

配置审计

常见问题

文档版本 01
发布日期 2025-04-29



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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云计算技术有限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，华为云计算技术有限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。

目 录

1 资源清单常见问题..... 1

2 资源合规常见问题..... 3

3 资源记录器常见问题..... 5

1 资源清单常见问题

“资源清单”页面中怎么无法删除资源？

“资源清单”页面只提供查看、导出资源功能，如果要对资源进行删除等管理类的操作，请单击右侧操作列的“查看详情”，跳转至资源所属的服务页面进行操作。

图 1-1 查看资源详情



为什么云服务资源发生了变化，“资源清单”中相应资源未发生变化？

资源数据同步到Config存在延迟。

对于已开启资源记录器且在监控范围内的资源，Config会在24小时内校正资源数据。如您未开启资源记录器，或相关资源不在资源记录器配置的监控范围内，则Config不会校正这些资源的数据。

另外，并非已对接Config的云服务资源发生的所有变化都会被Config收集，这取决于各对接服务向Config上报的资源属性，例如IAM用户的SK（SecretAccessKey）属性未上报Config，那么SK字段的变化Config不会感知。

为什么某些云服务的资源存在标签，但无法在 Config 中使用该资源的标签进行相关的业务操作，例如在“资源清单”中无法通过标签搜索到相应资源？

部分云服务资源的标签信息暂未上传至Config服务，“资源清单”页面无法获取相关的标签信息则会认为该资源无标签，因此无法通过标签搜索到相应资源。

另外，Config服务的高阶能力基于“资源清单”收集到的数据来进行分析，部分云服务资源的标签信息未上传至Config，还会导致相关资源涉及标签场景的资源合规评估结果可能出现误差。

Config服务将跟踪并持续推动相关云服务资源同步的完整性。

2 资源合规常见问题

最多可以添加多少个合规规则？

每个账号最多可以添加500个合规规则。

添加合规规则时，规则参数指的是什么？

规则参数和合规策略是对应的，例如：您选择了“资源具有指定的标签”预设策略，则需要配置该预设策略对应的规则参数“key”和“value”的具体值。

预设策略的规则参数无法增删，但是您可以根据需要为其设置不同的参数值，将合规策略重用于不同的方案。

自定义策略的规则参数由您自行配置，您可以根据需要为自定义策略添加不同的规则参数，最多可添加10个。

图 2-1 规则参数赋值

规则参数	参数	描述	值
	specifiedTagKey	允许的标签键	参数值
	specifiedTagValue	允许的标签值列表	请输入如下格式参数: ["first","second"]。

添加“iam-password-policy”、“iam-user-mfa-enabled”等合规规则后，为什么没有合规评估结果？

资源合规的数据来源于Config服务在资源清单页面所收集到的全部资源。请检查相关资源在资源清单页面中是否正常展示，如未正常展示，可能是由于您没有开启资源记录器导致未收集到相应的资源数据。

如果您需要使用这些合规规则，请开启资源记录器并收集相关的资源数据；如不需要使用这些规则，请停用未收集资源数据对应的合规规则，避免造成混淆或产生不必要的费用。

组织合规规则和组织合规包创建完成后，为什么会在部分组织成员账号中部署异常，且提示“tracker-config needs to be enabled”？

是因为这些组织成员账号未开启资源记录器导致的部署异常。

Config服务的相关功能均依赖于资源记录器收集的资源数据，因此账号必须开启资源记录器才可正常使用合规规则和合规规则包功能。

在组织合规规则和组织合规规则包场景下，除下发规则和合规规则包的组织管理员或Config服务的委托管理员之外，所部署的组织成员账号也需要开启资源记录器，才能正常下发合规规则和合规规则包。

3 资源记录器常见问题

资源快照和资源变更消息是存储在同一个 OBS 桶里面吗？

是存储在同一个OBS桶中的。

如果您在开启并配置资源记录器时，配置了对象存储OBS桶和消息通知SMN主题，则资源快照及资源变更的消息均会定期存储在该OBS桶中。

资源存储和资源变更消息存储的周期分别是多长时间？

您在开启并配置了资源记录器的资源转储和主题功能后，资源记录器会定期（24小时）将**资源快照**存储至您配置的OBS桶中，会定期（6小时）将**资源变更消息**存储至您配置的OBS桶中。

开启并配置资源记录器时，“主题”和“资源转储”是必须配置的吗？

主题（SMN主题）和资源转储（OBS桶）至少需要配置一个。其中主题是可选配置的，但如果您先配置了SMN主题，则也可以不配置资源转储（OBS桶）。

配置了资源记录器，但在资源发生变更时，为什么没有收到消息通知？

没有收到消息通知，主要有以下几种情况：

- 在配置资源记录器时，未配置“主题”，即未配置SMN主题。修改资源记录器，配置SMN主题即可解决。
- 在配置资源记录器时，配置了“主题”，但只**创建主题**，未执行“**添加订阅**”和“**请求订阅**”操作。
- 对接服务未上报此资源变更情况。
- SMN存在消息同步或消息发送的延迟。

配置了资源记录器，为什么资源变更消息没有存储在配置的 OBS 桶中？

资源变更消息存储功能需要您同时配置SMN主题（创建主题 -> 添加订阅 -> 请求订阅）和对象存储OBS桶。

请检查您是否同时配置了SMN主题和对象存储OBS桶。

为什么我没有对资源进行操作，却收到了资源消息通知？

用户开启资源记录器的消息通知功能后，当资源属性发生变化，Config就会向用户发送消息通知，其中包括非用户操作导致的属性变化和资源属性的数据结构变化等，具体请参见[消息通知](#)。因此，不建议使用“短信”或“邮件”接收Config的消息通知，推荐使用“HTTPS”或“FunctionGraph（函数）”方式。

如何获取各对接云服务上报 Config 的资源属性？

获取各对接云服务上报Config的资源属性有如下两种方式：

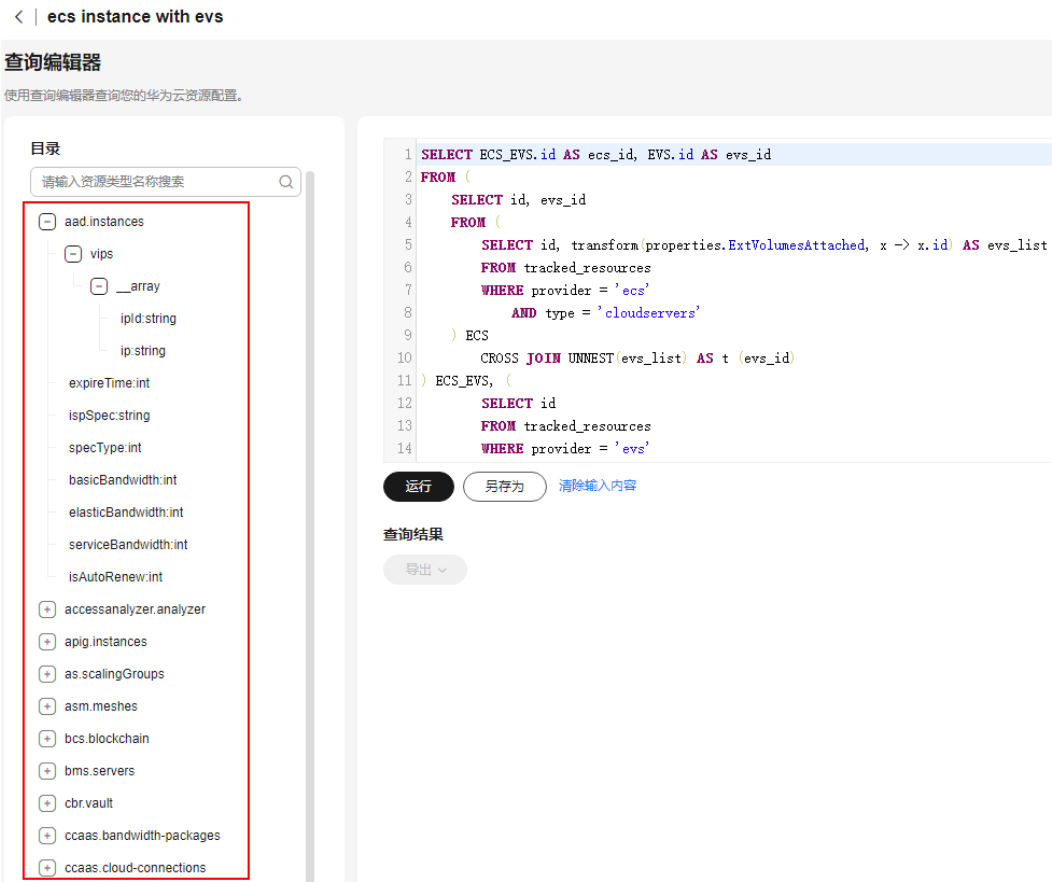
- 通过Config管理控制台的高级查询功能，进入查询编辑器即可在界面左侧获取，如下步骤仅为进入查询编辑器的其中一种方式。
 - 登录管理控制台。
 - 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”。
 - 在左侧的导航栏中，选择“高级查询”。
 - 在“预设查询”列表中单击任一查询操作列的“使用查询”。

图 3-1 使用查询



- 进入查询编辑器，界面左侧显示各对接云服务资源类型的详细属性，并支持输入资源类型名称进行搜索。

图 3-2 查看资源类型详细属性



- 通过“[列举高级查询Schema](#)”接口获取，其中type字段为资源类型，schema字段为此资源类型上报Config的资源属性。

为什么开启并配置资源记录器后，将数据转储至当前账号或其他账号的 OBS 桶时报错？

如果界面出现“Failed to write the ConfigWritabilityCheckFile file to the OBS bucket because the OBS bucket or the IAM agency is invalid.”报错，则需要确认如下场景：

- 资源记录器使用的IAM委托权限中，需要具有OBS服务的“obs:object:PutObject”权限；
- 将数据存储至当前账号的OBS桶时，桶策略不能显式Deny掉来自IAM委托的PutObject操作（Action）；如果是跨账号存储场景，桶策略需要显式Allow来自IAM委托的PutObject操作（Action），具体请参见[跨账号授权](#)，关于桶策略的权限判断逻辑请参见[桶策略参数说明](#)；
- 用于存储的OBS桶是否开启服务端加密。如果已开启服务端加密，则还需要配置KMS的权限，具体请参见[资源变更消息和资源快照转储至OBS加密桶](#)。