ALIBABA CLOUD

阿里云

配置审计

配置审计公共云合集

文档版本：20220704

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.合规包

1.1. 概述

合规包帮助您动态且持续地检查资源的合规性，对于不合规资源，提醒您及时修复。本文介绍12种合规包的主要功能。

CIS网络安全框架检查

CIS（Center for Internet Security）网络安全框架检查，为您动态且持续地监控您保有在阿里云上的资源是否符合CIS网络安全框架要求。满足这些要求，可以大幅度降低网络安全风险。

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。CIS网络安全框架检查支持的功能如下表所示。

功能	说明
检查账号	检查阿里云账号及RAM用户的密码设置、权限策略等。
检查网络	检查实例的网络归属、安全组设置、端口是否开放、流量监控等。
检查虚拟机	检查虚拟机的磁盘是否加密、端口是否开放、系统补丁、端点保护等。
检查对象存储OSS	检查存储空间的读写设置、安全传输、内容加密等。
检查数据库	检查数据库的连接类型、数据加密、数据库审计等。

等保三级预检

基于等保2.0三级标准，等保三级预检为您动态且持续地监控阿里云上资源的合规性，从而避免正式检查时反复整改，帮助您快速通过等保检查。关于等保2.0，请参见什么是等保2.0。

等保三级预检检查的功能如下表所示。

功能	说明
检查网络类型	检查ECS实例和数据库实例的网络类型是否为专有网络。如果为专有网络，且关联的专有网络在指定参数范围内，则视为“合规”。
检查防护设置	检查ECS实例和数据库的IP白名单是否设置为0.0.0.0/0，以及ECS数据磁盘加密是否开启。
检查对象存储OSS	检查OSS存储空间的读写设置是否为只读，以及同城冗余存储和服务端OSS完全托管加密是否开启。
检查带宽	检查负载均衡SLB和弹性公网IP的带宽是否满足最低要求。

OSS合规管理最佳实践

对象存储OSS（Object Storage Service）是很多客户用来存储业务数据的重要存储服务。如果存储空间（Bucket）设置不符合安全防护要求，则可能带来数据泄露甚至丢失的巨大业务风险。OSS合规管理最佳实践可以帮助您动态且持续地监控存储空间的不合规设置，并提醒您及时修复。

OSS合规管理最佳实践检查的功能如下表所示。

功能	说明
检查读写设置	全局检查存储空间权限是否为公共读或公共读写。
检查防护设置	为进一步提升数据安全性，要求存储空间必须设置文件加密和防盗链。
检查同城冗余	检查存储空间是否启用同城冗余存储。

网络合规管理最佳实践

网络合规管理最佳实践持续检查网络架构、负载额度和安全设置的合规性，帮助您动态且持续地监控网络的不合规设置，提醒您及时修复。

网络合规管理最佳实践检查的功能如下表所示。

功能	说明
避免业务中断	如果网络负载额度达不到业务峰值要求，则服务可能在业务高峰期中断。
实现公网隔离	如果网络设置存在疏漏，则可能将业务系统暴露到公网环境，面对潜在的公网攻击和数据泄露。
及时发现网络问题	如果网络监控的实时监测未启用，则无法及时发现网络疏漏，带来潜在的业务风险。

账号权限合规管理最佳实践

账号权限合规管理最佳实践将对阿里云账号和RAM用户进行全面的合规检查，帮助您提前发现和规避系统性风险。

账号权限合规管理最佳实践检查的功能如下表所示。

功能	说明
检查阿里云账号和RAM用户登录	检查阿里云账号和RAM用户密码的有效期，以及是否开启MFA。
检查安全设置	检查是否存在无效的RAM用户、用户组和策略，以及是否存在阿里云账号下的密钥对。
检查授权	检查RAM用户是否直接绑定策略，以及是否存在全量授权。

数据库合规管理最佳实践

数据库合规管理最佳实践持续检查云数据库RDS、Redis、MongoDB、PolarDB实例的加密防护和访问控制的合规性，避免数据泄露风险。

数据库合规管理最佳实践检查的功能如下表所示。

功能	说明
检查数据库到期时间	检查数据库实例的到期时间。
检查数据库防护设置	检查数据库实例是否开启释放保护，以及IP白名单是否设置为0.0.0.0/0。

功能	说明
检查数据库网络类型	检查数据库实例的网络类型是否为专有网络，以及关联的专有网络是否在指定参数范围内。

ECS合规管理最佳实践

ECS合规管理最佳实践持续检查云服务器ECS的运行状态、安全设置、防护设置、快照设置的合规性，避免业务中断和成本溢出的风险。

ECS合规管理最佳实践检查的功能如下表所示。

功能	说明
检查运行状态	检查ECS实例的运行状态。
检查安全设置	检查ECS实例的到期时间和安全组。
检查防护设置	检查ECS实例是否开启释放保护和数据磁盘加密。
检查快照设置	检查ECS磁盘是否设置自动快照策略和自动锁定，以及自动快照保留天数是否满足要求。

RMiT金融标准检查合规包

RMiT金融标准检查基于马来西亚金融行业通用的IT风险控制标准，持续检查云上IT系统的合规性。

RMiT金融标准检查支持的功能如下表所示。

功能	说明
检查账号	检查RAM用户的密码设置、权限策略、登录，以及是否开启MFA。
检查负载均衡SLB	检查SLB实例是否开启释放保护和HTTPS监听，以及阿里云签发的证书是否已过期。
检查云服务器ECS	检查ECS实例的网络类型是否为专有网络、是否开启数据磁盘加密、是否绑定IPv4公网IP地址等。
检查对象存储OSS	检查存储空间是否开启服务端KMS加密、是否开启服务端默认加密、是否开启日志存储等。
检查云数据库RDS	检查RDS实例是否开启历史事件、是否开启TDE加密、是否使用多可用区实例等。
检查操作审计	检查操作审计是否存在一个开启状态的跟踪，以及是否开启全量日志跟踪。

云治理中心合规实践

云治理中心合规实践统一配置和开启规则，保障云治理中心创建的资源结构和基础配置不被修改，同时保证多账号环境的安全性。

安全组最佳实践

安全组最佳实践持续检查安全组规则的合规性，降低安全风险。

OceanBase最佳实践

OceanBase最佳实践基于安全组最佳实践持续检查OceanBase的合规性。

资源稳定性最佳实践

资源稳定性最佳实践从高可用基础架构、容量保护、变更管理、监控管理、备份管理和故障隔离六大维度对云上资源的稳定性进行检测，有助于您提前发现隐患，提升资源稳定性和运维效率。

1.2. 启用合规包

合规包是配置审计根据合规场景定制的一组规则的集合。启用合规包时，您可以选择合规包模板中的规则，也可以选择托管规则和规则列表中的规则。启用合规包后，您可以从规则维度或账号维度查看关联资源的合规结果。

背景信息

配置审计默认提供12种合规包模板。更多信息，请参见概述。

启用合规包后，将在规则列表中自动新建托管规则，您可以对这些规则执行修改、删除、启用和停用操作。

合规包的使用限制如下：

- 普通账号只能新建5个合规包。
- 企业管理账号只能在**当前账号**或每个账号组页签下新建5个合规包。

普通账号

普通账号可以为当前账号新建合规包。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击右上角的**启用合规包**。
4. 在**基本信息**页面，设置合规包名称和风险等级，单击**下一步**。
5. 在**选择规则**页面，从合规包模板、规则列表或托管规则中选择规则，单击**下一步**。
6. 在**规则设置**页面，设置规则的名称、风险等级、描述和参数，单击**完成**。

企业管理账号

企业管理账号可以为当前账号和所有账号组内的成员账号新建合规包。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标账号组页签。
4. 在目标账号组页签，单击右上角的**启用合规包**。
5. 在**基本信息**页面，设置合规包名称和风险等级，单击**下一步**。
6. 在**选择规则**页面，从合规包模板、规则列表或托管规则中选择规则，单击**下一步**。
7. 在**规则设置**页面，设置规则的名称、风险等级、描述和参数，单击**完成**。

1.3. 修改合规包

您可以修改目标合规包的风险等级，也可以为合规包添加规则或修改合规包中已有规则。

普通账号

普通账号可以修改当前账号中的合规包。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标合规包名称对应**操作**列的**编辑**。
4. 修改目标合规包的基本信息。
   i. 在**基本信息**区域，单击右上角的**编辑**。
   ii. 在**基本信息**页面，选择合规包的风险等级。
   iii. 单击**完成**。
5. 为合规包添加规则或修改合规包中已有规则。
   - 为合规包添加规则。
     a. 单击**添加合规包规则**。
     b. 在**选择规则**页面，从合规包模板、规则列表或托管规则中选择规则，单击**下一步**。
     c. 在**规则设置**页面，设置规则的名称、风险等级、描述和参数，单击**完成**。
   - 修改合规包中已有规则。
     - 单击目标规则对应**操作**列的**编辑**，根据界面提示修改规则。

       当前合规包和规则列表中的目标规则同时被修改。具体操作，请参见修改规则。
     - 先单击目标规则对应**操作**列的**删除**，再单击**确定**。

       目标规则从当前合规包和规则列表中删除。
     - 单击目标规则对应**操作**列的**移出**。

       目标规则仅从当前合规包中删除，规则列表中保留。

企业管理账号

企业管理账号可以修改当前账号和所有账号组内成员账号中的合规包。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标合规包名称对应**操作**列的**编辑**。
5. 修改目标合规包的基本信息。
   i. 在**基本信息**区域，单击右上角的**编辑**。
   ii. 在**基本信息**页面，选择合规包的风险等级。
   iii. 单击**完成**。
6. 为合规包添加规则或修改合规包中已有规则。
   - 为合规包添加规则。
     a. 单击**添加合规包规则**。
     b. 在**选择规则**页面，从合规包模板、规则列表或托管规则中选择规则，单击**下一步**。
     c. 在**规则设置**页面，设置规则的名称、风险等级、描述和参数，单击**完成**。

- 修改合规包中已有规则。
  - 单击目标规则对应**操作**列的**编辑**，根据界面提示修改规则。

    当前合规包和规则列表中的目标规则同时被修改。具体操作，请参见修改规则。
  - 先单击目标规则对应**操作**列的**删除**，再单击**确定**。

    目标规则从当前合规包和规则列表中删除。
  - 单击目标规则对应**操作**列的**移出**。

    目标规则仅从当前合规包中删除，规则列表中保留。

1.4. 删除合规包

当您无需通过某个合规包检查资源时，可以删除该合规包。删除合规包后，以合规包名称为前缀的规则将自动被删除，原有的检查结果和报告也将被删除。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标合规包名称对应**操作**列的**删除**。
4. 在**删除**对话框，单击**确定**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标合规包名称对应**操作**列的**删除**。
5. 在**删除**对话框，单击**确定**。

1.5. 查看合规包的合规检查结果

当您启用合规包后，配置审计自动为您新建多条以合规包名称为前缀的规则，您可以从规则和账号维度查看资源的检查结果。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标合规包名称或合规包名称对应**操作**列的**详情**。
4. 在**合规包详情**页面，查看合规检查的基本信息和检查结果。
   - 基本信息

     您可以查看合规包的名称、描述信息、风险等级、合规包状态、合规包创建时间和生效范围。
   - 规则维度

     您可以查看不合规的规则数和目标合规包检查的所有规则。单击左侧某条规则名称，您可以在右侧筛选出该规则关联的所有资源。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标合规包名称或合规包名称对应**操作**列的**详情**。
5. 在**合规包详情**页面，查看合规检查的基本信息和检查结果。
   - 基本信息

     您可以查看合规包的名称、描述信息、风险等级、合规包状态、合规包创建时间和生效范围。
   - 规则维度

     您可以查看不合规的规则数和目标合规包检查的所有规则。单击左侧某条规则名称，您可以在右侧筛选出该规则关联的所有资源。
   - 账号维度

     您可以查看不合规的账号数和目标合规包检查的所有账号。单击左侧某个账号，您可以在右侧筛选出该账号下的所有资源。

1.6. 下载合规包的合规检查报告

您可以将合规检查报告下载到本地，便于云下分配任务并跟进资源配置的修改。

普通账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标合规包名称或合规包名称对应**操作**列的**详情**。
4. 在**合规包详情**页面，单击右上角的**报告下载**。

   您可以获得一份Excel格式的检查报告。在该检查报告中，您可以查看**检测概览**和**不合规资源**。

企业管理账号

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**合规包**。
3. 在**合规包**页面，单击目标账号组页签。
4. 在目标账号组页签，单击目标合规包名称或合规包名称对应**操作**列的**详情**。
5. 在**合规包详情**页面，单击右上角的**报告下载**。

   您可以获得一份Excel格式的检查报告。在该检查报告中，您可以查看**检测概览**和**不合规资源**。

1.7. 合规包模板

1.7.1. CIS网络安全框架检查模板

CIS网络安全框架检查模板包含对CIS Alibaba Cloud Foundation Benchmark v1.0.0部分建议的规则，本文为您介绍该合规包模板中的规则及其对应的CIS建议项。

> **说明**
>
> - 合规包模板为您提供通用的合规性框架，通过输入规则参数和修正设置，可以帮助您快速创建符合目标场景的合规包。规则的“合规”仅指符合规则定义本身的合规性描述，不确保您符合特定法规或行业标准的所有要求。
> - 关于CIS合规标准的更多信息，请参见CIS_Alibaba_Cloud_Foundation_Benchmark_v1.0.0。

规则名称	规则描述	建议项编号	建议项说明
阿里云账号不存在AccessKey	阿里云账号不存在“已启用”或“已禁用”状态的AccessKey，视为“合规”。	1.2	Ensure no root account access key exists.
阿里云账号开启MFA	阿里云账号开启MFA，视为“合规”。	1.3	Ensure MFA is enabled for the "root" account.
RAM用户开启MFA	RAM用户开启MFA，视为“合规”。	1.4	Ensure that multi-factor authentication is enabled for all RAM users that have a console password.
RAM用户在指定时间内有登录行为	如果RAM用户在最近90天有登录行为，视为“合规”；如果RAM用户的最近登录时间为空，则检查更新时间，当更新时间小于等于90天时，视为“合规”。	1.5	Ensure users not logged on for 90 days or longer are disabled for console logon.
RAM用户的AccessKey在指定时间内轮换	RAM用户的AccessKey创建时间距离检查时间不超过指定天数，视为“合规”。	1.6	Ensure access keys are rotated every 90 days or less.
RAM用户密码策略符合要求	RAM用户密码策略中各项配置满足参数设置的值，视为“合规”。	1.7	Ensure RAM password policy requires at least one uppercase letter.
		1.8	Ensure RAM password policy requires at least one lowercase letter.
		1.9	Ensure RAM password policy require at least one symbol.
		1.10	Ensure RAM password policy require at least one number.
		1.11	Ensure RAM password policy requires minimum length of 14 or greater.
		1.12	Ensure RAM password policy prevents password reuse.

规则名称	规则描述	建议项编号	建议项说明
		1.13	Ensure RAM password policy expires passwords within 90 days or less.
		1.14	Ensure RAM password policy temporarily blocks logon after 5 incorrect logon attempts within an hour.
不存在超级管理员	RAM用户、RAM用户组、RAM角色均未拥有Resource为*和Action为*的超级管理员权限，视为“合规”。	1.15	Ensure RAM policies that allow full "*:*" administrative privileges are not created.
不直接授权给RAM用户	无直接绑定到RAM用户的权限策略，视为“合规”。	1.16	Ensure RAM policies are attached only to groups or roles.
操作审计开启全量日志跟踪	操作审计中存在开启状态的跟踪，且跟踪全部地域和全部事件类型，视为“合规”。	2.1	Ensure that ActionTrail are configured to export copies of all Log entries.
OSS公开存储空间设置权限策略且不能为匿名账号授予任何权限	为读写权限公开的OSS存储空间设置授权策略，且授权策略中不能为匿名账号授予任何读写的操作权限，视为“合规”；读写权限为私有的OSS存储空间视为“不适用”。	2.2	Ensure the OSS used to store ActionTrail logs is not publicly accessible.
		5.1	Ensure that OSS bucket is not anonymously or publicly accessible.
VPC开启流日志记录	VPC开启流日志（Flowlog）记录功能，视为“合规”。	2.5	Ensure virtual network flow log service is enabled.
		3.3	Ensure VPC flow logging is enabled in all VPCs.
WAF实例开启日志采集	已接入WAF进行防护的域名均开启日志采集，视为“合规”。	2.7	Ensure Web Application Firewall access and security log service is enabled.
使用专有网络类型的ECS实例	如果未指定参数，则检查ECS实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查ECS实例的专有网络实例在指定参数范围内，视为“合规”。	3.1	Ensure legacy networks does not exist.
安全组不允许对全部网	当安全组入方向网段未设置为0.0.0.0/0时，视为“合规”；当安	3.2	Ensure that SSH access is restricted from the internet.
		3.5	Ensure the security group are configured with fine grained rules.

规则名称		建议项编号	建议项说明
安全组不允许对全部网段开启风险端口	全组入方向网段设置为0.0.0.0/0，规则描述为风险端口为关闭状态时，视为“合规”。		
		4.3	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22.
		4.4	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389.
VPC自定义网段已设置路由	VPC自定义网段在关联路由表中存在至少一条网段内IP地址的路由信息，视为“合规”。	3.4	Ensure routing tables for VPC peering are "least access".
使用中的ECS数据磁盘开启加密	使用中的ECS数据磁盘开启加密，视为“合规”。	4.1	Ensure that 'Unattached disks' are encrypted.
		4.2	Ensure that ‘Virtual Machine’s disk’ are encrypted.
待挂载的ECS数据磁盘开启加密	待挂载的ECS数据磁盘开启加密，视为“合规”。	4.1	Ensure that 'Unattached disks' are encrypted.
		4.2	Ensure that ‘Virtual Machine’s disk’ are encrypted.
所有ECS实例漏洞都已修复	云安全中心发现的所有ECS实例的漏洞均已修复，视为“合规”。	4.5	Ensure that the latest OS Patches for all Virtual Machines are applied.
		8.7	Ensure that scheduled vulnerability scan is enabled on all servers.
ECS实例均已安装云安全中心代理	所有ECS实例均已安装云安全中心代理，视为“合规”。	4.6	Ensure that the endpoint protection for all Virtual Machines is installed.
		8.2	Ensure that all assets are installed with security agent.
OSS存储空间开启日志存储	OSS存储空间的日志管理中开启日志存储，视为“合规”。	5.3	Ensure that logging is enabled for OSS buckets.
OSS存储空间权限策略设置安全访问	OSS存储空间权限策略中包含读写操作的访问方式设置为HTTPS，或者拒绝访问的访问方式设置为HTTP，视为“合规”。	5.4	Ensure that 'Secure transfer required' is set to 'Enabled'.
OSS存储空间权限策略设置IP限制	OSS存储空间读写权限设置为私有，或权限策略中包含只允许特定IP访问的策略，视为“合规”。	5.7	Ensure network access rule for storage bucket is not set to
OSS存储空间ACL禁止公共读	OSS存储空间的ACL策略禁止公共读，视为“合规”。		

规则名称	规则描述	建议项编号	publicly accessible. 建议项说明
OSS存储空间ACL禁止公共读写	OSS存储空间的ACL策略禁止公共读写，视为“合规”。		
OSS存储空间开启服务端加密	OSS存储空间开启服务端OSS完全托管加密，视为“合规”。	5.8	Ensure server-side encryption is set to ‘Encrypt with Service Key’.
OSS存储空间使用自定义KMS密钥加密	OSS存储空间已使用自定义的KMS密钥加密，视为“合规”。	5.9	Ensure server-side encryption is set to ‘Encrypt with BYOK’.
RDS实例使用SSL证书	RDS实例的数据安全性设置开启SSL证书，视为“合规”。	6.1	Ensure that RDS instance requires all incoming connections to use SSL.
RDS实例未申请外网地址	RDS实例未申请外网地址，视为“合规”。	6.2	Ensure that RDS Instances are not open to the world.
RDS实例开启SQL审计	RDS实例的SQL审计状态为开启，视为“合规”。	6.3	Ensure that 'Auditing' is set to 'On' for applicable database instances.
RDS实例MySQL类型数据库的SQL审计日志保留天数满足指定要求	RDS实例MySQL类型数据库开启SQL审计且日志保留天数大于等于指定值，视为“合规”。	6.4	Ensure that 'Auditing' Retention is 'greater than 6 months'.
RDS实例开启TDE加密	RDS实例的数据安全性设置开启TDE加密，视为“合规”。	6.5	Ensure that 'TDE' is set to 'Enabled' on for applicable database instance.
RDS实例PostgreSQL类型数据库参数log_connections设置为on	RDS实例PostgreSQL类型数据库参数log_connections设置为on，视为“合规”。	6.7	Ensure parameter 'log_connections' is set to 'ON' for PostgreSQL Database.
RDS实例PostgreSQL类型数据库参数log_disconnections设置为on	RDS实例PostgreSQL类型数据库参数log_disconnections设置为on，视为“合规”。	6.8	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server.
RDS实例PostgreSQL类型数据库参数log_duration设置为on	RDS实例PostgreSQL类型数据库参数log_duration设置为on，视为“合规”。	6.9	Ensure server parameter 'log_duration is set to 'ON' for PostgreSQL Database Server.
ACK集群使用Terway网络插件	ACK集群使用Terway网络插件，视为“合规”。	7.7	Ensure Network policy is enabled on Kubernetes Engine Clusters.
		7.8	Ensure ENI multiple IP mode support for Kubernetes Cluster.
ACK集群未设置公网连接端点	ACK集群未设置公网连接端点，视为“合规”。	7.9	Ensure Kubernetes Cluster is created with Private cluster enabled.

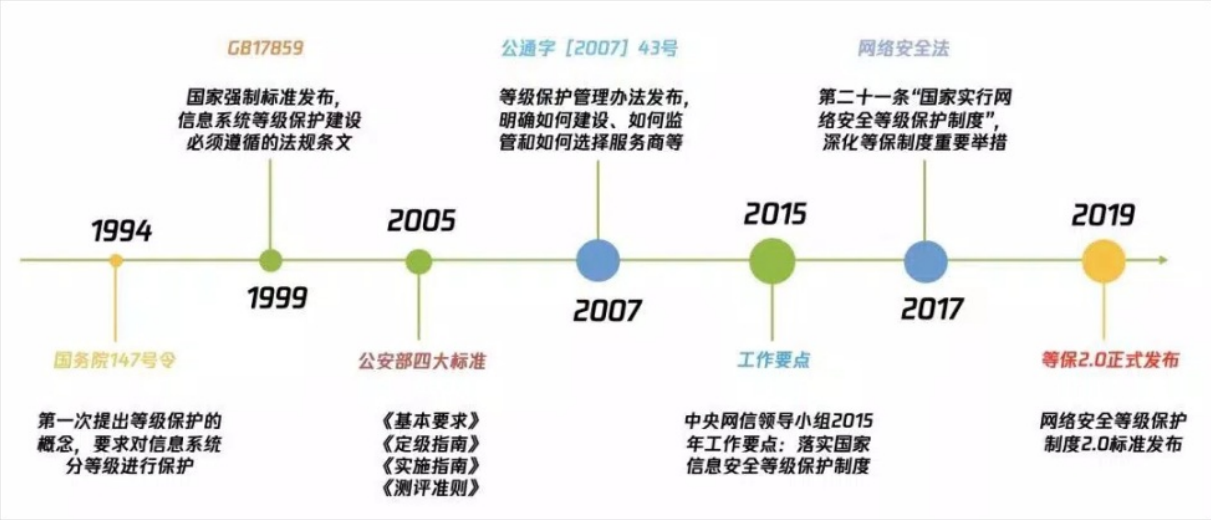
规则名称	规则描述	建议项编号	建议项说明
使用云安全中心企业版	使用云安全中心企业版或者更高级别的版本，视为“合规”。	8.1	Ensure that Security Center is Advanced or Enterprise Edition.
云安全中心通知项目已设置通知方式	云安全中心通知项目均已设置通知方式，视为“合规”。	8.5	Ensure that notification is enabled on all high risk items.

1.7.2. 等保三级预检模板

本文为您解读等保2.0的具体内容，以及等保三级预检合规包中的默认规则。

什么是等保2.0

等保2.0是指网络安全等级保护制度2.0国家标准，该标准已于2019年05月13日正式发布，并于2019年12月01日正式实施。等保2.0的发展和演进史如下图所示。



等保2.0的重要变化

- 云上信息系统纳入检测范围。

  基于等保1.0的网络和信息系统，新增了云计算平台、大数据平台、物联网、移动互联技术系统、工业控制系统。充分考虑了当前企业信息系统的业务多样性和复杂性。

- 云上租户的信息系统成为独立的检测对象。

  在等保1.0中，企业托管资源的云平台通过相应等保等级，即认为相应云上租户通过了相应等级。随着云上服务的复杂度和灵活性日渐成熟，云上租户对托管的资源具有越来越高的控制权，所以从等保2.0开始，云上租户使用云平台服务所构建的云上信息系统将作为独立的检测对象。

- 强调持续的安全能力构建，而非一次性检测。

  等保1.0主要关注在检测当时系统的合规状态，检测完成后，系统是否能持续保持安全合规是无法监管的。等保2.0在制定过程中，将对系统的持续合规要求融入到条例中，引导并监督企业构建一个可持续保护信息系统的安全能力。以PPDR（以策略为中心，构建防护、检测和响应防护机制）为核心思想、以可信认证为基础、以访问控制为核心，构建可信、可控和可管的立体化纵深防御体系。

分类	说明
可信	以可信计算技术为基础，构建一个可信的业务系统执行环境，即用户、平台、程序都是可信的，确保用户无法被冒充、病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现非预期的流程，从而保障了业务系统安全可信。
可控	以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对用户访问权限的控制可以确保系统中的用户不会出现越权操作，永远都按系统设计的方式进行资源访问，保证了系统的信息安全可控。
可管	通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建了一个工作平台，使其可以借助于本平台对系统进行更好的管理，从而弥补了我们现在重机制、轻管理的不足，保证信息系统安全可管。

等保2.0以“一个中心，三重防护”为网络安全技术设计的总体思路，其中一个中心即安全管理中心，三重防护即安全计算环境、安全区域边界和安全通信网络。

- 安全管理中心要求在系统管理、安全管理、审计管理三个方面实现集中管控，从被动防护转变成主动防护，从静态防护转变成动态防护，从单点防护转变成整体防护，从粗放防护转变成精准防护。
- 三重防护要求企业通过安全设备和技术手段实现身份鉴别、访问控制、入侵防范、数据完整性、保密性、个人信息保护等安全防护措施，实现平台的全方位安全防护。

等保1.0和2.0的差异如下表所示。

等保1.0	等保2.0
事前预防、事中响应、事后审计的纵深防御思路。	在“一个中心、三重防护”的理念基础上，注重全方位主动防御、安全可信、动态感知和全面审计。
0分以上基本符合。等保三级每年检测一次，等保四级每半年检测一次。	70分以上基本符合，等保三级和四级每年检测一次。

云上信息系统过等保的五大困难

等保2.0侧重视持续的合规监管能力，且要求等保三级和等保四级均每年检测一次。但资源托管在云端，云上信息系统过等保，具体困难如下表所示。

困难	说明
云上检测范围不明确	虚拟化IT设施与传统IT的部分概念不同，面对复杂的云上配置，无从下手。
无集中的资源管理	云平台如果不提供配置管理数据库CMDB（Configuration Management Database）能力，在等保的反复检测和整改过程中，仅向检测结构举证和演示云上系统详情，操作就非常繁琐。
自己不掌握系统数据	资源托管在云端，等保2.0要求举证管理行为的日志和合规情况，需要依赖云平台对审计数据的输出。
无法自建自动化检测	通常云下企业都有自己的配置管理数据库CMDB，只要合规和要求明确，完全可以自己写脚本扫描配置完成自检和监控。现在资源托管在云上，如果想通过脚本实现自检，则需要持续同步云上配置到云下，仅配置同步就消耗巨大的成本。
混合云截断成两部分	混合云的技术选型导致同一个业务系统部分在云上，部分在云下，无论是自检、扫描、监控或检测，都必须分开两次，人力和时间成本巨大。

借助云平台能力，实现持续监管

针对以上五大困难，阿里云在配置审计服务中，为您提供免费的等保预检能力，在等保预检和整改环节为企业助力。

配置审计将等保2.0条例解读为云上的合规检测规则，并持续监控资源的变更，动态实时的执行合规评估，及时推送不合规告警，让企业能时刻掌握云上信息系统的合规性。

等保三级预检模板

等保三级预检模板包含对等保2.0部分建议的规则，该合规包模板中的规则及其对应的建议项如下表所示。

> **说明** 合规包模板为您提供通用的合规性框架，通过输入规则参数和修正设置，可以帮助您快速创建符合目标场景的合规包。规则的“合规”仅指符合规则定义本身的合规性描述，不确保您符合特定法规或行业标准的所有要求。

规则名称	规则描述	建议项编号	建议项说明
使用专有网络类型的ECS实例	如果未指定参数，检查ECS实例的网络类型为专有网络，视为“合规”；如果指定参数，检查ECS实例的专有网络实例在指定参数范围内，视为“合规”。	8.1.2.1	a）应保证网络设备的业务处理能力满足业务高峰期需要。
		8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
		8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
		8.1.2.1	e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
		8.1.2.2	a）应采用密码技术保证通信过程中数据的完整性。
		8.1.2.2	b）应采用密码技术保证通信过程中数据的保密性。
使用专有网络类型的RDS实例	如果未指定参数，检查RDS实例的网络类型为专有网络，视为“合规”；如果指定参数，检查RDS实例的专有网络实例在指定参数范围内，视为“合规”。	8.1.2.1	a）应保证网络设备的业务处理能力满足业务高峰期需要。
		8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
		8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
		8.1.2.1	e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。

规则名称	规则描述	建议项编号	建议项说明
		8.1.2.2	a）应采用密码技术保证通信过程中数据的完整性。
		8.1.2.2	b）应采用密码技术保证通信过程中数据的保密性。
使用专有网络类型的Redis实例	如果未指定参数，检查Redis实例的网络类型为专有网络，视为“合规”；如果指定参数，检查Redis实例的专有网络实例在指定参数范围内，视为“合规”。	8.1.2.1	a）应保证网络设备的业务处理能力满足业务高峰期需要。
		8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
		8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
		8.1.2.1	e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
		8.1.2.2	a）应采用密码技术保证通信过程中数据的完整性。
		8.1.2.2	b）应采用密码技术保证通信过程中数据的保密性。
使用专有网络类型的MongoDB实例	如果未指定参数，则检查MongoDB实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查MongoDB实例的专有网络实例在指定参数范围内，视为“合规”。	8.1.2.1	a）应保证网络设备的业务处理能力满足业务高峰期需要。
		8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
		8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
		8.1.2.1	e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
		8.1.2.2	a）应采用密码技术保证通信过程中数据的完整性。
		8.1.2.2	b）应采用密码技术保证通信过程中数据的保密性。
		8.1.2.1	a）应保证网络设备的业务处理能力满足业务高峰期需要。
		8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。

规则名称 推荐使用	规则描述 如果未指定参数，则检查PolarDB实例的	建议项编号	建议项说明
专有网络类型的PolarDB实例	网络类型为专有网络，视为“合规”；如果指定参数，则检查PolarDB实例的专有网络实例在指定参数范围内，视为“合规”。	8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
		8.1.2.1	e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
		8.1.2.2	a）应采用密码技术保证通信过程中数据的完整性。
		8.1.2.2	b）应采用密码技术保证通信过程中数据的保密性。
弹性IP实例带宽满足最低要求	弹性公网IP实例的可用带宽大于等于您设置的参数，视为“合规”。	8.1.2.1	b）应保证网络各个部分的带宽满足业务高峰期需要。
SLB实例满足指定带宽要求	SLB实例的可用带宽大于等于规则中指定的参数值，视为“合规”。	8.1.2.1	b）应保证网络各个部分的带宽满足业务高峰期需要。
安全组不允许对全部网段开启风险端口	当安全组入方向网段未设置为0.0.0.0/0时，视为“合规”；当安全组入方向网段设置为0.0.0.0/0，但指定的风险端口为关闭状态时，视为“合规”。	8.1.3.1	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
		8.1.4.4	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。
安全组入网设置有效	安全组入方向授权策略为允许，当端口范围-1/-1和授权对象0.0.0.0/0未同时出现时，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
SLB实例未绑定公网IP	SLB实例未绑定公网IP地址，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
RDS实例未申请外网地址	RDS实例未申请外网地址，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
		8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。

规则名称	规则描述	建议项编号	建议项说明
ECS实例未绑定公网地址	ECS实例未直接绑定IPv4公网IP或弹性公网IP，视为“合规”。	8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
OSS存储空间ACL禁止公共读	OSS存储空间的ACL策略禁止公共读，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
Redis实例IP白名单不设置为全网段	Reids实例的IP白名单未设置为0.0.0.0/0，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
MongoDB实例IP白名单不设置为全网段	MongoDB实例的IP白名单未设置为0.0.0.0/0，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
PolarDB实例IP白名单不能设置为全网段	PolarDB实例的IP白名单未设置为0.0.0.0/0，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
SLB访问控制列表不允许配置所有地址段	SLB实例开启白名单方式的访问控制，且访问控制策略组的IP地址段未设置为0.0.0.0/0，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
RDS实例正确开启安全白名单	RDS实例已开启安全白名单，且安全白名单中不包含0.0.0.0/0，视为“合规”。	8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
OSS存储空间ACL禁止公共读	OSS存储空间的ACL策略禁止公共读，视为“合规”。	8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
		8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

规则名称	规则描述	建议项编号	建议项说明
操作审计开启跟踪状态	操作审计中存在开启状态的跟踪，视为“合规”。	8.1.3.5	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
		8.1.4.3	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
RAM用户开启MFA	RAM用户开启MFA，视为“合规”。	8.1.4.1	d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
SLB开启HTTPS监听	为SLB实例在规则中指定的监听端口开启HTTPS监听，视为“合规”。	8.1.4.7	a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
CDN域名开启HTTPS加密	CDN域名开启HTTPS协议加密，视为“合规”。	8.1.4.7	a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
OSS存储空间开启服务端加密	OSS存储空间开启服务端的OSS完全托管加密，视为“合规”。	8.1.4.7	b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
		8.1.4.8	b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
ECS数据磁盘开启加密	ECS数据磁盘开启加密，视为“合规”。	8.1.4.7	b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
使用高可用的RDS实例	RDS实例为高可用版，视为“合规”。	8.1.4.9	a）应提供重要数据的本地数据备份与恢复功能。
		8.1.4.9	b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。
		8.1.4.9	c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
使用多可用区的RDS实例	RDS实例支持多个可用区，视为“合规”。	8.1.4.9	c）应提供重要数据处理系统的热冗余，保证系统的高可用性。

规则名称	规则描述	建议项编号	建议项说明
OSS存储空间开启同城冗余存储	OSS存储空间开启同城冗余存储，视为“合规”。	8.1.4.9	c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
使用数据库代理模式访问SQL Server	RDS实例的SQL Server类型数据库的访问模式为代理模式，视为“合规”。	8.1.4.9	c）应提供重要数据处理系统的热冗余，保证系统的高可用性。

1.7.3. RMiT金融标准检查模板

本文为您介绍RMiT金融标准检查合规包中的默认规则。

规则名称	规则描述
操作审计开启全量日志跟踪	操作审计中存在开启状态的跟踪，且跟踪追踪全部地域和全部事件类型，视为“合规”。
操作审计开启跟踪状态	操作审计开启跟踪状态，视为“合规”。
OSS存储空间使用指定KMS加密	OSS存储空间已使用您指定的KMS加密，视为“合规”。
ECS数据磁盘设置自动快照策略	ECS数据磁盘已设置自动快照策略，视为“合规”。
ECS数据磁盘开启加密	ECS数据磁盘开启加密，视为“合规”。
ECS实例未分配IPv4公网地址	ECS实例未绑定IPv4公网IP地址，视为“合规”。
使用专有网络类型的ECS实例	如果未指定参数，则检查ECS实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查ECS实例的专有网络实例在指定参数范围内，视为“合规”。
SLB使用证书为阿里云签发	SLB使用证书为阿里云签发，视为“合规”。
SLB服务器证书在有效期内	SLB服务器证书在有效期内，视为”合规“。
SLB实例开启释放保护	SLB实例开启释放保护，视为“合规”。
SLB开启HTTPS监听	SLB开启HTTPS监听80/8080端口，视为“合规”。
RAM用户组非空	RAM用户组至少包含一个RAM用户，视为“合规”。
RAM用户密码策略符合要求	RAM用户密码策略中各项配置满足参数设置的值，视为“合规”。
不存在超级管理员	RAM用户、RAM用户组、RAM角色均未拥有Action为*的超级管理员权限，视为“合规”。
阿里云账号不存在AccessKey	阿里云账号不存在“已启用”状态的AccessKey，视为“合规”。
RAM用户归属用户组	所有RAM用户均归属于RAM用户组，视为“合规”。

规则名称	规则描述
RAM用户开启MFA	RAM用户开启MFA，视为“合规”。
不直接授权给RAM用户	无直接绑定到RAM用户的权限策略，视为“合规”。
RAM用户在指定时间内有登录行为	如果RAM用户在最近90天有登录行为，视为“合规”；如果RAM用户的最近登录时间为空，则检查更新时间，当更新时间小于等于90天时，视为“合规”。
RDS实例IP白名单未设置为全网段	RDS实例的IP白名单未设置为0.0.0.0/0，视为“合规”。
RDS实例开启历史事件	RDS实例开启历史事件日志，视为“合规”。
使用多可用区的RDS实例	RDS实例为多可用区实例，视为“合规”。
RDS实例开启TDE加密	RDS实例的数据安全性设置开启TDE加密，视为“合规”。
OSS存储空间开启日志存储	OSS存储空间的日志管理中开启日志存储，视为“合规”。
OSS存储空间权限策略不能为匿名账号授予任何权限	OSS存储空间读写权限设置为私有，而且权限策略中不能为匿名账号授予任何读写的操作权限，视为“合规”。
OSS存储空间开启服务端默认加密	OSS存储空间开启服务端OSS完全托管加密，视为“合规”。
OSS存储空间开启服务端KMS加密	OSS存储空间开启服务端KMS加密，视为“合规”。
OSS存储空间开启版本控制	OSS存储空间开启版本控制，视为“合规”。
VPC开启流日志记录	VPC开启流日志（Flowlog）记录功能，视为“合规”。
IPsec VPN连接正常	IPsec VPN连接状态为“已建立”，视为“合规”。
WAF实例开启日志采集	已接入WAF进行防护的域名均开启日志采集，视为“合规”。
OSS存储空间权限策略设置安全访问	OSS存储空间权限策略中包含读写操作的访问方式设置为HTTPS，或者拒绝访问的访问方式设置为HTTP，视为“合规”。
安全组入网设置有效	安全组入方向授权策略为允许，当端口范围-1/-1和授权对象0.0.0.0/0未同时出现时，视为“合规”。
密钥管理服务设置主密钥自动轮转	密钥管理服务中的主密钥设置为自动轮转，视为“合规”。
使用专有网络服务的Elasticsearch实例	如果未指定参数，则检查Elasticsearch实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查Elasticsearch实例的专有网络实例在指定参数范围内，视为“合规”。

1.7.4. OSS合规管理最佳实践模板

本文为您介绍OSS合规管理最佳实践合规包中的默认规则。

规则名称	规则描述
OSS存储空间ACL禁止公共读	OSS存储空间的ACL策略禁止公共读，视为“合规”。
OSS存储空间ACL禁止公共读写	OSS存储空间的ACL策略禁止公共写，视为“合规”。
OSS存储空间开启服务端加密	OSS存储空间开启服务端OSS完全托管加密，视为“合规”。
OSS存储空间开启防盗链功能	OSS存储空间开启防盗链功能，视为“合规”。
OSS存储空间开启同城冗余存储	OSS存储空间开启同城冗余存储，视为“合规”。
OSS存储空间开启日志存储	OSS存储空间的日志管理中开启日志存储，视为“合规”。
OSS存储空间开启版本控制	OSS存储空间开启版本控制，视为“合规”。

1.7.5. 网络合规管理最佳实践模板

本文为您介绍网络合规管理最佳实践合规包中的默认规则。

规则名称	规则描述
SLB实例满足指定带宽要求	SLB实例可用带宽大于等于指定参数值，视为“合规”。
SLB开启HTTPS监听	SLB开启HTTPS监听80/8080端口，视为“合规”。
安全组入网设置有效	安全组入方向授权策略为允许，当端口范围-1/-1和授权对象0.0.0.0/0未同时出现时，视为“合规”。
安全组不允许对全部网段开启风险端口	当安全组入网网段设置为0.0.0.0/0时，且已关闭端口22或3389，视为“合规”。
弹性IP实例带宽满足最低要求	弹性IP实例可用带宽大于等于指定参数值，视为“合规”。
CDN域名开启HTTPS加密	CDN域名开启HTTPS协议加密，视为“合规”。
SLB使用证书为阿里云签发	SLB使用证书为阿里云签发，视为“合规”。
IPsec VPN开启健康检查	IPsec VPN开启健康检查，视为“合规”。
VPC开启流日志记录	VPC开启流日志（Flowlog）记录功能，视为“合规”。
SLB实例开启释放保护	SLB实例开启释放保护，视为“合规”。
SLB服务器证书在有效期内	SLB服务器证书在有效期内，视为”合规“。
SLB实例状态为运行中	SLB实例的运行状态为运行中，视为“合规”。
SLB服务器证书到期检查	SLB服务器证书的到期时间距离检查时间大于等于参数设定的时间范围，视为“合规”。
SLB预付费实例到期检查	SLB预付费实例的到期时间距离检查时间大于等于参数设定的时间范围，视为“合规”。

规则名称	规则描述
SLB实例为性能保障型实例	SLB实例为性能保障型实例，视为“合规”。
SLB预付费实例开启自动续费	SLB预付费实例开启自动续费，视为“合规”。
SLB实例负载权重不为0	SLB实例已设置后端服务器，且后端服务器设置的权重不为0，视为“合规”。

1.7.6. 账号权限合规管理最佳实践模板

本文为您介绍账号权限合规管理最佳实践合规包中的默认规则。

规则名称	规则描述
阿里云账号开启MFA	阿里云账号开启MFA，视为“合规”。
RAM用户组非空	RAM用户组至少包含一个RAM用户，视为“合规”。
阿里云账号不存在AccessKey	阿里云账号不存在“已启用”或“已禁用”状态的AccessKey，视为“合规”。
不直接授权给RAM用户	无直接绑定到RAM用户的权限策略，视为“合规”。
不存在超级管理员	RAM用户、RAM用户组、RAM角色均未拥有Resource为 `*` 和Action为 `*` 的超级管理员权限，视为“合规”。
RAM用户密码策略符合要求	RAM用户密码策略中各项配置满足参数设置的值，视为“合规”。
RAM用户归属用户组	所有RAM用户均归属于RAM用户组，视为“合规”。
高权限的RAM用户开启MFA	已被授予指定高风险权限策略的RAM用户开启MFA，视为“合规”。
不存在闲置的RAM权限策略	RAM权限策略至少绑定一个RAM用户组、RAM角色或RAM用户，视为“合规”。
RAM用户登录检查	RAM用户未同时开启控制台登录和AccessKey登录，视为“合规”。
RAM用户的AccessKey在指定时间内轮换	RAM用户的AccessKey创建时间距离检查时间不超过指定天数，视为“合规”。
RAM用户在指定时间内有登录行为	如果RAM用户在最近90天有登录行为，视为“合规”；如果RAM用户的最近登录时间为空，则检查更新时间，当更新时间小于等于90天时，视为“合规”。

1.7.7. 数据库合规管理最佳实践模板

本文为您介绍数据库合规管理最佳实践合规包中的默认规则。

规则名称	规则描述
MongoDB预付费集群到期检查	MongoDB预付费集群到期时间距离检查时间大于等于设置的天数，视为“合规”。
HBase预付费集群到期检查	HBase预付费集群到期时间距离检查时间大于等于设置的天数，视为“合规”。

规则名称	规则描述
RDS实例使用高安全白名单模式	RDS实例使用高安全白名单模式，视为“合规”。
PolarDB产品系列为集群版	PolarDB产品系列为集群版，视为“合规”。
Redis实例开启释放保护	Redis实例开启释放保护，视为“合规”。
Redis实例禁用高风险命令	Redis实例已设置禁用高风险命令，视为“合规”。
HBase集群类型为集群版	HBase集群类型为集群版，视为“合规”。
使用专有网络类型的HBase集群	如果未指定参数，则检查HBase集群的网络类型为专有网络，视为“合规”；如果指定参数，则检查HBase集群的专有网络实例在指定参数范围内，视为“合规”。
HBase集群配置为高可用	HBase集群的配置为高可用，视为“合规”。
HBase集群开启删除保护	HBase集群开启删除保护，视为“合规”。
MongoDB实例开启释放保护	MongoDB实例开启释放保护，视为“合规”。
MongoDB实例未被锁定	MongoDB实例的锁定状态为正常，视为“合规”。
MongoDB集群开启审计日志	MongoDB集群开启审计日志，视为“合规”。
RDS预付费实例到期检查	RDS预付费实例到期时间距离检查时间大于等于设置的天数，视为“合规”。
PolarDB预付费集群到期检查	PolarDB预付费集群到期时间距离检查时间大于等于设置的天数，视为“合规”。
Redis预付费集群到期检查	Redis预付费集群到期时间距离检查时间大于等于设置的天数，视为“合规”。
RDS实例开启SQL审计	RDS实例的SQL审计状态为开启，视为“合规”。
RDS实例IP白名单未设置为全网段	RDS实例的IP白名单未设置为0.0.0.0/0，视为“合规”。
使用高可用的RDS实例	RDS实例为高可用实例，视为“合规”。
使用专有网络类型的RDS实例	如果未指定参数，则检查RDS实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查RDS实例的专有网络实例在指定参数范围内，视为“合规”。
使用多可用区的RDS实例	RDS实例为多可用区实例，视为“合规”。
RDS实例使用SSL证书	RDS实例的数据安全性设置开启SSL证书，视为“合规”。
RDS实例开启TDE加密	RDS实例的数据安全性设置开启TDE加密，视为“合规”。
使用专有网络类型的Redis实例	如果未指定参数，则检查Redis实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查Redis实例的专有网络实例在指定参数范围内，视为“合规”。
Redis实例IP白名单未设置为全网段	Reids实例IP白名单未设置为0.0.0.0/0，视为“合规”。
使用集群版的Redis实例	Redis实例的架构类型为集群版，视为“合规”。

规则名称	规则描述
MongoDB实例IP白名单未设置为全网段	MongoDB实例IP白名单未设置为0.0.0.0/0，视为“合规”。
使用专有网络类型的MongoDB实例	如果未指定参数，则检查MongoDB实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查MongoDB实例的专有网络实例在指定参数范围内，视为“合规”。
PolarDB实例IP白名单未设置为全网段	PolarDB实例IP白名单未设置为0.0.0.0/0，视为“合规”。
推荐使用专有网络类型的PolarDB实例	如果未指定参数，则检查PolarDB实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查PolarDB实例的专有网络实例在指定参数范围内，视为“合规”。
RDS实例MySQL类型数据库的SQL审计日志保留天数满足指定要求	RDS实例MySQL类型数据库开启SQL审计且日志保留天数大于等于指定值，视为“合规”。
RDS实例开启历史事件	RDS实例开启历史事件日志，视为“合规”。

1.7.8. ECS合规管理最佳实践模板

本文为您介绍ECS合规管理最佳实践合规包中的默认规则。

规则名称	规则描述
ECS实例状态非已停止状态	ECS实例状态非已停止状态，视为“合规”。
ECS预付费实例到期检查	ECS预付费实例到期时间距离检查时间大于等于设置的天数，视为“合规”。
ECS实例开启释放保护	ECS实例开启释放保护，视为“合规”。
使用专有网络类型的ECS实例	如果未指定参数，则检查ECS实例的网络类型为专有网络，视为“合规”；如果指定参数，则检查ECS实例的专有网络实例在指定参数范围内，视为“合规”。
ECS数据磁盘开启加密	ECS数据磁盘开启加密，视为“合规”。
不存在闲置的ECS数据磁盘	ECS数据磁盘均已挂载到ECS实例，视为“合规”。
安全组不允许对全部网段开启风险端口	当安全组入网网段设置为0.0.0.0/0时，且已关闭端口22或3389，视为“合规”。
安全组入网设置有效	安全组入方向授权策略为允许，当端口范围-1/-1和授权对象0.0.0.0/0未同时出现时，视为“合规”。
ECS实例在指定安全组中	ECS实例在指定的安全组中，视为“合规”。
ECS使用指定镜像实例	ECS实例系统镜像在参数设置的范围内，视为“合规”。
ECS实例漏洞均已修复	云安全中心发现的所有ECS实例的漏洞均已修复，视为“合规”。

规则名称	规则描述
ECS实例已安装云安全中心代理	所有ECS实例均已安装云安全中心代理，视为“合规”。
ECS实例未被锁定	ECS实例未因欠费或安全等原因而被锁定，视为“合规”。
弹性伸缩组开启ECS实例健康检查	弹性伸缩组开启对ECS实例的健康检查，视为“合规”。
ECS数据磁盘设置自动快照策略	ECS数据磁盘已设置自动快照策略，视为“合规”。
ECS数据磁盘未被锁定	ECS数据磁盘未因欠费或安全等原因而被锁定，视为“合规”。
ECS数据磁盘释放时保留自动快照	设置ECS数据磁盘释放时保留自动快照，视为“合规”。
ECS自动快照保留天数满足指定要求	ECS自动快照策略设置的快照保留天数大于等于设置的天数，视为“合规”。

1.7.9. 云治理中心合规实践模板

本文为您介绍云治理中心合规实践合规包中的默认规则。

规则名称	规则描述
OSS存储空间开启服务端默认加密	OSS存储空间开启服务端OSS完全托管加密，视为“合规”。
OSS存储空间ACL禁止公共读	OSS存储空间的ACL策略禁止公共读，视为“合规”。
OSS存储空间ACL禁止公共读写	OSS存储空间的ACL策略禁止公共读写，视为“合规”。
阿里云账号不存在AccessKey	阿里云账号不存在“已启用”或“已禁用”状态的AccessKey，视为“合规”。
阿里云账号开启MFA	阿里云账号开启MFA，视为“合规”。
ECS数据磁盘开启加密	ECS数据磁盘开启加密，视为“合规”。
安全组不允许对全部网段开启风险端口	当安全组入网网段设置为0.0.0.0/0时，关闭端口22和3389，视为“合规”。
安全组入网设置有效	安全组入方向授权策略为允许，当端口范围-1/-1和授权对象0.0.0.0/0未同时出现时，视为“合规”。
使用专有网络类型的RDS实例	如果未指定参数，则检查RDS实例的网络类型为专有网络；如果指定参数，则检查RDS实例的专有网络实例在指定参数范围内，视为“合规”。
RDS实例开启TDE加密	RDS实例的数据安全性设置开启TDE加密，视为“合规”。
RDS实例IP白名单不是全网段	RDS实例的IP白名单未设置为0.0.0.0/0，视为“合规”。
RAM用户密码策略符合要求	RAM用户密码策略中各项配置满足参数设置的值，视为“合规”。

规则名称	规则描述
RAM用户不存在闲置AccessKey	RAM用户AccessKey的最后使用时间与当前时间之差小于参数设置的时间，视为“合规”。
ECS实例开启释放保护	ECS实例开启释放保护，视为“合规”。
SLB实例开启释放保护	SLB实例开启释放保护，视为“合规”。
阿里云账号拥有指定名称的角色	阿里云账号拥有指定名称的角色，视为“合规”。
RAM用户开启MFA	RAM用户开启MFA，视为“合规”。
SLB开启HTTPS监听	SLB开启HTTPS监听80和8080端口，视为“合规”。
资源归属指定区域范围	资源归属于参数指定的区域范围，视为“合规”。
RAM用户在指定时间内有登录行为	如果RAM用户在最近90天有登录行为，视为“合规”；如果RAM用户的最近登录时间为空，则检查更新时间，当更新时间小于等于90天时，视为“合规”。
满足多标签值的一种枚举	参数可指定一个标签的Key和Value的多种取值，资源具备其中一种取值，视为“合规”。
存在所有指定标签	最多可定义6组标签，资源需同时具有指定的所有标签，视为“合规”。
OSS存储空间开启日志存储	OSS存储空间的日志管理中开启日志存储，视为“合规”。

1.7.10. 安全组最佳实践

本文为您介绍安全组最佳实践合规包中的默认规则。

规则名称	规则描述
安全组非白名单端口入网设置有效	除指定的白名单端口外，其余端口不能有授权策略设置为允许且来源为0.0.0.0/0的入方向规则，视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。
安全组不允许对全部网段开启风险端口	当入网网段未设置为0.0.0.0/0时，即使端口范围包含指定的风险端口，也视为“合规”；当安全组入网网段设置为0.0.0.0/0时，端口范围不包含指定风险端口，也视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。
ECS实例在指定安全组下	ECS实例在指定的安全组下，视为“合规”。
安全组入网设置有效	安全组入方向授权策略为允许，当端口范围-1/-1和授权对象0.0.0.0/0未同时出现，或者被优先级更高的授权策略拒绝，视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。
安全组入网设置中不能有对所有端口开放的访问规则	安全组入方向授权策略为允许，当端口范围未设置为-1/-1时，视为“合规”；如果端口范围设置为-1/-1，但被优先级更高的授权策略拒绝，视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。

规则名称	规则描述
安全组入网设置不能有对所有协议开放的访问规则	安全组入方向授权策略为允许，当端协议类型未设置为All时，视为“合规”；如果协议类型设置为All，但被优先级更高的授权策略拒绝，视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。
安全组入网设置允许的来源IP不包含公网IP	安全组入网方向授权策略为允许的来源IP地址段不包含公网IP，视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。
安全组出方向未设置为全通	安全组出网方向未设置为全通，视为“合规”；云服务或虚商所使用的安全组不适用本规则，视为“不适用”。

1.7.11. OceanBase最佳实践

本文为您介绍OceanBase最佳实践合规包中的默认规则。

规则名称	规则描述
OceanBase集群开启SQL诊断功能	OceanBase集群开启SQL诊断，视为“合规”。
OceanBase集群开启数据库备份	OceanBase集群开启数据库备份，视为“合规”。
OceanBase租户开启TDE加密	OceanBase租户开启TDE加密，视为“合规”。
OceanBase租户IP白名单分组设置有效	OceanBase租户所有IP白名单分组都不包含0.0.0.0，视为“合规”。
OceanBase集群开启SSL加密	OceanBase集群开启了SSL加密，视为“合规”。

1.7.12. 资源稳定性最佳实践

本文为您介绍资源稳定性最佳实践合规包中的默认规则。

规则名称	规则描述
ECS实例使用指定名称的操作系统	ECS实例使用的操作系统英文名称在指定的白名单范围中，或操作系统英文名称不在指定的黑名单范围中，视为“合规”。
运行中的ECS实例在指定的专有网络中	如果未指定参数，则检查ECS实例的网络类型为专有网络；如果指定参数，则检查ECS实例的专有网络实例在指定参数范围内，视为“合规”；非运行中的ECS实例，视为“合规”。
ECS预付费实例到期检查	ECS预付费实例到期时间距离检查时间大于设置的天数，视为“合规”。
为自动快照策略设置合理的创建时间点	自动快照策略中设置的快照创建时间点在参数指定的时间点范围内，视为“合规”。
ECS实例规格符合标准要求	检查ECS实例的规格存在于您设置的阈值中，视为“合规”。
使用专有网络服务的Elasticsearch实例	如果指定参数，则检查Elasticsearch实例关联的专有网络在指定参数范围内视为“合规”；如果未指定参数，则检查Easticsearch实例的网络类型为专有网络，视为“合规”。

规则名称	规则描述
运行中的ECS实例安装了云监控插件	运行中的ECS实例已安装云监控插件，视为“合规”；非运行中的ECS实例不适用本规则，视为“不适用”。
ECS磁盘设置自动快照策略	ECS磁盘设置了自动快照策略，视为“合规”。
Elasticsearch实例未开启公网访问	Elasticsearch实例未开启公网访问，视为“合规”。
为域名设置CDN缓存	为域名设置了CDN缓存和过期时间，视为“合规”。

2.账号组

2.1. 概述

本文介绍账号组的概念、应用场景、使用限制，以及资源目录和账号组中成员账号变更对配置审计的影响。

概念

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。

应用场景

企业管理账号可以将资源目录中的所有或部分成员账号加入到同一个账号组中。账号组作为一个跨账号合规管理的管理单元，对云上多个业务和阿里云账号的企业用户实现了集中地合规管理和数据采集。

账号组的具体应用场景如下：

- 跨账号查看全局资源。企业管理账号可以查看账号组内所有成员账号的资源，还可以在资源列表筛选或搜索目标资源，并查看资源的详情和配置时间线。
- 跨账号设置合规基线。企业管理账号可以在账号组中新建规则和合规包。这些规则和合规包对账号组内所有成员账号的资源生效，且成员账号不能对其执行修改和删除操作，实现企业管理账号对多个成员账号强制设置统一的合规基线。
- 跨账号查看合规视图。企业管理账号可以查看每个成员账号中某条规则对资源的合规检查结果，也可以查看某条规则对多个成员账号中所有资源的合规检查结果，便于对多业务、多账号进行集中合规管理。
- 跨账号收集资源数据。新建账号组之后，企业管理账号同时接管了成员账号的部分配置审计权限。企业管理账号可以设置统一的数据投递，将所有成员账号的资源配置历史数据投递到企业统一用于存储IT配置数据的企业管理账号或成员账号中，作为企业全局的数据管理中心。
- 跨账号发送资源事件。企业管理账号可以设置将所有成员账号中的资源变更和资源不合规事件统一发送到消息服务MNS的主题中。

> **说明** 如果您使用过企业版配置审计，则在账号组中默认出现一个包含资源目录中所有成员账号的账号组，且已有规则仍然有效。

使用限制

账号组的使用限制如下：

- 目前仅允许资源目录中的企业管理账号新建账号组。新建的账号组中可以包括资源目录中的所有成员账号或部分成员账号。
- 每个企业管理账号最多新建5个账号组，每个账号组中最多包含200个成员账号。

资源目录中成员账号变更对配置审计的影响

资源目录中成员账号变更，对配置审计的影响如下表所示。

操作	说明
新加入成员账号	• 配置审计中的全局账号组感知该变更。资源目录中新加入的成员账号自动加入到全局账号组。 • 配置审计中的自定义账号组不感知该变更。资源目录中新加入的成员账号不会自动加入到自定义账号组，需要企业管理账号手动添加。
修改成员账号归属的资源夹	配置审计不感知该变更。针对该变更配置审计不做任何处理。
移除成员账号	配置审计感知该变更。当您将某个成员账号移除资源目录时，企业管理账号失去对该成员账号的管理权限，该成员账号自动从所有账号组移除。

成员账号被加入账号组前后和被移除账号组的功能变化

成员账号被加入账号组前后和被移除账号组的功能变化，如下表所示。

分类	说明
未被加入任何账号组	作为独立阿里云账号使用配置审计。
被加入某个账号组	• 如果成员账号未新建配置审计服务关联角色，则会自动新建。 • 成员账号已有的规则和合规包会被保留。 • 成员账号已设置的资源投递和资源事件通知自动被清空且剥夺设置权限，只能遵从企业管理账号的设置。 • 成员账号在**概览**、**资源**、**合规包**和**规则**菜单，看到**当前账号**和归属账号组页签。成员账号可以查看自己的资源，以及企业管理账号在账号组内新建的规则和合规包。成员账号不能修改规则和合规包，且查看规则与合规包详情时，只能看到自己的资源。 • 账号组中已有的规则和合规包自动对成员账号生效。
被移除某个账号组	• 成员账号在**概览**、**资源**、**合规包**和**规则**菜单，不再看到**当前账号**和曾经归属的账号组页签。 • 账号组中已有的规则和合规包对成员账号失效。 • 成员账号的配置审计服务关联角色被保留。 • 成员账号自己新建的规则和合规包被保留。 • 资源投递和资源事件通知的历史配置自动被清空，成员账号重新获得设置资源投递和资源事件通知的权限。 • 成员账号作为独立的阿里云账号使用配置审计服务，不受原有企业管理账号的管理。

2.2. 管理委派管理员账号

资源目录的企业管理账号可以将资源目录中的成员账号设置为配置审计的委派管理员账号。设置成功后，委派管理员账号将获得企业管理账号的授权，代替企业管理账号管理账号组、查看账号组内成员账号的资源、管理账号组内的合规包和规则，并设置资源数据投递。

前提条件

- 您必须使用企业管理账号登录。

- 请确保您已开通资源目录。具体操作，请参见开通资源目录。
- 请确保您已在资源目录中创建成员或邀请成员。具体操作，请参见创建成员和邀请阿里云账号加入资源目录。

背景信息

关于委派管理员账号的更多信息，请参见什么是委派管理员账号。

应用场景

为配置审计添加委派管理员账号，可以将企业内的组织管理职能和审计管理职能从IT架构上隔离开，这对于企业云上IT的安全管理至关重要。

企业管理账号作为企业的中心管理者默认具有超级管理员权限，在企业IT管理的最佳实践中应使企业管理账号聚焦在对资源目录的组织管理上，尽量减少对其他云上配置的管理职责，避免超大权限的误操作。但是当企业在云上使用多账号时，需要有一些面向整个资源目录的操作，此时就需要企业管理账号能够通过委派管理员账号来分担职责。例如：企业管理账号指定某个成员账号作为配置审计的委派管理员账号，该账号被企业内审计部门所拥有和使用，审计部门通过该账号来统一审计资源的合规性和设置资源数据投递。

添加委派管理员账号

企业可以在资源目录中指定一个成员账号作为专职的审计账号，即配置审计的委派管理员账号。配置审计的委派管理员账号将获得企业管理账号对配置审计的所有操作权限，且与企业管理账号共同管理账号组、查看账号组内成员账号的资源、管理账号组内的合规包和规则，并设置资源数据投递。

您可以使用企业管理员账号在资源管理控制台添加委派管理员账号。具体操作，请参见添加委派管理员账号。

> **说明** 企业管理账号只能为配置审计添加一个委派管理员账号。

更换委派管理员账号

当您为配置审计添加委派管理员账号后，不建议更换该账号。如果您必须更换委派管理员账号，请先移除原有委派管理员账号（账号A），然后添加新的委派管理员账号（账号B）。

1. 在资源管理控制台，使用企业管理账号在资源目录中移除配置审计原有委派管理员账号（账号A）。

   具体操作，请参见移除委派管理员账号。

   > **说明** 仅移除原有委派管理员账号（账号A）对配置审计的管理权限，该账号的所有配置保留。

2. 在资源管理控制台，添加新的委派管理员账号（账号B）。

   具体操作，请参见添加委派管理员账号。

   > **说明** 新的委派管理员账号（账号B）继承原有委派管理员账号（账号A）的所有配置。

3. 在配置审计控制台，新的委派管理员账号（账号B）可以在原有委派管理员账号（账号A）的基础上继续管理账号组、查看账号组内成员账号的资源、管理账号组内的合规包和规则，并设置资源数据投递。
   - 关于如何管理账号组，请参见管理账号组。
   - 关于如何设置资源数据投递，请参见设置资源数据投递。

2.3. 新建账号组

资源目录中的企业管理账号或委派管理员账号可以在配置审计控制台新建账号组，在账号组中集中地管理多个成员账号的资源、合规包和规则。建议您将需要遵从统一合规基线的成员账号添加到同一账号组，便于后续统一在账号组内新建一致的合规包和规则。

前提条件

您必须使用企业管理账号或委派管理员账号登录。

背景信息

您新建账号组之后，配置审计变化如下：

- 配置审计自动在**概览**、**资源**、**合规包**和**规则**菜单分别增加一个账号组页签。如果您新建多个账号组，则会增加多个账号组页签。多个账号组内可能会包含同一个成员账号，当您在多个账号组内查看同一个成员账号的资源和合规结果时，查看到的资源相同，查看到的合规结果可能因账号组内规则的不同而不同。
- 配置审计自动为每个账号组内的成员账号新建配置审计服务关联角色，该角色允许配置审计获取成员账号内资源的配置信息。
- 配置审计自动为每个成员账号构建资源列表，大约需要2~10分钟时间，请您耐心等待。

配置审计支持的账号组类型如下表所示。

账号组类型	说明
全局账号组	全局账号组包含的成员账号将自动与资源目录保持一致。企业管理账号或委派管理员账号选中全局账号组之后，该账号组会自动感知资源目录中成员账号的新增，并自动同步加入到该全局账号组中，确保合规管理的账号范围始终与资源目录保持一致。 每个企业管理账号或委派管理员账号只能新建一个全局账号组。
自定义账号组	企业管理账号或委派管理员账号新建自定义账号组时，主动从资源目录中选择所有或部分成员账号。当资源目录中新增成员账号时，自定义账号组并不会自动同步，需要企业管理账号或委派管理员账号手动将新增的成员账号加入到自定义账号组中。 当企业管理账号或委派管理员账号从资源目录中移除成员账号时，企业管理账号或委派管理员账号无权对该成员账号进行合规管理，自定义账号组自动感知该变化，并将该成员账号从自定义账号组中移除。 如果企业管理账号或委派管理员账号未选中全局账号组，则配置审计默认为自定义账号组，即使新建账号组时选择了资源目录中的所有成员账号，仍然是自定义账号组。

新建全局账号组

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**账号组**。
3. 在**账号组**页面，单击**新建账号组**。
4. 在**新建账号组**页面，先设置账号组名称和描述，再选择**账号组类型**为**全局**。
5. 单击**提交**。

   在**账号组**列表中，目标账号组的状态为**创建完成**，说明新建账号组成功。您还可以查看目标账号组的名称、描述、成员账号数量、账号组类型和创建时间。

新建自定义账号组

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**账号组**。
3. 在**账号组**页面，单击**新建账号组**。
4. 在**新建账号组**页面，先设置账号组名称和描述，再单击**添加成员**。
5. 在资源目录中选中目标成员账号，单击**确定**。
6. 单击**提交**。

   在**账号组**列表中，目标账号组的状态为**创建完成**，说明新建账号组成功。您还可以查看目标账号组的名称、描述、成员账号数量、账号组类型和创建时间。

2.4. 更新账号组的配置

资源目录中的企业管理账号或委派管理员账号可以修改账号组的名称和描述，也可以添加或移除成员账号。账号组的配置更新后，企业管理账号或委派管理员账号需要手动刷新**概览**、**资源**、**合规包**和**规则**菜单中的目标账号组页签。

前提条件

您必须使用企业管理账号或委派管理员账号登录。

背景信息

> **说明** 只有自定义账号组的配置可以更新，全局账号组的配置不能更新。

企业管理账号或委派管理员账号在账号组中添加或移除成员账号后，对企业管理账号或委派管理员账号，以及成员账号的影响如下表所示。

操作	对企业管理账号或委派管理员账号的影响	对成员账号的影响
添加成员账号	• 企业管理账号或委派管理员账号可以查看该成员账号的资源数据。 • 企业管理账号或委派管理员账号为该账号组新建的规则和合规包，对该成员账号生效。 • 企业管理账号或委派管理员账号设置的资源投递和资源事件通知，对该成员账号生效。	• 如果成员账号未新建配置审计服务关联角色，则会自动新建。 • 成员账号已有的规则和合规包会被保留。 • 成员账号已设置的资源投递和资源事件通知自动被清空且剥夺设置权限，只能遵从企业管理账号或委派管理员账号的设置。 • 成员账号在**概览**、**资源**、**合规包**和**规则**菜单，看到**当前账号**和归属账号组页签。成员账号可以查看自己的资源，以及企业管理账号或委派管理员账号在账号组内新建的规则和合规包。成员账号不能修改规则和合规包，且查看规则与合规包详情时，只能看到自己的资源。 • 账号组中已有的规则和合规包自动对成员账号生效。

操作	对企业管理账号或委派管理员账号的影响	对成员账号的影响
移除成员账号	• 企业管理账号或委派管理员账号无法查看该成员账号的资源数据。 • 企业管理账号或委派管理员账号为该账号组新建的规则和合规包，对该成员账号失效。 • 企业管理账号或委派管理员账号设置的资源投递和资源事件通知，对该成员账号失效。	• 成员账号在**概览**、**资源**、**合规包**和**规则**菜单，不再看到**当前账号**和曾经归属的账号组页签。 • 账号组中已有的规则和合规包对成员账号失效。 • 成员账号的配置审计服务关联角色被保留。 • 成员账号自己新建的规则和合规包被保留。 • 资源投递和资源事件通知的历史配置自动被清空，成员账号重新获得设置资源投递和资源事件通知的权限。 • 成员账号作为独立的阿里云账号使用配置审计服务，不受原有企业管理账号或委派管理员账号的管理。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**账号组**。
3. 在**账号组**页面，单击目标账号组对应**操作**列的**编辑**。
4. 在**编辑账号组**页面，先设置账号组名称和描述，再单击**编辑成员**。
5. 在资源目录中选择目标成员账号，单击**确定**。
   - 添加成员账号：在**资源目录**区域，单击待添加成员账号前面的复选框。在**已选择的账号**区域，显示该成员账号。
   - 移除成员账号：在**已选择的账号**区域，单击待移除成员账号前面的复选框，移除该成员账号。
6. 单击**提交**。

   在**账号组**列表中，查看目标账号组的修改结果。您可以查看目标账号组的名称、描述和成员账号数量。

2.5. 删除账号组

资源目录中的企业管理账号或委派管理员账号可以删除账号组。删除账号组后，企业管理账号或委派管理员账号不能再集中查看该账号组中所有成员账号的资源，企业管理账号或委派管理员账号在该账号组中新建的规则和合规包也将自动被删除，且不能恢复。该账号组中成员账号自己新建的规则和合规包将会被保留。

前提条件

您必须使用企业管理账号或委派管理员账号登录。

背景信息

您删除账号组之后，配置审计变化如下：

- **概览**、**资源**、**合规包**和**规则**菜单的账号组页签自动被删除。
- 账号组中的规则和合规包自动被删除，且不可恢复。
- 账号组中产生的所有合规结果自动被删除，且不可恢复。
- 账号组中成员账号的配置审计服务关联角色被保留。
- 如果某个成员账号所属的账号组均被删除，则该成员账号作为独立的阿里云账号使用配置审计服务。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**账号组**。
3. 在**账号组**页面，单击目标账号组对应**操作**列的**删除**。
4. 在**删除账号组**对话框，单击**确定**。

2.6. 查看账号组内的资源

企业管理账号或委派管理员账号可以查看账号组内所有成员账号跨地域聚合的资源清单，可以通过筛选或搜索功能找到账号组中的指定资源并查看该资源的配置信息。企业管理账号或委派管理员账号还可以快速跳转到自己资源的云服务控制台对资源进行管理，但是不能对成员账号下的资源进行管理。

前提条件

您必须使用企业管理账号或委派管理员账号登录。

背景信息

- 企业管理账号或委派管理员账号可以查看其新建的账号组中任意成员账号的任意资源的配置详情、配置时间线、合规时间线和关联资源。
- 如果企业管理账号或委派管理员账号在多个账号组内添加了同一个成员账号，则在每个账号组的资源列表中都能看到该成员账号的资源。
- 如果企业管理账号或委派管理员账号为多个账号组新建了不同的规则，即使账号组内的成员账号和资源都相同的，每个资源在不同账号组中的合规性、关联的规则和合规时间线都不同。

查看资源列表

具体操作，请参见查看资源列表。

查看资源详情

具体操作，请参见查看资源信息。

查看资源配置时间线

具体操作，请参见查看资源配置时间线。

查看资源合规时间线

具体操作，请参见查看资源合规时间线。

2.7. 管理账号组内的合规包

在账号组中新建的合规包属于该账号组，对该账号组内的所有成员账号的资源生效。

前提条件

您必须使用企业管理账号或委派管理员账号登录。

背景信息

在账号组内查看合规包详情时，可以从规则维度和账号维度查看资源的合规状态；在单账号内查看合规包详情时，只能从规则维度查看资源的合规状态。

启用合规包

具体操作，请参见启用合规包。

修改合规包

具体操作，请参见修改合规包。

删除合规包

具体操作，请参见删除合规包。

查看合规包的合规检查结果

具体操作，请参见查看合规包的合规检查结果。

下载合规检查报告

具体操作，请参见下载合规包的合规检查报告。

2.8. 管理账号组内的规则

在账号组中新建的规则属于该账号组，对该账号组内所有成员账号的资源生效。

前提条件

您必须使用企业管理账号或委派管理员账号登录。

背景信息

单账号和账号组均支持托管规则及其自动修正。

新建规则

具体操作，请参见使用托管规则新建规则。

修改规则

具体操作，请参见修改规则。

停用规则

具体操作，请参见停用规则。

删除规则

具体操作，请参见删除规则。

手动执行规则

具体操作，请参见手动执行审计。

3.操作审计

3.1. 查看操作事件详情

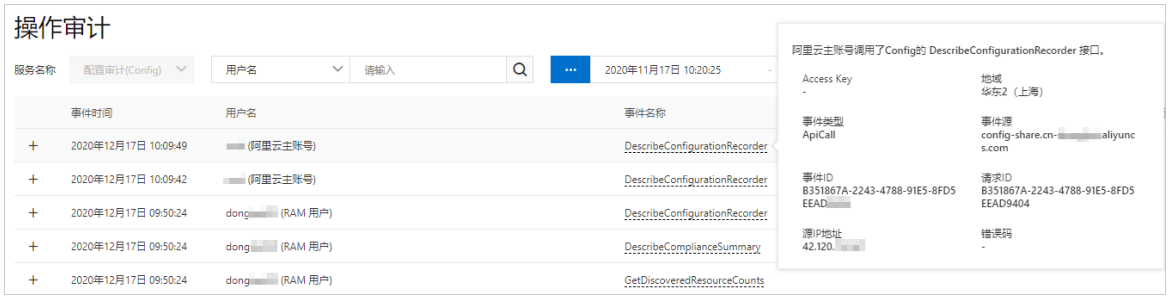
您可以查看当前阿里云账号及其所有RAM用户最近90天在配置审计服务中进行的管控操作，包括访问配置审计控制台和OpenAPI。

背景信息

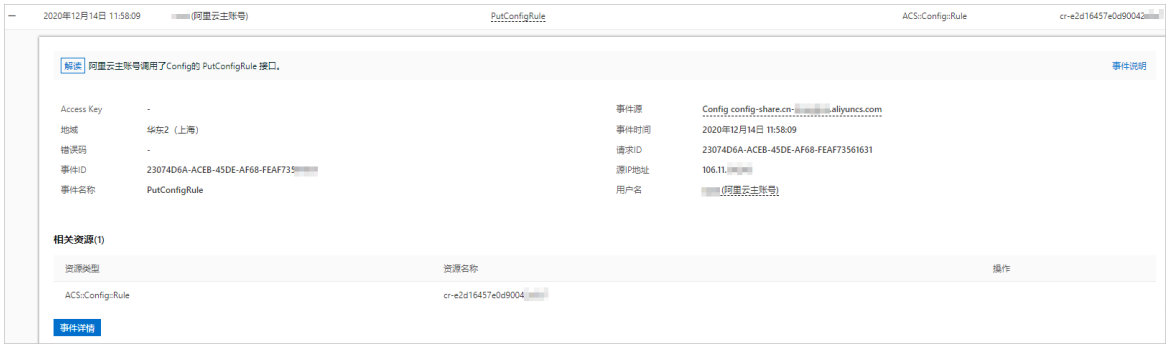
- 操作事件的参数含义，请参见操作事件结构定义。
- 配置审计支持的API接口，请参见API概览。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**操作审计**。
3. 在**操作审计**页面，通过筛选过滤出目标事件。
4. 鼠标悬停至目标事件的**事件名称**，查看该事件的详细信息。



5. 如果您需要查看操作事件的相关资源和代码记录，单击目标事件前面的+图标。



3.2. 操作事件结构定义

本文为您介绍一个操作事件包含的关键字段及其含义，并为您提供相关的示例。

操作事件的关键字段

名称	类型	是否非空	示例	描述
acsRegion	String	是	cn-hangzhou	阿里云地域。

名称	类型	是否非空	示例	描述
apiVersion	String	否	2014-05-26	当eventType取值为*ApiCall*时，操作事件代表一个API的调用。此时，该字段为API的版本信息。
eventId	String	是	F23A3DD5-7842-4EF9-9DA1-3776396A****	事件ID。操作审计为每个操作事件所产生的一个GUID。
eventName	String	是	CreateNetworkInterface	事件名称。 • 如果eventType取值为*ApiCall*，该字段为API的名称。 • 如果eventType取值不为*ApiCall*，该字段为简单的英文短句，表示事件含义。
eventSource	String	是	ecs.aliyuncs.com	事件来源。
eventTime	String	是	2020-01-09T12:12:14Z	事件的发生时间（UTC格式）。
eventType	String	是	ApiCall	发生的事件类型。取值： • *ApiCall*：OpenAPI调用事件。大多阿里云控制台基于OpenAPI开发，对应的操作行为也会记录为ApiCall。 • *ConsoleOperation（ConsoleCall）*：部分控制台或售卖页的操作事件。由于这些控制台或售卖页并不是基于OpenAPI来开发的，因此操作审计会将此类事件类型记录为ConsoleOperation或ConsoleCall。此类事件的名称并不一定是API名称，但能够传达基本操作行为的含义。 • *AliyunServiceEvent*：此类事件为阿里云平台对您的资源执行的操作事件，目前主要是预付费实例的到期自动释放事件。 • *PasswordReset*：密码重置事件。 • *ConsoleSignin*：控制台登录事件。 • *ConsoleSignout*：控制台登出事件。
eventVersion	String	是	1	操作事件格式的版本，当前版本为1。
errorCode	String	否	NoPermission	云服务处理API请求发生错误时，记录的错误码。·
errorMessage	String	否	You are not authorized.	云服务处理API请求发生错误时，记录的错误消息。

名称	类型	是否非空	示例	描述
requestId	String	是	F23A3DD5-7842-4EF9-9DA1-3776396AD58D	请求ID。
requestParameters	字典	否	不涉及	API请求的输入参数。
responseElements	字典	否	不涉及	API响应的数据。
referencedResources	字典	否	不涉及	事件影响的资源列表。
serviceName	String	是	Ecs	事件相关的云服务名称。
sourceIpAddress	String	是	11.168.XX.XX	事件发起的源IP地址。
userAgent	String	是	Apache-HttpClient/4.5.7 (Java/1.8.0_152)	发送API请求的客户端代理标识。取值示例： • *AlibabaCloud (Linux 3.10.0-693.2.2.el7.x86_64;x86_64) Python/2.7.5 Core/2.13.16 python-requests/2.18.3*。 • *Apache-HttpClient/4.5.7 (Java/1.8.0_152)*。
userIdentity	字典	是	不涉及	请求者的身份信息。

userIdentity包含的字段如下表所示。

名称	类型	是否非空	示例	描述
type	String	是	ram-user	身份类型。当前支持的身份类型包括： • *root-account*：阿里云账号。 • *ram-user*：RAM用户。 • *assumed-role*：RAM角色。 • *system*：阿里云服务。
principalId	String	是	28815334868278****	当前请求者的ID。 • 如果type取值为*root-account*，则记录阿里云主账号ID。 • 如果type取值为*ram-user*，则记录RAM用户ID。 • 如果type取值为*assumed-role*，则记录RoleID:RoleSessionName。

名称	类型	是否非空	示例	描述
accountId	String	是	112233445566****	阿里云账号ID。
accessKeyId	String	否	55nCtAwmPLkk****	• 如果请求者通过SDK访问API，则记录该字段。 • 如果请求者通过控制台登录，则该字段不显示。
userName	String	否	B**	• 如果type取值为*ram-user*，则记录RAM用户名。 • 如果type取值为assumed-role，则记录RoleName:RoleSessionName。
sessionContext	String	否	{"attributes": {"mfaAuthenticated": "true", "creationDate": "2015-12-31T06:33:14Z" }	请求者通过临时安全令牌调用API或通过控制台登录时记录该字段。该字段的内容包括： • `creationDate`：创建时间。 • `mfaAuthenticated`：用户登录控制台时是否使用多因素认证。

示例

```
{
  "eventId": "F23A3DD5-7842-4EF9-9DA1-3776396A****",
  "responseElements": {
    "RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
    "NetworkInterfaceId": "eni-bp12f9rjbjqauktz****"
  },
  "eventVersion": "1",
  "requestParameters": {
    "Tag.1.Key": "CreatedBy",
    "RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
    "SecurityGroupId": "sg-bp10mvd8143rlfks****",
    "Tag.1.Value": "StreamCompute",
    "VSwitchId": "vsw-bp1iqqmaj41noh2c8****",
    "RegionId": "cn-hangzhou",
    "SignatureType": "",
    "stsTokenPlayerUid": 165266556947****
  },
  "eventSource": "ecs.aliyuncs.com",
  "sourceIpAddress": "11.168.XX.XX",
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-01-09T12:12:14Z"
      }
    },
    "accessKeyId": "STS.NUnj6nuqKaEoMZGsT****",
    "accountId": "116214825062****",
    "principalId": "31645666448606****:116214825062****",
    "userName": "aliyunstreamdefaultrole:116214825062****",
    "type": "assumed-role"
  },
  "eventType": "ApiCall",
  "referencedResources": {
    "VSwitch": [
      "vsw-bp1iqqma1noh402c8****"
    ],
    "SecurityGroup": [
      "sg-bp10mvd143r6lfks****"
    ]
  },
  "serviceName": "Ecs",
  "additionalEventData": {
    "Scheme": "http"
  },
  "apiVersion": "2014-05-26",
  "requestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
  "eventTime": "2020-01-09T12:12:14Z",
  "acsRegion": "cn-hangzhou",
  "eventName": "CreateNetworkInterface",
  "__expanded": true
}
```

3.3. 配置审计支持被审计的事件说明

配置审计已与操作审计服务集成，您可以在操作审计中查询用户操作配置审计产生的管控事件。操作审计支持将管控事件投递到日志服务SLS的日志库（LogStore）或对象存储OSS的存储空间（Bucket）中，满足实时审计、问题回溯分析等需求。

操作审计记录了用户通过OpenAPI或控制台等方式操作云资源时产生的管控事件，配置审计支持在操作审计中查询的事件如下表所示。

OpenAPI名称	描述
ActiveAggregateConfigRules	启用账号组内的规则。
ActiveConfigRules	批量启用指定规则。
AttachAggregateConfigRuleToCompliancePack	将账号组内的规则加入合规包。
AttachConfigRuleToCompliancePack	将规则加入合规包。
CheckServiceLinkedRoleForDeleting	检查服务角色是否可删除。
CopyCompliancePacks	复制合规包。
CopyConfigRules	复制规则。
CreateAdvancedSearchFile	生成搜索结果，并下载文件。
CreateAggregateAdvancedSearchFile	账号组生成搜索结果，并下载文件。
CreateAggregateCompliancePack	为账号组创建合规包。
CreateAggregateConfigDeliveryChannel	为账号组创建投递渠道。
CreateAggregateConfigRule	为账号组创建规则。
CreateAggregateRemediation	为账号组创建修正设置。
CreateAggregator	创建账号组。
CreateCompliancePack	创建合规包。
CreateConfigDeliveryChannel	创建投递渠道。
CreateConfigRule	创建规则。
CreateDeliveryChannel	创建投递渠道。
CreateRemediation	创建修正设置。
DeactiveAggregateConfigRules	停用账号组内的规则。
DeactiveConfigRules	停用规则。
DeleteAggregateCompliancePacks	删除账号组内的合规包。

OpenAPI名称	描述
DeleteAggregateConfigDeliveryChannel	删除账号组内的投递渠道。
DeleteAggregateConfigRules	删除规则。
DeleteAggregateRemediations	删除账号组内的修正设置。
DeleteAggregators	删除账号组。
DeleteCompliancePacks	删除合规包。
DeleteConfigDeliveryChannel	删除投递渠道。
DeleteConfigRules	批量删除规则。
DeleteRemediations	删除修正设置。
DescribeCompliance	查询资源的合规结果。
DescribeComplianceHistory	查询资源的合规时间线。
DescribeComplianceReport	查询资源的合规报告详情。
DescribeComplianceSummary	查询资源的合规结果统计概要。
DescribeConfigRule	查询规则详情。
DescribeConfigurationRecorder	查询资源的监控范围。
DescribeDeliveryChannels	查询投递渠道信息。
DescribeDiscoveredResource	查询资源配置详情。
DescribeDiscoveredResourceBatch	批量获取资源详情。
DescribeEvaluationResults	查询规则评估结果。
DescribeIntegratedServiceStatus	查询集成云服务的授权状态。
DescribeProductComplianceSummary	查询云服务合规结果统计概要。
DescribeRemediation	查询修正设置。
DetachAggregateConfigRuleToCompliancePack	将账号组内的规则从合规包中移出。
DetachConfigRuleToCompliancePack	将规则从合规包中移出。
GenerateAggregateCompliancePackReport	为账号组内的合规包生成评估报告。
GenerateAggregateConfigRulesReport	为账号组内规则列表中的所有规则生成评估报告。
GenerateAggregateResourceInventory	为账号组生成资源清单。

OpenAPI名称	描述
GenerateCompliancePackReport	生成合规包评估报告。
GenerateConfigRulesReport	生成规则列表评估报告。
GenerateResourceInventory	获取资源清单报告。
GetAdvancedSearchFile	查询搜索结果，并下载文件。
GetAggregateAccountComplianceByPack	查询账号组内合规包中成员的合规结果。
GetAggregateCompliancePack	查询账号组内的合规包详情。
GetAggregateCompliancePackReport	查询账号组内的合规包评估报告。
GetAggregateConfigDeliveryChannel	查询账号组内的投递渠道信息。
GetAggregateConfigRule	查询账号组内的规则详情。
GetAggregateConfigRuleComplianceByPack	查询账号组内合规包规规则的合规结果。
GetAggregateConfigRulesReport	查询账号组内规则列表的评估报告。
GetAggregateConfigRuleSummaryByRiskLevel	查询账号组内规则风险等级的合规概要。
GetAggregateDiscoveredResource	查询账号组内的资源详情。
GetAggregateResourceComplianceByConfigRule	查询账号组内规则的评估结果。
GetAggregateResourceComplianceByPack	查询账号组内合规包的资源合规统计。
GetAggregateResourceComplianceGroupByRegion	查询账号组内规则的地域合规统计。
GetAggregateResourceComplianceGroupByResourceType	查询账号组内规则的资源合规统计。
GetAggregateResourceComplianceTimeline	查询账号组内资源合规时间线。
GetAggregateResourceConfigurationTimeline	查询账号组内资源配置时间线。
GetAggregateResourceCountsGroupByRegion	从地域维度查询账号组内资源的统计结果。
GetAggregateResourceCountsGroupByResourceType	从资源类型维度查询账号组内资源的统计结果。
GetAggregateResourceInventory	查询账号组内资源清单报告。
GetAggregator	查询账号组详情。
GetCompliancePack	查询合规包详情。
GetCompliancePackReport	查询合规包评估报告。
GetConfigDeliveryChannel	查询投递渠道。

OpenAPI名称	描述
GetConfigRule	查询规则详情。
GetConfigRuleComplianceByPack	查询合规包中规则维度的合规统计。
GetConfigRulesReport	查询规则列表评估报告。
GetConfigRuleSummaryByRiskLevel	查询规则风险等级维度的合规概要。
GetDiscoveredResource	查询资源详情。
GetDiscoveredResourceCounts	查询资源数量。
GetDiscoveredResourceCountsGroupByRegion	查询资源的地域维度的统计结果。
GetDiscoveredResourceCountsGroupByResourceType	查询资源的资源类型维度的统计结果。
GetDiscoveredResourceSummary	查询监控中的资源概览。
GetManagedRule	查询托管规则详情。
GetResourceComplianceByConfigRule	查询规则的资源合规统计。
GetResourceComplianceByPack	查询合规包的资源合规结果。
GetResourceComplianceGroupByRegion	从地域维度查询资源的合规统计。
GetResourceComplianceGroupByResourceType	从资源类型维度查询资源的合规统计。
GetResourceComplianceTimeline	查询资源合规时间线。
GetResourceConfigHistory	查询资源配置历史记录。
GetResourceConfigurationTimeline	查询资源配置时间线。
GetResourceInventory	查询资源清单报告信息。
GetServiceQuota	查询服务配额。
GetSupportedResourceTypes	查询配置审计支持的资源类型列表。
GetSupportedResourceTypesForSpec	查询配置审计支持的资源类型列表。
GetSupportedResourceTypesInfo	查询配置审计支持的资源类型核心配置信息。
IgnoreAggregateEvaluationResults	忽略账号组内规则的评估结果。
IgnoreEvaluationResults	忽略规则评估结果。
ListAggregateCompliancePacks	查询账号组内的合规包列表。
ListAggregateConfigDeliveryChannels	查询账号组内的投递渠道列表。

OpenAPI名称	描述
ListAggregateConfigRuleEvaluationResults	查询账号组内规则的评估结果列表。
ListAggregateConfigRules	查询账号组内的规则列表。
ListAggregateDiscoveredResourceRelations	查询账号组内的资源关系列表。
ListAggregateDiscoveredResources	查询账号组内的资源列表。
ListAggregateDiscoveredResourcesByAdvancedSearch	搜索账号组内的资源列表。
ListAggregateRemediations	查询账号组内的所有修正设置列表。
ListAggregateResourceEvaluationResults	查询账号组内规则的评估结果列表。
ListAggregators	查询账号组列表。
ListCadtAppResource	查询应用架构下关联的资源列表。
ListCompliancePacks	查询合规包列表。
ListCompliancePackTemplates	查询合规包模板。
ListConfigDeliveryChannels	查询投递渠道列表。
ListConfigRuleEvaluationResults	查询资源评估列表。
ListConfigRules	查询规则列表。
ListDiscoveredResourceRelations	查询资源关系列表。
ListDiscoveredResourceRelationsBatch	批量查询资源关系列表。
ListDiscoveredResources	查询资源列表信息。
ListDiscoveredResourcesByAdvancedSearch	搜索资源列表。
ListIntegratedService	查询授权与配置审计集成的云服务。
ListManagedRules	查询托管规则列表。
ListRemediations	查询修正设置列表。
ListRemediationTemplates	查询修正模板列表。
ListResourceEvaluationResults	查询资源评估结果。
ListResourceOwnerInAllAggregator	查询账号组内的成员信息。
ListServiceQuotas	查询服务配额列表。
ListSupportedProducts	查询配置审计支持的云服务列表。

OpenAPI名称	描述
ListTagResources	获取资源的标签列表。
PutConfigRule	新建或修改规则。
PutConfigurationRecorder	修改监控中的资源类型。
PutDeliveryChannel	创建或更新投递渠道。
PutEvaluations	提交评估结果。
RevertAggregateEvaluationResults	恢复已忽略的账号组内的评估结果。
RevertEvaluationResults	恢复已忽略的评估结果。
StartAggregateConfigRuleEvaluation	手动执行账号组内的规则。
StartAggregateRemediation	手动执行账号组内规则的修正设置。
StartConfigRuleEvaluation	启用规则。
StartConfigurationRecorder	设置资源监控范围。
StartRemediation	手动执行修正设置。
StopConfigRules	批量停用指定规则。
StopConfigurationRecorder	停用配置审计服务。
TagResources	为指定资源绑定标签。
UntagResources	为指定资源删除标签。
UpdateAggregateCompliancePack	更新账号组内的合规包信息。
UpdateAggregateConfigDeliveryChannel	更新账号组内的投递渠道信息。
UpdateAggregateConfigRule	更新账号组内的规则。
UpdateAggregateRemediation	更新修正设置。
UpdateAggregator	更新账号组。
UpdateCompliancePack	更新合规包信息。
UpdateConfigDeliveryChannel	更新投递渠道信息。
UpdateConfigRule	更新规则。
UpdateDeliveryChannel	更新投递渠道信息。
UpdateIntegratedServiceStatus	更新云服务集成用户状态。

OpenAPI名称	描述
UpdateRemediation	更新修正设置。

4.投递服务

4.1. 概述

配置审计持续且自动为您评估云上IT资源的合规性，您可以设置将资源数据投递到对应云服务，便于您对资源数据执行相关操作。

计费说明

配置审计的投递服务不收费，当资源数据投递到对应云服务时，该云服务需要收费。计费标准如下：

- 关于日志服务SLS如何计费，请参见日志服务SLS计费说明。
- 关于对象存储OSS的存储空间如何计费，请参见对象存储OSS计费说明。
- 关于消息服务MNS的主题如何计费，请参见消息服务MNS计费说明。

应用场景

投递服务的具体应用场景如下：

- 查询和分析资源数据。

  您可以设置将资源的配置变更历史或不合规事件投递到日志服务SLS的指定日志库。
- 查看和下载JSON格式的资源数据。

  您可以设置将资源的定时快照或配置变更历史投递到对象存储OSS的指定存储空间。
- 发送资源事件。

  您可以设置将资源配置变更历史和资源不合规事件投递到消息服务MNS的指定主题。

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

4.2. 投递到日志服务SLS

4.2.1. 设置投递数据到日志服务SLS

当您需要将资源的配置变更历史和不合规事件投递到日志服务SLS的指定日志库时，需要设置日志项目（Project）和日志库（Logstore）。资源数据投递到指定日志库后，您可以查询和分析日志。

前提条件

请确保您已开通日志服务SLS。当您首次使用日志服务时，需要登录日志服务控制台，根据页面提示开通日

志服务。更多信息，请参见什么是日志服务。

普通账号

普通账号可以设置将自己的资源数据投递到日志服务SLS的指定日志库中。

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**投递服务 > 投递到日志服务SLS**。
3. 在**投递到日志服务SLS**页面，打开**设置日志服务SLS**开关。
4. 设置资源投递数据的相关参数。

   资源投递数据的相关参数如下表所示。

参数	描述
选择接收内容	选择日志服务SLS接收的资源投递内容。取值： ○ **配置变更历史**：当资源配置变更时，配置审计向日志服务SLS投递资源配置变更历史。 ○ **资源不合规事件**：当资源的审计结果不合规时，配置审计向日志服务SLS投递资源不合规事件。
日志项目地域	日志项目所在地域。
日志项目名称	日志服务SLS中日志项目的名称。同一账号同一地域下，日志项目名称不能重复。 ○ 当您选中**本账号中新建日志项目**时，通过配置审计控制台新建日志项目，输入日志项目名称。 ○ 当您选中**选择本账号中已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。
日志库名称	日志服务SLS中日志库的名称。同一账号同一地域下，日志库名称不能重复。 ○ 当您选中**本账号中新建日志项目**时，通过配置审计控制台新建日志库，输入日志库名称。 ○ 当您选中**选择本账号中已有的日志项目**时，在日志服务SLS中选择已有日志库名称。
超大文件接收地址	配置审计向日志服务SLS投递的超大文件接收地址。 ○ 如果您设置了该参数，当配置审计向日志服务SLS投递的文件超过1 MB时，该文件自动转存到对象存储OSS的目标存储空间。 ○ 如果您未设置该参数，当配置审计向日志服务SLS投递的文件超过1 MB时，超过部分自动丢弃。 **说明** 超大文件接收地址中的**地域**和**账号**根据**接收内容和接收地址**区域设置的参数自动生成，您只需选择目标存储空间。

5. 单击**确定**。

企业管理账号

企业管理账号可以设置将自己和资源目录中所有成员账号的资源投递数据，统一投递到企业管理账号或指定成员账号的日志库中。成员账号无权设置资源数据投递，只能按照企业管理账号的设置进行投递。

> **说明** 如果企业管理账号设置了配置审计的委派管理员账号，该账号可代替企业管理账号设置资源数据投递。关于如何添加配置审计的委派管理员账号，请参见添加委派管理员账号。

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**投递服务 > 投递到日志服务SLS**。
3. 在**投递到日志服务SLS**页面，打开**设置日志服务SLS**开关。
4. 设置资源事件投递的相关参数。

   您可以在当前企业管理账号中新建日志项目，也可以选择当前企业管理账号或其他成员账号中已有日志项目。该日志项目用于接收企业管理账号和所有成员账号的资源投递数据。

   - 当您需要将企业管理账号和所有成员账号的资源日志统一投递到当前企业管理账号的指定日志项目时，需要选择**本账号中新建日志项目**或**选择本账号中已有的日志项目**。资源投递数据的相关参数如下表所示。

参数	描述
选择接收内容	选择日志服务SLS接收的资源投递内容。取值： ■ **配置变更历史**：当资源配置变更时，配置审计向日志服务SLS投递资源配置变更历史。 ■ **资源不合规事件**：当资源的审计结果不合规时，配置审计向日志服务SLS投递资源不合规事件。
日志项目地域	日志项目所在地域。
日志项目名称	日志服务SLS中日志项目的名称。同一账号同一地域下，日志项目名称不能重复。 ■ 当您选中**本账号中新建日志项目**时，通过配置审计控制台新建日志项目，输入日志项目名称。 ■ 当您选中**选择本账号中已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。
日志库名称	日志服务SLS中日志库的名称。同一账号同一地域下，日志库名称不能重复。 ■ 当您选中**本账号中新建日志项目**时，通过配置审计控制台新建日志库，输入日志库名称。 ■ 当您选中**选择本账号中已有的日志项目**时，在日志服务SLS中选择已有日志库名称。
超大文件接收地址	配置审计向日志服务SLS投递的超大文件接收地址。 ■ 如果您设置了该参数，当配置审计向日志服务SLS投递的文件超过1 MB时，该文件自动转存到对象存储OSS的目标存储空间。 ■ 如果您未设置该参数，当配置审计向日志服务SLS投递的文件超过1 MB时，超过部分自动丢弃。 **说明** 超大文件接收地址中的**地域**和**账号**根据**接收内容和接收地址**区域设置的参数自动生成，您只需选择目标存储空间。

- 当您需要将企业管理账号和所有成员账号的资源日志统一投递到指定成员账号的指定日志项目时，需要选择**选择其他账号已有的日志项目（仅支持企业管理账号）**。设置日志项目相关参数之前，请您确保该成员账号中已有可用日志项目。资源投递数据的相关参数如下表所示。

参数	描述
选择接收内容	选择日志服务SLS接收的资源投递内容。取值： ■ **配置变更历史**：当资源配置变更时，配置审计向日志服务SLS投递资源配置变更历史。 ■ **资源不合规事件**：当资源的审计结果不合规时，配置审计向日志服务SLS投递资源不合规事件。
目标账号中日志库的ARN	目标成员账号中日志库的ARN，包括：**地域**、**成员账号**、**日志项目名称**和**日志库名称**。您可以直接从下拉列表中选择目标成员账号，以及该成员账号的日志项目名称、日志库名称和地域。
目标账号中需扮演角色的ARN	目标成员账号需要扮演角色的ARN，包括：成员账号和配置审计服务关联角色。您可以直接从下拉列表中选择目标成员账号，配置审计服务关联角色保持默认。
超大文件接收地址	配置审计向日志服务SLS投递的超大文件接收地址。 ■ 如果您设置了该参数，当配置审计向日志服务SLS投递的文件超过1 MB时，该文件自动转存到对象存储OSS的目标存储空间。 ■ 如果您未设置该参数，当配置审计向日志服务SLS投递的文件超过1 MB时，超过部分自动丢弃。 **说明** 超大文件接收地址中的**地域**和**账号**根据**接收内容和接收地址**区域设置的参数自动生成，您只需选择目标存储空间。

5. 单击**确定**。
6. 在**该修改将自动在所有成员账号中生效，请确认修改**对话框，单击**确定**。

后续步骤

资源日志投递到指定日志库后，您可以在该日志库中查询和分析指定时间段内所有的资源日志。具体操作，请参见查询和分析日志。

关于JSON格式文件的内容示例，请参见资源配置变更历史内容示例和资源不合规事件内容示例。

4.2.2. 资源配置变更历史内容示例

通过本文您可以了解配置审计的资源配置变更历史投递到日志服务SLS的内容示例和主要参数说明。

内容示例

创建资源、修改资源和删除资源的配置变更历史投递到日志服务SLS的内容示例如下：

- 创建资源

普通账号 `110803419679****` 在云服务器ECS的呼和浩特地域创建云盘 `test_disk` ，在 `configurationDiff` 中显示云盘的变更前信息 `null` 和变更后详细信息，
在 `relationship` 和 `relationshipDiff` 中显示云盘新增相关资源 `i-8psdh7l6lphbn10l****` 。

```
accountId:110803419679****
arn:acs:sls:ap-cn-huhehaote:110803419679****:sls_test
availabilityZone:cn-huhehaote-a
captureTime:1642411308000
configAggregators:
configuration:{"DetachedTime":"","Category":"cloud_efficiency","KMSKeyId":"","Description":"","ResourceGroupId":"rg-aekzmdckngg****","Size":40,"Encrypted":false,"DeleteAutoSnapshot":false,"DiskChargeType":"PrePaid","Attachments":{"Attachment":[{"AttachedTime":"2022-01-17T09:20:14Z","InstanceId":"i-8psdh7l6lphbn10l****","Device":"/dev/xvda"}]},"MultiAttach":"Disabled","ExpiredTime":"2022-02-17T16:00Z","ImageId":"win2012r2_9600_x64_dtc_en-us_40G_alibase_20211217.vhd","StorageSetId":"","Tags":{"Tag":[]},"Status":"In_use","AttachedTime":"2022-01-17T09:20:14Z","StorageClusterId":"","ZoneId":"cn-huhehaote-a","InstanceId":"i-8psdh7l6lphbn10l****","ProductCode":"","SourceSnapshotId":"","Device":"/dev/xvda","PerformanceLevel":"","DeleteWithInstance":true,"EnableAutomatedSnapshotPolicy":false,"EnableAutoSnapshot":true,"AutoSnapshotPolicyId":"","DiskName":"","test_disk":"","OperationLocks":{"OperationLock":[]},"Portable":true,"Type":"system","SerialNumber":"8psdh7l6lphbn10i******","CreationTime":"2022-01-17T09:20:10Z","RegionId":"cn-huhehaote","DiskId":"d-8psdh7l6lphbn10i****"}
configurationDiff:{"Category":[null,"cloud_efficiency"],"ResourceGroupId":[null,"rg-aekzmdckngg****"],"Size":[null,40],"Encrypted":[null,false],"DeleteAutoSnapshot":[null,false],"DiskChargeType":[null,"PrePaid"],"Attachments":[null,{"Attachment":[{"AttachedTime":"2022-01-17T09:20:14Z","InstanceId":"i-8psdh7l6lphbn10l****","Device":"/dev/xvda"}]}],"MultiAttach":[null,"Disabled"],"ExpiredTime":[null,"2022-02-17T16:00Z"],"ImageId":[null,"win2012r2_9600_x64_dtc_en-us_40G_alibase_20211217.vhd"],"Tags":[null,{"Tag":[]}],"Status":[null,"In_use"],"AttachedTime":[null,"2022-01-17T09:20:14Z"],"ZoneId":[null,"cn-huhehaote-a"],"InstanceId":[null,"i-8psdh7l6lphbn10l****"],"Device":[null,"/dev/xvda"],"DeleteWithInstance":[null,true],"EnableAutomatedSnapshotPolicy":[null,false],"EnableAutoSnapshot":[null,true],"OperationLocks":[null,{"OperationLock":[]}],"Portable":[null,true],"Type":[null,"system"],"SerialNumber":[null,"8psdh7l6lphbn10i****"],"CreationTime":[null,"2022-01-17T09:20:10Z"],"RegionId":[null,"cn-huhehaote"],"DiskId":[null,"d-8psdh7l6lphbn10i****"]}
dataType:ConfigurationItemChangeNotification
regionId:cn-huhehaote
relationship:[{"regionId":"cn-huhehaote","relationType":"IsAttachedTo","resourceId":"i-8psdh7l6lphbn10l****","resourceType":"ACS::ECS::Instance"}]
relationshipDiff:{"relationship_diff":{"relationship_add":[{"regionId":"cn-huhehaote","relationType":"IsAttachedTo","resourceId":"i-8psdh7l6lphbn10l****","resourceType":"ACS::ECS::Instance"}],"relationship_delete":[]}}
requestId:be30368b-71dd-4367-9871-d00e565f8679
resourceCreateTime:1642411210000
resourceEventType:DISCOVERED
resourceGroupId:rg-aekzmdckngg****
resourceId:d-8psdh7l6lphbn10i****
resourceName:test_disk
resourceStatus:In_use
resourceType:ACS::ECS::Disk
tags:{}
```

- 修改资源

普通账号 `118239008140****` 在云服务器ECS的杭州地域为云盘 `test_disk` 关联标签 `key1` ，在 `configurationDiff` 中显示云盘的标签变更前信息 `null` 和变更后信息 `key1` ，在 `relationship` 和 `relationshipDiff` 中显示云盘删除相关资源 `i-bp1g9rukkdar0dro****` 。

```
accountId:118239008140****
arn:acs:sls:cn-hangzhou:118239008140****:sls_test
availabilityZone:cn-hangzhou-i
captureTime:1630422042000
configAggregators:
configuration:{"DetachedTime":"2022-01-17T09:27:40Z","Category":"cloud_efficiency","KMSKeyId":"","Description":"","ResourceGroupId":"","Size":20,"Encrypted":false,"DeleteAutoSnapshot":true,"DiskChargeType":"PostPaid","MultiAttach":"Disabled","ExpiredTime":"2999-09-08T16:00Z","ImageId":"","StorageSetId":"","Tags":{"Tag":[{"TagKey":"key1","TagValue":""}]},"Status":"Available","AttachedTime":"2022-01-17T09:02:01Z","StorageClusterId":"","ZoneId":"cn-hangzhou-i","InstanceId":"","ProductCode":"","SourceSnapshotId":"","Device":"","PerformanceLevel":"","DeleteWithInstance":false,"EnableAutomatedSnapshotPolicy":false,"EnableAutoSnapshot":true,"AutoSnapshotPolicyId":"","DiskName":"test_disk","BdfId":"","OperationLocks":{"OperationLock":[]},"Portable":true,"Type":"data","SerialNumber":"bp1fybs4hwesp8kv****","CreationTime":"2021-08-19T09:11:48Z","RegionId":"cn-hangzhou","DiskId":"d-bp1fybs4hwesp8kv****"}
configurationDiff:{"Tags":[{"Tag":[]},{"Tag":[{"TagKey":"key1","TagValue":""}]}]}
dataType:ConfigurationItemChangeNotification
regionId:cn-hangzhou
relationship:
relationshipDiff:{"relationship_diff":{"relationship_add":[],"relationship_delete":[{"regionId":"cn-hangzhou","relationType":"IsAttachedTo","resourceId":"i-bp1g9rukkdar0dro****","resourceType":"ACS::ECS::Instance"}]}}
requestId:4f9a90a9-63bf-43bd-981d-bc15658c423e
resourceCreateTime:1630422000000
resourceEventType:MODIFY
resourceGroupId:rg-acfmwvtff2y***
resourceId:d-bp1fybs4hwesp8kv****
resourceName:test_disk
resourceStatus:Available
resourceType:ACS::ECS::Disk
tags:{"key1":[""]}
```

- 删除资源

  普通账号 `120886317861****` 在云服务器ECS的呼和浩特地域删除云盘 `test_disk` ，在 `configurationDiff` 中显示云盘变更前信息和变更后信息 `null` ，在 `relationship` 和 `relationshipDiff` 中显示云盘无相关资源。

```
accountId:120886317861****
arn:acs:ecs:cn-huhehaote:120886317861****:disk/d-hp33mwzuof9qoa22****
availabilityZone:cn-huhehaote-a
captureTime:1629875147000
configAggregators:
configuration:{"DetachedTime":"","Category":"cloud_essd","KMSKeyId":"","Description":"","
ResourceGroupId":"","Size":40,"Encrypted":false,"DeleteAutoSnapshot":false,"DiskChargeTyp
e":"PostPaid","MultiAttach":"Disabled","ExpiredTime":"2999-09-08T16:00Z","ImageId":"","St
orageSetId":"","Tags":{"Tag":[]},"Status":"Available","AttachedTime":"","StorageClusterId
":"","ZoneId":"cn-huhehaote-a","InstanceId":"","ProductCode":"","SourceSnapshotId":"","De
vice":"","PerformanceLevel":"PL1","DeleteWithInstance":false,"EnableAutomatedSnapshotPoli
cy":false,"EnableAutoSnapshot":true,"AutoSnapshotPolicyId":"","DiskName":"test_disk","Bdf
Id":"","OperationLocks":{"OperationLock":[]},"Portable":true,"Type":"data","SerialNumber"
:"hp33mwzuof9qoa22****","CreationTime":"2021-08-25T06:52:35Z","RegionId":"cn-huhehaote","
DiskId":"d-hp33mwzuof9qoa22****"}
configurationDiff:{"Status":["Available",null],"Category":["cloud_essd",null],"ZoneId":["
cn-huhehaote-a",null],"Size":[40,null],"Encrypted":[false,null],"PerformanceLevel":["PL1"
,null],"DeleteAutoSnapshot":[false,null],"DeleteWithInstance":[false,null],"EnableAutomat
edSnapshotPolicy":[false,null],"DiskChargeType":["PostPaid",null],"EnableAutoSnapshot":[t
rue,null],"DiskName":["test_disk",null],"MultiAttach":["Disabled",null],"OperationLocks":
[{"OperationLock":[]},null],"Portable":[true,null],"Type":["data",null],"SerialNumber":["
hp33mwzuof9qoa22ic6q",null],"ExpiredTime":["2999-09-08T16:00Z",null],"CreationTime":["202
1-08-25T06:52:35Z",null],"RegionId":["cn-huhehaote",null],"Tags":[{"Tag":[]},null],"DiskI
d":["d-hp33mwzuof9qoa22****",null]}
dataType:ConfigurationItemChangeNotification
regionId:cn-huhehaote
relationship:
relationshipDiff:{"relationship_diff":{"relationship_add":[],"relationship_delete":[]}}
requestId:d9bca2bc-75ba-4e4c-92dd-7cc38e779806
resourceCreateTime:1629874355000
resourceEventType:REMOVE
resourceGroupId:rg-acfmw3ty5y7****
resourceId:d-hp33mwzuof9qoa22****
resourceName:test_disk
resourceStatus:Available
resourceType:ACS::ECS::Disk
tags:{}
```


参数说明

资源配置变更历史投递到日志服务SLS的主要参数说明如下表所示。

参数	说明
accountId	资源归属的账号ID。配置审计支持如下账号类型： • 普通账号：未被企业管理账号加入资源目录的独立的阿里云账号。 • 企业管理账号：开通资源目录并管理成员账号的阿里云账号。 • 成员账号：资源目录中的成员账号。
arn	资源ARN。关于各云服务资源类型对应的ARN格式，请参见ARN格式。
availabilityZone	资源可用区。

参数	说明
captureTime	配置审计发现资源配置变更并生成日志的时间戳。关于时间戳的转换方法，请参见Unix时间戳。
configAggregators	账号组信息，包括创建账号组的企业管理账号ID和账号组ID。根据资源归属账号类型不同，该参数显示如下： • 当资源归属普通账号时，该参数为空。 • 当资源归属企业管理账号时，该参数为当前企业管理账号创建的账号组信息。 • 当资源归属成员账号时，该参数为成员账号归属的企业管理账号创建的账号组信息。
configuration	资源的详细配置。
configurationDiff	资源配置变更的具体变更项及变更前后信息。
dataType	日志服务SLS的接收内容。取值： • `ConfigurationItemChangeNotification`：资源配置变更历史。 • `NonCompliantNotification`：资源不合规事件。
regionId	资源所在地域ID。
relationship	相关资源的详细信息，包括相关资源所在地域ID、资源关系、资源ID和资源类型。根据资源是否有相关资源，该参数显示如下： • 当资源有相关资源时，该参数为相关资源的详细信息。 关于配置审计支持的资源关系，请参见配置审计支持的资源类型和资源关系。 • 当资源无相关资源时，该参数为空。
relationshipDiff	相关资源的变更项。
resourceCreateTime	创建资源的时间戳。关于时间戳的转换方法，请参见Unix时间戳。
resourceEventType	资源变更事件的类型。取值： • `DISCOVERED`：创建资源事件。 • `MODIFY`：修改资源事件。 • `REMOVE`：删除资源事件。
resourceGroupId	资源归属的资源组ID。根据资源类型是否支持资源组，该参数显示如下： • 当资源类型支持资源组时，该参数为资源组ID。 关于支持资源组的云服务，请参见支持资源组的云服务。 • 当资源类型不支持资源组时，该参数为空。
resourceId	资源ID。
resourceName	资源名称。

参数	说明
resourceStatus	资源状态。资源的状态取决于各云服务对资源的定义，该参数可能为空。例如： • 当资源类型为ACS::ECS::Instance时，由于ECS实例有状态，因此该参数为 `Running` 或 `Stopped` 。 • 当资源类型为ACS::OSS::Bucket时，由于OSS Bucket无状态，因此该参数为空。
resourceType	资源类型。关于支持配置审计的资源类型，请参见配置审计支持的资源类型和资源关系。
tags	资源标签。

4.2.3. 资源不合规事件内容示例

通过本文您可以了解配置审计的资源不合规事件投递到日志服务SLS的内容示例和主要参数说明。

内容示例

普通账号 `120886317861****` 中对象存储OSS的北京地域的存储空间 `test_bucket` 的不合规事件投递到日志服务SLS，内容示例如下：

```
accountId:120886317861****
annotation:{"configuration":"public-read","desiredValue":"read","operator":"NotStringContains","property":"$.AccessControlList.Grant"}
compliancePackId:null
complianceType:NON_COMPLIANT
configAggregatorId:null
configRuleInvokedTimestamp:1630481784685
dataType:NonCompliantNotification
evaluationResultIdentifier:{"orderingTimestamp":1630481784685,"evaluationResultQualifier":{"resourceId":"test_bucket","configRuleName":"OSS存储空间ACL禁止公共读","configRuleId":"cr-2d736457e0d90044****","captureTime":1630481784685,"resourceName":"test_bucket","configRuleArn":"acs:config::120886317861****:rule/cr-2d736457e0d90044****","regionId":"cn-beijing","resourceOwnerId":120886317861****,"resourceType":"ACS::OSS::Bucket"}}
eventName:NonCompliant
eventType:ResourceCompliance
invokingEventMessageType:Manual
notificationCreationTime:1630481787932
requestId:62e70b45-1171-4648-8db0-233d18f6adb5
resultRecordedTimestamp:1630481784781
resultToken:null
riskLevel:Critical
```

参数说明

资源不合规事件投递到日志服务SLS的主要参数说明如下表所示。

参数	说明

参数	说明
accountId	资源归属的账号ID。配置审计支持如下账号类型： • 普通账号：未被企业管理账号加入资源目录的独立的阿里云账号。 • 企业管理账号：开通资源目录并管理成员账号的阿里云账号。 • 成员账号：资源目录中的成员账号。
annotation	资源不合规描述信息。
compliancePackId	合规包ID。当规则不属于任何合规包时，该参数为 `null` 。
complianceType	合规类型。取值为 `NON_COMPLIANT` （不合规）。
configAggregators	账号组信息，包括创建账号组的企业管理账号ID和账号组ID。根据资源归属账号类型不同，该参数显示如下： • 当资源归属普通账号时，该参数为 `null` 。 • 当资源归属企业管理账号时，该参数为当前企业管理账号创建的账号组信息。 • 当资源归属成员账号时，该参数为成员账号归属的企业管理账号创建的账号组信息。
configRuleInvokedTimestamp	调用规则评估资源时的时间戳。关于时间戳的转换方法，请参见Unix时间戳。
dataType	日志服务SLS的接收内容。取值： • `ConfigurationItemChangeNotification` ：资源配置变更历史。 • `NonCompliantNotification` ：资源不合规事件。
evaluationResultIdentifier	资源合规评估的详细信息。
eventName	事件名称。取值为 `NonCompliant` （资源不合规事件）。
eventType	事件类型。取值： • `ResourceChange` ：资源配置变更历史事件。 • `ResourceCompliance` ：资源不合规事件。
invokingEventMessageType	规则的触发机制。取值： • `NonCompliantNotification` ：不合规通知。 • `ConfigurationItemChangeNotification` ：配置变更通知。 • `Manual` ：手动执行。
notificationCreationTime	创建通知的时间戳。关于时间戳的转换方法，请参见Unix时间戳。
resultRecordedTimestamp	资源评估结果的时间戳。关于时间戳的转换方法，请参见Unix时间戳。

参数	说明
riskLevel	规则风险等级。取值： • `Info`：低风险。 • `Warning`：中风险。 • `Critical`：高风险。

4.3. 设置集成服务

配置审计支持的集成服务包括云速搭CADT（Cloud Architect Design Tool）和事件总线EventBridge。配置审计记录资源的配置数据，并及时感知资源变更。配置审计可以将资源数据投递到云速搭CADT，云速搭CADT根据资源变更自动调整应用架构中的资源配置，帮助您实时且准确地管理应用架构。配置审计还可以将资源的配置变更历史和不合规事件投递到事件总线EventBridge，帮助您一站式解决事件消费和分发问题。

前提条件

- 请确保您已开通云速搭CADT。当您首次使用云速搭CADT时，需要登录云速搭CADT控制台，根据页面提示开通云速搭CADT。
- 请确保您已开通事件总线EventBridge。具体操作，请参见开通事件总线EventBridge并授权。

普通账号

普通账号可以设置将自己的资源数据投递到云速搭CADT和事件总线EventBridge。

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**投递服务 > 集成服务设置**。
3. 设置云速搭CADT和事件总线EventBridge的启用状态。
   - 云速搭CADT
     a. 在**云速搭（Cloud Architect Design Tools）**区域，打开**启用状态**开关。
     b. 在**确认操作**对话框，单击**确定**。
   - 事件总线EventBridge

     在**事件总线EventBridge**区域，默认打开**启用状态**开关，且不能关闭。

企业管理账号

企业管理账号和成员账号只能设置将自己账号中的资源数据投递到云速搭CADT和事件总线EventBridge中，企业管理账号无法投递成员账号中的资源数据。

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**投递服务 > 集成服务设置**。
3. 设置云速搭CADT和事件总线EventBridge的启用状态。
   - 云速搭CADT
     a. 在**云速搭（Cloud Architect Design Tools）**区域，打开**启用状态**开关。
     b. 在**确认操作**对话框，单击**确定**。
   - 事件总线EventBridge

在**事件总线EventBridge**区域，默认打开**启用状态**开关，且不能关闭。

5.服务关联角色

5.1. 配置审计服务关联角色

配置审计服务关联角色（AliyunServiceRoleForConfig）是在某些场景下，为了完成配置审计的某个功能，需要获取其他云服务的访问权限而提供的RAM角色。

> **说明** 更多关于服务关联角色的信息，请参见服务关联角色。

应用场景

- 当配置审计调用各云服务的API查询接口，获取云资源的配置信息时，需要通过服务关联角色获取云资源配置信息的读取权限。
- 当您设置对象存储OSS的存储空间（Bucket）用于接收资源快照时，配置审计需向您指定的存储空间写入快照文件，需要通过服务关联角色获取存储空间的写入权限。
- 当您设置日志服务SLS的日志库（Logstore）用于接收资源日志时，配置审计需向您指定的日志库写入日志文件，需要通过服务关联角色获取日志库的写入权限。
- 当您设置消息服务MNS的主题用于接收资源事件时，配置审计需向您指定的主题写入资源事件，需要通过服务关联角色获取主题的写入权限。

角色说明

配置审计服务关联角色的详细信息如下：

- 角色名称：AliyunServiceRoleForConfig。
- 角色权限策略名称：AliyunServiceRolePolicyForConfig。
- 角色权限策略说明：授予配置审计服务读取云资源配置信息的权限，以及资源快照写入对象存储OSS存储空间、资源日志写入日志服务SLS日志库和资源事件写入消息服务MNS的权限。

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "arms:GetPrometheusApiToken"
      ],
      "Resource": "*"
    },
    {
      "Action": [
        "alikafka:List*",
        "alikafka:Get*",
        "cr:List*",
        "cr:GetInstance",
        "cr:GetNamespace",
        "cr:GetRepository",
        "oceanbase:Describe*",
        "oceanbase:List*",
        "bpstudio:Get*",
        "bpstudio:List*",
```

```
        "opensearch:List*",
        "opensearch:Describe*",
        "smartag:Describe*",
        "smartag:List*",
        "smartag:Get*",
        "alb:List*",
        "alb:Get*",
        "emr:List*",
        "emr:Describe*",
        "iot:List*",
        "iot:Get*",
        "iot:Query*",
        "eventbridge:Get*",
        "eventbridge:List*",
        "*:ListTagResources",
        "ecs:Describe*",
        "ess:Describe*",
        "vpc:Describe*",
        "rds:DescribeDBInstance*",
        "rds:DescribeRegions",
        "rds:DescribeBackup*",
        "rds:DescribeParameters",
        "rds:DescribeSQLCollector*",
        "rds:DescribeActionEventPolicy",
        "slb:Describe*",
        "*:DescribeTags",
        "oss:GetService",
        "oss:GetBucket*",
        "oss:ListBuckets",
        "oss:ListObjects",
        "ram:List*",
        "ram:Get*",
        "actiontrail:LookupEvents",
        "actiontrail:Describe*",
        "actiontrail:Get*",
        "ots:BatchGet*",
        "ots:Describe*",
        "ots:Get*",
        "ots:List*",
        "ocs:Describe*",
        "cms:Get*",
        "cms:List*",
        "cms:Query*",
        "cms:BatchQuery*",
        "cms:Describe*",
        "kvstore:Describe*",
        "fc:Get*",
        "fc:List*",
        "kms:DescribeKey",
        "kms:DescribeRegions",
        "kms:ListAliases",
        "kms:ListAliasesByKeyId",
        "kms:ListKeys",
        "kms:DescribeKeyVersion",
```

```
        "kms:ListKeyVersions",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ListResourceTags",
        "cdn:Describe*",
        "yundun*:Get*",
        "yundun*:Describe*",
        "yundun*:Query*",
        "yundun*:List*",
        "polardb:Describe*",
        "dds:Describe*",
        "cen:Describe*",
        "mns:ListTopic",
        "mns:GetTopicAttributes",
        "resourcemanager:GetAccount",
        "resourcemanager:ListAccountsForParent",
        "resourcemanager:ListAccounts",
        "resourcemanager:GetFolder",
        "resourcemanager:ListFoldersForParent",
        "resourcemanager:ListAncestors",
        "resourcemanager:GetResourceDirectory",
        "resourcemanager:ListHandshakesForResourceDirectory",
        "resourcemanager:GetHandshake",
        "resourcemanager:ListResourceGroups",
        "resourcemanager:GetResourceGroup",
        "resourcemanager:ListDelegatedAdministrators",
        "composer:GetFlow",
        "composer:DescribeFlow",
        "nas:Describe*",
        "hbase:Describe*",
        "hbase:Get*",
        "hbase:List*",
        "hbase:Query*",
        "cs:Get*",
        "cs:List*",
        "cs:Describe*",
        "dms:List*",
        "dms:Get*",
        "mq:OnsInstanceInServiceList",
        "mq:OnsInstanceBaseInfo",
        "mq:OnsTopicList",
        "mq:OnsGroupList",
        "mq:QueryInstanceBaseInfo",
        "mq:PUB",
        "mq:SUB",
        "alidns:Describe*",
        "alidns:List*",
        "mse:Query*",
        "mse:List*",
        "ros:Describe*",
        "ros:Get*",
        "ros:List*",
        "elasticsearch:List*",
```

```
        "elasticsearch:Describe*",
        "dcdn:Describe*",
        "hcs-sgw:Describe*",
        "eci:Describe*",
        "kms:ListSecrets",
        "kms:DescribeSecret",
        "privatelink:List*",
        "privatelink:Get*",
        "brain-industrial:List*",
        "brain-industrial:Get*",
        "imagesearch:List*",
        "imagesearch:Describe*",
        "hitsdb:Describe*",
        "apigateway:Describe*",
        "sas:DescribeGroupedVul",
        "sas:DescribeFieldStatistics",
        "cmn:List*",
        "cmn:Get*",
        "ledgerdb:Describe*",
        "pvtz:Describe*",
        "oos:Search*",
        "oos:List*",
        "oos:Get*",
        "adb:Describe*",
        "edas:Read*",
        "drds:Describe*",
        "gpdb:Describe*",
        "log:ListProject",
        "log:GetProject",
        "log:ListLogStores",
        "log:GetLogStore",
        "dts:Describe*",
        "arms:Get*",
        "arms:List*",
        "polardbx:Describe*",
        "hbr:Describe*",
        "live:Describe*",
        "vod:Describe*",
        "vod:List*",
        "vod:Get*",
        "lindorm:Get*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "oss:PutObject",
        "fc:InvokeFunction",
        "mns:PublishMessage",
        "composer:GroupInvokeFlow",
        "composer:CreateFlow",
        "log:PostLogStoreLogs"
      ],
```

```
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "config:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "config.aliyuncs.com"
        }
      }
    }
  ]
}
```

创建服务关联角色

在配置审计控制台上，创建服务关联角色的操作方法如下：

- 普通账号

  普通账号使用配置审计服务之前，需要创建服务关联角色。具体操作，请参见授权服务。

- 企业管理账号

  当企业管理账号将资源目录中的所有或部分成员账号添加到账号组时，配置审计自动为该账号组中的所有成员账号创建服务关联角色。关于账号组，请参见账号组。

删除服务关联角色

配置审计服务关联角色不能直接删除。删除方法如下：

1. 登录配置审计控制台，关闭配置审计服务。

   具体操作，请参见关闭配置审计服务。

2. 登录RAM控制台，删除配置审计服务关联角色。

   具体操作，请参见删除RAM角色。

5.2. 自动修正功能的服务关联角色

本文为您介绍自动修正功能的服务关联角色（AliyunServiceRoleForConfigRemediation）的应用场景、权限策略、创建及删除操作。

应用场景

当您使用配置审计的自动修正功能修正不合规资源时，需要获取不合规资源的访问权限。此时，配置审计提供了服务关联角色（AliyunServiceRoleForConfigRemediation），解决跨服务授权问题。

> **说明** 更多关于服务关联角色的信息，请参见服务关联角色。

角色说明

自动修正功能的服务关联角色的详细信息如下：

- 角色名称：AliyunServiceRoleForConfigRemediation。
- 角色权限策略名称：AliyunServiceRolePolicyForConfigRemediation。
- 角色权限策略说明：授予配置审计访问对应云服务中资源的权限。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "actiontrail:CreateTrail",
        "actiontrail:StartLogging",
        "cbn:TagResources",
        "cdn:SetDomainServerCertificate",
        "cdn:TagResources",
        "cen:TagResources",
        "composer:CreateFlow",
        "composer:GroupInvokeFlow",
        "composer:InvokeFlow",
        "cs:GetClusterInfo",
        "cs:ListClusters",
        "cs:TagResources",
        "cs:UpdateClusterTags",
        "ddoscoo:CreateTagResources",
        "ddoscoo:TagResources",
        "dds:TagResources",
        "ecs:DescribeInstances",
        "ecs:ModifyInstanceAttribute",
        "ecs:ModifyInstanceNetworkSpec",
        "ecs:TagResources",
        "hbase:TagResources",
        "kms:TagResource",
        "kms:UpdateRotationPolicy",
        "kms:DescribeKey",
        "kms:SetDeletionProtection",
        "kvstore:ModifyAuditLogConfig",
        "kvstore:TagResources",
        "kvstore:ReleaseInstancePublicConnection",
        "kvstore:DescribeSecurityIps",
        "kvstore:ModifySecurityIps",
        "kvstore:ModifyInstanceConfig",
        "kvstore:DescribeDBInstanceNetInfo",
        "nas:AddTags",
        "nas:TagResources",
        "oos:StartExecution",
        "oos:TagResources",
        "oss:GetBucketTagging",
        "oss:PutBucketTagging",
```

```
        "oss:PutBucketACL",
        "oss:PutBucketEncryption",
        "oss:PutBucketLogging",
        "oss:PutBucketReferer",
        "oss:PutBucketVersioning",
        "polardb:TagResources",
        "ram:SetPasswordPolicy",
        "ram:UpdateLoginProfile",
        "rds:MigrateSecurityIPMode",
        "rds:ModifyActionEventPolicy",
        "rds:ModifySQLCollectorPolicy",
        "rds:ModifySQLCollectorRetention",
        "rds:TagResources",
        "rds:ModifySecurityIps",
        "rds:DescribeDBInstanceIPArrayList",
        "rds:DescribeDBInstanceNetInfo",
        "rds:ReleaseInstancePublicConnection",
        "slb:DescribeLoadBalancerAttribute",
        "slb:SetLoadBalancerDeleteProtection",
        "slb:SetLoadBalancerModificationProtection",
        "slb:TagResources",
        "tag:ListTagResources",
        "tag:TagResources",
        "tag:UntagResources",
        "vpc:TagResources",
        "vpc:DescribeNatGateways",
        "vpc:DescribeForwardTableEntries",
        "vpc:DeleteForwardEntry",
        "yundun-ddoscoo:TagResources",
        "yundun-ddoscoo:CreateTagResources",
        "yundun-high:TagResources",
        "yundun-high:CreateTagResources",
        "yundun-waf:ModifyLogServiceStatus",
        "yundun-waf:ModifyProtectionModuleStatus",
        "apigateway:DescribeApi",
        "apigateway:AbolishApi",
        "apigateway:DescribeApiGroups",
        "apigateway:ModifyApiGroupNetworkPolicy",
        "apigateway:ModifyInstanceAttribute",
        "apigateway:ModifyApi",
        "apigateway:TagResources"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:PassRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "acs:Service": [
            "composer.aliyuncs.com",
            "oos.aliyuncs.com"
```

```
            ]
          }
        }
      },
      {
        "Action": "ram:DeleteServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": "remediation.config.aliyuncs.com"
          }
        }
      }
    ]
}
```

创建自动修正功能的服务关联角色

如果您针对规则设置了修正模板，当配置审计通过该规则检测资源为不合规时，会自动在RAM控制台创建自动修正服务关联角色。

删除自动修正功能的服务关联角色

1. 删除修正设置。
   - 删除规则的修正设置。具体操作，请参见删除修正设置。
   - 删除已设置修正的所有规则。具体操作，请参见删除规则。
2. 删除自动修正功能的服务关联角色。

   具体操作，请参见删除RAM角色。

   自动修正功能的服务关联角色不能自动删除，只能登录RAM控制台，主动删除。具体操作，请参见删除RAM角色。

相关操作

- 设置自动修正
- 设置手动修正
- 删除修正设置

6.API参考

6.1. API版本说明

请您根据应用场景选择对应版本的API。

应用场景	描述	API版本	API版本关系
合规包	管理合规包。	2020-09-07	无
账号组	管理账号组。	2020-09-07	无
资源监控范围	管理资源监控范围。	2019-01-08	无
资源	查询资源列表、资源数量、资源统计结果等。	• 2020-09-07 • 2019-01-08	2020-09-07版本API是对2019-01-08版本API的扩充，且API区分账号类型，即普通账号API、企业管理账号API和成员账号API。当两个版本中的API功能相同时，推荐您使用2020-09-07版本。
规则	管理规则，并查询规则对资源的评估结果和评估报告。	• 2020-09-07（推荐） • 2019-01-08	2020-09-07版本API区分账号类型，即普通账号API、企业管理账号API和成员账号API。
投递渠道	管理投递渠道。	• 2020-09-07 • 2019-01-08	2020-09-07版本API是对2019-01-08版本API功能的升级（支持设置投递服务的接收内容和超大文件接收地址），且API区分账号类型，即普通账号API和企业管理账号API。当两个版本中的API功能相同时，推荐您使用2020-09-07版本。

7.最佳实践

7.1. 通过MNS通知机制实现不合规资源的自动修复

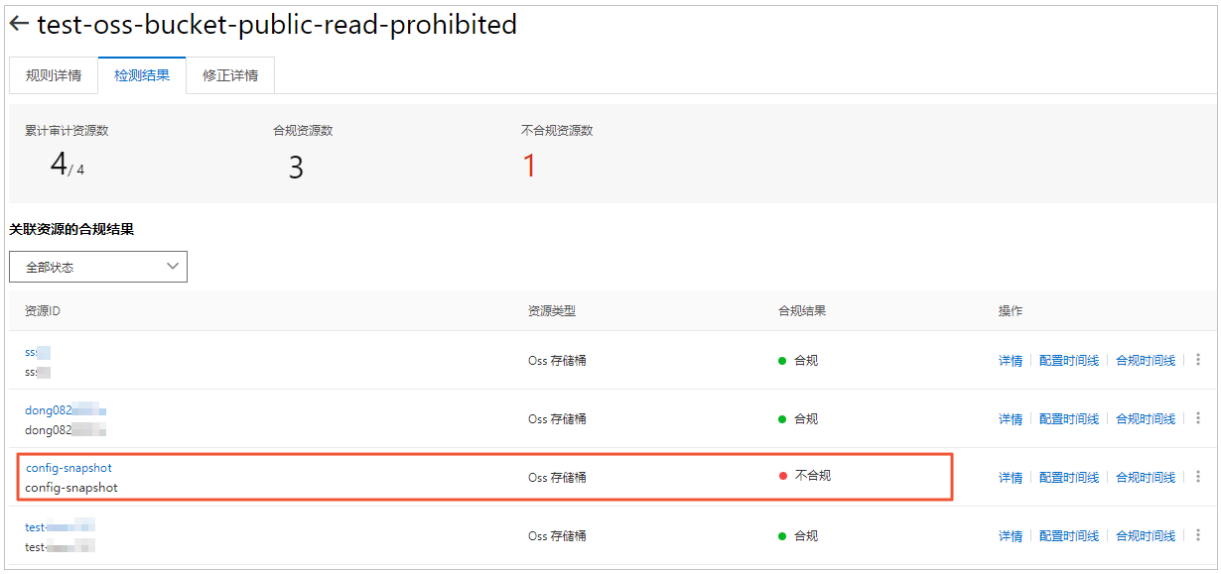
当配置审计发现资源配置有变更且不合规时，以事件通知的形式将告警推送到您指定的消息服务MNS主题。当您收到不合规告警时，通过函数计算实现不合规资源的自动修复。

前提条件

- 请确保您已使用托管规则新建规则。具体操作，请参见授权服务和使用托管规则新建规则。
- 请确保您已开通消息服务MNS服务。具体操作，请参见开通消息服务MNS并授权。
- 请确保您已开通对象存储OSS服务，且已新建存储空间（Bucket）。具体操作，请参见开通OSS服务和创建存储空间。
- 请确保您已开通函数计算服务。具体操作，请参见使用控制台创建函数。

应用场景

您在配置审计控制台通过托管规则“test-oss-bucket-public-read-prohibited”新建一条资源类型为“OSS存储桶”的规则，配置审计自动审计当前账号下所有OSS存储空间的资源，其中一条资源的合规结果为**不合规**，如下图所示。



数据规划

本文以修复对象存储OSS的存储空间的读写权限为例，为您介绍通过配置审计的MNS通知机制实现不合规资源自动修复的操作方法。相关数据规划如下表所示。

云服务	参数	示例
配置审计	托管规则	test-oss-bucket-public-read-prohibited

云服务	参数	示例
	规则名称	test-oss-bucket-public-read-prohibited
消息服务	主题名称	MNSTestConfig
	主题地域	华东2（上海）
对象存储OSS	OSS Bucket	config-snapshot
	Bucket ACL	公共读
函数计算	服务	resource_repair
	服务的系统模板权限	AliyunOSSFullAccess
	函数	oss_repair_acl_trigger
	触发器	ConfigRuleNonComplianceMNSTrigger

说明

由于配置审计部署在华东2（上海），为了减少网络损耗，建议消息服务MNS的主题地域选择**华东2（上海）**。

操作流程

通过配置审计的MNS通知机制实现不合规资源自动修复的操作流程如下图所示。

操作步骤

1. 登录配置审计控制台，设置资源合规事件投递到消息服务MNS的指定主题（Topic），例如：MNSTestConfig。

   具体操作，请参见设置投递数据到消息服务MNS。

2. 新建服务。
   i. 登录函数计算控制台。
   ii. 在左侧导航栏，单击**服务及函数**。
   iii. 在顶部菜单栏，选择地域，例如：华东2（上海）。
   iv. 在**服务列表**页面，单击**创建服务**。
   v. 在**创建服务**面板，**名称**输入resource_repair。
   vi. 单击**确定**。
3. 授权目标服务修改OSS存储空间的权限。
   i. 在服务resource_repair的左侧导航栏，单击**服务详情**。
   ii. 在**角色配置**区域，单击**编辑**。
   iii. 选择已有角色AliyunFCLogExecutionRole。

   角色AliyunFCLogExecutionRole中包含权限策略AliyunOSSFullAccess。
   iv. 单击**保存**。
4. 新建函数。

i. 在服务resource_repair的左侧导航栏，单击**函数管理**。

ii. 单击**创建函数**。

iii. 在**创建函数**页面，**名称**输入oss_repair_acl_trigger，**运行环境**选择Python 3，**函数触发方式**选择**通过事件触发**，其他参数保持默认值。

iv. 单击**创建**。

5. 配置函数的环境变量。

i. 在函数oss_repair_acl_trigger的**函数代码**页签，单击**函数配置**页签。

ii. 在**环境变量**区域，单击**编辑**。

iii. 单击**添加变量**，输入该环境变量的变量名称和变量值。

- **变量**为prepareRuleName。

  prepareRuleName与函数计算自动修复代码中参数ENV_RULE_NAME的取值保持一致。

- **值**为test-oss-bucket-public-read-prohibited。

  test-oss-bucket-public-read-prohibited为配置审计中的规则名称。

iv. 单击**保存**。

6. 新建触发器。

i. 在函数oss_repair_acl_trigger的**函数配置**页签，单击**触发器管理**页签。

ii. 单击**创建触发器**。

iii. 选择**触发器类型**为**消息服务MNS**。

iv. 设置消息服务MNS触发器的相关参数。

参数设置如下：

- **名称**输入ConfigRuleNonComplianceMNSTrigger。
- **MNS地域**选择**华东2（上海）**。
- **主题**选择MNSTestConfig。
- **Event格式**选择JSON。
- **角色名称**选择AliyunMNSNotificationRole。

v. 单击**确定**。

新建触发器完成后，当配置审计对目标资源进行评估时，您会接收到该资源的不合规事件通知。

7. 配置自动修复代码。

i. 在函数oss_repair_acl_trigger的**触发器管理**页签，单击**函数代码**页签。

ii. 单击文件index.py。

iii. 拷贝并粘贴如下代码至文件index.py。

```
# -*- coding: utf-8 -*-
import logging
import json
import os
import base64
import binascii
from aliyunsdkcore.acs_exception.exceptions import ClientException, ServerException
IDENTIFIER = 'evaluationResultIdentifier'
QUALIFIER = 'evaluationResultQualifier'
```

```
RULE_NAME = 'configRuleName'
ENV_RULE_NAME = 'prepareRuleName'
RESOURCE_ID = 'resourceId'
REGION_ID = 'regionId'
FAIL = 'fail'
SUCC = 'success'
logger = logging.getLogger()
def handler(event, context):
    logger.info("mns_topic trigger event = {}".format(event))
    decoded = None
    if event:
        try:
            decoded = base64.b64decode(event)
        except binascii.Error as ex:
            logger.exception('mns_topic trigger event malformed!')
            return FAIL
    if not decoded:
        return FAIL
    notify_json = json.loads(decoded)
    if notify_json and IDENTIFIER in notify_json:
        evaluationResultIdentifier = notify_json.get(IDENTIFIER)
        if QUALIFIER in evaluationResultIdentifier and RULE_NAME in evaluationResul
tIdentifier.get(QUALIFIER):
            evaluationResultQualifier = evaluationResultIdentifier.get(QUALIFIER)
            configRuleName = evaluationResultQualifier.get(RULE_NAME)
            # os.environ.get(ENV_RULE_NAME) 获取您设置的规则名称，例如：test-oss-bucket
-public-read-prohibited。
            if configRuleName == os.environ.get(ENV_RULE_NAME):
                if RESOURCE_ID in evaluationResultQualifier and REGION_ID in evalua
tionResultQualifier:
                    bucket_name = evaluationResultQualifier.get(RESOURCE_ID)
                    region = evaluationResultQualifier.get(REGION_ID)
                    if region and bucket_name:
                        try:
                            remedy_by_fc_assume(context, region, bucket_name)
                        except Exception as ex:
                            logger.exception('remedy fail!')
    return FAIL
def remedy_by_fc_assume(context, region, bucket_name):
    creds = context.credentials
    auth = oss2.StsAuth(creds.access_key_id, creds.access_key_secret, creds.securit
y_token)
    bucket = oss2.Bucket(auth, 'http://oss-' + region + '.aliyuncs.com', bucket_nam
e)
    bucket.put_bucket_acl(oss2.BUCKET_ACL_PRIVATE)
    logger.info('bucket {bucket_name} in {region} acl remedy succ.'.format(bucket_n
ame=bucket_name, region=region))
```

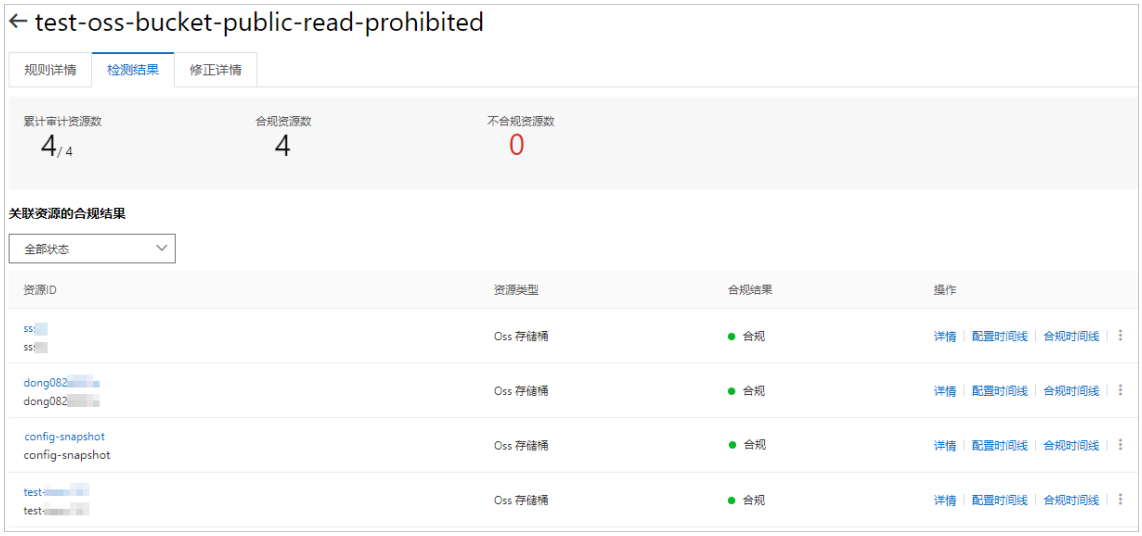
> **说明** 本段代码以规则名称prepareRuleName为例，为您介绍不合规资源的自动修复方法。如需通过其他参数修复，请参见资源不合规事件内容示例。

iv. 单击右上角的**保存并部署**。

8. 十分钟后，查看修复结果。

> **说明** 当资源配置无变更，且审计结果为不合规时，您还需要手动执行审计，然后再执行此步骤。手动执行审计的操作方法，请参见手动执行审计。

- 通过配置审计控制台查看



- 通过OSS控制台查看

7.2. 通过自定义规则检测指定RAM用户是否开启MFA

为RAM用户开启多因素认证（MFA），可以提高RAM用户的使用安全。通过配置审计的托管规则（高权限的RAM用户开启MFA），可以检测所有RAM用户是否开启MFA。如果您只想检测指定RAM用户（例如：高风险用户）是否开启MFA，请使用本文所述的自定义规则的方法。

前提条件

- 请确保您已开通消息服务MNS服务。具体操作，请参见开通消息服务MNS并授权。
- 请确保您已开通函数计算服务。具体操作，请参见使用控制台创建函数。
- 请确保您已创建RAM用户Alice，且已授予系统权限AliyunECSFullAccess（管理云服务器ECS的权限）。具体操作，请参见创建RAM用户和为RAM用户授权。

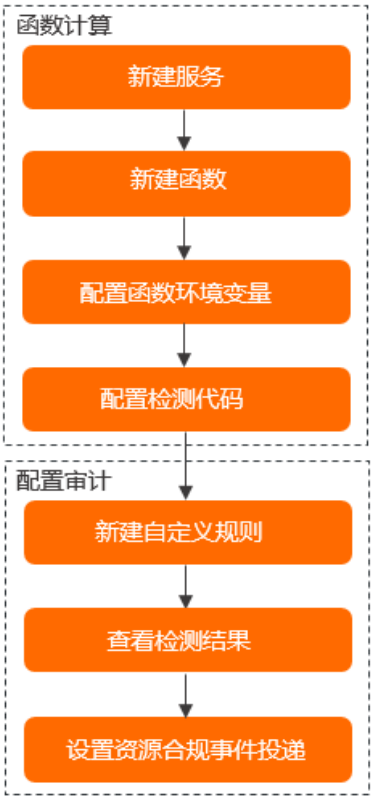
数据规划

数据规划如下表所示。

云服务	参数	示例
配置审计	规则名称	RAMUserMFA
	规则触发机制	配置变更，周期执行
	触发频率	1小时
	规则入参名称	dangerousActions
	期望值	ecs:*,oss:*,log:*
消息服务	主题名称	MNSTestConfig
	主题地域	华东2（上海） **说明** 由于配置审计部署在华东2（上海），为了减少网络损耗，建议消息服务MNS的主题地域选择**华东2（上海）**。
访问控制	RAM用户名称	Alice
	RAM用户ID	25849250231246****
	默认权限策略	AliyunECSFullAccess
函数计算	服务	Ram_User
	函数	RamDangerousPolicyUserBindMFA

操作流程

操作流程如下图所示。



操作步骤

1. 新建服务。
   i. 登录函数计算控制台。
   ii. 在左侧导航栏，单击**服务及函数**。
   iii. 在顶部菜单栏，选择地域，例如：华东2（上海）。
   iv. 在**服务列表**页面，单击**创建服务**。
   v. 在**创建服务**面板，**名称**输入Ram_User。
   vi. 单击**确定**。
2. 新建函数。
   i. 在服务Ram_User的**函数管理**页面，单击**创建函数**。
   ii. 在**创建函数**页面，**名称**输入RamDangerousPolicyUserBindMFA，**运行环境**选择Python 3，**函数触发方式**选择**通过事件触发**，其他参数保持默认值。
   iii. 单击**创建**。
3. 配置函数的环境变量。
   i. 在函数RamDangerousPolicyUserBindMFA的**函数代码**页签，单击**函数配置**页签。
   ii. 在**环境变量**区域，单击**编辑**。

iii. 单击**添加变量**，输入该环境变量的变量名称和变量值。

变量	值	示例
AK	当前阿里云账号的AccessKey ID。关于如何获取AccessKey ID，请参见获取AccessKey。	LTAI4G6JZSANb8MZMkm1****
SK	当前阿里云账号的AccessKey Secret。关于如何获取AccessKey Secret，请参见获取AccessKey。	EMLHThhpD2UJqH1DXuAKii2sI****
ResourceTypes	资源类型。	ACS::RAM::User

iv. 单击**保存**。

4. 配置检测RAM用户是否开启MFA的代码。

i. 在函数**RamDangerousPolicyUserBindMFA**的**函数代码**页签，单击文件**index.py**。

ii. 拷贝并粘贴如下代码至文件**index.py**。

```
#!/usr/bin/env python
# -*- encoding: utf-8 -*-
import logging
import json
import os
from aliyunsdkcore.client import AcsClient
from aliyunsdkram.request.v20150501 import ListPoliciesForUserRequest
from aliyunsdkram.request.v20150501 import GetPolicyRequest
from aliyunsdkram.request.v20150501 import GetUserMFAInfoRequest
from aliyunsdkcore.auth.credentials import StsTokenCredential
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkcore.request import CommonRequest
logger = logging.getLogger()
# AccessKey/SecretKey, need AliyunConfigFullAccess policy
AK = 'LTAI4FgrMeKLB7NqDmPe****'
SK = 'dylEiakiwLFB1CufDyxyCwlCxZ****'
# Valid compliace type
COMPLIACE_TYPE_COMPLIANT = 'COMPLIANT'
COMPLIACE_TYPE_NON_COMPLIANT = 'NON_COMPLIANT'
COMPLIACE_TYPE_NOT_APPLICABLE = 'NOT_APPLICABLE'
COMPLIACE_TYPE_INSUFFICIENT_DATA = 'INSUFFICIENT_DATA'
def handler(event, context):
    # Validate event
    evt = validate_event(event)
    if not evt:
        return None
    rule_parameters = evt.get('ruleParameters')
    result_token = evt.get('resultToken')
    ordering_timestamp = evt.get('orderingTimestamp')
    invoking_event = evt.get('invokingEvent')
    # Initilize
    compliance_type = COMPLIACE_TYPE_NOT_APPLICABLE
    annotation = None
```

```
    configuration_item = invoking_event.get('configurationItem')
    if not configuration_item:
        logger.error('Configuration item is empty.')
        return None
    resource_id = configuration_item.get('resourceId')
    resource_type = configuration_item.get('resourceType')
    region_id = configuration_item.get('regionId')
    creds = context.credentials
    # Get compliace result
    compliance_type, annotation = evaluate_configuration_item(rule_parameters, conf
iguration_item, creds)
    # Compliance result
    evaluations = [
        {
            'complianceResourceId': resource_id,
            'complianceResourceType': resource_type,
            'complianceRegionId': region_id,
            'orderingTimestamp': ordering_timestamp,
            'complianceType': compliance_type,
            'annotation': annotation
        }
    ]
    put_evaluations(context, result_token, evaluations)
    return evaluations
def evaluate_configuration_item(rule_parameters, configuration_item, creds):
    # Initilize
    compliance_type = COMPLIACE_TYPE_NOT_APPLICABLE
    annotation = None
    # Get resource type and configuration
    resource_type = configuration_item['resourceType']
    full_configuration = configuration_item['configuration']
    # Check configuration
    if not full_configuration:
        annotation = 'Configuration is empty.'
        return compliance_type, annotation
    # Parse to json object
    configuration = parse_json(full_configuration)
    if not configuration:
        annotation = 'Configuration:{} in invald.'.format(full_configuration)
        return compliance_type, annotation
    # =========== Customer code start =========== #
    if 'UserPrincipalName' in configuration and configuration['UserPrincipalName']:
        user_name = configuration_item['resourceName']
        user_principal_name = configuration['UserPrincipalName']
        if rule_parameters and 'dangerousActions' in rule_parameters and rule_param
eters['dangerousActions']:
            actions = rule_parameters['dangerousActions'].split(',')
            isvalid, reason = validate_user_bind_MFADevice(user_name, user_principa
l_name, actions)
            if isvalid:
                compliance_type, annotation = COMPLIACE_TYPE_COMPLIANT, None
            else:
                compliance_type, annotation = COMPLIACE_TYPE_NON_COMPLIANT, reason
        else:
```

```
            compliance_type, annotation = COMPLIACE_TYPE_COMPLIANT, 'rule parameter
:{dangerousActions} not specified'
    else:
        compliance_type, annotation = COMPLIACE_TYPE_INSUFFICIENT_DATA, 'ram user n
ot named'
    # =========== Customer code end =========== #
    return compliance_type, annotation
def validate_user_bind_MFADevice(user_name, user_principal_name, input_actions):
    client = AcsClient(AK, SK)
    # Get user ploicy list
    list_user_policy_req = ListPoliciesForUserRequest.ListPoliciesForUserRequest()
    list_user_policy_req.set_UserName(user_name)
    list_user_policy_res = None
    try:
        list_user_policy_res = client.do_action_with_exception(list_user_policy_req
)
    except ServerException as se:
        if se.get_http_status() == 404 and se.get_error_code() == 'EntityNotExist.U
ser':
            return True, None
        else:
            return False, se.get_error_msg()
    if list_user_policy_res is None:
        return True, None
    list_user_policy_json_res = json.loads(list_user_policy_res)
    user_policies = list_user_policy_json_res['Policies']['Policy']
    if user_policies is None or len(user_policies) == 0:
        return True, None
    # Get user ploicy filter by input_actions
    policy_action_list = list()
    for policy in user_policies:
        get_policy_req = GetPolicyRequest.GetPolicyRequest()
        get_policy_req.set_PolicyName(policy['PolicyName'])
        get_policy_req.set_PolicyType(policy['PolicyType'])
        get_policy_res = None
        try:
            get_policy_res = client.do_action_with_exception(get_policy_req)
            policy_document = json.loads(json.loads(get_policy_res)['DefaultPolicyV
ersion']['PolicyDocument'])
            for action in list(map(lambda x: x['Action'],
                                   list(filter(lambda x: x['Effect'] == 'Allow', po
licy_document['Statement'])))):
                if type(action) is list:
                    policy_action_list.extend(action)
                else:
                    policy_action_list.append(action)
        except ServerException as se:
            logger.error(se)
        except Exception as ex:
            logger.error(ex)
    policy_action_set = set(policy_action_list)
    logger.info('Policy actions: {}, input: {} .'.format(str(policy_action_set), st
r(input_actions)))
    # Verify policy actions contains input_actions
    if policy_action_set.intersection(set(input_actions)):
```

```
    if policy_action_set.intersection(set(input_actions)):
        get_user_mfa_req = GetUserMFAInfoRequest.GetUserMFAInfoRequest()
        get_user_mfa_req.set_UserName(user_principal_name)
        get_user_mfa_res = None
        try:
            get_user_mfa_res = client.do_action_with_exception(get_user_mfa_req)
            logger.info('GetUserMFAInfo user_name: {}, result: {} .'.format(user_na
me, str(get_user_mfa_res)))
            if ('SerialNumber' not in get_user_mfa_res) or ('MFADevice' not in get_
user_mfa_res):
                return False, 'user MFADevice empty'
            else:
                return True, None
        except ServerException as se:
            return False, se.get_error_msg()
    else:
        return True, None
def validate_event(event):
    if not event:
        logger.error('Event is empty.')
    evt = parse_json(event)
    logger.info('Loading event: %s .' % evt)
    if 'resultToken' not in evt:
        logger.error('ResultToken is empty.')
        return None
    if 'ruleParameters' not in evt:
        logger.error('RuleParameters is empty.')
        return None
    if 'invokingEvent' not in evt:
        logger.error('InvokingEvent is empty.')
        return None
    return evt
def parse_json(content):
    try:
        return json.loads(content)
    except Exception as e:
        logger.error('Parse content:{} to json error:{}.'.format(content, e))
        return None
def put_evaluations(context, result_token, evaluations):
    # ak/sk, need AliyunConfigFullAccess policy
    client = AcsClient(AK, SK, 'cn-shanghai')
    # Open api request
    request = CommonRequest()
    request.set_domain('config.cn-shanghai.aliyuncs.com')
    request.set_version('2019-01-08')
    request.set_action_name('PutEvaluations')
    request.add_body_params('ResultToken', result_token)
    request.add_body_params('Evaluations', evaluations)
    request.set_method('POST')
    try:
        response = client.do_action_with_exception(request)
        logger.info('PutEvaluations with request: {}, response: {}.'.format(request
, response))
    except Exception as e:
        logger.error('PutEvaluations error: %s' % e)
```

```
#!/usr/bin/env python
# -*- encoding: utf-8 -*-
import logging
import json
import os
from aliyunsdkcore.client import AcsClient
from aliyunsdkram.request.v20150501 import ListPoliciesForUserRequest
from aliyunsdkram.request.v20150501 import GetPolicyRequest
from aliyunsdkram.request.v20150501 import GetUserMFAInfoRequest
from aliyunsdkcore.auth.credentials import StsTokenCredential
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkcore.request import CommonRequest
logger = logging.getLogger()
# AccessKey/SecretKey, need AliyunConfigFullAccess policy
AK = 'LTAI4FgrMeKLB7NqDmPe****'
SK = 'dylEiakiwLFB1CufDyxyCwlCxZ****'
# Valid compliace type
COMPLIACE_TYPE_COMPLIANT = 'COMPLIANT'
COMPLIACE_TYPE_NON_COMPLIANT = 'NON_COMPLIANT'
COMPLIACE_TYPE_NOT_APPLICABLE = 'NOT_APPLICABLE'
COMPLIACE_TYPE_INSUFFICIENT_DATA = 'INSUFFICIENT_DATA'
def handler(event, context):
    # Validate event
    evt = validate_event(event)
    if not evt:
        return None
    rule_parameters = evt.get('ruleParameters')
    result_token = evt.get('resultToken')
    ordering_timestamp = evt.get('orderingTimestamp')
    invoking_event = evt.get('invokingEvent')
    # Initilize
    compliance_type = COMPLIACE_TYPE_NOT_APPLICABLE
    annotation = None
    configuration_item = invoking_event.get('configurationItem')
    if not configuration_item:
        logger.error('Configuration item is empty.')
        return None
    resource_id = configuration_item.get('resourceId')
    resource_type = configuration_item.get('resourceType')
    region_id = configuration_item.get('regionId')
    creds = context.credentials
    # Get compliace result
    compliance_type, annotation = evaluate_configuration_item(rule_parameters, conf
iguration_item, creds)
    # Compliance result
    evaluations = [
        {
            'complianceResourceId': resource_id,
            'complianceResourceType': resource_type,
            'complianceRegionId': region_id,
            'orderingTimestamp': ordering_timestamp,
            'complianceType': compliance type,
```

```
            'annotation': annotation
        }
    ]
    put_evaluations(context, result_token, evaluations)
    return evaluations
def evaluate_configuration_item(rule_parameters, configuration_item, creds):
    # Initilize
    compliance_type = COMPLIACE_TYPE_NOT_APPLICABLE
    annotation = None
    # Get resource type and configuration
    resource_type = configuration_item['resourceType']
    full_configuration = configuration_item['configuration']
    # Check configuration
    if not full_configuration:
        annotation = 'Configuration is empty.'
        return compliance_type, annotation
    # Parse to json object
    configuration = parse_json(full_configuration)
    if not configuration:
        annotation = 'Configuration:{} in invald.'.format(full_configuration)
        return compliance_type, annotation
    # =========== Customer code start =========== #
    if 'UserPrincipalName' in configuration and configuration['UserPrincipalName']:
        user_name = configuration_item['resourceName']
        user_principal_name = configuration['UserPrincipalName']
        if rule_parameters and 'dangerousActions' in rule_parameters and rule_param
eters['dangerousActions']:
            actions = rule_parameters['dangerousActions'].split(',')
            isvalid, reason = validate_user_bind_MFADevice(user_name, user_principa
l_name, actions)
            if isvalid:
                compliance_type, annotation = COMPLIACE_TYPE_COMPLIANT, None
            else:
                compliance_type, annotation = COMPLIACE_TYPE_NON_COMPLIANT, reason
        else:
            compliance_type, annotation = COMPLIACE_TYPE_COMPLIANT, 'rule parameter
:{dangerousActions} not specified'
    else:
        compliance_type, annotation = COMPLIACE_TYPE_INSUFFICIENT_DATA, 'ram user n
ot named'
    # =========== Customer code end =========== #
    return compliance_type, annotation
def validate_user_bind_MFADevice(user_name, user_principal_name, input_actions):
    client = AcsClient(AK, SK)
    # Get user ploicy list
    list_user_policy_req = ListPoliciesForUserRequest.ListPoliciesForUserRequest()
    list_user_policy_req.set_UserName(user_name)
    list_user_policy_res = None
    try:
        list_user_policy_res = client.do_action_with_exception(list_user_policy_req
)
    except ServerException as se:
        if se.get_http_status() == 404 and se.get_error_code() == 'EntityNotExist.U
ser':
```

```
            return True, None
        else:
            return False, se.get_error_msg()
    if list_user_policy_res is None:
        return True, None
    list_user_policy_json_res = json.loads(list_user_policy_res)
    user_policies = list_user_policy_json_res['Policies']['Policy']
    if user_policies is None or len(user_policies) == 0:
        return True, None
    # Get user ploicy filter by input_actions
    policy_action_list = list()
    for policy in user_policies:
        get_policy_req = GetPolicyRequest.GetPolicyRequest()
        get_policy_req.set_PolicyName(policy['PolicyName'])
        get_policy_req.set_PolicyType(policy['PolicyType'])
        get_policy_res = None
        try:
            get_policy_res = client.do_action_with_exception(get_policy_req)
            policy_document = json.loads(json.loads(get_policy_res)['DefaultPolicyV
ersion']['PolicyDocument'])
            for action in list(map(lambda x: x['Action'],
                                   list(filter(lambda x: x['Effect'] == 'Allow', po
licy_document['Statement'])))):
                if type(action) is list:
                    policy_action_list.extend(action)
                else:
                    policy_action_list.append(action)
        except ServerException as se:
            logger.error(se)
        except Exception as ex:
            logger.error(ex)
    policy_action_set = set(policy_action_list)
    logger.info('Policy actions: {}, input: {} .'.format(str(policy_action_set), st
r(input_actions)))
    # Verify policy actions contains input_actions
    if policy_action_set.intersection(set(input_actions)):
        get_user_mfa_req = GetUserMFAInfoRequest.GetUserMFAInfoRequest()
        get_user_mfa_req.set_UserName(user_principal_name)
        get_user_mfa_res = None
        try:
            get_user_mfa_res = client.do_action_with_exception(get_user_mfa_req)
            logger.info('GetUserMFAInfo user_name: {}, result: {} .'.format(user_na
me, str(get_user_mfa_res)))
            if ('SerialNumber' not in get_user_mfa_res) or ('MFADevice' not in get_
user_mfa_res):
                return False, 'user MFADevice empty'
            else:
                return True, None
        except ServerException as se:
            return False, se.get_error_msg()
    else:
        return True, None
def validate_event(event):
    if not event:
```

```
        logger.error('Event is empty.')
    evt = parse_json(event)
    logger.info('Loading event: %s .' % evt)
    if 'resultToken' not in evt:
        logger.error('ResultToken is empty.')
        return None
    if 'ruleParameters' not in evt:
        logger.error('RuleParameters is empty.')
        return None
    if 'invokingEvent' not in evt:
        logger.error('InvokingEvent is empty.')
        return None
    return evt
def parse_json(content):
    try:
        return json.loads(content)
    except Exception as e:
        logger.error('Parse content:{} to json error:{}.'.format(content, e))
        return None
def put_evaluations(context, result_token, evaluations):
    # ak/sk, need AliyunConfigFullAccess policy
    client = AcsClient(AK, SK, 'ap-southeast-1')
    # Open api request
    request = CommonRequest()
    request.set_domain('config.ap-southeast-1.aliyuncs.com')
    request.set_version('2019-01-08')
    request.set_action_name('PutEvaluations')
    request.add_body_params('ResultToken', result_token)
    request.add_body_params('Evaluations', evaluations)
    request.set_method('POST')
    try:
        response = client.do_action_with_exception(request)
        logger.info('PutEvaluations with request: {}, response: {}.'.format(request
, response))
    except Exception as e:
        logger.error('PutEvaluations error: %s' % e)
```

本段代码用于检测RAM用户是否开启MFA，代码中主要参数说明如下表所示。

参数	说明	示例
AK	当前阿里云账号的AccessKey ID。该参数必须与步骤 3中的AK相同。	LTAI4FgrMeKLB7NqDmPe****
SK	当前阿里云账号的AccessKey Secret。该参数必须与步骤 3中的SK相同。	dylEiakiwLFB1CufDyxyCwlCxZ****
user_name	RAM用户。	无。
rule_parameters	规则参数。	dangerousActions
input_actions	指定的危险操作。	ecs:*,oss:*,log:*

参数	说明	示例
configuration_item	资源的配置详情。	请参见自定义规则的数据结构如何。

> **说明** 本段代码以检测RAM用户是否开启MFA为例。如果您需要通过其他参数检测RAM用户，请参见自定义规则的数据结构是什么。

iii. 单击右上角的**保存并部署**。

5. 新建自定义规则。
   i. 登录配置审计控制台。
   ii. 在左侧导航栏，单击**规则**。
   iii. 在**规则**页面，单击**新建规则**。
   iv. 在**新建规则**页面，单击**新建自定义规则**。
   v. 在**基本属性**页面，**函数Arn**的**所在地域**选择**华东2（上海）**、**服务**选择**Ram_User**、**函数**选择**RamDangerousPolicyUserBindMFA**，**规则名称**输入**RamUserMFA**，**规则触发机制**选择**配置变更**和**周期执行**，**触发频率**选择**1小时**，单击**下一步**。

vi. 在**评估资源范围**页面，先单击**自定义资源类型**，再选择规则关联的资源类型为**Ram用户**，单击**下一步**。

vii. 在**参数设置**页面，单击**添加规则入参**，**规则入参名称**输入**dangerousActions**，**期望值**输入**ecs:*,oss:*,log:***，单击**下一步**。

> 说明 **规则入参名称**和**期望值**必须与步骤 4中的参数rule_parameters和input_actions保持一致。

viii. 在**修正设置**页面，单击**下一步**。

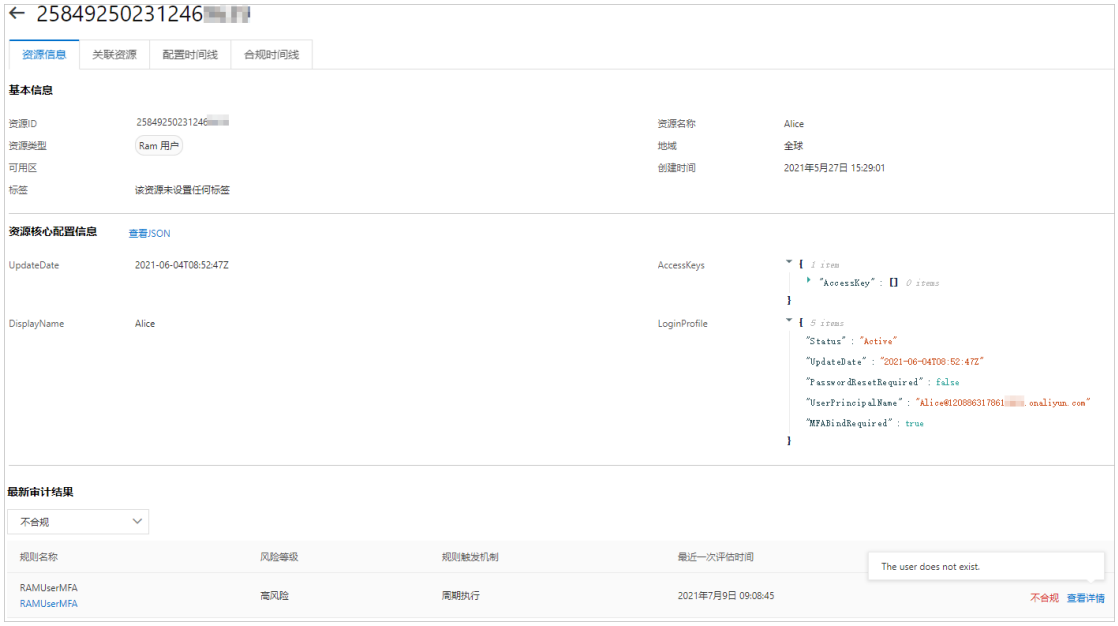
ix. 在**预览并保存**页面，单击**提交**。

6. 查看RAM用户Alice的检测结果。

i. 在**新建规则**成功页面，单击**查看规则详情**。

ii. 单击**检测结果**页签。

iii. 在**关联资源的合规结果**区域，单击目标资源ID链接，查看该资源的合规结果。



7. 设置资源合规事件投递。

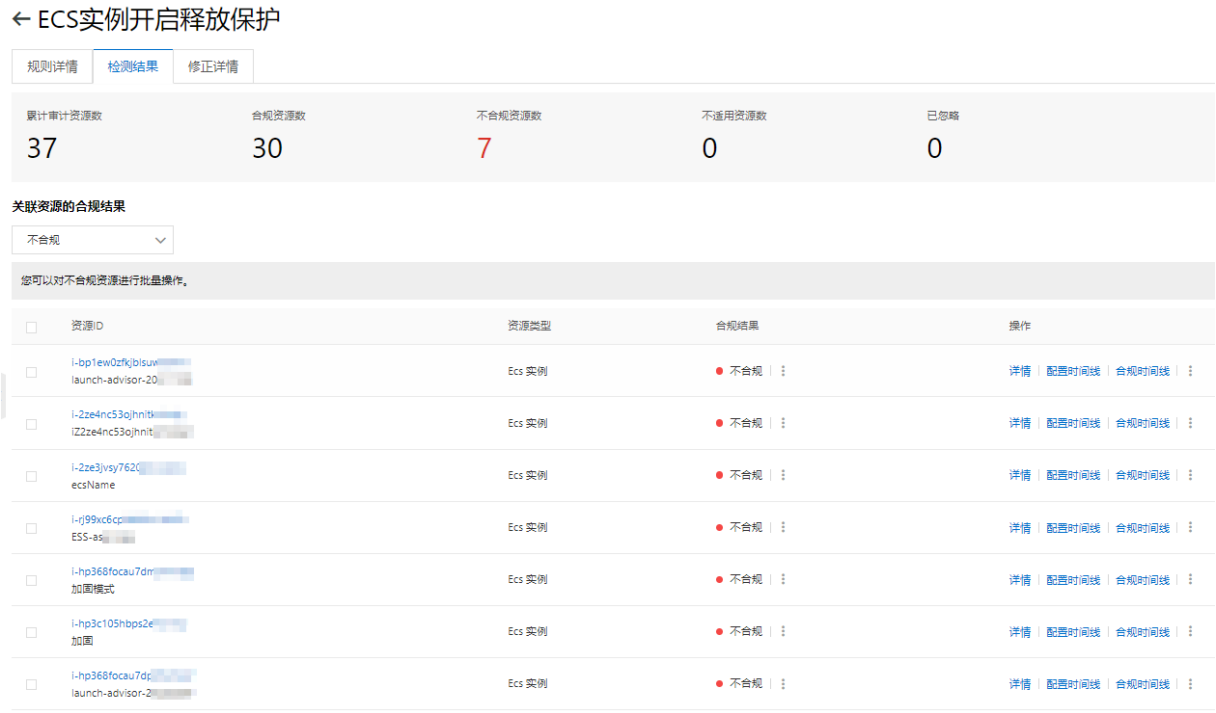
   设置资源合规事件MNSTestConfig投递到消息服务MNS的指定主题（Topic）后，您会收到来自消息服务MNS的不合规通知。具体操作，请参见设置投递数据到消息服务MNS。

7.3. 通过云监控实现不合规事件的报警通知

当资源配置不合规时，配置审计会将不合规事件自动投递到云监控。您可以在云监控中查看不合规事件，还可以基于云监控的事件报警功能触发报警通知。

应用场景

您在配置审计控制台通过托管规则“ECS实例开启释放保护”创建一条风险等级为“高风险”的规则。配置审计自动审计当前账号下所有ECS实例，其中部分ECS实例的合规结果为不合规，如下图所示。



步骤一：创建规则

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击右上角的**新建规则**。
4. 在**新建规则**页面，搜索托管规则**ECS实例开启释放保护**。
5. 单击**应用规则**。
6. 在**基本属性**页面，规则名称、风险等级和备注均保持系统默认值，单击**下一步**。
7. 在**评估资源范围**页面，资源类型保持默认值，单击**下一步**。
8. 在**参数设置**页面，单击**下一步**。
9. 在**修正设置**页面，单击**下一步**。
10. 在**预览并保存**页面，确认规则设置，单击**提交**。
11. 查看规则的检测结果。

    先单击**查看规则详情**，然后单击**检测结果**，您可以查看该规则对ECS实例的检测结果。

步骤二：创建报警

1. 创建报警联系人。
    i. 登录云监控控制台。
    ii. 在左侧导航栏，选择**报警服务 > 报警联系人**。
    iii. 在**报警联系人**页签，单击**新建联系人**。

iv. 在**设置报警联系人**面板，填写报警联系人的姓名、手机号码、邮箱、旺旺和钉钉机器人，**报警通知信息语言**保持默认值**自动**。

> **说明** **自动**表示云监控根据当前阿里云账号注册时的语言，自动适配报警通知信息的语言。

v. 信息验证无误后，单击**确认**。

vi. （可选）报警联系人邮箱和手机号码激活。

如果您设置了报警联系人的邮箱和手机号码，默认处于**等待激活**状态。报警联系人需要根据邮件和短消息中的激活链接，在24小时内进行激活，否则无法收到报警通知。激活后，您可以在报警联系人列表中看到目标报警联系人的手机号码和邮箱。

2. 创建报警联系组。

i. 在**报警联系人**页面，单击**报警联系组**页签。

ii. 在**报警联系组**页签，单击**新建联系组**。

iii. 在**新建联系组**面板，填写报警联系组的组名，并选择报警联系人。

iv. 单击**确认**。

3. 创建系统事件报警规则。

配置审计将所有不合规事件投递到云监控后，您可以根据所需创建报警规则，用于接收报警通知。

i. 在左侧导航栏，选择**事件监控 > 系统事件**。

ii. 单击**事件报警规则**页签。

iii. 单击**创建报警规则**。

iv. 在**创建/修改事件报警**面板，设置系统事件的报警规则参数。

- **基本信息**：根据所需输入系统事件的报警规则名称。
- **事件报警规则产品类型**选择**配置审计**，**事件类型**选择Notification，**事件等级**选择**信息**，**事件名称**选择**不合规事件**，**关键词过滤**输入Critical，**条件**选择**满足不包含上面任何一个关键词**。
- **报警方式**：先单击**报警通知**前面的复选框，然后选择**联系人组**为步骤 2创建的报警联系组，选择**通知方式**为Info（**邮件+钉钉机器人**）。

v. 单击**确定**。