阿里云
配置审计

用户指南

文档版本：20190918

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 资源列表

1.1 查看资源列表

开通配置审计服务后，您可以获得账号下跨区域聚合的资源清单，并通过检索找到指定资源实体进而查看资源的详细配置。

说明：由于配置审计仅支持部分阿里云产品，资源清单中可能只有您的部分资源。配置审计服务正在逐步扩大对阿里云产品的覆盖，努力为您提供更加完整的资源清单。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击资源列表，可以看到您账号下在服务支持范围内发现的资源列表。

在资源列表中可以看到资源Id、名称、创建时间等常规信息，下面为您解释列表中看到的其他信息：

1. 标签。您管理资源时，为资源设置的标签（Tag）信息，若您没有配置则该项为空。
2. 监控状态。配置审计通过监控您的资源变更帮助您记录变更历史和自动审计资源配置合规性。该项表示，基于您在配置审计设置的监控范围，该资源目前的被监控状态。关于监控范围管理，您可以参见管理资源监控范围。
3. 资源类型。资源类型定义请参见#unique_6/unique_6_Connect_42_section_f3x_kwn_kwh，配置审计将持续扩大对云产品的支持范围，请关注服务支持的资源类型。

1.2 搜索资源

当您在阿里云多个区域部署资源时，资源的搜索非常困难。您需要先找到正确的区域才能搜索到想找的资源。配置审计的资源跨区域聚合资源列表可以作为您资源管理的集中入口。

基于资源列表，您可以通过所属区域、所属产品、资源类型、监控状态作为过滤条件快速筛选资源，您也可以直接使用资源Id、名称来搜索指定的资源，帮助您快捷找到账号下各区域的资源。

1.3 查看资源当前配置

基于资源列表，通过筛选和检索找到指定资源后，您可以查看各个资源的当前配置信息。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击资源列表。
3. 使用过滤器检索资源，或使用资源Id找到指定资源。

4. 单击资源Id可看到资源的关键信息，包括资源Id、名称、创建时间、所属区域。单击展开可看到详细完整的配置信息。

1.4 管理资源

找到指定资源后，您可以快速跳转到该资源在云产品控制台的管理页面，进一步操作资源。

1. 登录配置审计控制台。
2. 在左侧菜单，单击资源列表。
3. 通过检索找到指定资源后，单击操作列的管理资源。

2 资源监控范围

2.1 管理资源监控范围

配置审计通过监控您账号下的资源变更，实现变更记录和实时的合规审计。您可以通过简单配置来管理资源监控的范围。

1. 您开通配置审计服务时，默认添加所有服务支持的资源类型进入监控范围。
2. 若您的监控范围选择为“服务支持的所有资源类型”，当配置审计支持新的资源类型时，会默认添加到监控范围内。
3. 若您有其他定制化的监控范围策略，您可以前往“管理监控范围”页面，根据页面提示设置监控的资源类型。

暂停监听

1. 当您把某资源类型移出监控范围，则您账号下该资源类型的实体资源将停止记录配置变更，直到您下次将其移回时再重新开始记录。这期间的配置变更记录无法追回。
2. 处于监控范围的资源类型的实体资源，在资源列表中的“监控状态”会显示为“监控中”，移出的资源类型的实体资源，在资源列表中的“监控状态”会显示为“暂停监听”。

恢复监听

1. 在“管理监控范围”页面，把资源类型加回到监控范围，则状态从“暂停监听”变回“监听中”。
2. 暂停监听期间发生的配置变更，无法补回。

2.2 服务支持的资源类型

参见#unique_8。

3 资源配置历史

3.1 查看资源配置时间线

配置审计记录监控中的资源的每一次配置变更详情，并整理为#unique_6/unique_6_Connect_42_section_qtr_675_v4f，也就是资源配置随时间推进的演变记录。

配置时间线上的点

- 起点：对于您开通配置审计服务时已保有的资源，配置时间线的起点是服务开通时间。对于您开通配置审计服务后新创建的资源，配置时间线起点是资源创建时间。
- 节点：配置审计定隔10分钟刷新资源配置快照，若发现与10分钟前的快照存在差异，则会呈现一个配置变更记录，就是配置时间线上的一个节点。
- 断点：若您把某资源类型移出监控范围，则相关实体资源均停止监控，也不会更新配置时间线，直到您把资源类型移回监控范围，再重新开始监控跟踪。停止监控期间的变更历史不可追溯。

配置时间线的内容

配置时间线属于某具体资源实体，是一组历史资源配置记录。

- 您先看到的是资源当前的配置快照，向下每一个节点是一次历史配置快照。
- 每个节点包括当次变更结果配置详情，包括与上次变更结果的对比详情，还包括当次变更涉及的#unique_15。

【注意】配置审计每10分钟整理一次资源变更，若在10分钟窗口期内资源发生配置变更又快速恢复到变更之前，则无法感知相应变更，也就无法呈现对应的操作事件。

您可以在线查阅上述信息，也可以通过API获取或下载到您自己的OSS存储空间，方便您离线整合分析。OpenAPI和快照下载能力正在快速迭代中，敬请期待。

3.2 查看资源变更事件

配置审计服务与操作审计服务打通，您除了能看到窗口期前后配置的变更之外，还能看到使配置发生如此变更的操作事件列表和事件详情，包括用户、IP、时间、API名称等操作信息。

若您未开通操作审计服务，则该部分内容显示为空，您可前往 操作审计 产品完成开通。

4 资源合规审计

4.1 规则的定义及运行原理

合规性即代码，规则是企业合规要求的代码式诠释，把合规条款对应成一段规则代码，代码的本质是对一项资源配置的判断逻辑。配置审计服务使用函数计算服务的函数来承载规则代码，称之为“规则函数”，在配置审计服务中引用规则函数后，配置关联的资源、触发机制等信息后，就构成了配置审计服务中的规则。

在实际的合规监控中，就是通过实时的资源配置变更触发规则函数的执行，来判断某个资源配置是否合规的。多个规则的组合就实现了对整个资源配置的合规监控。

规则的定义

规则的本质是一段判断逻辑，判断资源的某一个配置项是否合规，具备以下特点：

- 规则函数的入参是通过资源的查询API，可以获取的配置项，如资源的规格、所属Region、名称、状态、端口/网口开关状态等。入参名称与配置项名称保持一致。
- 规则函数的逻辑是对入参值的判断，判断逻辑由您的代码决定，比如当SLB的HTTPS监听状态为“开”时，认为“合规”。那么入参就是SLB的资源上代表HTTPS监听状态的配置字段，而当该字段值表示“关闭”时，认为“不合规”。
- 规则函数的出参是合规的结果。

规则指向的资源类型

在函数计算中定义完的规则函数，此时还不具有目标指向性，并没有声明指向哪个资源类型，且不同资源间可能存在同名的配置参数，仅仅根据规则函数的入参设置无法实现准确的合规评估。

所以需要在配置审计中，将已经创建好的规则函数与确定的资源类型绑定。当该类型类型的实体资源发生配置变更时，系统先找到资源关联的规则有哪些，再根据具体哪个配置发生了变更来决定要触发哪条规则。

规则的触发

上述已经提到，资源发生配置变更时，配置审计能够准确知道是哪些配置发生了变更。以变更了的参数作为入参的规则函数就会被触发执行，评估本次变更的结果是否合规。所以，规则函数的入参名称要与实际资源配置的参数名称保持一致。

此外，配置审计还支持您将规则设置为定时触发，可定期为您执行合规评估。

合规评估的结果

配置审计将获取的变更结果作为入参传入规则函数，规则函数返回合规结果给配置审计，在配置审计控制台以各种方式为您呈现和统计。可参考查看规则评估结果的说明。

您可以在函数计算服务中自定义规则函数，参见#unique_20。也可以使用配置审计为您准备的预设规则，参见#unique_21。

4.2 阿里云预设规则列表

以下为配置审计服务为您准备好的规则，您在控制台创建规则时可直接选用以下规则。该规则列表将支持更新。

若您有额外的规则需求，可通过工单提交给我们，我们评估后会酌情支持，将具备普遍适用性的规则实现为系统预设规则。

下述规则列表中，“适用的资源类型”是以Namespace的方式呈现，您可以在#unique_8列表中查阅对应的中文描述。

检查您当前账号是否启用了操作审计产品

- 规则函数名称：actiontrail-enabled
- 适用的资源类型：ACS::ActionTrail::Trail
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：账号开启操作审计服务，视为“合规”
- 规则使用场景说明：为满足企业内部合规，一般要求账号开启操作审计服务，实时监控并记录账号下对资源进行的操作日志。使用该规则检测账号是否开启操作审计

检查ECS实例的CPU数量不能低于某阈值

- 规则函数名称：ecs-您可以cpu-min-count-limit
- 适用的资源类型：ACS::ECS::Instance
- 规则入参：cpuCount=阈值，cpuCount是ECS实例的核数，阈值需您在控制台定义
- 触发机制：配置变更
- 规则合规说明：当您账号下的ECS实例cpuCount大于等于您设置的阈值，视为“合规”
- 规则使用场景说明：您可以使用该规则监控账号下的ECS实例规格，CPU数量不能低于您设置的阈值

检查账号下的ECS实例是否为指定的实例类型

- 规则函数名称：ecs-desired-instance-type

- 适用的资源类型：ACS::ECS::Instance
- 规则入参：instanceTypes=阈值，阈值为逗号分隔的 ECS 实例类型列表 (例如“t2.small, m4.large, i2.xlarge”)，您需要在控制台定义该阈值
- 触发机制：配置变更
- 规则合规说明：您账号下所有的ECS实例类型均已在阈值中列举出，视为“合规”
- 规则使用场景说明：您可以使用该规则限定账号下只能购买某几种类型的ECS实例

检查处于连接状态的ECS磁盘是否已加密

- 规则函数名称：ecs-disk-encrypted
- 适用的资源类型：ACS::ECS::Disk
- 规则入参：kmsIds=阈值，若您不配置阈值，则规则只会检测磁盘是否加密；若您配置了阈值，规则会检测加密的密钥Id是否在您设定的阈值中。kmsIds支持多个密钥Id用“,”分隔
- 触发机制：配置变更
- 规则合规说明：您账号下所有处于关联状态的磁盘均已加密；若您配置阈值，则磁盘加密的Id需存在您列出的阈值中，视为“合规”
- 规则使用场景说明：您可以使用该规则监控磁盘的加密状态和加密合规

检查ECS磁盘是否在使用中

- 规则函数名称：ecs-disk-in-use
- 适用的资源类型：ACS::ECS::Disk
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：您账号下所有ECS磁盘处于使用中，视为“合规”
- 规则使用场景说明：您可以使用该规则监控磁盘的使用状态

检查ECS实例是否已关联到VPC实例

- 规则函数名称：ecs-instances-in-vpc
- 适用的资源类型：ACS::ECS::Instance
- 规则入参：vpcIds=阈值，若您不配置阈值，则规则只会检测ECS实例是否已关联到某VPC上；若您配置了阈值，规则会检测ECS实例关联的VPC是否在您设定的阈值中。vpcIds支持多个VpcId用“,”分隔
- 触发机制：配置变更
- 规则合规说明：您账号下所有ECS实例已关联到VPC；若您配置阈值，则关联的VpcId需存在您列出的阈值中，视为“合规”

- 规则使用场景说明：您可以使用该规则监控您的ECS实例是否都挂载到VPC上，或是否够挂载到指定的VPC上

检查ECS实例的GPU数量不能低于某阈值

- 规则函数名称：ecs-gpu-min-count-limit
- 适用的资源类型：ACS::ECS::Instance
- 规则入参：gpuCount=阈值，gpuCount为gsc实例包含cpu数量，阈值需要您在控制台定义
- 触发机制：配置变更
- 规则合规说明：您账号下的gsc实例的cpu数量需大于等于您设置的阈值，视为“合规”
- 规则使用场景说明：您可以使用该规则监控gsc实例的cpu数量合规

检查ECS实例的内存容量不小于某阈值

- 规则函数名称：ecs-memory-min-size-limit
- 适用的资源类型：ACS::ECS::Instance
- 规则入参：memorySize=阈值，memorySize是ECS实例内存容量，您需要在控制台配置阈值
- 触发机制：配置变更
- 规则合规说明：您账号下的ECS实例内存容量大于等于您设置的阈值，视为“合规”
- 规则使用场景说明：您可以使用该规则监控ECS实例内存容量大小合规

检测 OSS Bucket是否允许公网访问

- 规则函数名称：oss-bucket-public-acl-check
- 适用的资源类型：ACS::OSS::Bucket
- 规则入参：无
- 触发机制：周期执行
- 规则合规说明：账号下的 OSS Bucket 均不允许公网访问，视为“合规”
- 规则使用场景说明：您可以使用该规则检测您的OSS Bucket公网访问状态

检查 RDS 实例的CPU数量不小于某阈值

- 规则函数名称：rds-cpu-min-count-limit
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：cpuCount=阈值，cpuCount是RDS实例cpu数量，您需要在控制台配置阈值
- 触发机制：配置变更
- 规则合规说明：您账号下的RDS实例cpu数量大于等于您设置的阈值，视为“合规”
- 规则使用场景说明：您可以使用该规则监控RDS实例cpu数量合规

检查账号下的RDS实例是否为指定的实例类型

- 规则函数名称：rds-desired-instance-type
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：instanceTypes=阈值，阈值为逗号分隔的 RDS 实例类型列表 (例如"rds.mysql.s2.large,mysql.n1.micro.1")，您需要在控制台定义该阈值
- 触发机制：配置变更
- 规则合规说明：您账号下所有的RDS实例类型均已在阈值中列举出，视为“合规”
- 规则使用场景说明：您可以使用该规则限定账号下只能购买某几种类型的RDS实例

检查RDS实例是否具备高可用能力

- 规则函数名称：rds-high-availability-category
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：账号下RDS实例具备高可用能力，视为“合规”
- 规则使用场景说明：您可以使用该规则监控您账号下RDS实例的高可用能力配置

检查ECS实例是否已关联到VPC实例

- 规则函数名称：rds-instances-in-vpc
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：vpcIds=阈值，若您不配置阈值，则规则只会检测RDS实例是否已关联到某VPC上；若您配置了阈值，规则会检测RDS实例关联的VPC是否在您设定的阈值中。vpcIds支持多个VpcId用“,”分隔
- 触发机制：配置变更
- 规则合规说明：您账号下RDS实例已关联到VPC；若您配置阈值，则关联的VpcId需存在您列出的阈值中，视为“合规”
- 规则使用场景说明：您可以使用该规则监控您的RDS实例是否都挂载到VPC上，或是否够挂载到指定的VPC上

检查RDS实例的存储空间不小于某阈值

- 规则函数名称：rds-instance-storage-min-size-limit
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：storageSize=阈值，storageSize是rds实例存储空间，您需要在控制台配置阈值
- 触发机制：配置变更
- 规则合规说明：您账号下的RDS实例存储空间大于等于您设置的阈值，视为“合规”

- 规则使用场景说明：您可以使用该规则监控RDS实例存储空间大小合规

检查RDS实例的内存容量不小于某阈值

- 规则函数名称：rds-memory-min-size-limit
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：memorySize=阈值，memorySize是RDS实例内存容量，您需要在控制台配置阈值
- 触发机制：配置变更
- 规则合规说明：您账号下的RDS实例内存容量大于等于您设置的阈值，视为“合规”
- 规则使用场景说明：您可以使用该规则监控RDS实例内存容量大小合规

检查RDS实例是否支持多可用区

- 规则函数名称：rds-multi-az-support
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：账号下RDS实例支持多可用区，视为“合规”
- 规则使用场景说明：您可以使用该规则监控RDS实例对多可用区的支持合规

检查RDS实例是否允许公网访问

- 规则函数名称：rds-public-access-check
- 适用的资源类型：ACS::RDS::DBInstance
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：账号下RDS实例不允许公网访问，视为“合规”
- 规则使用场景说明：您可以使用该规则监控RDS实例的公网访问合规

检查指定资源是否具有指定标签

- 规则函数名称：
- 适用的资源类型：ACS::RDS::DBInstance；ACS::SLB::LoadBalancer；ACS::ECS::Disk；ACS::ECS::SecurityGroup；ACS::ECS::Instance；ACS::ECS::NetworkInterface
- 规则入参：tag1Key，指定标签的Key；tag1Value，指定标签的值。
- 触发机制：配置变更
- 规则合规说明：关联的资源类型下实体资源均已有指定标签，视为“合规”
- 规则使用场景说明：您可以使用该规则监控您的资源是否打了完整的标签

检查安全组是否配置为0.0.0.0/0

- 规则函数名称：sg-public-acces-check
- 适用的资源类型：ACS::ECS::SecurityGroup
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：账号下ECS安全组配置不为“0.0.0.0/0”，视为“合规”
- 规则使用场景说明：您可以使用该规则监控ECS安全组是否为有效配置

检查负载均衡是否开通HTTPS监听

- 规则函数名称：slb-listener-https-enabled
- 适用的资源类型：ACS::SLB::LoadBalancer
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：负载均衡开启HTTPS监听，视为“合规”
- 规则使用场景说明：您可以使用该规则监控负载均衡监听合规

检查弹性公网IP是否绑定到ECS或SLB实例上

- 规则函数名称：eip-attached
- 适用的资源类型：ACS::VPC::EipAddress
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：EIP已绑定到ECS或SLB实例，视为“合规”
- 规则使用场景说明：您可以使用该规则监控弹性公网IP的生效状态合规

检查ECS实例是否绑定公网Ip

- 规则函数名称：ecs-instance-no-public-ip
- 适用的资源类型：ACS::ECS::Instance
- 规则入参：无
- 触发机制：配置变更
- 规则合规说明：ECS实例未直接绑定公网IP，视为“合规”。该规则仅适用于 IPv4 协议
- 规则使用场景说明：您可以使用该规则监控ECS的公网访问合规

4.3 自定义规则的开发

配置审计服务为您提供数十款预设规则，参见阿里云预设规则列表。同时也支持您自定义规则函数。

自定义规则与系统预设规则的运行原理相同，区别仅在于系统预设规则是配置审计服务已经在函数计算服务中构建好了规则函数，使用时您直接在配置审计控制台选择要用的函数即可；而自定义规则需要您自己提前在函数计算服务中定义好规则函数，使用时在配置审计控制台需要录入规则函数的ARN。

通过自定义规则您可以更好的支持个性化的合规场景。

自定义规则的创建

一共分为两个步骤，第一步是在函数计算服务创建函数，第二步是跟预设规则一样，在配置审计服务创建规则。本文重点讲解第一步，第二步请参见创建规则的说明。

要创建一个自定义规则，首先要在函数计算（FC，以下将使用FC指代函数计算）控制台创建一个FC函数。目前在函数计算服务中，支持的编程语言有Java8、Nodejs6、Nodejs8、Python2.7、Python3、PHP7.2、dotnetcore2.1。Java8和dotnetcore值支持代码包上传（包含oss上传），其他语言级支持代码包上传，也支持在线编辑。函数计算相关内容，请参考：https://help.aliyun.com/product/50980.html 。

接下来以一个规则样例为您讲解如何自定义规则。

- 规则场景：评估ECS实例是否由特定镜像启动
- 函数语言使用Python3

在函数计算服务中创建规则函数并在配置审计引用

函数计算创建内容，请参考：https://help.aliyun.com/product/50980.html

- 在函数计算创建规则函数后，会自动生成一个函数ARN。函数ARN可以在创建好的FC函数的概览页面中查看。

· 在配置审计服务控制台实际引用该规则函数时，需要填入上图的ARN。

规则函数的代码构建

规则的本质是一段逻辑判断代码，这段代码放在刚刚创建的规则函数中。在实际的持续审计中，通过触发该规则函数的执行来实现评估。

- 以下为规则样例的示例代码。本函数代码主要有两个函数，handler为入口函数，即自定义合规触发时调用的函数。hander需在在构建FC函数时进行配置。

- 另一个函数为put_evaluations，在handler中调用，返回合规结果。

```
#!/usr/bin/env python
# -*- encoding: utf-8 -*-
'''
@File    :   index.py
@Time    :   2019/07/29 18:19:00
@Author  :   wb510457
@Version :   1.0
@License :   (C)Copyright 2017-2018, Alibaba inc.
@Desc    :   None
'''

# here put the import lib
import logging
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkcore.request import CommonRequest

logger = logging.getLogger()

#函数处理入口
def handler(event, context):
    """
    处理函数
    :param event: 事件
    :param context: 上下文
    :return: 评估结果
    """
    # Event数据格式转换
    evt = json.loads(event)
    if not evt:
        return None

   #入参
    rule_parameters = evt.get('ruleParameters')
    #入参--镜像实例id
```

```
    image_id = rule_parameters.get(imageIds)
    #用户在fc中回调
    result_token = evt.get('resultToken')
    #函数执行参数信息
    invoking_event = evt.get('invokingEvent')

    # 初始化返回值
    compliance_type = 'NOT_APPLICABLE'
    annotation = None

    # 获取配置项
    configuration_item = invoking_event.get('configurationItem')
    if not configuration_item:
        logger.error('Configuration item is empty.')
        return None
    #进行评估
    if image_id in configuration_item
      compliance_type = 'COMPLIANCE'
    if not image_id in configuration_item
      compliance_type = 'NON_COMPLIANCE'
   #执行命令开始时间
    ordering_timestamp = configuration_item.get('captureTime')
    #资源id
    resource_id = configuration_item.get('resourceId')
    #资源类型
    resource_type = configuration_item.get('resourceType')

    # 评估结果
    evaluations = [
        {
            'complianceResourceId': resource_id,
            'complianceResourceType': resource_type,
            'orderingTimestamp': ordering_timestamp,
            'complianceType': compliance_type,
            'annotation': annotation
        }
    ]

    # 回写评估结果--评估结果数据写入
    put_evaluations(context, result_token, evaluations)
    return evaluations
#回写评估结果 -- 评估结果数据写入
def put_evaluations(context, result_token, evaluations):
    """
    回调Config Open API 回写评估结果
    :param context: 函数计算上下文
    :param result_token: 回调令牌
    :param evaluations: 评估结果
    :return: None
    """
    # 创建AcsClient实例
    client = AcsClient(
        context.credentials.access_key_id,
        context.credentials.access_key_secret,
        context.region,
    )

    # 创建request，并设置参数
    request = CommonRequest()
    request.set_domain('config.cn-hangzhou.aliyuncs.com')
    request.set_version('2018-12-24')
    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: %s, response: %s' %
                    (request, response))
    except Exception as e:
        logger.error('PutEvaluations error: %s' % e)
```

规则函数的入参

event参数。在规则函数中输入的入参信息保存在ruleParameters中，其他内容为在规则触发时自动生成事件信息。JSON格式如下所示：

```
{
    version:"版本号",
    orderingTimestamp:"命令执行开始时间",
    invokingEvent:{
      messageType:"消息类型",
        configurationItem: {
          "accountId":"用户id",
            "arn":"资源ARN",
            "availabilityZone":"可用区",
            "regionId":"区域id",
            "configuration":"字符串形式的资源本身配置信息,各类资源有所不同",
            "configurationDiff":"配置变更内容",
            "relationship":"关系",
            "relationshipDiff":"关系内容变更",
            "captureTime":"捕获时间",
            "resourceCreationTime":"资源创建时间",
            "resourceStatus":"资源状态",
            "resourceId":"资源ID",
      "resourceName":"资源名称",
            "resourceType":"资源类型",
            "supplementaryConfiguration":"补充配置",
            "tags":"标签"
        },
        notificationCreationTimestamp:"事件消息生成时间"
    },
    ruleParameters: {
      "key":"value"
    },
    resultToken:"用户在FC中的回调信息"
}
```

context参数。上下文信息，规则触发时自动带入

- context.credentials.access_key_id:"accessKey值"
- context.credentials.access_key_secret:"accessSecret值"
- context.region:"区域信息"

以上完成自定义规则在函数计算服务的创建后，copy函数的ARN，就可以在配置审计服务继续进行规则的创建了。

4.4 规则管理

4.4.1 规则列表

在配置审计服务控制台左侧菜单单击“规则管理”。

初次进入页面列表是空的，您完成规则创建之后，可在该列表看到您所有的规则。当前支持按照合规状态或规则的运行状态进行筛选。

在列表页您可以看到规则的基本信息，其中需要注意的是“合规评估情况”和“规则状态”。

合规评估情况

该列代表该规则当前执行情况，有四个状态：

状态值	描述
合规	表示该规则的历史评估结果均为“合规”。
资源不合规（N）	表示该规则的历史评估中有N个资源出现不合规。您需要进入规则详情，查看具体哪些资源不合规。
数据不足	表示该规则暂未被触发执行过，所以无法判断是否合规。
不适用	该状态的范围比较广泛，指该规则被触发执行过，但配置审计并未拿到符合预期的评估结果，可以认为是规则执行异常的标记。

规则状态

该列表示规则自身的运行状态，有五个状态：

状态值	描述
应用中	表示规则目前处于监听状态，一旦出现相关的配置变更，就会开始评估。若您希望保留规则配置，同时暂停合规审计，那么可以在规则管理列表页对应规则条目后方找到操作列，依次点击“更多——停用规则”使规则进入“已停用”状态。
评估中	表示规则已被触发，正在进行评估。
删除评估结果中	配置审计支持您删除某规则的评估结果，方便您在正式的合规监控开始前，清空测试数据。

状态值	描述
已停用	表示规则目前处于停止监听状态，虽然规则配置仍然存在，但永远不会被触发执行。您可以在规则管理列表页面对应规则条目的后方找到操作列，依次点击“更多——启用规则”使规则重新进入“应用中”状态。
删除中	表示规则被操作“删除”，当前正在删除处理中。

4.4.2 创建规则

规则的本质是放在函数计算服务的函数中的逻辑判断代码，您可以引用配置审计为您准备的预设规则，参见#unique_21。也可以在函数计算服务中自定义规则函数，参见#unique_20。您还可以把您的需求通过工单提交给我们，评估后有机会实现为系统预设规则。

在规则管理页面，点击“新建规则”：

1. 选择规则创建方式：您可以选择一个系统预设规则，也可以选择“自定义规则”。注意，如果您选择自定义规则，您需要在下一步填写您在函数计算服务中配置好的规则函数的名称。
2. 基本信息：您需要给规则设置一个可读的名称，填写“备注”即描述内容，然后填写规则函数的名称。（若为系统预设规则，函数名称是预填好的。）
3. 触发机制：选择规则的触发方式。支持实时配置变更触发和周期执行两种方式。实时配置变更触发是指当配置审计服务监控到规则关联的资源类型发生配置变更时，变更的实际内容与规则的入参相关联，则触发规则执行。周期执行目前支持每1、3、6、12、24小时定时执行规则。
4. 监控范围：配置规则关联的资源类型，规则将监听您账号下该资源类型的所有实体资源。一个规则可以关联多个资源类型。
5. 规则参数：若您选择系统预设规则，您需要为规则既定参数设置判断的阈值。若您选择自定义规则，则需要设置规则入参的Key和判断阈值。注意规则参数的Key是规则函数的入参名称，该入参名称需要跟资源实际的配置名称一致。
6. 点击“确定”，规则创建完毕且状态为“应用中”。

4.4.3 规则修改和删除

简单介绍规则更多的管理操作。

规则的修改/停止/启动/手动评估/删除

- 规则修改：与规则创建相似，您可以编辑修改规则的基本信息、运行信息配置。您更改规则时，规则仍按照原配置执行，您保存更改后才会用新配置运行。
- 停止规则：若您希望保留规则配置，同时暂停合规审计，那么可以在规则管理列表页对应规则条目后方找到操作列，依次点击“更多——停用规则”使规则进入“已停用”状态。

- 启动规则：您可以在规则管理列表页面“已停用”规则条目的后方找到操作列，依次点击“更多——启用规则”使规则重新进入“应用中”状态。
- 手动执行评估：您可以在规则列表页右上角、规则详情页右上角“重新评估”、规则详情页关联资源列表右上角，三个位置执行单个规则或多个规则的手动评估。
- 删除评估结果：配置审计支持您删除某规则的评估结果，方便您在正式的合规监控开始前，清空测试数据。您可在规则详情下方“关联的资源列表”右上角操作。
- 删除规则：规则需先停用，后删除。删除后规则配置将不做保留。

4.4.4 查看规则详情

规则详情主要包括以下几部分信息。

规则详情

在规则列表页面对应规则条目后点击“详情”，您可以查看该规则的全部信息。

规则评估统计

在规则详情页顶部有该规则执行的概况统计：（统计中说的“资源数”指真实的实体资源，而不是资源类型数。）

数据项	描述
累计审计资源数	该规则从启用初始至今，累计评估过的资源数。包括您已经释放的资源。
当前关联资源数	该规则当前有效关联的账号下的资源数，不包括已经释放的资源。
合规资源数	当前关联资源中，上一次评估结果为“合规”的资源数量。
不合规资源数	当前关联的资源中，上一次评估结果为“不合规”的资源数量。

规则基本信息

- 资源名称、创建时间、上一次评估时间等基本信息，不一一列举，以页面内容为准。
- 资源的触发机制、监控范围等运行配置。

规则当前关联的资源列表

规则的监控范围是以资源类型作为维度的，该列表是资源实体的列表。例如某规则关联到云服务器ECS的实例上，该账号下有20台ECS实例，那么列表就是20个ECS实例。

该列表展示实体资源的Id，以及最近一次的评估结果。您还可以通过后方的快捷操作，快速跳转到该资源对应的配置时间线、合规时间线来纵向的查看该资源的详情，同时您可以快速跳转到云产品控制台，进行资源管理。

4.5 查看合规结果

4.5.1 查看规则评估结果

目前在配置审计控制台，有三处可以查看规则的执行情况：

- 概览页右侧边栏“合规性统计”。规则：不合规规则数/合规规则数；资源：不合规资源数/合规资源数。
- 规则管理列表页，每个规则的当前“合规评估情况”，具体可参见规则列表对“合规评估情况”的解读。
- 每个规则的规则详情页面顶部，有该条规则的评估统计，具体可参见规则详情中的说明。

4.5.2 资源合规时间线

在配置审计服务中，每个资源实体有属于自己的合规时间线记录。当该资源被规则评估时，将产生合规评估记录，持续的合规评估形成了资源的合规时间线。

合规时间线上的点

- 起点：该资源第一次被规则评估的时间，资源被规则评估可能是定时周期评估、手动执行评估或实时的配置变更触发评估。
- 节点：每一次的规则评估都会形成合规时间线上的一个节点，每次评估可能涉及1个及以上的规则。
- 断点：不同于资源的配置时间线（查看资源配置时间线），规则评估是根据实时的配置变更情况触发的，并不具备连续性，也就不存在断点。

合规时间线的内容

- 合规时间线属于某具体资源实体，是一组历史合规评估记录。
- 在合规时间线的左侧，每个节点除了标注时间之外，还会清晰的标注该次合规评估是通过哪种触发机制发起的，这也说明了资源被评估的原因，包括手动、周期执行、变更触发。
- 在合规时间线的左侧，每个节点还会标注该次评估的结果“合规”或“不合规”。方便您快速找到需要关注的节点。
- 每个节点的详情包括资源基本信息、关联的规则列表（规则及该次评估结果），若该次评估是由实时变更触发的，则还会显示本次变更的详细内容，以便您尽快定位“不合规”的具体配置。

您可以在线查阅上述信息，也可以通过API获取或下载到您自己的OSS存储空间，方便您离线整合分析。OpenAPI和快照下载能力正在快速迭代中，敬请期待。