配置审计

快速入门

文档版本 01

发布日期 2023-10-25

华为技术有限公司

商标声明

HUAWEI和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

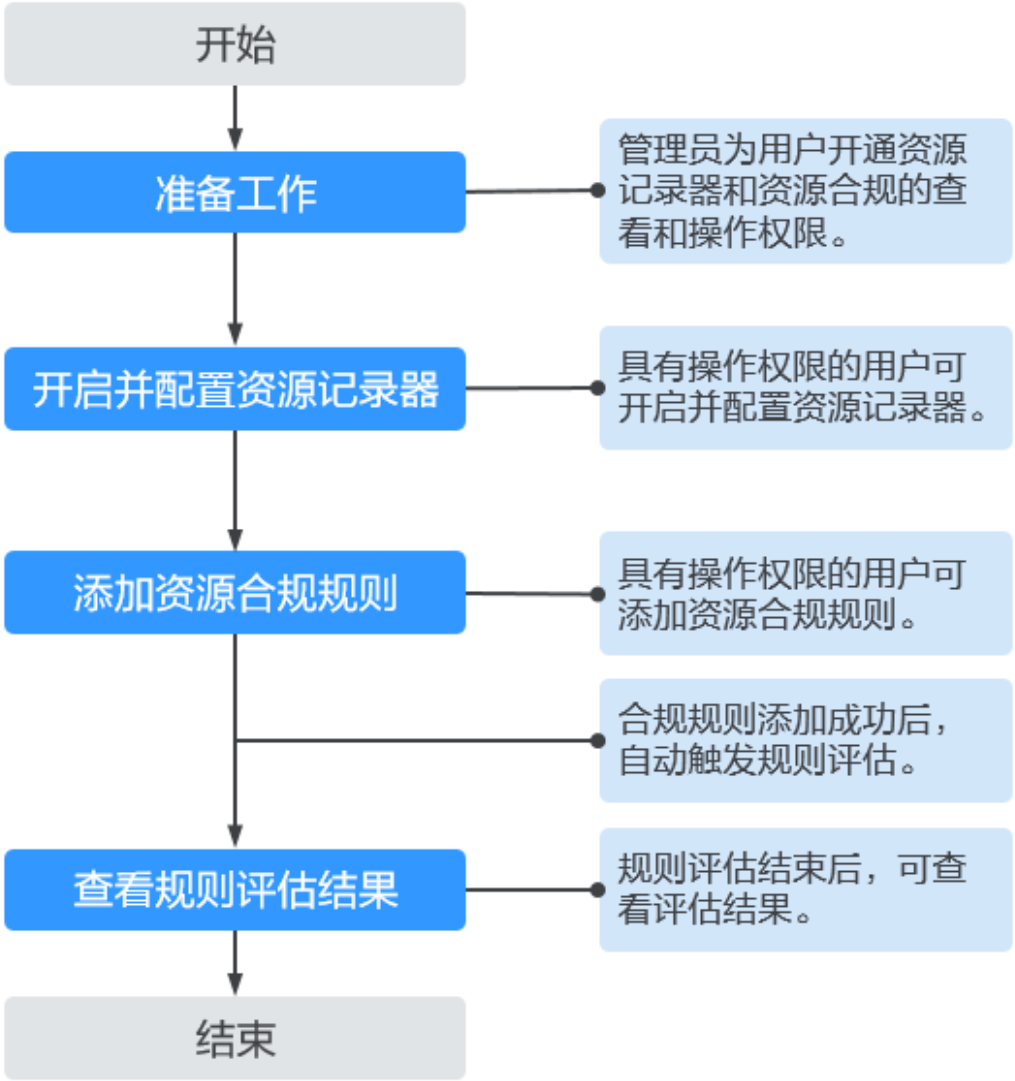
目 录

1 快速入门

如果您首次使用配置审计服务，建议参考本章节。它可以帮助您快速使用配置审计服务的主要功能。配置审计服务的约束与限制请参见**约束与限制**。

快速入门操作流程图如下：

图 1-1 配置审计（Config）快速入门流程图



开启并配置资源记录器

开启并配置资源记录器后，当您的资源变更（被创建、修改、删除）、资源关系变更时，您均可收到通知，同时还可对您的资源变更消息和资源快照进行定期存储。

步骤1 登录管理控制台。

步骤2 单击页面左上角的☰图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源记录器”，进入“资源记录器”页面。

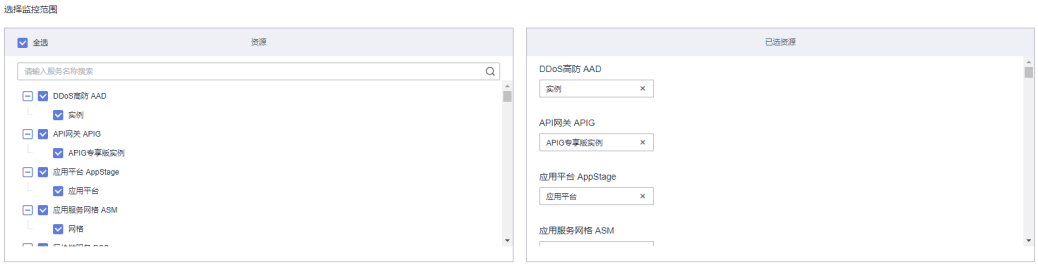
步骤4 打开资源记录器开关，在弹出的确认框中单击“是”，资源记录器开启成功。

图 1-2 开启资源记录器

步骤5 选择资源的监控范围。

默认情况下，资源记录器的监控范围会覆盖当前所有支持的资源。您可以修改资源记录器的监控范围，选择指定的资源类型进行监控。

图 1-3 选择监控范围



步骤6 配置资源转储。

选择OBS桶，用于存储资源变更消息及资源快照。如无OBS桶，则需先创建OBS桶，详见《对象存储服务用户指南》。

- **配置当前账号下OBS桶：**

  选择您账号下的OBS桶，用于存储资源变更消息及资源快照，如果用于转储的OBS桶指定了前缀，则还需添加桶前缀。如您的账号下无OBS桶，则需先创建OBS桶，详见《对象存储服务用户指南》。

- **配置其他账号下OBS桶：**

  选择“另一账号的桶”，并输入区域ID和桶名称，如果用于转储的OBS桶指定了前缀，则还需添加桶前缀。需先使用其他账号对当前账号授予相关OBS桶的权限，具体操作请参见跨账号授权。

说明

开启资源记录器时，如果指定了当前账号或其他账号下的OBS桶，Config会向目标OBS桶中写入一个名为ConfigWritabilityCheckFile的空文件，此文件用来验证资源转储是否能够成功写入OBS桶。

图 1-4 配置资源转储

步骤7 配置数据保留周期。

资源记录器收集到的资源配置信息数据默认保留7年（2557天），您可以将配置信息数据设置自定义保留周期，自定义数据保留周期的可设置范围为最短30天，最长7年（2557天）。

说明

虽然Config使用SMN和OBS发送资源变更消息通知和存储资源变更消息及资源快照，但Config自身也会保存资源的历史变更信息。此处配置的数据保留时间仅针对于Config，不会对SMN和OBS存储的数据产生影响。

当您配置数据保留周期后，Config会在指定周期内保留您的资源历史数据，超出指定周期的数据将会被删除。

图 1-5 配置数据保留周期

步骤8 开启并配置消息通知（SMN）主题。

打开主题开关，选择主题所在区域和主题名，用于接收资源变更时产生的消息通知。如无SMN主题，则需先创建SMN主题，详见《消息通知服务用户指南》。

- **配置当前账号下消息通知主题：**

  选择“您自己的主题”，并选择主题所在区域和主题名，用于接收资源变更时产生的消息通知。如无SMN主题，则需先创建SMN主题，详见《消息通知服务用户指南》。

- **配置其他账号下消息通知主题：**

  选择“另一账号的主题”，并输入主题URN。需先使用其他账号对当前账号授予相关SMN主题的权限，具体操作请参见跨账号授权。

说明

创建SMN主题后，还需执行“添加订阅”和“请求订阅”操作，消息通知才会生效。详见《消息通知服务用户指南》。

图 1-6 配置 SMN 主题

步骤9 进行授权，选择“快速授权”或“自定义授权”。

- **快速授权：**将为您快速创建一个名为“rms_tracker_agency”的委托权限，该权限是可以让资源记录器正常工作的权限，包含调用消息通知服务（SMN）发送通知的权限和对象存储服务（OBS）的写入权限（例如SMN Administrator和OBS OperateAccess权限）。由于快速授权的委托中并不包含KMS的相关权限，因此资源记录器无法将资源变更消息和资源快照存储到“使用KMS方式加密的OBS桶”中。如有需要，您可以在委托中添加对应权限（KMS Administrator）或使用自定义授权，具体请参见资源变更消息和资源快照转储至OBS加密桶。
- **自定义授权：**您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，授权对象为云服务RMS，但必须包含可以让资源记录器正常工作的权限（调用消息通知服务（SMN）发送通知的权限和对象存储服务（OBS）的写入权限）。如果需要将资源变更消息和资源快照存储到“使用KMS方式加密的OBS桶”中，还需要添加KMS的密钥管理员权限（KMS Administrator），具体请参见资源变更消息和资源快照转储至OBS加密桶。创建委托详见《统一身份认证服务用户指南》。

  说明

  此处的授权为**委托授权**，授权消息通知服务（SMN）的发送通知权限和对象存储服务（OBS）的写入权限给Config服务，允许资源记录器将消息通知发送到您的SMN主题和将资源变更消息以及资源快照存储到您的OBS桶。

  图 1-7 授权

步骤10 配置完成后，单击“保存”。

步骤11 在弹出的确认框中单击“是”，资源记录器配置成功。

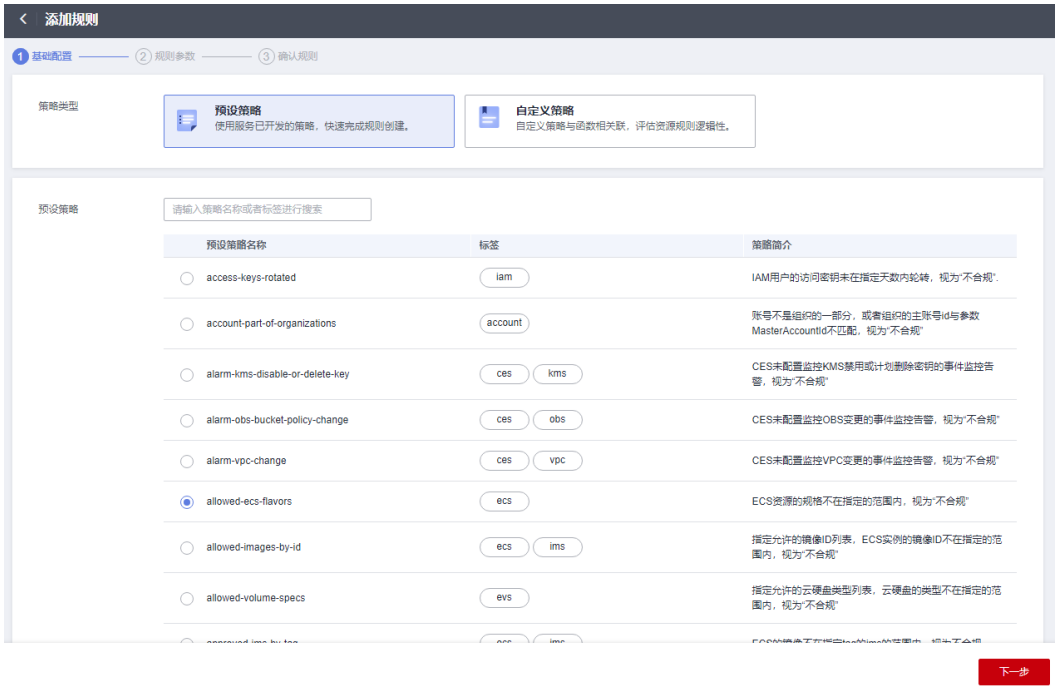
----结束

添加资源合规规则

步骤1 单击左侧的“资源合规”，进入“资源合规”页面。

步骤2 在“规则”页签下单击“添加规则”，进入“基础配置”页面，基础配置完成后，单击页面右下角的“下一步”。

图 1-8 添加合规规则-基础配置



相关参数配置，详见**表1 基础配置参数说明**。

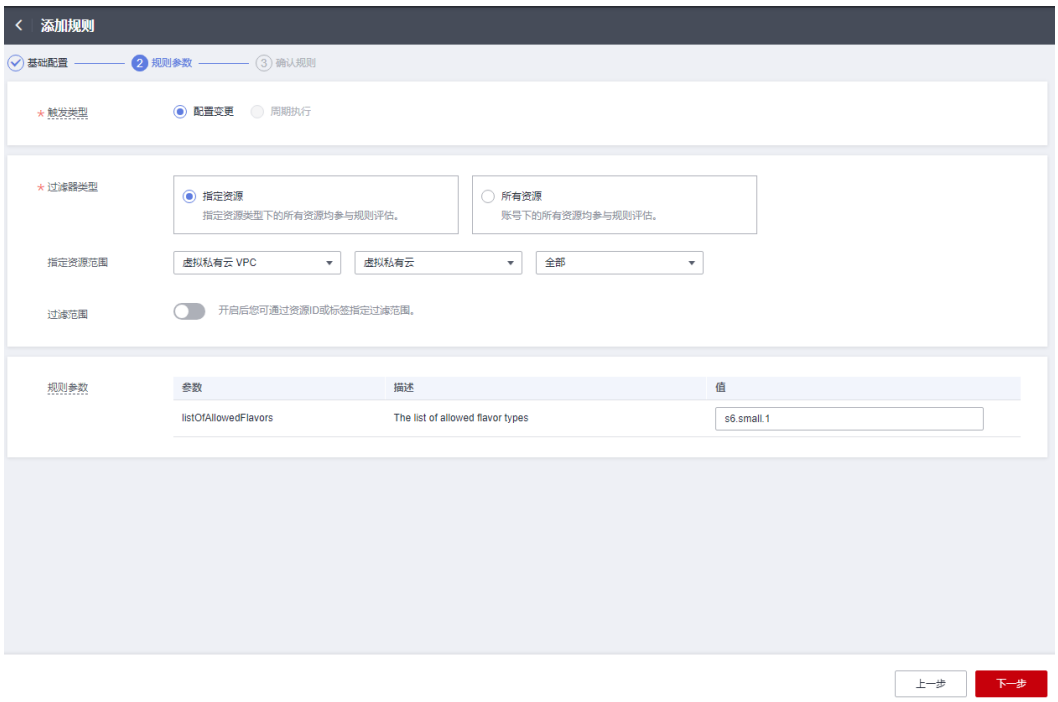
表 1-1 基础配置参数说明

参数	说明
策略类型	策略类型有： ● 预设策略 ● 自定义策略
预设策略	预设策略即服务已开发的策略。 使用服务已开发的策略，快速完成合规规则创建。 预设策略详情见**系统内置预设策略**。
自定义策略	允许用户通过自定义策略来创建合规规则。 自定义策略详情见**添加自定义合规规则**。
规则名称	规则名称默认复用所选择预设策略的名称，不能与已存在的合规规则名称重复，如有重复需自行修改。 合规规则名称仅支持数字、字母、下划线和中划线。
规则简介	规则简介默认复用所选择预设策略的简介，也可自行修改。 目前对合规规则简介的内容不做限制。
FunctionGraph 函数	用户自定义策略执行函数的urn。 创建FunctionGraph函数请参见**创建FunctionGraph函数**。 仅当“策略类型”选择“自定义策略”时需配置此参数。

参数	说明
授权	此处的授权为**委托授权**，授权函数工作流（FunctionGraph）的只读权限和调用权限给Config服务，允许自定义合规规则查询函数工作流以及将事件发送至函数工作流。 仅当“策略类型”选择“自定义策略”时需配置此参数。 **说明** • **快速授权**：将为您快速创建一个名为“rms_custom_policy_agency”的委托权限，该权限是可以让自定义合规规则正常工作的权限，包含函数工作流（FunctionGraph）的只读权限和调用权限。 • **自定义授权**：您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，但必须包含可以让自定义合规规则正常工作的权限（函数工作流（FunctionGraph）的只读权限和调用权限），创建委托详见**《统一身份认证服务用户指南》**。

步骤3 进入“规则参数”页面，规则参数配置完成后，单击“下一步”。

图 1-9 添加合规规则-规则参数



相关参数配置，详见**表2 合规规则参数说明**。

表 1-2 合规规则参数说明

参数	说明
触发类型	用于触发资源合规规则。 触发类型有： ● 配置变更：在指定的云资源发生更改时触发规则评估。 ● 周期执行：按照您设定的频率运行。
过滤器类型	用于指定资源类型参与规则评估。 过滤器类型分为： ● 指定资源：指定资源类型下的所有资源均参与规则评估。 ● 所有资源：账号下的所有资源均参与规则评估。 仅当“触发类型”为“配置变更”时需配置此参数。
指定资源范围	过滤器类型选择“指定资源”后，需选择指定资源范围。 ● 服务：选择资源所属的服务； ● 资源类型：选择对应服务下的资源类型； ● 区域：选择资源所在的区域。 仅当“触发类型”为“配置变更”时需配置此参数。
过滤范围	使用过滤范围可指定资源类型下的某个具体资源参与规则评估。 过滤范围开启后您可通过资源ID或标签指定过滤范围。 仅当“触发类型”为“配置变更”时需配置此参数。
周期频率	设置合规规则周期执行的频率。 仅当“触发类型”为“周期执行”时需配置此参数。
规则参数	此处的“规则参数”和第一步所选的“预设策略”或“自定义策略”相对应，是对第一步所选的预设策略或自定义策略进行具体参数设置。 例如：第一步预设策略选择“required-tag-check”，指定一个标签，不具有此标签的资源，视为“不合规”，则这里的规则参数就需要指定具体的标签键和值作为判断是否合规的依据。 有的“预设策略”需要添加规则参数，有的“预设策略”不需要添加规则参数（例如：volumes-encrypted-check：已挂载的云硬盘未进行加密，视为“不合规”）。 自定义策略的规则参数最多可以设置10个，由您自行配置。

步骤4 进入“确认规则”页面，确认规则信息无误后，单击“提交”按钮，完成合规规则添加。

图 1-10 添加合规规则-确认规则

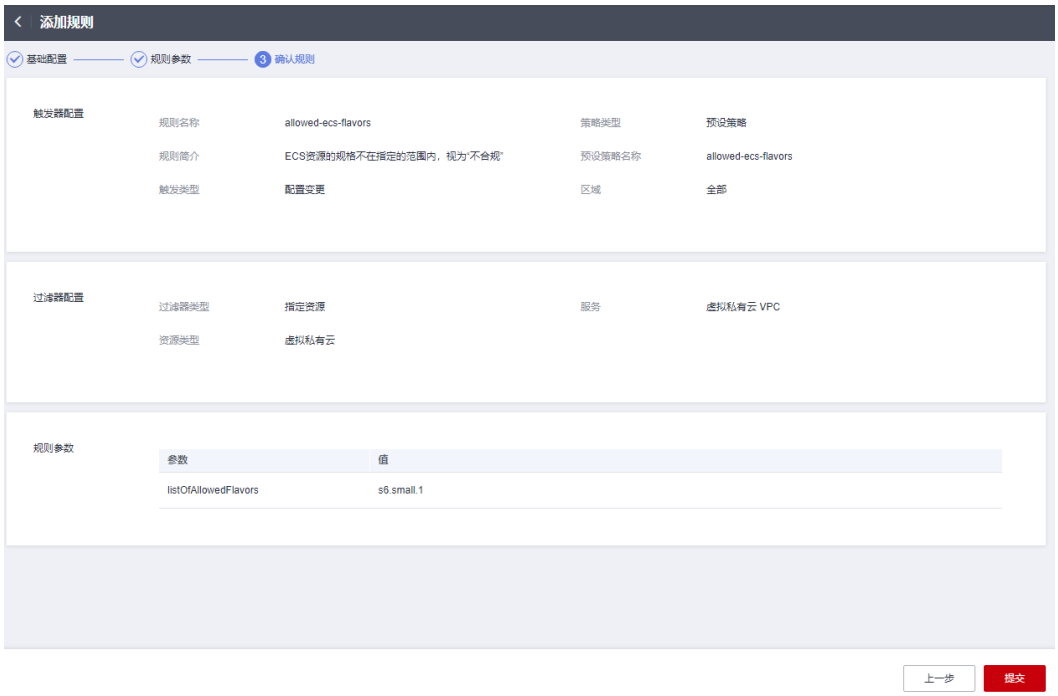


图 1-11 查看创建的合规规则

说明

合规规则创建后会立即自动触发首次评估。

----结束

查看规则评估结果

资源合规规则添加完成后，您可以在规则列表中查看所有已添加的合规规则，进入规则详情页可查看规则的评估结果和规则详情配置等信息。

步骤1 登录管理控制台。

步骤2 单击页面左上角的☰图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

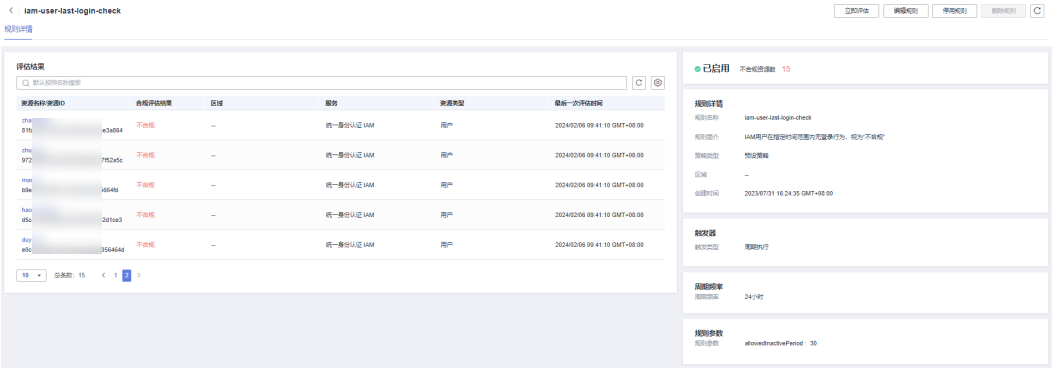
步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的列表中，可查看所有已添加的合规规则以及其运行状态、合规评估结果等信息。

步骤5 在规则列表中单击合规规则的规则名称，进入“规则详情页”。

页面左侧为此合规规则评估结果的详细信息，页面右侧为此合规规则的配置详情。

图 1-12 规则详情



说明

合规规则的运行状态分为：

- 已启用：表示此合规规则可用。
- 已停用：表示此合规规则已停用。
- 评估中：表示正在使用此合规规则进行资源评估。
- 提交中：表示自定义合规规则正在提交评估任务给FunctionGraph函数。

当规则评估正在进行中时，规则的运行状态显示为“评估中”，当规则评估结束后，规则的运行状态变为“已启用”，此时可查看规则评估结果。

----结束

高级查询概述

配置审计服务提供高级查询能力，通过使用ResourceQL自定义查询用户当前的单个或多个区域的资源配置状态。

高级查询支持用户自定义浏览、筛选和查询华为云云服务资源，用户可以通过ResourceQL在查询编辑器中编辑和查询。

ResourceQL是结构化的查询语言（SQL）SELECT 语法的一部分，它可以对当前资源数据执行基于属性的查询和聚合。查询的复杂程度不同，既可以是简单的标签或资源标识符匹配，也可以是更复杂的查询，例如查看指定具体OS版本的云服务器。

您可以使用高级查询来实现：

- 库存管理。例如检索特定规格的云服务器实例的列表。
- 安全合规检查。例如检索已启用或禁用特定配置属性（公网IP，加密磁盘）的资源的列表。
- 成本优化。例如查找未挂载到任何云服务器实例的云磁盘的列表。

资源聚合器概述

配置审计服务提供多账号资源数据聚合能力，通过使用资源聚合器聚合其他华为云账号或者组织成员账号的资源配置和合规性数据到单个账号中，方便统一查询。

资源聚合器提供只读视图，仅用于查看聚合的源账号的资源信息和合规性数据。资源聚合器不提供对源账号资源数据的修改访问权限。例如，无法通过资源聚合器部署规则，也无法通过资源聚合器从源账号提取快照文件。

合规规则包概述

配置审计服务提供合规规则包能力，合规规则包是多个合规规则的集合，帮助您统一创建和管理合规规则，并统一查询合规性数据。