonBandwidthPackage）
		挂载	ECS实例（ACS::ECS::Instance）
		挂载	ECS弹性网卡（ACS::ECS::NetworkInterface）
		挂载	NAT网关（ACS::NAT::NATGateway）
		挂载	SLB负载均衡（ACS::SLB::LoadBalancer）
容器服务Kubernetes版	ACK集群（ACS::ACK::Cluster）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
		关联	ECS安全组（ACS::ECS::SecurityGroup）
弹性伸缩ESS	ESS伸缩配置（ACS::ESS::ScalingConfiguration）	关联	ECS安全组（ACS::ECS::SecurityGroup）
		关联	ESS伸缩组（ACS::ESS::ScalingGroup）
	ESS伸缩组（ACS::ESS::ScalingGroup）	包含	SLB负载均衡（ACS::SLB::LoadBalancer）
		被包含	VPC专有网络（ACS::VPC::VPC）
		包含	RDS实例（ACS::RDS::DBInstance）
		被包含	VPC交换机（ACS::VPC::Vswitch）
		关联	ESS伸缩规则（ACS::ESS::ScalingRule）
		关联	ESS伸缩配置（ACS::ESS::ScalingConfiguration）

云服务	资源类型	关系	相关资源
	ESS伸缩规则（ACS::ESS::ScalingRule）	关联	ESS伸缩组（ACS::ESS::ScalingGroup）
VPN网关	VPN网关（ACS::VPN::VpnGateway）	挂载	VPN IPsec连接（ACS::VPN::VpnConnection）
		挂载	VPC专有网络（ACS::VPC::VPC）
		挂载	VPC交换机（ACS::VPC::Vswitch）
	VPN IPsec连接（ACS::VPN::VpnConnection）	挂载	VPN网关（ACS::VPN::VpnGateway）
		挂载	VPN用户网关（ACS::VPN::CustomerGateway）
	VPN用户网关（ACS::VPN::CustomerGateway）	挂载	VPN IPsec连接（ACS::VPN::VpnConnection）
云企业网CEN	CEN实例（ACS::CEN::CenInstance）	挂载	CEN流日志（ACS::CEN::Flowlog）
		挂载	CEN带宽包（ACS::CEN::CenBandwidthPackage）
	CEN流日志（ACS::CEN::Flowlog）	挂载	CEN实例（ACS::CEN::CenInstance）
	CEN带宽包（ACS::CEN::CenBandwidthPackage）	挂载	CEN实例（ACS::CEN::CenInstance）
Web应用防火墙	WAF实例（ACS::WAF::Instance）	包含	WAF域名（ACS::WAF::Domain）
	WAF域名（ACS::WAF::Domain）	被包含	WAF实例（ACS::WAF::Instance）
NAT网关	NAT网关（ACS::NAT::NATGateway）	被包含	VPC专有网络（ACS::VPC::VPC）
		挂载	EIP弹性公网IP（ACS::EIP::EipAddress）
阿里云Elasticsearch	Elasticsearch Logstash实例（ACS::Elasticsearch::Logstash）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
	Elasticsearch实例（ACS::Elasticsearch::Instance）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
堡垒机	堡垒机实例（ACS::Bastionhost::Instance）	关联	ECS安全组（ACS::ECS::SecurityGroup）
		被包含	VPC专有网络（ACS::VPC::VPC）

云服务	资源类型	关系	相关资源
		被包含	VPC交换机（ACS::VPC::Vswitch）
消息队列MQ	RocketMQ消费集群组（ACS::Ons::Group）	被包含	消息队列RocketMQ版（ACS::Ons::Instance）
	RocketMQ消费订阅主题（ACS::Ons::Topic）	被包含	消息队列RocketMQ版（ACS::Ons::Instance）
	消息队列RocketMQ版（ACS::Ons::Instance）	包含	RocketMQ消费集群组（ACS::Ons::Group）
		包含	RocketMQ消费订阅主题（ACS::Ons::Topic）
私网连接Private Link	终端节点（ACS::PrivateLink::VpcEndpoint）	关联	ECS安全组（ACS::ECS::SecurityGroup）
		被包含	终端节点服务（ACS::PrivateLink::VpcEndpointService）
		被包含	VPC专有网络（ACS::VPC::VPC）
	终端节点服务（ACS::PrivateLink::VpcEndpointService）	包含	终端节点（ACS::PrivateLink::VpcEndpoint）
时间序列数据库TSDB	TSDB实例（ACS::TSDB::Instance）	被包含	VPC专有网络（ACS::VPC::VPC）
		被包含	VPC交换机（ACS::VPC::Vswitch）
共享带宽CBWP	CBWP共享带宽包（ACS::CBWP::CommonBandwidthPackage）	挂载	EIP弹性公网IP（ACS::EIP::EipAddress）
文件存储NAS	NAS文件系统（ACS::NAS::FileSystem）	挂载	ECS自动快照策略（ACS::ECS::AutoSnapshotPolicy）
密钥管理服务	KMS主密钥（ACS::KMS::Key）	关联	ECS云盘（ACS::ECS::Disk）
访问控制RAM	RAM角色（ACS::RAM::Role）	无	无
	RAM策略（ACS::RAM::Policy）	无	无
	RAM用户（ACS::RAM::User）	无	无
	RAM用户组（ACS::RAM::Group）	无	无
CDN	CDN域名（ACS::CDN::Domain）	无	无
对象存储OSS	OSS存储空间（ACS::OSS::Bucket）	无	无

云服务	资源类型	关系	相关资源
DDoS高防	DDoS实例（ACS::DdosCoo::Instance）	无	无
文件存储NAS	NAS文件系统（ACS::NAS::FileSystem）	无	无
	NAS挂载点（ACS::NAS::MountTarget）	无	无
	NAS权限组（ACS::NAS::AccessGroup）	无	无
消息队列MQ	MQ实例（ACS::MQ::Instance）	无	无
资源管理	资源组（ACS::RM::ResourceGroup）	无	无
云解析DNS	DNS实例（ACS::DNS::Instance）	无	无
	DNS域名分组（ACS::DNS::DomainGroup）	无	无
	DNS域名（ACS::DNS::Domain）	无	无
微服务引擎	MSE集群（ACS::MSE::Cluster）	无	无
运维编排OOS	应用程序清单（ACS::OOS::Inventory.Application）	无	无
	文件清单（ACS::OOS::Inventory.File）	无	无
	实例详细信息（ACS::OOS::Inventory.InstanceInformation）	无	无
	网络配置清单（ACS::OOS::Inventory.Network）	无	无
	服务清单（ACS::OOS::Inventory.Service）	无	无
	Windows注册表清单（ACS::OOS::Inventory.WindowsRegistry）	无	无
	Windows角色清单（ACS::OOS::Inventory.WindowsRole）	无	无

云服务	资源类型	关系	相关资源
	Windows更新清单（ACS::OOS::Inventory.WindowsUpdate）	无	无
资源编排	ROS资源栈（ACS::ROS::Stack）	无	无
	ROS资源栈组（ACS::ROS::StackGroup）	无	无

6.普通账号、成员账号和企业管理账号的使用差异

本文介绍了普通账号、成员账号和企业管理账号的使用差异。

普通账号、成员账号和企业管理账号的使用差异如下表所示。

差异项	普通账号	成员账号	企业管理账号
账号	未被企业管理账号加入资源目录的独立的阿里云账号。	被企业管理账号加入资源目录的阿里云账号。	开通资源目录并管理成员账号的阿里云账号。
菜单	在**概览**、**资源**、**合规包**和**规则**菜单，默认显示当前账号的资源、合规包和规则。	在**概览**、**资源**、**合规包**和**规则**菜单，只能看到**当前账号**和所属账号组页签。	在**概览**、**资源**、**合规包**和**规则**菜单，既能看到**当前账号**页签，还能看到所有账号组页签。
资源	查看当前账号下的资源列表、资源配置时间线和资源合规时间线。	只能查看当前账号下的资源列表、资源配置时间线和资源合规时间线。	查看当前账号和所有账号组内成员账号的资源列表、资源配置时间线和资源合规时间线。
合规包	新建、修改、删除和查看合规包，并下载合规检查报告。	如果成员账号被加入到账号组内，会显示**当前账号**和账号组页签。 • 在**当前账号**页签，成员账号可以新建、修改、删除和查看合规包，并下载合规检查报告。该合规包只对当前成员账号生效。 • 在账号组页签，成员账号只能被动接受企业管理账号在该账号组中新建的合规包，且对当前成员账号生效。当前成员账号只能查看合规包和合规检查结果。	为当前账号和所有账号组内的成员账号新建、修改、删除和查看合规包，并下载合规检查报告。
规则	新建、修改、删除、启用、停用和查看规则，并下载合规检查报告。	如果成员账号被加入到账号组内，会显示**当前账号**和账号组页签。 • 在**当前账号**页签，成员账号可以新建、修改、删除、启用、停用和查看规则，并下载合规检查报告。该规则只对当前成员账号生效。 • 在账号组页签，成员账号只能被动接受企业管理账号在该账号组中新建的规则，且对当前成员账号生效。当前成员账号只能查看规则和合规检查结果。	为当前账号和所有账号组内的成员账号新建、修改、删除、启用、停用和查看规则，并下载合规检查报告。

差异项	普通账号	成员账号	企业管理账号
账号组	不能新建、修改、删除和查看账号组。	不能新建、修改、删除和查看账号组。仅作为某个账号组内的成员账号存在。	新建、修改、删除和查看账号组。
配置审计服务关联角色	授权配置审计服务时，自动新建配置审计服务关联角色。	如果成员账号未新建配置审计服务关联角色，则在企业管理账号新建账号组时，自动为账号组内的成员账号新建配置审计服务关联角色。	授权配置审计服务时，自动新建配置审计服务关联角色。
资源投递和资源事件通知	独立为当前账号设置资源投递和资源事件通知。	被动遵从企业管理账号设置的资源投递和资源事件通知。	为当前企业管理账号和所有账号组内的成员账号设置资源投递和资源事件通知。