配置审计

操作指南

腾讯云

文档目录

操作指南
资源
查看资源列表

最近更新时间：2024-04-10 22:07:32

1. 登录 配置审计控制台，单击**资源**菜单，可进入资源列表，查看配置审计最近一次更新的资源清单。

2. 所有资源支持跨地域检索。您也可以通过资源 id、资源名称、资源类型、资源状态、标签、地域等进一步检索资源信息。

> **注意：**
> 为了简化您的查看体验，对于访问管理中的策略这一资源类型（QCS::CAM::Policy），当前资源列表仅展示自定义策略，不展示系统预设策略。

3. 单击资源列表中的**资源名称**，可跳转至**资源详情**页面，查看资源的详细信息；单击**管理资源**，可跳转至资源对应的产品控制台，对资源进行进一步的管理；单击**资源时间线**，可跳转至资源时间线页面，查看资源的配置变更历史记录。

查看资源详细信息

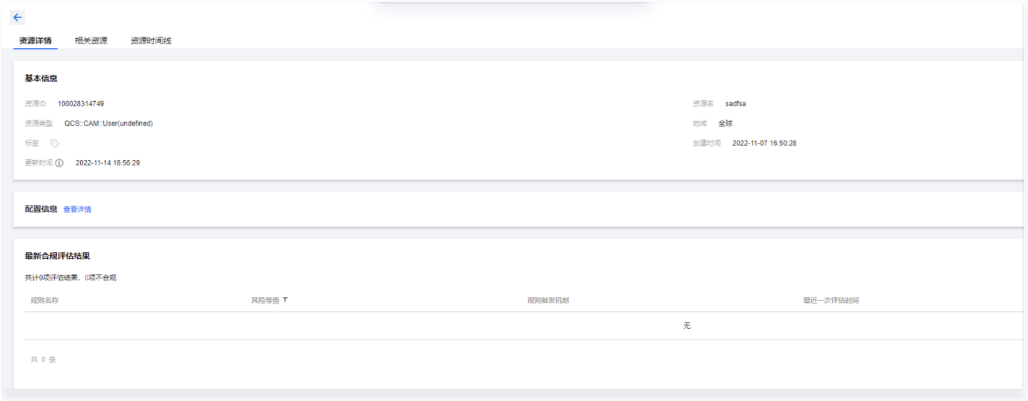
最近更新时间：2024-11-04 15:49:21

资源详情信息

在资源列表，单击资源名称，可查看**资源详情**信息，该页面有三个子页面。

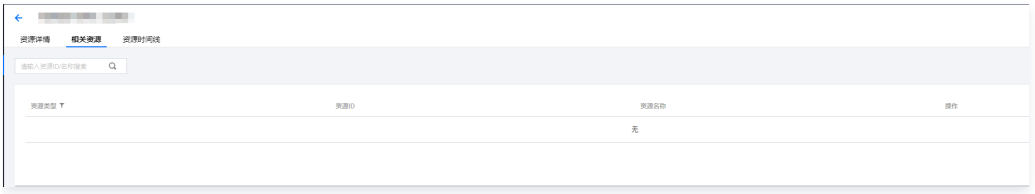
资源详情

资源详情展示资源最新更新的属性信息、配置信息、资源的最新合规评估结果。具体请参见 词汇表 。



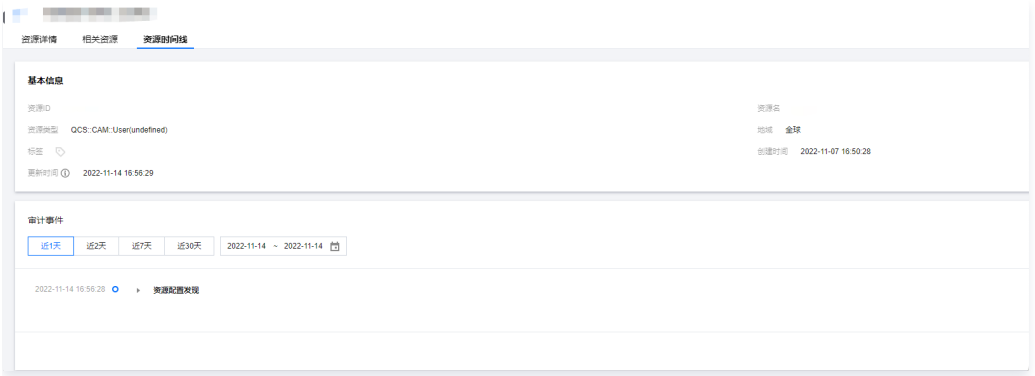
查看相关资源

切换到**相关资源**页面，可查看当前资源关联的具体资源。具体配置审计支持的资源关系请参见 支持的资源类型 。



查看资源时间线

切换至**资源时间线**页面，可以查询近一年内该资源的所有配置变更历史记录。



1. 时间线中节点的类别

资源每一次的配置变更将对应生成一个时间线的节点，每一节点的具体配置信息通过**配置项（ConfigurationItem）**来定义和展示。

- **时间线的起点**

如您的资源在被配置审计监控前已创建，则资源时间线的起点为配置审计首次识别并记录该资源配置信息的时间；如您的资源为开启配置审计监控后创建，则时间线的起点为资源首次创建的时间。

- **时间线的终点**

如该资源在配置审计监控期间被删除，则终点为资源删除的时间，如未删除，则终点为最近一次配置变更的时间。

2. 时间线中节点的格式

时间线中每一节点的配置信息通过标准的配置项（ConfigurationItem）来展示。配置项指某一时间点资源的各类属性、配置信息的集合，由元数据（Metadata）、资源属性（Attribute）、关联资源（Relationship）、详细配置信息（Configuration）组成。具体如下：

组成部分	字段名称	字段说明
基本信息 Metadata	Version ID	Config 版本号，新版本从1.0开始
	ConfigurationTime	该配置项生成的时间
	Status	-ResourceDiscovered (资源配置首次发现) -ResourceRecorded (资源配置记录，非首次发现) -ResourceChanged (资源配置变更，且资源未删除) -ResourceDeleted (该资源被删除)
	StateID	配置项id，配置项的唯一键
	EventType	事件类型： -Configuration (当资源配置发现或记录时，配置审计生成资源配置事件) -ConfigurationChange (当资源配置变更或资源被删除时，配置审计生成配置变更事件) -Compliance (当触发了资源关联规则的评估时，配置审计生成合规评估事件)
资源属性 Attribute	AccountId	主账号 uin
	ResourceID	资源ID
	ResourceName	资源名称
	ResourceType	资源类型，如 QCS::CVM::Instance
	ResourceTypeName	资源类型描述，如云服务器-实例
	Tags	资源标签键对值
	Product	云产品，如 cvm 等
	QCS	资源六段式
	Region	资源地域名称，如 ap-guangzhou ，对于无地域属性的全局资源，取 global
	CreatedTime	资源创建时间
关联资源 Relationship	ResourceID	关联资源 id，仅展示当前 config 支持的资源类型范围内的资源 id，没有则置空
	ResourceName	关联资源名称
	ResourceType	关联资源类型
	RelationshipType	当前资源与关联资源的关系类型
	RelationshipTypeName	关系类型名称
配置信息 Configuration	-	详细配置信息，每一资源类型的个性化配置信息字段不同

3. 时间线中的事件类别

根据事件配置项中展示信息的不同，可将每一节点分为以下几类：

- **资源配置事件**

  指对资源配置的首次发现或记录，一般来自对系统对资源的快照。由用户首次开启配置审计服务、手动修改监控的资源类型时触发。
- **配置变更事件**

  指对资源配置变更的记录。如您资源的最新配置与上一次记录的配置存在差异，则节点会展示为资源配置变更。一般由操作审计日志触发抓取或手动、自动执行的资源快照触发。如配置变更由操作审计触发，则会相应记录关联的操作审计事件。
- **合规评估事件**

  指对资源配置评估结果的记录，规则触发机制可参见 规则评估 。

规则
支持的托管规则

最近更新时间：2023-10-13 11:21:21

配置审计支持以下托管规则。如您需要系统支持更多的托管规则，可 提交工单 申请。

云服务	资源类型	托管规则
访问管理 CAM	访问管理-用户 QCS::CAM::User	CAM 访问管理用户必须开启敏感操作 MFA
	访问管理-用户 QCS::CAM::User	CAM 访问管理用户必须开启登录保护 MFA
	访问管理-用户组 QCS::CAM::Group	CAM 访问管理没有闲置用户组
	访问管理-用户 QCS::CAM::User 访问管理-用户组 QCS::CAM::Group	CAM 访问管理子账号必须关联用户组
	访问管理-用户 QCS::CAM::User	CAM 访问管理子账号没有直接授权策略
	访问管理-用户 QCS::CAM::User	CAM 访问管理用户，用户组，角色下不存在超级管理员权限
	访问管理-用户 QCS::CAM::User 访问管理-用户组 QCS::CAM::Group 访问管理-角色 QCS::CAM::Role	CAM 访问管理不允许授权指定高风险权限
	访问管理-策略 QCS::CAM::Policy	CAM 访问管理不存在闲置的权限策略
	访问管理-策略 QCS::CAM::Policy	CAM 访问管理登录权限检测
	访问管理-用户 QCS::CAM::User	CAM 访问管理用户的密钥 KEY 在指定时间内轮换
	访问管理-用户 QCS::CAM::User	CAM 访问管理用户在指定时间内有登录行为
CVM	QCS::CVM::Instance	CVM 实例关联指定安全组
	QCS::CVM::Instance	CVM 实例未进入回收站
	QCS::CVM::Instance	CVM 实例需要添加指定角色
	QCS::CVM::Instance	CVM 实例开启自动续费
	QCS::CVM::Instance	CVM 实例预付费，按量计费到期提醒
	QCS::CVM::Instance	CVM 实例按量计费过期保护
	QCS::VPC::SecurityGroup	没有闲置安全组
	QCS::CVM::Instance	CVM 实例使用私有网络
	QCS::CVM::Instance	未存在没有分配项目的 CVM 实例
	QCS::CVM::Instance	CVM 实例停机未超过指定天数
	QCS::CVM::Instance	CVM 实例租约期限满足指定天数
	QCS::CVM::Instance	CVM 实例绑定 IP4 公网地址
CBS	QCS::CBS::Disk	没有闲置 CBS 云盘
	QCS::CBS::Disk	云硬盘开启了到期欠费保护
	QCS::CBS::Disk	CBS 云硬盘开启加密状态
	QCS::CBS::Disk	CBS 云硬盘（可卸载类型）未进入回收站

TAG	QCS::CVM::Instance	资源存在指定标签
SecurityGroup	QCS::VPC::SecurityGroup	安全组不允许全网段开启远程访问风险端
	QCS::VPC::SecurityGroup	安全组不允许全放通规则
Subnet	QCS::VPC::Subnet	VPC 子网可用 IP 数大于指定值

托管规则详情
CAM 访问管理用户必须开启敏感操作 MFA

最近更新时间：2023-07-13 22:07:32

规则含义：检查 CAM 访问管理是否开启了敏感操作 MFA
合规检测逻辑：CAM 访问管理开启了敏感操作 MFA，则符合规则
规则标识符：`cam-account-action-mfa-enabled`
风险等级：高
适用的资源类型：`QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，MFA
规则入参：无

CAM 访问管理用户必须开启登录保护MFA

最近更新时间：2023-05-22 11:36:13

规则含义：检查 CAM 访问管理是否开启了登录保护 MFA。
合规检测逻辑：CAM 访问管理开启了登录保护 MFA，则符合规则。
规则标志符：`cam-account-login-mfa-enabled`
风险等级：高
适用的资源类型：`QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，MFA
规则入参：无

CAM 访问管理没有闲置用户组

最近更新时间：2023-07-13 22:07:32

规则含义：检查 CAM 访问管理是否有闲置用户组。
合规检测逻辑：CAM 访问管理用户组中至少存在一个用户，则符合规则。
规则标志符：`cam-group-user-bound`
风险等级：低
适用的资源类型：`QCS::CAM::Group`
规则触发类型：周期执行，24小时
关键词：用户，用户组
规则入参：无

CAM 访问管理子账号必须关联用户组

最近更新时间：2023-05-22 11:36:13

规则含义：检查 CAM 访问管理子账号是否关联用户组。
合规检测逻辑：账号访问管理中用户至少关联一个用户组，则符合规则。
规则标识符：`cam-user-group-bound`
风险等级：低
适用的资源类型：`QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，用户组
规则入参：无

CAM 访问管理子账号没有直接授权策略

最近更新时间：2023-05-22 11:36:13

规则含义：检查 CAM 访问管理子账号是否直接授权策略。
合规检测逻辑：账号访问管理子账号下，没有直接添加的授权策略，则符合规则。
规则标识符：`cam-user-policy-directly-bound`
风险等级：低
适用的资源类型：`QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，策略
规则入参：无

CAM 访问管理用户、用户组、角色下不存在超级管理员权限

最近更新时间：2023-05-22 11:36:13

规则含义：检查 CAM 访问管理用户，用户组，角色下是否存在超级管理员权限。
合规检测逻辑：账号访问管理下的用户，用户组，角色没有超级管理员（AdministratorAccess）权限，则符合规则。
规则标识符：`cam-policy-admin-access-bound`
风险等级：高
适用的资源类型：`QCS::CAM::User`，`QCS::CAM::Group`，`QCS::CAM::Role`
规则触发类型：周期执行，24小时
关键词：用户，用户组，角色，策略
规则入参：无

CAM 访问管理不允许授权指定高风险权限

最近更新时间：2023-05-22 11:36:14

规则含义：检查 CAM 访问管理是否授权指定高风险权限
合规检测逻辑：账号访问管理下的用户，用户组，角色，若没有授权指定的高风险权限，则符合规则
规则标识符： `cam-user-risky-policy-bound`
风险等级：低
适用的资源类型： `QCS::CAM::User` ， `QCS::CAM::Group` ， `QCS::CAM::Role`
规则触发类型：周期执行，24小时
关键词：用户，用户组，角色,策略
规则入参：

参数名称	默认值	关系
policies	AdministratorAcces	包含

CAM 访问管理不存在闲置的权限策略

最近更新时间：2023-05-22 11:36:14

规则含义：检查 CAM 访问管理是否存在闲置的权限策略。
合规检测逻辑：账号访问管理策略下，每个策略至少都有一个关联的用户，用户组，角色，则符合规则。
规则标识符：`cam-policy-in-use`
风险等级：低
适用的资源类型：`QCS::CAM::Policy`
规则触发类型：周期执行，24小时
关键词：用户，用户组，角色，策略
规则入参：无

CAM 访问管理登录权限检测

最近更新时间：2023-05-22 11:36:14

规则含义：检查 CAM 访问管理登录权限。
合规检测逻辑：账号访问管理，任意用户下控制台登录访问权限和 API 密钥启用开启且只开启一个，则符合规则。
规则标识符：`cam-user-login-check`
风险等级：低
适用的资源类型：`QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，登录，密钥
规则入参：无

CAM 访问管理用户的密钥 KEY 在指定时间内轮换

最近更新时间：2023-05-22 11:36:14

规则含义：检查 CAM 访问管理用户的密钥 KEY 是否在指定时间内轮换。
合规检测逻辑：账号访问管理中，用户的密钥在指定时间内有更换，则符合规则。
规则标识符： `cam-user-ak-rotated`
风险等级：高
适用的资源类型： `QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，密钥
规则入参：

参数名称	默认值	关系
days	90	小于等于

CAM 访问管理用户在指定时间内有登录行为

最近更新时间：2023-09-28 15:30:53

规则含义：检查 CAM 访问管理用户在指定时间内是否有登录行为
合规检测逻辑：账号访问管理中，用户在指定时间内若有登录行为，则符合规则
规则标识符： `cam-user-logged-in`
风险等级：中
适用的资源类型： `QCS::CAM::User`
规则触发类型：周期执行，24小时
关键词：用户，登录
规则入参：

参数名称	默认值	关系
days	90	小于等于

CVM 实例关联指定安全组

最近更新时间：2025-01-13 16:19:02

规则含义：检查 CVM 实例是否关联指定的安全组。
合规检测逻辑：CVM 实例关联指定的安全组，则符合要求。
规则标识符：`cbs-disk-noidle`
风险等级：高。
适用的资源类型：`QCS::CBS::Disk`
规则触发类型：周期执行，24小时。
关键词：安全组，云服务器。
规则入参：无。

CVM 实例未进入回收站

最近更新时间：2025-01-13 16:19:02

规则含义：检查 CVM 实例是否进入回收站。
合规检测逻辑：CVM 实例未因欠费、销毁等原因进入回收站，则符合要求。
规则标识符：`cvm-instance-no-recycle-bin`
风险等级：高。
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：配置变更触发。
关键词：云服务器。
规则入参：无。

CVM 实例需要添加指定角色

最近更新时间：2025-01-13 16:19:03

规则含义：检查 CVM 实例是否添加指定角色。
合规检测逻辑：CVM 实例需关联指定操作角色，则符合要求。
规则标识符：`cvm-instance-specified-role`
风险等级：低。
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：配置变更触发。
关键词：云服务器。
规则入参：无。

CVM 实例开启自动续费

最近更新时间：2025-01-13 16:19:03

规则含义：检查 CVM 实例是否开启自动续费。
合规检测逻辑：CVM 实例需开启自动续费标识，则符合要求。
规则标识符：`cvm-instance-automatic-renewal`
风险等级：高。
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：配置变更，周期执行，24小时。
关键词：云服务器。
规则入参：无。

CVM 实例预付费，按量计费到期提醒

最近更新时间：2025-01-13 16:19:03

规则含义：检查 CVM 实例是否开启实例预付费，按量计费到期提醒。
合规检测逻辑：CVM 预付费，按量计费实例到期时间距离检查时间大于设置的天数，则符合要求。默认值：30天。
规则标识符： `cvm-instance-prepaid`
风险等级：高。
适用的资源类型： `QCS::CVM::Instance`
规则触发类型：周期执行，24小时。
关键词：云服务器。
规则入参：

参数名称	默认值	关系
days	30	大于等于

没有闲置安全组

最近更新时间：2023-09-28 15:30:53

规则含义：检查有无闲置安全组
合规检测逻辑：检查未存在闲置未绑定的安全组，则符合要求。
规则标识符： `cvm-no-sg`
风险等级：中
适用的资源类型： `QCS::VPC::SecurityGroup`
规则触发类型：配置变更触发
关键词：安全组
规则入参：无

CVM 实例使用私有网络

最近更新时间：2025-01-13 16:19:03

规则含义：检查CVM 实例是否使用私有网络。
合规检测逻辑：CVM 实例在指定的VPC下，则符合规则。
规则标识符： `cvm-instance-vpc`
风险等级：中。
适用的资源类型： `QCS::CVM::Instance`
规则触发类型：配置变更触发。
关键词：云服务器，私有网络。
规则入参：

参数名称	默认值	关系
vpcids	空	包含

未存在没有分配项目的CVM实例

最近更新时间：2023-09-28 15:30:54

规则含义：检查 CVM 实例是否分配到一个项目
合规检测逻辑：CVM 实例都分配到了一个项目，则符合规则。
规则标识符：`cvm-no-assigned-items`
风险等级：中
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：配置变更触发
关键词：云服务器
规则入参：无

CVM 实例停机未超过指定天数

最近更新时间：2025-01-13 16:19:03

规则含义：检查 CVM 实例停机是否超过指定天数。
合规检测逻辑：CVM 实例停机未超过指定天数，则符合规则。
规则标识符： `cvm-instance-shutdown`
风险等级：中。
适用的资源类型： `QCS::CVM::Instance`
规则触发类型：周期执行，24小时。
关键词：云服务器。
规则入参：

参数名称	默认值	关系
days	空	小于等于

CVM 实例租约期限满足指定天数

最近更新时间：2023-09-28 15:30:54

规则含义：检查 CVM 实例租约期限是否满足指定天数
合规检测逻辑：CVM 实例租约期限是在指定的配置天数范围内，则符合规则。
规则标识符： `cvm-instance-lease-duration`
风险等级：低
适用的资源类型： `QCS::CVM::Instance`
规则触发类型：周期执行，24小时
关键词：云服务器
规则入参：

参数名称	默认值	关系
days	空	大于

CVM 实例绑定IP4公网地址

最近更新时间：2025-01-13 16:19:03

规则含义：检查 CVM 实例是否绑定 IP4 公网地址。
合规检测逻辑：CVM 实例下绑定了 IP4 公网地址，则符合规则（此规则仅适用于 IPv4）。
规则标识符：`cvm-instance-publicipv4-bound`
风险等级：中。
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：配置变更触发。
关键词：云服务器，公网 IP。
规则入参：无。

资源存在指定标签

最近更新时间：2025-01-13 16:19:03

规则含义：检查资源是否存在指定标签。
合规检测逻辑：实例关联指定的标签，则符合要求。
规则标识符：`cvm-resource-exists-specified-tag`
风险等级：高。
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：配置变更触发。
关键词：云服务器，标签，存储桶。
规则入参：无。

安全组不允许全网段开启远程访问风险端

最近更新时间：2023-09-28 15:30:54

规则含义：检查安全组是否全网段开启远程访问风险端
合规检测逻辑：当安全组设置全网段规则（0.0.0.0/0或::/0）时，端口范围不包括指定的风险端口，当安全组未设置全网段规则，端口范围可包含指定的风险端口，满足以上条件则符合规则。
规则标识符：`cvm-sg-no-remote-access`
风险等级：高
适用的资源类型：`QCS::VPC::SecurityGroup`
规则触发类型：配置变更触发
关键词：安全组
规则入参：无

安全组不允许全放通规则

最近更新时间：2023-12-04 17:36:22

规则含义：检查安全组是否全网段开启远程访问风险端
合规检测逻辑：当安全组设置全网段规则（0.0.0.0/0或::/0）时，端口范围不能为 ALL，当安全组未设置全网段规则，端口范围可以是 ALL，以上条件满足则符合规则。
规则标识符：`cvm-sg-no-remote-access`
风险等级：高
适用的资源类型：`QCS::VPC::SecurityGroup`
规则触发类型：配置变更触发
关键词：安全组
规则入参：无

云硬盘开启了到期欠费保护

最近更新时间：2023-09-28 15:30:54

规则含义：检查云硬盘是否开启了到期欠费保护
合规检测逻辑：CBS云硬盘开启了到期欠费保护，则符合规则。
规则标识符： `cbs-disk-open-arrears-protection`
风险等级：中
适用的资源类型： `QCS::CBS::Disk`
规则触发类型：配置变更触发
关键词：云硬盘
规则入参：无

CBS云硬盘开启加密状态

最近更新时间：2025-01-13 16:19:03

规则含义：检查云硬盘是否开启了到期欠费保护。
合规检测逻辑：CBS 云硬盘开启了加密，则符合规则。
规则标识符：`cbs-disk-encrypted`
风险等级：中。
适用的资源类型：`QCS::CBS::Disk`
规则触发类型：配置变更触发。
关键词：云硬盘。
规则入参：无。

CBS云硬盘（可卸载类型）未进入回收站

最近更新时间：2023-09-28 15:30:55

规则含义：检查 CBS 云硬盘（可卸载类型）是否进入回收站
合规检测逻辑：CBS 云硬盘（可卸载类型）包年包月计费的情况下，未因欠费、退还等原因进入回收站，则符合规则。
规则标识符： `cbs-disk-no-trash`
风险等级：中
适用的资源类型： `QCS::CBS::Disk`
规则触发类型：配置变更触发
关键词：云硬盘
规则入参：无

VPC子网可用IP数大于指定值

最近更新时间：2024-11-04 15:49:21

规则含义：检查 VPC 子网可用 IP 数是否大于指定值。
合规检测逻辑：VPC 子网的可用IP数如果大于配置的指定值，则符合规则。
规则标识符：`vpc-subnet-availip`
风险等级：低。
适用的资源类型：`QCS::VPC::Subnet`
规则触发类型：周期执行，24小时。
关键词：私有网络，子网。
规则入参：

参数名称	默认值	关系
numbers	空	大于等于

CVM 实例按量计费过期保护

最近更新时间：2025-01-13 16:19:03

规则含义：检查 CVM 实例是否开启按量计费过期保护。
合规检测逻辑：CVM 实例按量计费期间，实例未停机，且未超过租约有效期，则符合要求。
规则标识符：`cvm-instance-fee-expiration-protection`
风险等级：高。
适用的资源类型：`QCS::CVM::Instance`
规则触发类型：周期执行，24小时。
关键词：云服务器。
规则入参：无。

没有闲置CBS云盘

最近更新时间：2025-01-13 16:19:03

规则含义：检查是否存在没有闲置 CBS 云盘。
合规检测逻辑：未存在闲置的 CBS 云盘，且都开启了快照，则符合要求。
规则标识符：`cbs-disk-noidle`
风险等级：低。
适用的资源类型：`QCS::CBS::Disk`
规则触发类型：配置变更触发
关键词：云盘，快照。
规则入参：无。

使用规则
新建托管规则

最近更新时间：2023-12-04 17:36:22

操作场景

该任务指导您在配置审计控制台新建一个托管规则，帮助您对资源进行审计并且进行评估。

操作步骤

1. 登录**配置审计**控制台 > 规则 。
2. 在**规则**页面，单击**新建托管规则**。（可选择账号或者全局账号组进行创建，以实际账号为准）。

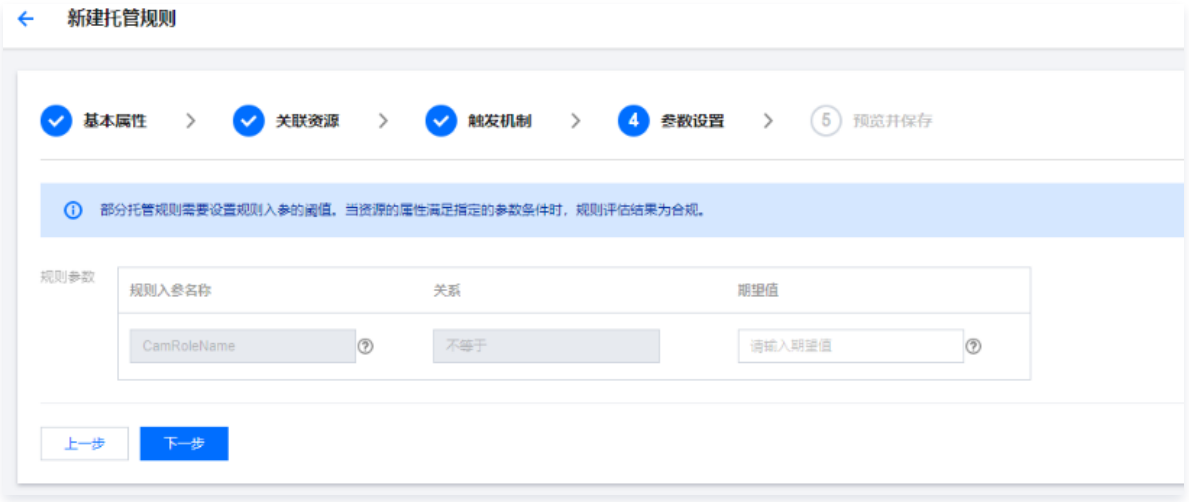
3. 在**新建托管规则**页面，选择需要应用的托管规则。更多支持托管规则的详细信息，请参见 支持的托管规则 。

4. 在**基本属性**页面，输入规则名称、风险等级、规则描述，单击**下一步**。

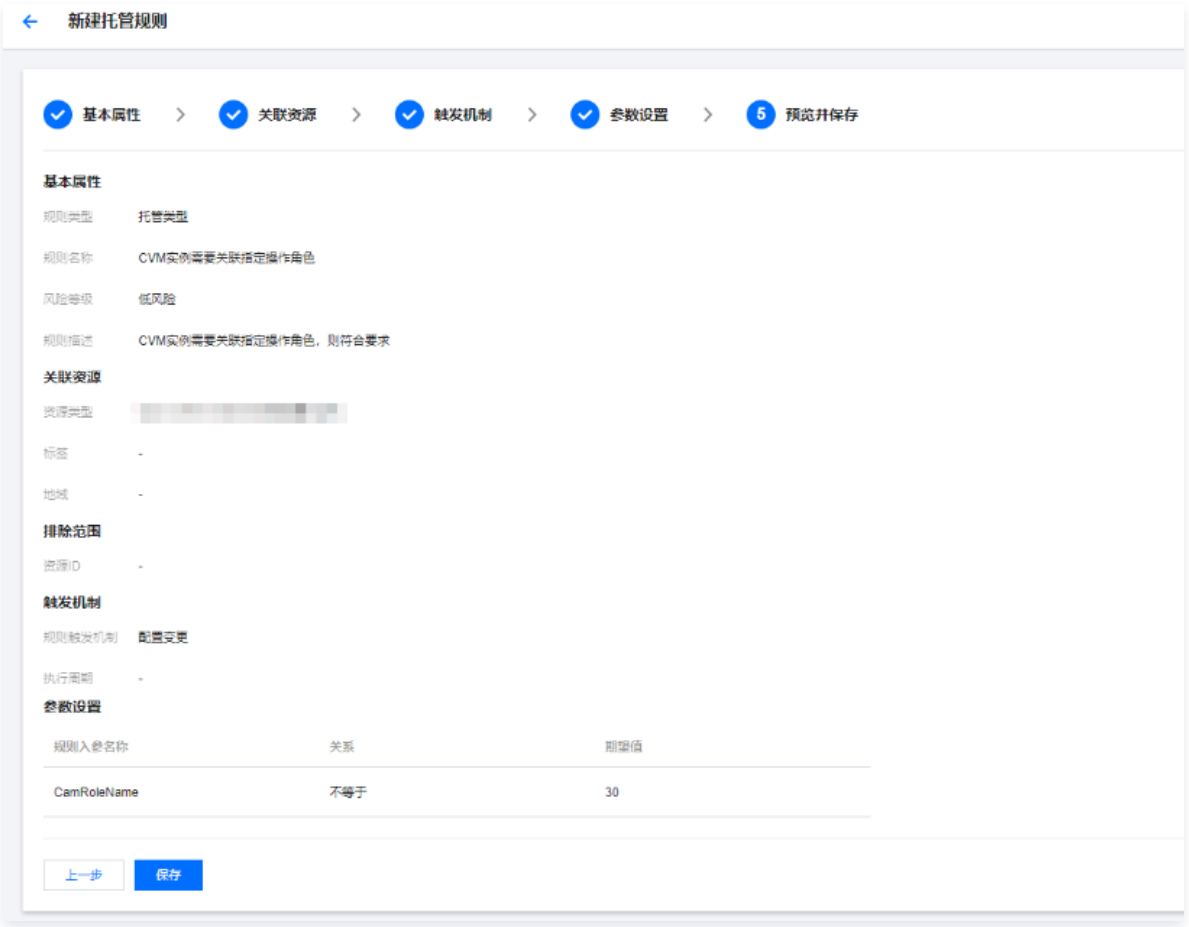
5. 在**关联资源**页面，选择您需要进行审计的资源，可以按需设置按标签或者按地域来确认应用范围，也可按资源 ID 排除范围，单击**下一步**。

6. 在**触发机制**页面，设置规则触发机制，单击**下一步**。

7. 在**参数设置**页面，设置规则函数的参数值，单击**下一步**。



8. 在**预览并保存**页面，您可以看到创建的规则信息，也可以根据需要返回上一步操作，确认无误后单击**保存**，即可创建成功。



说明：

如果用户在新建、编辑合规包时，选择来源为规则列表中已加入合规包的规则，或合规包模板中的托管规则、或托管规则中的托管规则，则在保存后，系统将相应为用户复制新增一条规则至当前合规包。

新建自定义托管规则

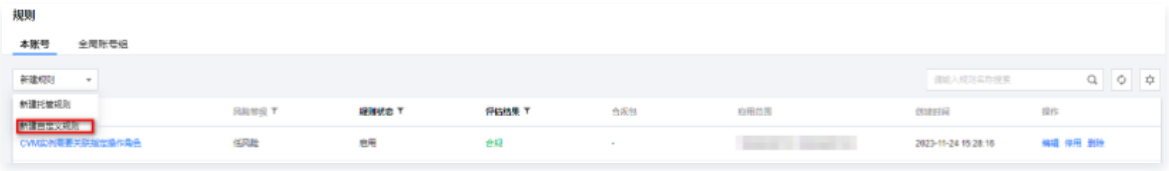
最近更新时间：2024-08-16 21:09:11

操作场景

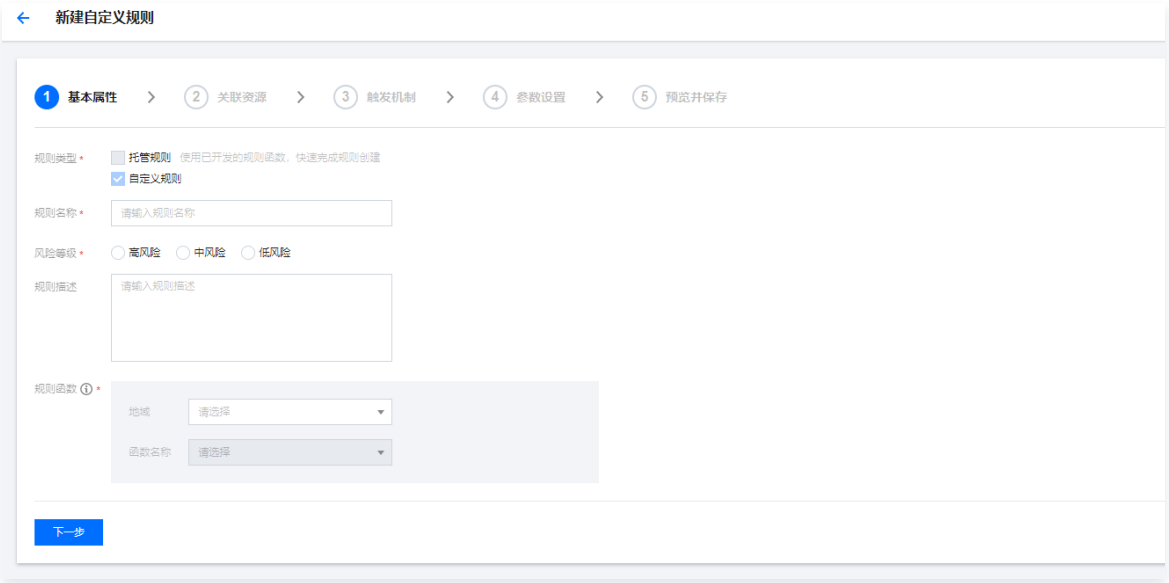
该任务指导您在配置审计控制台新建一个自定义的托管规则，帮助您对资源进行审计并且进行评估。

操作步骤

1. 登录**配置审计**控制台 > 规则
2. 在**规则**页面，单击**新建自定义规则**。（可选择账号或者全局账号组进行创建，根据实际登录账号为准）。



3. 在**新建自定义规则基本属性**页面，输入规则名称、风险等级、规则描述以及规则函数，单击**下一步**。



注意：

- **规则函数**为预先创建的 SCF 函数，需要预先在 云函数控制台 上创建服务和函数。具体操作，请参见 使用控制台创建一个事件函数 。
- 创建函数时，函数类型选择 SCF 事件函数，运行环境选择 python 3.7，其他参数均可根据实际需求设置，**函数代码示例如下：**

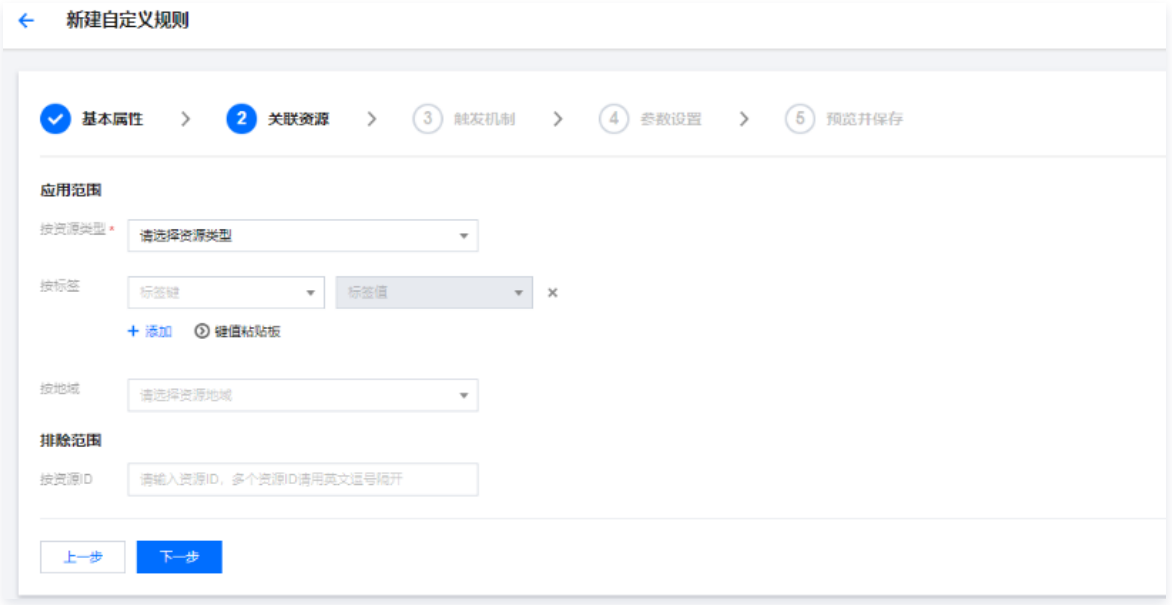
```
package main

import (
    "context"
    "encoding/json"
    "fmt"
    "github.com/tencentcloud/tencentcloud-sdk-go/tencentcloud/common"
    "github.com/tencentcloud/tencentcloud-sdk-go/tencentcloud/common/errors"
    "github.com/tencentcloud/tencentcloud-sdk-go/tencentcloud/common/profile"
    config "github.com/tencentcloud/tencentcloud-sdk-go/tencentcloud/config/v20220802"
    "github.com/tencentyun/scf-go-lib/cloudfunction"
)

// maingo
func main() {
```

```
    cloudfunction.Start(ReceiveMessage)
}

type Tag struct {
    TagKey   string
    TagValue string
}
type ClientContext struct {
    InvokingEvent      *InvokingEvent
    RuleParameters     map[string]string //规则参数
    ResultToken        string            //加密令牌
    OrderingTimestamp int64              //评估时间戳
}

type InvokingEvent struct {
    TriggerType       string
    ConfigurationItem *ConfigurationItem
}
type ConfigurationItem struct {
    AccountId            int64  //资源所属用户ID
    Region               string //资源地域
    Zone                 string //资源可用区
    Configuration        string //资源详细配置
    ResourceCreationTime int64  //资源创建时间戳
    ResourceType         string //资源类型
    ResourceId           string //资源ID
    ResourceStatus       string //资源ID
    ResourceName         string //资源名称
    Tags                 []Tag  //资源标签
    CaptureTime          int64  //资源快照时间戳
}

// ReceiveMessage 接受消费消息{
//    "InvokingEvent": {
//        "TriggerType": "MANUAL",
//        "ConfigurationItem": {
//            "AccountId": 100004293724,
//            "Region": "ap-guangzhou",
//            "Zone": "",
//            "Configuration": {  //每种资源类型Configuration内容字段不同
//                "CidrBlock": "172.16.0.0/16",
//                "IsDefault": true,
//                "Ipv6CidrBlock": "",
//                "DnsServerSet": null,
//                "DomainName": "",
//                "DhcpOptionsId": ""
//            },
//            "ResourceCreationTime": 1520431078,
//            "ResourceType": "QCS::VPC::Vpc",
//            "ResourceId": "vpc-q252nx9j",
//            "ResourceStatus": "",
//            "ResourceName": "Default-VPC",
//            "Tags": null,
//            "CaptureTime": 1686500243
//        }
//    },
//    "RuleParameters": {
//        "234": "324"
//    },
```

```
//    "ResultToken": "Wm9yZlY3WmlKa3cxaW1oQpgtklO2shRhG1gtxnC4qyszJtkSz5ZpZDshF6YyaaIAagGsEAcidC-
VFNJHtRfXfam_FHMR_RhhelEAT4ApsKFQIBEZNaWN284dZS02f7uRT6w_zwHz5E1dXmNYvancDRgiCQHip_uUrif0Toypdbh1tuLOD
HgVN1csbaPKu3hb2-O-PBh824HACVUkDXJAp2KMQnqhNagmlUULjY-GMyM=",
//    "OrderingTimestamp": 1686537830
//}
func ReceiveMessage(ctx context.Context, event ClientContext) error {

    eventStr, _ := json.Marshal(event)
    fmt.Println("SCF:ReceiveMessage:Event:", string(eventStr))
    putRuleResule(event)
    return nil
}

//自定义判断资源是否合规---对资源进行评估，需要根据实际业务自行实现评估逻辑，返回COMPLIANT、NON_COMPLIANT;以下代码仅
供参考
func getComplianceType(configurationStr string) string {
    return "COMPLIANT"
}

func putRuleResule(event ClientContext) {
    evaluations := make([]*config.Evaluation, 0)
    //1：设置评估结果，格式需符合以下示例要求。
    complianceType := getComplianceType(event.InvokingEvent.ConfigurationItem.Configuration)
    configuration := "xxxx"
    desiredValue := "xxxxx"
    evaluation := &config.Evaluation{
        ComplianceResourceId:   &event.InvokingEvent.ConfigurationItem.ResourceId,
        ComplianceResourceType: &event.InvokingEvent.ConfigurationItem.ResourceType,
        ComplianceRegion:       &event.InvokingEvent.ConfigurationItem.Region,
        ComplianceType:         &complianceType,
        Annotation: &config.Annotation{
            Configuration: &configuration,
            DesiredValue:  &desiredValue,
        },
    }
    evaluations = append(evaluations, evaluation)

    //2：上报评估结果
    //需具备权限Config_QCSLinkedRoleInConfigRecorder服务角色
    credential := common.NewCredential(
        "xxxx",
        "xxxxx",
    )
    cpf := profile.NewClientProfile()
    cpf.HttpProfile.Endpoint = "config.internal.tencentcloudapi.com"
    client, _ := config.NewClient(credential, "ap-guangzhou", cpf)
    request := config.NewPutEvaluationsRequest()
    request.ResultToken = &event.ResultToken
    request.Evaluations = evaluations
    response, err := client.PutEvaluations(request)
    if _, ok := err.(*errors.TencentCloudSDKError); ok {
        fmt.Printf("An API error has returned: %s", err)
        return
    }
    if err != nil {
        panic(err)
    }
    // 输出json格式的字符串回包
    fmt.Printf("%s", response.ToJsonString())
}
```

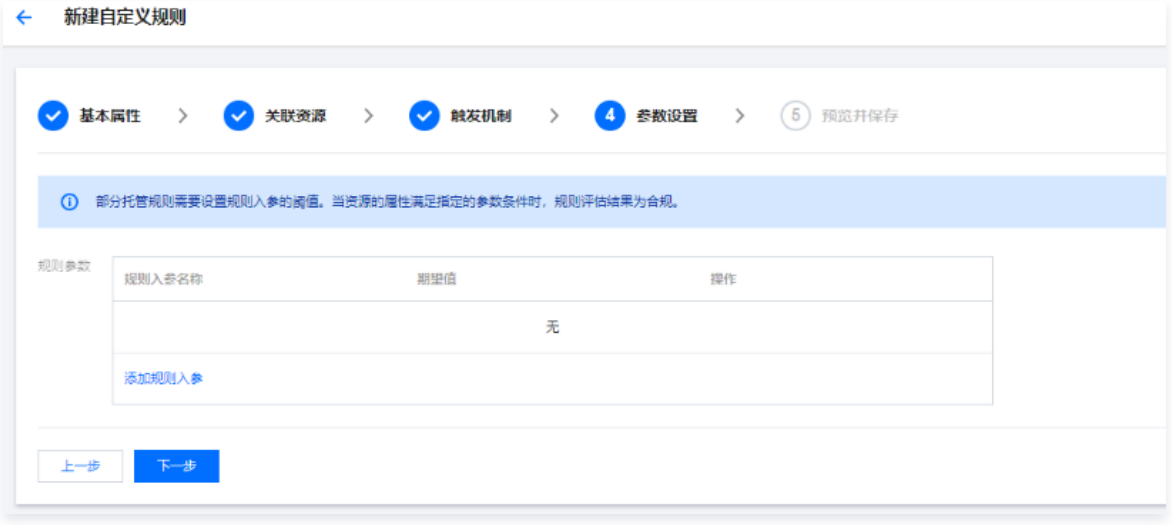
说明：
详细的函数说明可以查看上述代码的注释部分。

4. 在**新建自定义规则关联资源**页面，选择应用的资源类型，可以按需设置按标签或者按地域来确认应用范围，也可按资源 ID 排除范围，单击**下一步**。

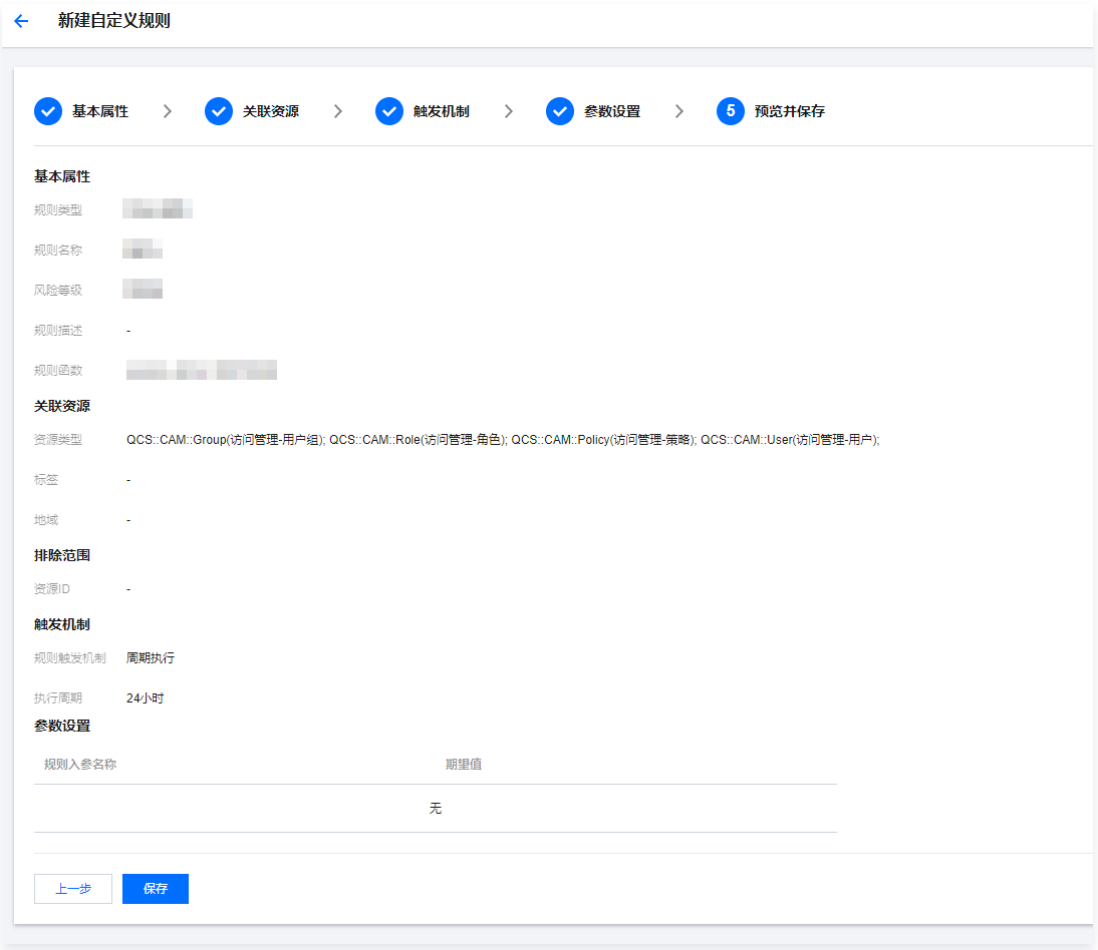


5. 在**新建自定义规则触发机制**页面，按需选择规则触发机制，单击**下一步**。

6. 在**新建自定义规则参数设置**页面，设置规则函数的参数值，单击**下一步**。



7. 在**新建自定义规则预览并保存**页面，您可以看到创建的自定义规则的信息，也可以根据需要返回上一步操作，确认无误后单击**保存**，即可创建成功。


新建自定义规则
基本属性
关联资源
触发机制
参数设置
5 预览并保存
基本属性
规则类型
规则名称
风险等级
规则描述 -
规则函数
关联资源
资源类型 QCS::CAM::Group(访问管理-用户组); QCS::CAM::Role(访问管理-角色); QCS::CAM::Policy(访问管理-策略); QCS::CAM::User(访问管理-用户);
标签 -
地域 -
排除范围
资源ID -
触发机制
规则触发机制 周期执行
执行周期 24小时
参数设置
规则入参名称
期望值
无
上一步
保存

管理规则
查看规则列表

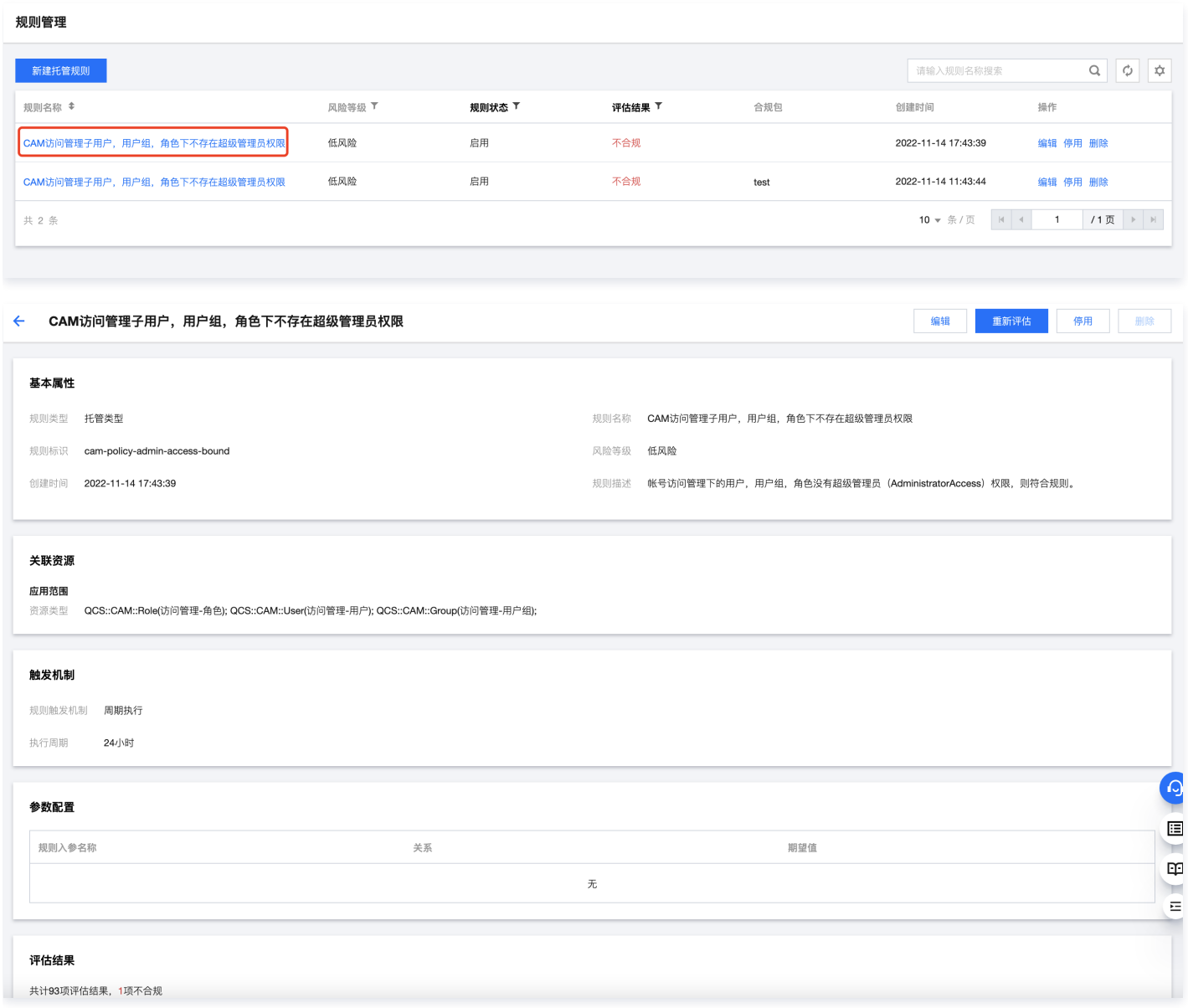
最近更新时间：2024-04-10 22:07:32

单击规则菜单，可进入规则页面，在该页面可查看该账号下的所有规则。您可以按照规则名称、风险等级、规则状态、评估结果等筛选规则。

查看规则详情

最近更新时间：2024-04-10 22:07:32

单击规则名称，可查看该规则的详细信息。规则详情中会展示规则的基本属性、关联资源、触发机制、参数配置情况及评估结果。您可以在详情页对规则进行编辑、手动评估、启用/停用、删除等操作。



编辑规则

最近更新时间：2024-04-10 22:07:33

在规则列表中找到需要编辑的规则，单击操作列的编辑规则，可以修改规则设置。

停用/启用规则

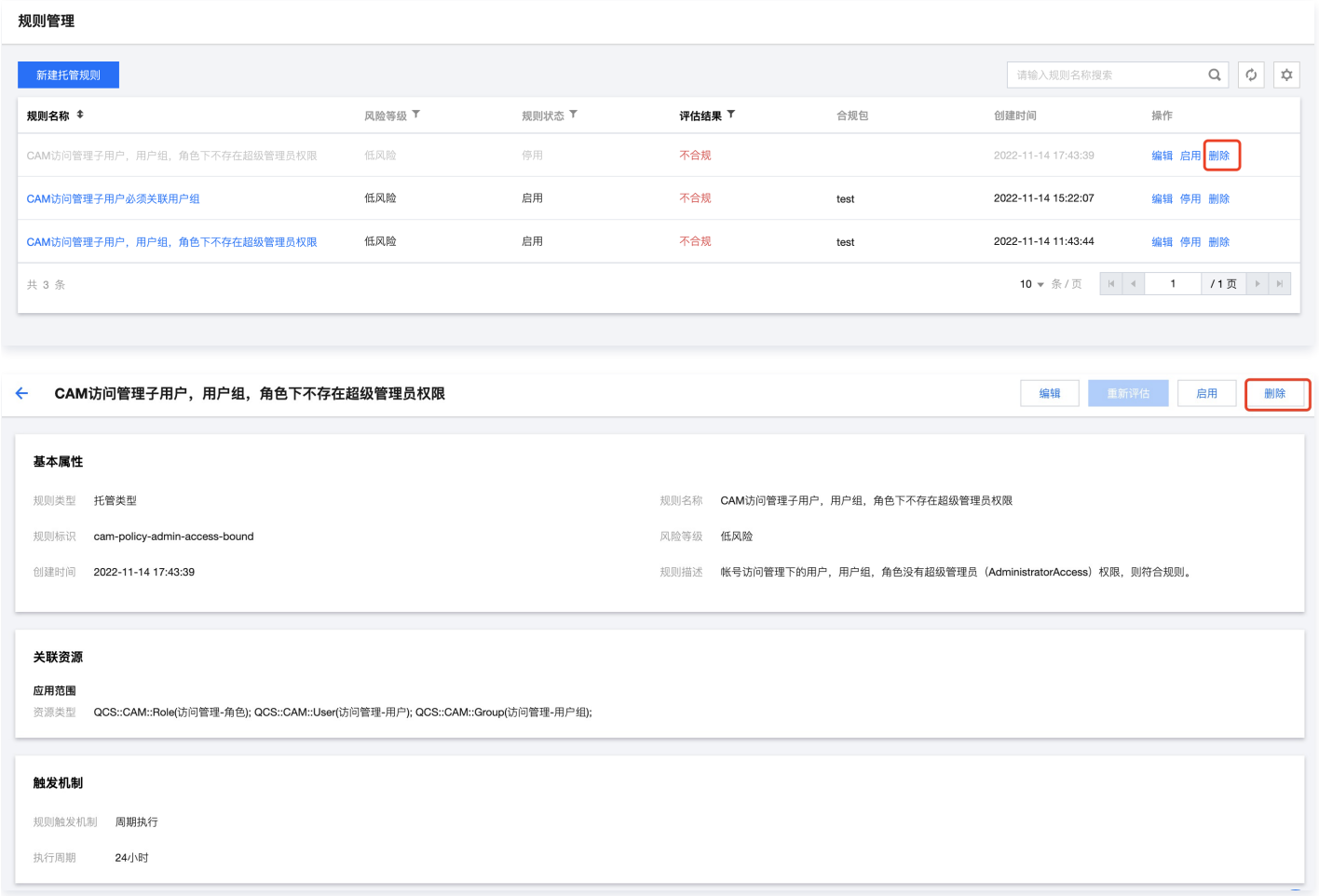
最近更新时间：2024-04-10 22:07:33

暂时不用的规则，可以在规则列表或规则详情页单击停用。规则停用后将不再运行，无论是否设置周期执行，或是单击重新评估，直至重新启用。

删除规则

最近更新时间：2024-04-10 22:07:33

对于不再需要的规则，可直接在规则列表单击删除或单击规则名称，进入规则详情页，在详情页单击删除。规则删除前需先停用，以防误删。已加入合规包的规则，也可以通过删除合规包批量删除。



规则评估

最近更新时间：2024-04-10 22:07:33

配置审计中已启用的规则，可以由系统自动触发，或手动触发执行。已停用的规则，需重新**启用**后才能触发执行。

手动触发

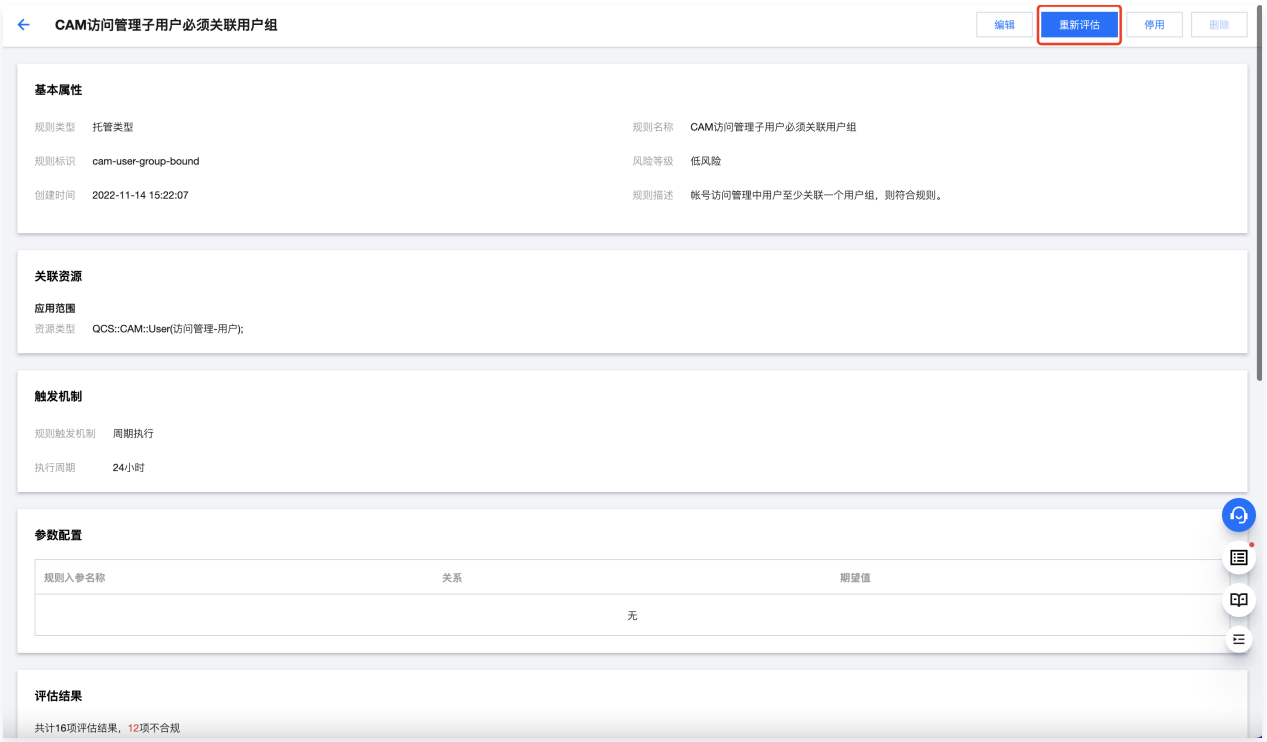
- 单条触发

  用户**新建**规则、**编辑**规则后保存。
  用户重新**启用**已停用的规则。
  用户在规则详情页单击**重新评估**。

- 批量触发

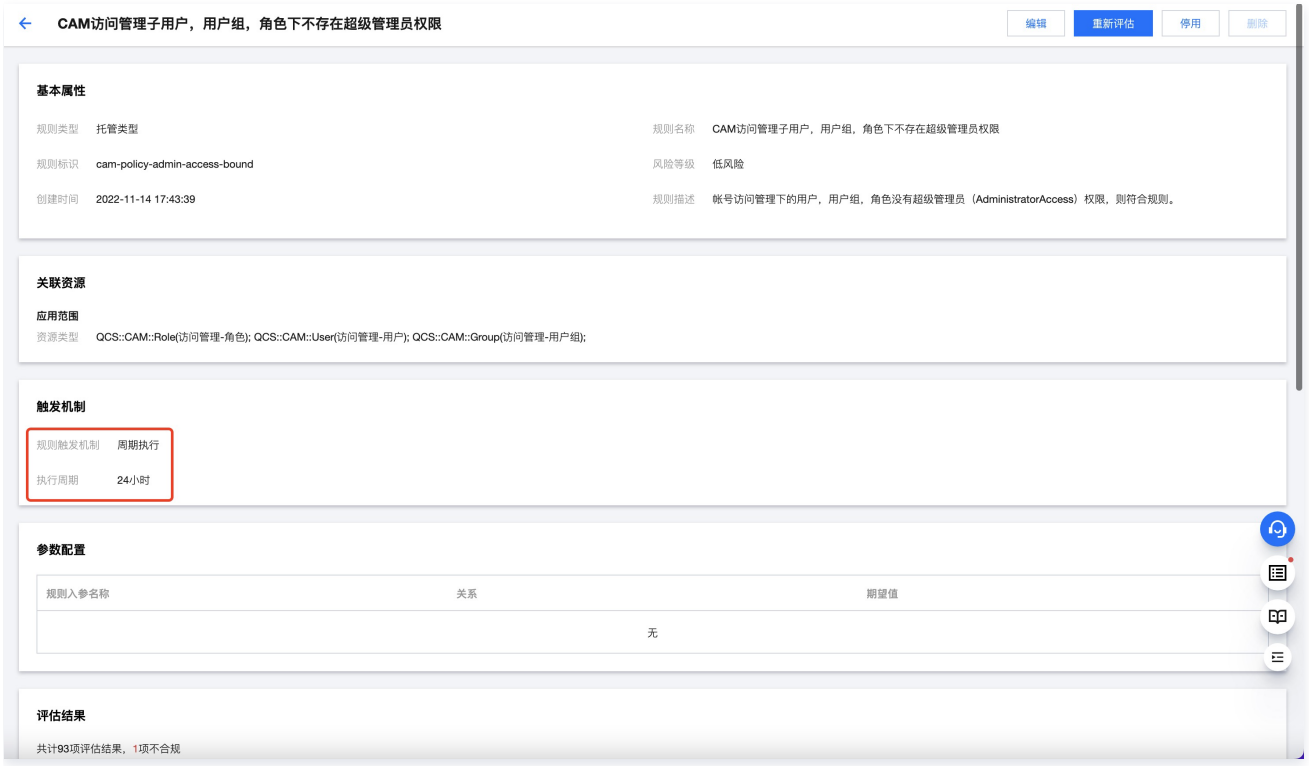
  用户将规则加入了合规包，则以下场景可批量触发合规包内规则的评估。
  用户新建合规包、编辑合规包后保存。

用户在合规包详情页单击**重新评估**。



自动触发

用户为规则或合规包配置了执行周期，则每日到点后规则会自动执行，每日首次自动开始执行的时间为00:30。



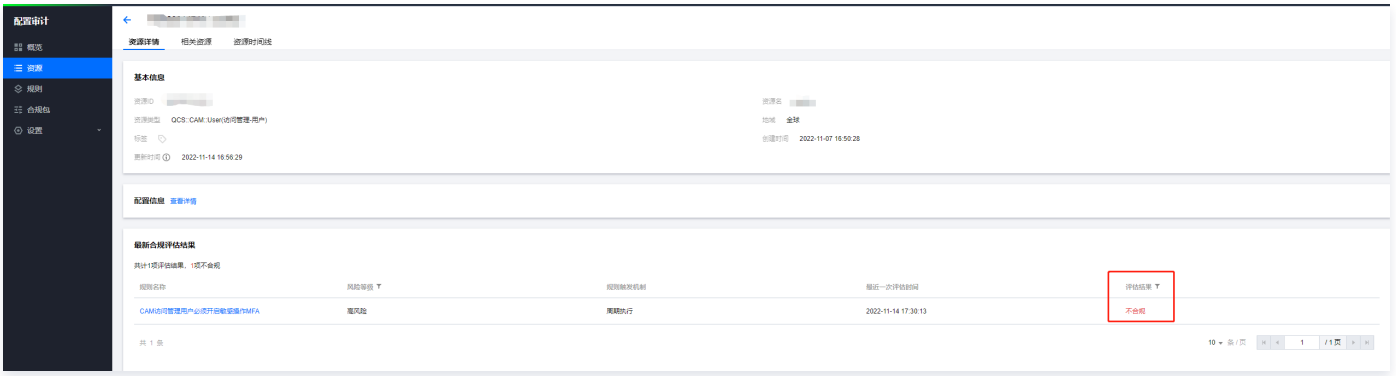
查看规则评估结果

最近更新时间：2024-04-11 17:45:11

规则评估完成后，可以通过以下方式查看其评估结果：

1. 单击**规则**菜单，进入**规则**页面，单击规则名称进入**规则详情**页，在评估结果中，即可查看该规则对所有关联资源的最新评估结果。

2. 单击**资源**菜单，进入**资源**页面，单击资源名称进入**资源详情**页，在最新合规评估结果部分，可查看该资源对所有关联规则的最新评估结果。



合规包
支持的合规包模板

最近更新时间：2023-07-13 22:07:33

当前配置审计支持账号权限安全最佳实践这一预设的合规包 。如您需要系统支持更多的预设合规包，可 提交工单 申请。

合规包模板	托管规则
账号权限安全最佳实践	CAM访问管理用户必须开启敏感操作MFA
	CAM访问管理用户必须开启登录保护MFA
	CAM访问管理没有闲置用户组
	CAM访问管理子账号必须关联用户组
	CAM访问管理子账号没有直接授权策略
	CAM访问管理用户，用户组，角色下不存在超级管理员权限
	CAM访问管理不允许授权指定高风险权限
	CAM访问管理不存在闲置的权限策略
	CAM访问管理登录权限检测
	CAM访问管理用户的密钥KEY在指定时间内轮换
	CAM访问管理用户在指定时间内有登录行为

管理合规包
查看合规包列表

最近更新时间：2024-09-18 17:20:41

单击合规包菜单，进入 合规包列表 页面。在该页面可查看账号下的所有合规包。您可以按照合规包名称、风险等级、合规包状态、评估结果等筛选规则。

查看合规包详情

最近更新时间：2024-09-18 17:20:41

在 **合规包列表** 单击合规包名称，可进入该**合规包详情**页。

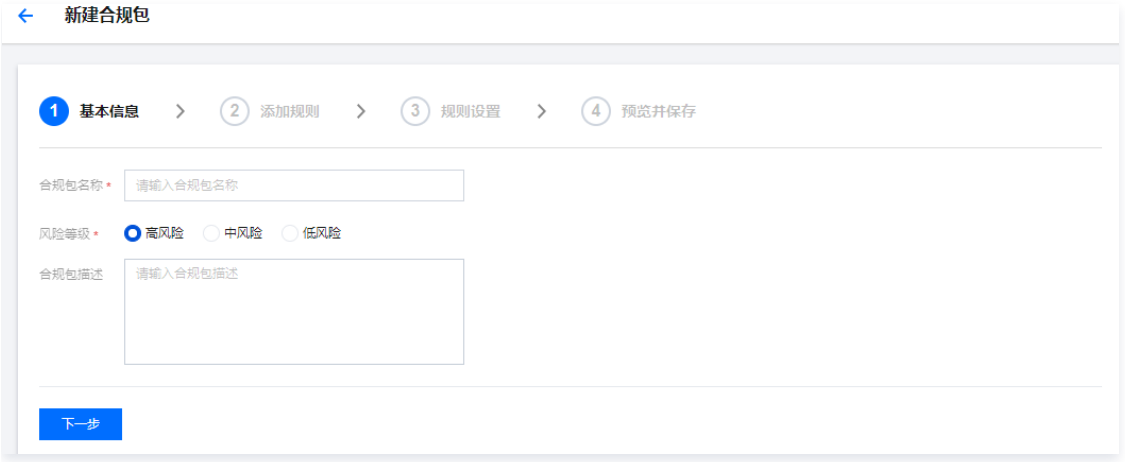
合规包详情中会展示合规包的基本属性、所包含的规则及规则评估结果。您可以在详情页操作**编辑**、**删除**合规包、触发合规包评估，或是**添加/移出/删除**规则等。

新建合规包

最近更新时间：2024-09-18 17:20:41

单击合规包菜单，进入合规包页面，单击新建合规包。

分别设置规则的基本属性、添加规则并设置规则参数，即可完成合规包的创建。



编辑合规包

最近更新时间：2024-09-18 17:20:41

在 合规包列表 中找到需要编辑的规则，单击操作列的编辑，可以编辑规则。

或在合规包详情页上方单击编辑，编辑规则。

添加/移出规则

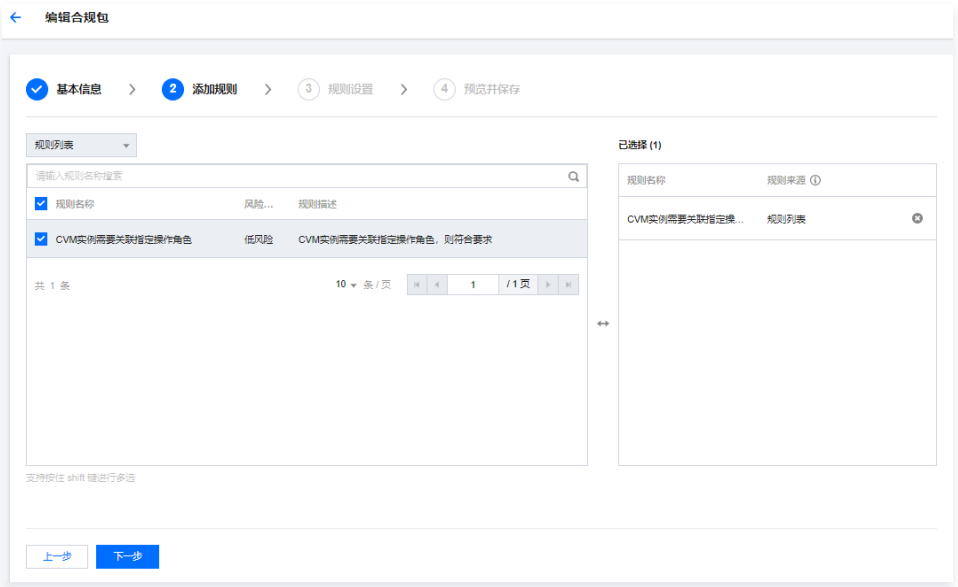
最近更新时间：2025-01-13 16:19:03

操作场景

用户可以直接将现有**规则列表**中的规则加入合规包，同时也可以将合规包中已有的规则移出。
如您选择的规则来源为托管规则模板、合规包模板、或现有规则列表中已加入合规包的规则，则系统将为您自动复制新增一条规则，并添加至当前合规包。

操作步骤

- 在 合规包 页面，单击目标合规包行的**编辑**，在**添加规则**页签，按需选择要添加的规则/移出的规则。单击**下一步**，直至完成操作。



- 在 合规包 页面，单击目标合规包名称。
  - 添加规则

    在**规则详情**页面，单击**添加规则**，选择要添加的规则。

  - 移出规则

    在**规则详情**页面，单击**移出**即可。

删除规则

最近更新时间：2023-07-13 22:07:34

在规则详情页，单击删除，可以直接删除当前合规包中已有的规则。

删除合规包

最近更新时间：2024-09-18 17:20:41

对于不再需要的合规包，可直接在 合规包列表 或合规包详情页单击删除，删除合规包时，合规包内规则将一并删除。

> **注意：**
> 若合规包存在未停用规则，则会删除失败。您可在**合规包详情页**移除规则后再删除合规包。

- 合规包列表

- 合规包详情页

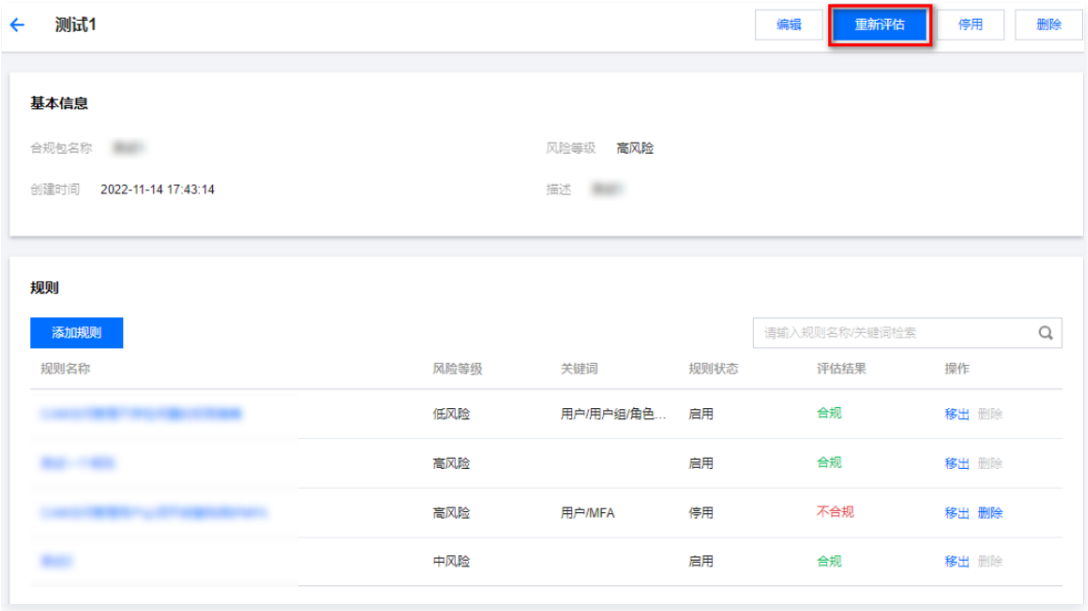
合规包评估

最近更新时间：2024-09-18 17:20:41

配置审计中已启用的合规包，可以由系统自动触发评估，或手动触发评估。

手动触发

用户操作**新建合规包**、**编辑**后保存。
用户在**合规包详情**页单击**重新评估**合规包。



自动触发

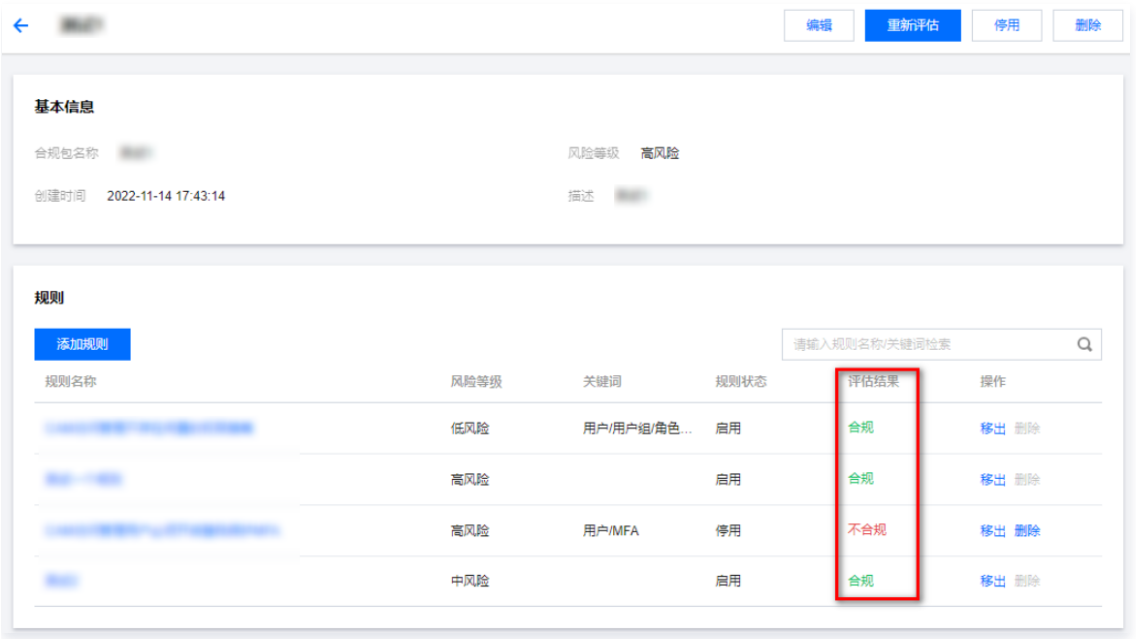
用户为合规包中的规则配置了执行周期，到期后规则将自动执行。

查看合规评估结果

最近更新时间：2024-09-18 17:20:41

您可以在合规包列表查看每一合规包的评估结果。合规包内所有规则均评估为合规，则合规包评估结果为合规，否则不合规。

如您需查看合规包中每一规则的评估结果，可单击合规包名称，进入合规包详情页查看。



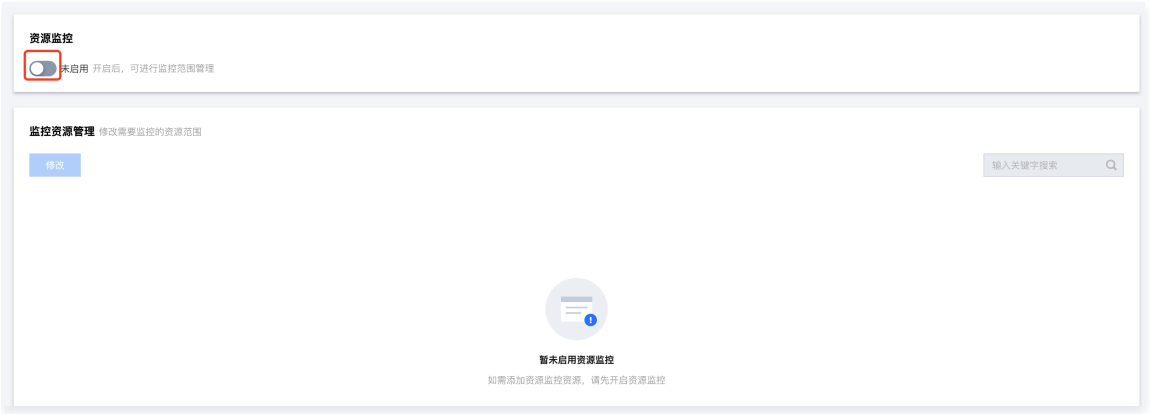
设置
监控管理

最近更新时间：2024-09-18 17:20:41

单击设置 > 服务设置 菜单，可开启服务并设置需监控的资源范围。

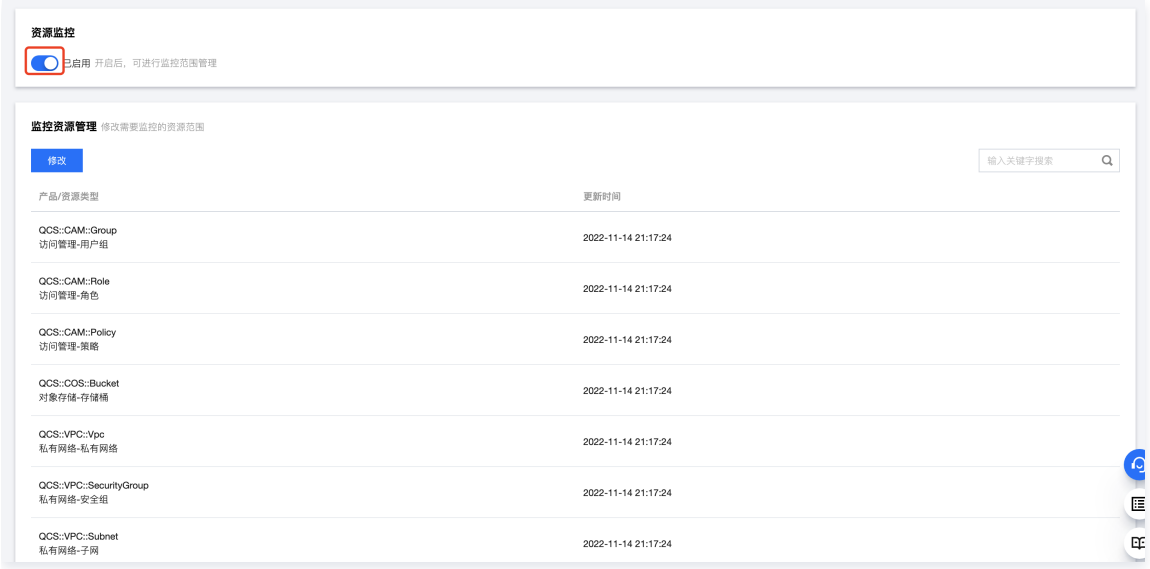
开启配置审计

您可以在监控管理页面单击开启或关闭配置审计。首次开通配置审计服务，需授权创建配置审计服务相关角色（Config_QCSLinkedRoleInConfigRecorder），并选择需监控的资源类型，当前配置审计支持的资源类型请参见 支持的资源类型 。

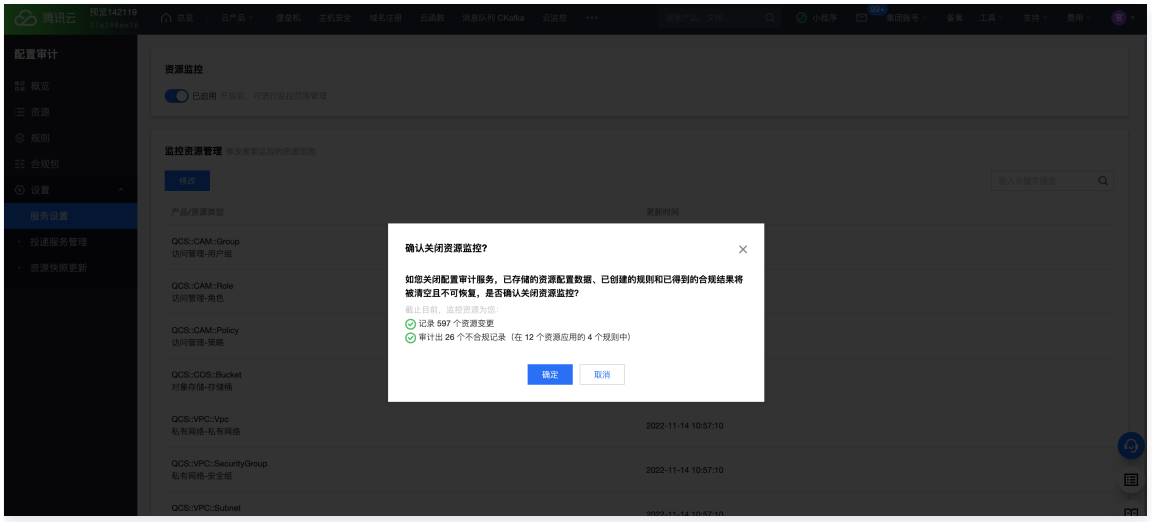


关闭配置审计

如您不再需要使用配置审计，可单击关闭停止使用。



在弹出的窗口中，单击确定。

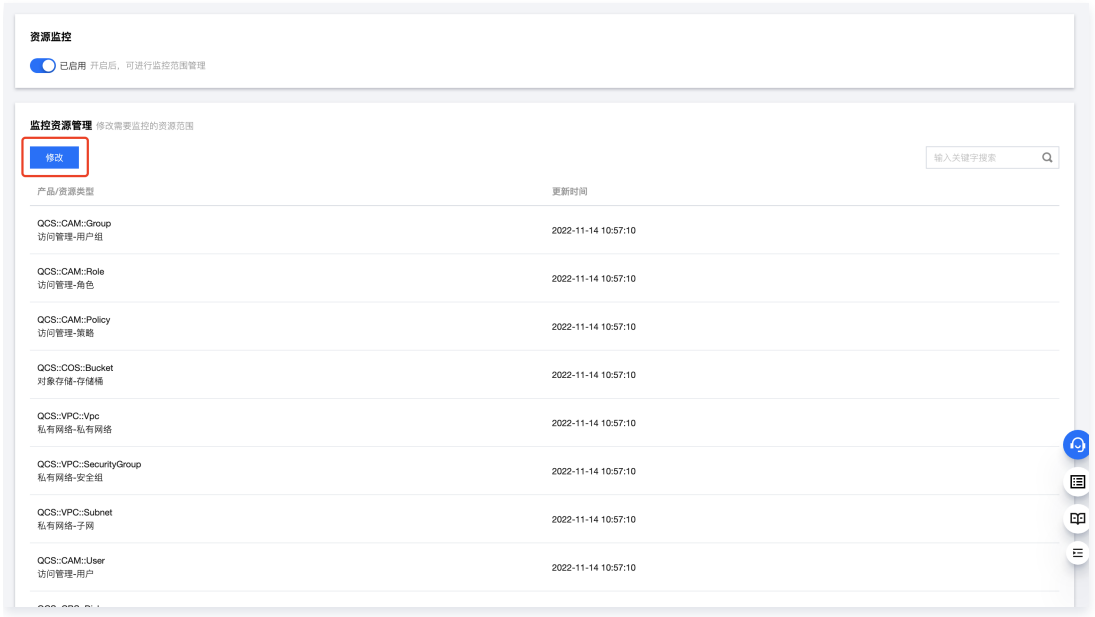


关闭后，配置审计将不再监控并更新资源配置变更，配置审计中已存储的资源配置数据、已创建的规则和已得到的合规结果将被清空且不可恢复。历史已投递至 COS 存储桶的数据不受影响。

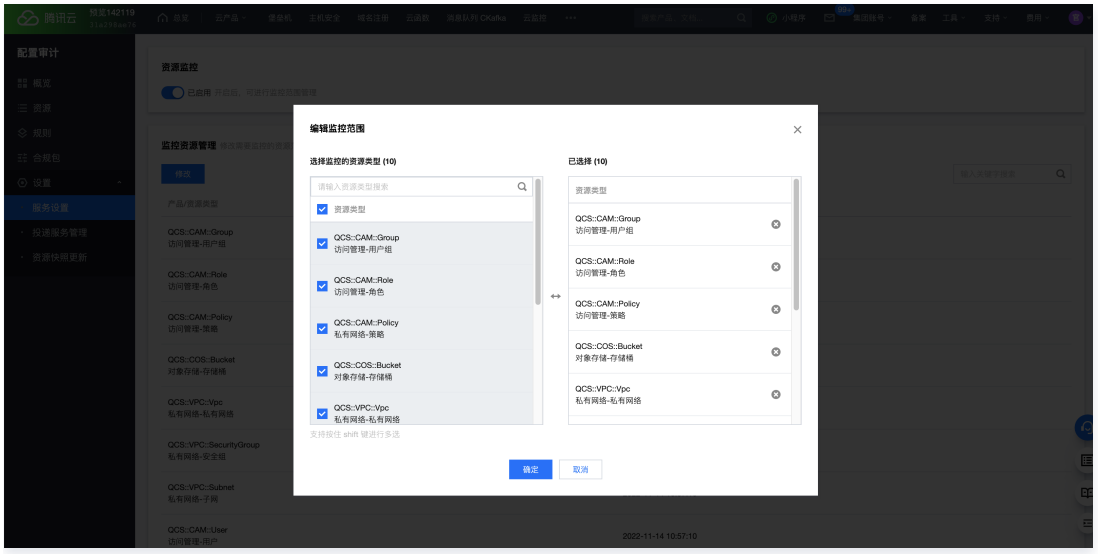
> **注意：**
> 如果您的账号集团存在账号组，则无法关闭配置审计。

修改监控范围

如您已开启配置审计，可单击**修改**，变更监控的资源类型。修改监控范围会导致资源列表新增资源及相应时间线的更新，以及您账号下已有规则，合规包的重新审计，预计将有10-15分钟的时间窗口，请耐心等待。



在弹出的窗口，您可按需变更监控的资源类型。


配置审计
概览
资源
规则
合规包
设置
服务设置
投递服务管理
资源快照更新
资源监控
已启用
监控资源管理
修改
产品/资源类型
QCS::CAM::Group
访问管理-用户组
QCS::CAM::Role
访问管理-角色
QCS::CAM::Policy
访问管理-策略
QCS::COS::Bucket
对象存储-存储桶
QCS::VPC::Vpc
私有网络-私有网络
QCS::VPC::SecurityGroup
私有网络-安全组
QCS::VPC::Subnet
私有网络-子网
QCS::CAM::User
访问管理-用户
2022-11-14 10:57:10
编辑监控范围
选择监控的资源类型 (10)
请输入资源类型搜索
资源类型
QCS::CAM::Group
访问管理-用户组
QCS::CAM::Role
访问管理-角色
QCS::CAM::Policy
私有网络-策略
QCS::COS::Bucket
对象存储-存储桶
QCS::VPC::Vpc
私有网络-私有网络
支持按住 shift 键进行多选
已选择 (10)
资源类型
QCS::CAM::Group
访问管理-用户组
QCS::CAM::Role
访问管理-角色
QCS::CAM::Policy
访问管理-策略
QCS::COS::Bucket
对象存储-存储桶
QCS::VPC::Vpc
私有网络-私有网络
确定
取消

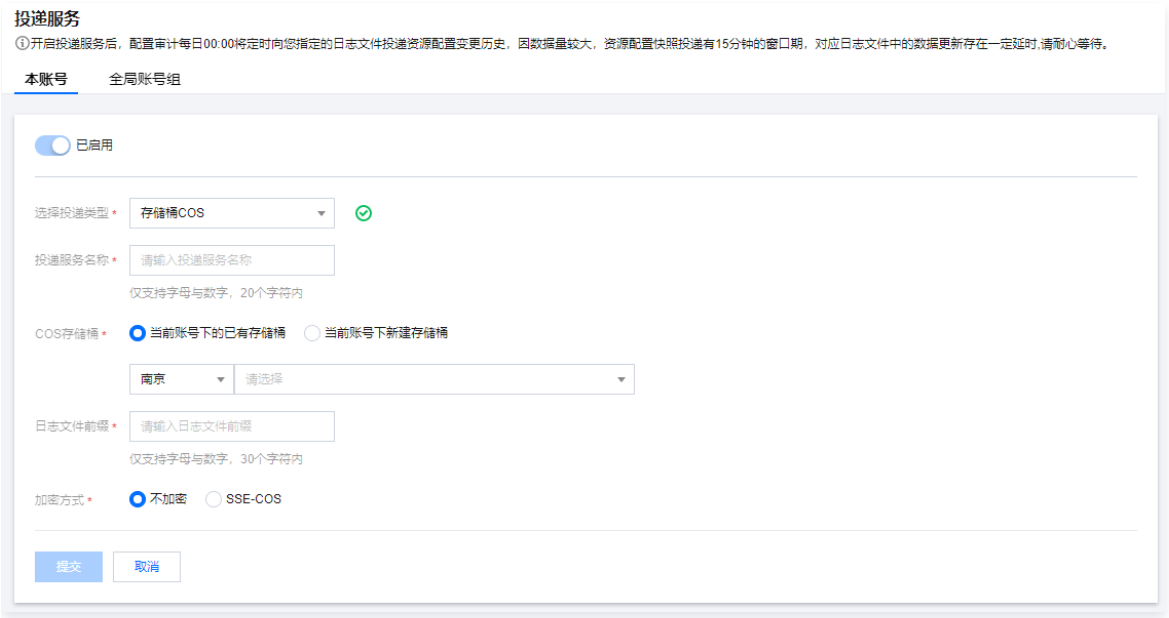
投递服务

最近更新时间：2024-11-08 16:07:52

投递资源时间线

单击**设置-投递服务**菜单，进入**投递服务**页面，单击**开启**即可创建投递服务，将资源时间线中的定时配置历史记录投递至您指定的投递类型中，以便于您对资源配置数据执行更为精细化的分析、以及更长时间的存储。

对于开启投递服务后，当时间线更新时，配置审计每日00:00将向您指定的 COS 存储桶投递资源配置变更历史。当您**关闭**投递服务，时间线的更新不会存储到对应的存储桶。



因数据量较大，资源配置快照拉取及投递到 COS 存储桶有10分钟的窗口期，导致投递至 COS 存储桶的数据更新存在一定延时，请耐心等待。

资源快照更新

最近更新时间：2023-07-13 22:07:34

单击手动更新，系统将立即拉取最新的资源快照数据，并根据捕捉的最新资源快照数据更新资源列表及相应的资源时间线。