

配置审计

快速入门

文档版本

01

发布日期

2024-09-30



版权所有 © 华为技术有限公司 2024。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 开启并配置资源记录器.....	1
2 查看和筛选资源.....	4
3 评估资源合规性.....	8

1 开启并配置资源记录器

操作场景

资源记录器为您提供面向资源的配置记录监控能力，帮您轻松实现海量资源的自主监管，用来跟踪您在云平台上且Config支持的云服务资源变更情况。

开启并配置资源记录器的资源转储和主题功能后，当对接服务上报Config的资源变更（被创建、修改、删除等）、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。

Config服务的相关功能均依赖于资源记录器收集的资源数据，不开启资源记录器将会影响其他功能的正常使用，例如资源清单页面无法获取资源最新数据、合规规则无法创建、修改、启用和触发规则评估、资源聚合器无法聚合源账号的资源数据等，因此使用Config时您必须保持资源记录器的开启状态。

本章节指导您如何开启并配置资源记录器，用于收集您的云上资源数据，为Config的其他功能提供必须的支持。

准备工作

1. 如果您已有一个华为账号，请忽略此步骤。如果您还没有华为账号，请参考以下步骤创建。
 - a. 打开[华为云官网](#)，单击“注册”。
 - b. 根据提示信息完成注册，详细操作请参见“[注册华为账号并开通华为云](#)”。注册成功后，系统会自动跳转至您的个人信息界面。
 - c. 参考[个人账号如何完成实名认证](#)或[企业账号如何完成实名认证](#)，完成个人或企业账号实名认证。
2. 为账号充值。


配置审计服务本身为免费服务，但使用资源记录器时资源转储OBS桶和消息通知SMN主题至少需要配置一个，因此资源记录器使用的消息通知服务（SMN）或对象存储服务（OBS）可能会产生相应的费用，具体请参见[SMN计费说明](#)和[OBS计费说明](#)。

您需要确保账号有足够的余额，避免因账号余额不足或欠费导致资源记录器的相关功能无法使用，从而影响Config的其他功能也无法使用。如何充值请参见[账户充值](#)。

操作步骤

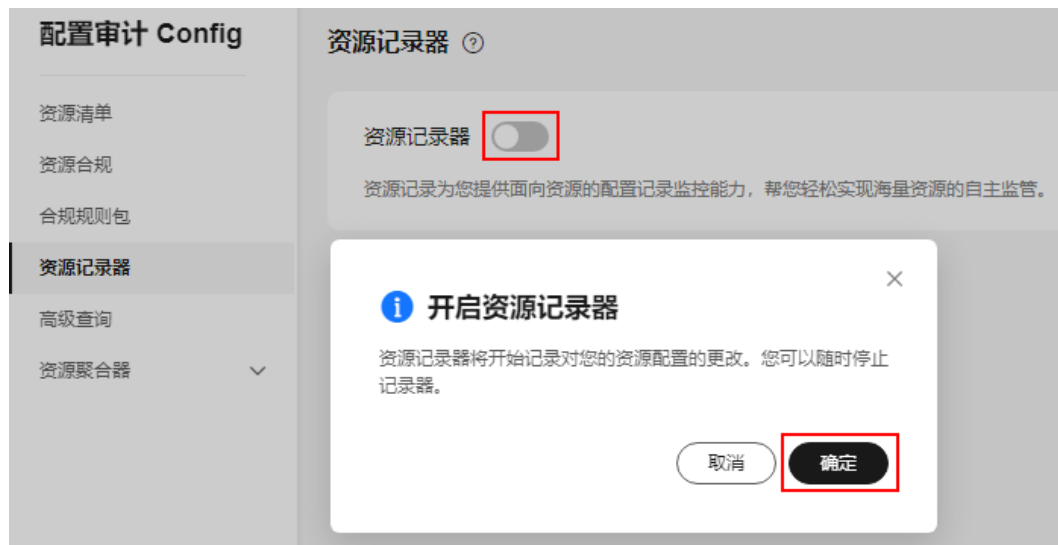
如下步骤仅针对资源记录器必须配置的参数进行介绍，其他参数保持默认即可，更多配置资源记录器的详细信息请参见[配置资源记录器](#)。

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”。

步骤3 单击左侧导航栏的“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“确定”，资源记录器开启成功。



步骤5 配置资源转储。

资源转储

将配置信息存储至您指定的对象存储服务 OBS 中。

您账号的桶 另一账号的桶

bucket-example002

桶前缀(可选)

[创建 OBS 桶](#)

选择“您账号的桶”，然后在下拉列表中选择您账号下的 OBS 桶，用于存储资源变更消息及资源快照。

如您的账号下无 OBS 桶，则需先创建 OBS 桶，详见[创建桶](#)。

步骤6 开启并配置消息通知（SMN）主题。

主题



将资源更改和通知传输到 SMN 主题。如果您选择电子邮件作为 SMN 主题的通知终端节点，则会产生大量电子邮件。

您自己的主题



as-test-msg



[创建主题](#)

打开主题开关，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。

如您无SMN主题，则需先创建SMN主题，详见[创建主题](#)。

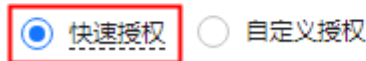
📖 说明

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。

步骤7 进行授权，选择“快速授权”。

授权

允许资源记录器将信息发送到您的SMN消息通知服务和对象存储服务。



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）。

步骤8 单击“保存”。

步骤9 在弹出的确认框中单击“确定”。

----结束

相关信息

资源记录器配置完毕后，您可以随时修改资源记录器的配置或关闭资源记录器。当前每天仅支持最多开启和修改资源记录器10次，每天0点将重置此次数。

- 在配置资源记录器的“资源转储”和“主题”功能时，支持选择其他账号下的OBS桶或SMN主题，但需先使用其他账号对当前账号进行授权，具体操作请参见[跨账号授权](#)。
- 在资源记录器的“授权”时，您可自行在统一身份认证服务（IAM）中创建委托，并进行“自定义授权”，授权对象为云服务Config，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）的写入权限至少包含一个）。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[委托其他云服务管理资源](#)。

2 查看和筛选资源

操作场景

本章节指导您如何通过Config的资源清单页面查看和筛选您账号下的资源，便于您了解拥有的资源及其所在区域、资源状态等信息。

说明

资源清单中的资源数据依赖于资源记录器所收集的资源数据，如果相关资源无法在资源清单页面查询到，请确认资源记录器是否开启，或该资源类型是否被资源记录器收集资源数据，或Config暂不支持该服务或资源类型。

资源数据同步到Config存在延迟，因此资源发生变化时不会实时更新“资源清单”中的数据。对于已开启资源记录器的用户，Config会在24小时内校正资源数据。

准备工作

1. 如果您已有一个华为账号，请忽略此步骤。如果您还没有华为账号，请参考以下步骤创建。
 - a. 打开[华为云官网](#)，单击“注册”。
 - b. 根据提示信息完成注册，详细操作请参见“[注册华为账号并开通华为云](#)”。注册成功后，系统会自动跳转至您的个人信息界面。
 - c. 参考[个人账号如何完成实名认证](#)或[企业账号如何完成实名认证](#)，完成个人或企业账号实名认证。
2. 为账号充值。


配置审计服务本身为免费服务，但使用资源记录器时资源转储OBS桶和消息通知SMN主题至少需要配置一个，因此资源记录器使用的消息通知服务（SMN）或对象存储服务（OBS）可能会产生相应的费用，具体请参见[SMN计费说明](#)和[OBS计费说明](#)。

您需要确保账号有足够的余额，避免因账号余额不足或欠费导致资源记录器的相关功能无法使用，从而影响Config的其他功能也无法使用。如何充值请参见[账户充值](#)。
3. [开启并配置资源记录器](#)。

资源清单中的资源数据依赖于资源记录器所收集的资源数据，因此必须保持资源记录器的开启状态。

操作步骤

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。

“资源清单”页面默认展示在资源记录器配置的监控范围内且您拥有的资源信息。



步骤3 通过选择服务、资源类型和区域来筛选资源，其中全局级服务无需选择区域。



步骤4 在页面中部的搜索框中通过多种筛选条件进行更精细的资源筛选。



筛选条件	说明
名称	资源名称支持模糊搜索，并且忽略大小写。
资源ID	资源ID支持模糊搜索，但不忽略大小写。
资源状态	通过资源状态对资源进行筛选。 资源状态分为以下两种： <ul style="list-style-type: none"> ● 保有中：资源正常使用中。 ● 已删除：资源已删除。
标签	直接在搜索框列表选择一个标签键，然后再选择此标签键相关的一个标签值或所有标签值，资源列表将自动筛选并展示此标签关联的资源。
企业项目	通过企业项目筛选框选择企业项目，资源列表将自动筛选并展示此企业项目下的资源。 说明 根据企业项目筛选资源的功能必须要先 开通企业项目 才可以使用，因此该筛选条件并非对每个用户可见。

---结束

相关信息

在“资源清单”页面筛选出您需要查看的资源后，您还可以进行如下操作：

- [查看单个资源详情](#)
- [导出资源列表](#)
- [查看资源合规](#)
- [查看资源关系](#)
- [查看资源历史](#)

Config服务还提供如下高阶功能，可对资源进行更精细复杂的查询，或聚合多账号的资源数据进行统一查看：

- [高级查询](#)
- [资源聚合器](#)

3 评估资源合规性

操作场景

资源合规特性帮助您快速创建一组合规规则，用于评估您的资源是否满足合规要求。您可以选择Config提供的[系统内置预设策略](#)或自定义策略，并指定需要评估的资源范围来创建一个合规规则；合规规则创建后，有多种机制[触发规则评估](#)，然后查看合规规则的评估结果来了解资源的合规情况。

本章节以添加预设策略“[IAM用户在指定时间内有登录行为](#)”为例，用于及时发现账号下不活跃的IAM用户，减少闲置用户或降低密码泄露的风险，提升账号安全。

准备工作

1. 如果您已有一个华为账号，请忽略此步骤。如果您还没有华为账号，请参考以下步骤创建。
 - a. 打开[华为云官网](#)，单击“注册”。
 - b. 根据提示信息完成注册，详细操作请参见“[注册华为账号并开通华为云](#)”。注册成功后，系统会自动跳转至您的个人信息界面。
 - c. 参考[个人账号如何完成实名认证](#)或[企业账号如何完成实名认证](#)，完成个人或企业账号实名认证。

2. 为账号充值。

配置审计服务本身为免费服务，但使用资源记录器时资源转储OBS桶和消息通知SMN主题至少需要配置一个，因此资源记录器使用的消息通知服务（SMN）或对象存储服务（OBS）可能会产生相应的费用，具体请参见[SMN计费说明](#)和[OBS计费说明](#)。

您需要确保账号有足够的余额，避免因账号余额不足或欠费导致资源记录器的相关功能无法使用，从而影响Config的其他功能也无法使用。如何充值请参见[账户充值](#)。


3. [开启并配置资源记录器](#)。

添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。且仅被资源记录器收集的资源可参与资源评估，为保证资源合规规则的评估结果符合预期，建议您配置资源记录器时选择监控全部资源。

步骤一：添加合规规则

如下步骤仅针对示例进行参数设置和介绍，其他参数的详细说明请参见[添加预定义合规规则](#)。

步骤1 登录管理控制台。

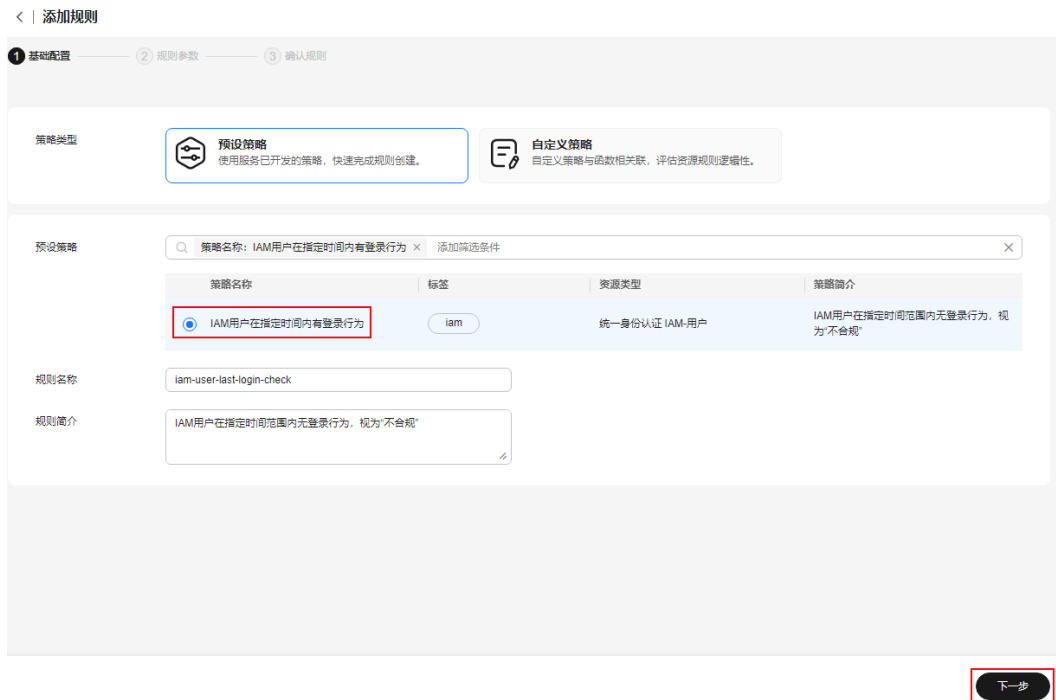
步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”。

步骤3 单击左侧导航栏的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下单击“添加规则”。



步骤5 进入“基础配置”页面，选择预设策略“IAM用户在指定时间内有登录行为”，单击“下一步”。



步骤6 进入“规则参数”页面，根据如下说明配置完成后，单击“下一步”。



参数	示例	说明
周期频率	24小时	设置合规规则周期执行的频率。 系统将按照您设定的频率，周期性的触发此规则的评估任务。 可选项：1小时、3小时、6小时、12小时、24小时。
指定资源范围	全部	指定待评估资源所在的区域。 合规规则将仅评估您指定区域下的相关资源。
规则参数	90	指定IAM用户未登录的天数，默认值为90。 若IAM用户在指定时间内没有登录行为，视为“不合规”。

步骤7 进入“确认规则”页面，确认规则信息无误后，单击“提交”按钮。

合规规则创建后会立即自动触发首次评估。

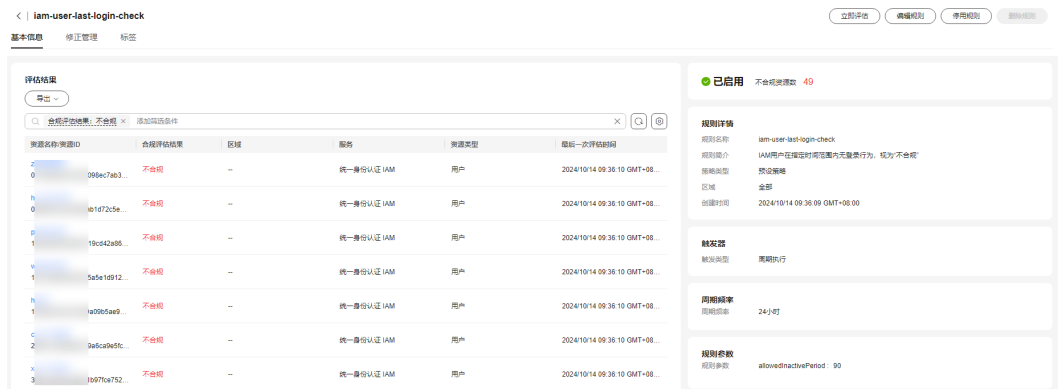
----结束

步骤二：查看规则评估结果

步骤1 在“规则”页签下的列表中，单击上一步骤添加的合规规则的规则名称。



步骤2 进入规则详情的“基本信息”页。



左侧的评估结果列表默认展示合规评估结果为“不合规”的资源，您可以在列表上方的筛选框中通过合规评估结果、资源名称或资源ID对评估结果进行筛选检索，还支持导出全部评估结果数据。

此合规规则的评估结果列表中展示的不合规资源，为超过90天未登录过管理控制台的IAM用户，您可以根据合规评估结果对这些闲置IAM用户进行处理。

----结束

相关信息

当您完成添加合规规则、查看规则评估结果等基本操作后，您还可以结合业务情况使用以下功能，满足不同资源合规审计场景的需求。

- **自定义合规规则**：当Config提供的系统内置预设策略不能满足检测资源合规性的需求时，您可以通过编写FunctionGraph函数代码，添加自定义策略来完成复杂场景的资源审计。
- **组织合规规则**：在使用资源合规时，如果您是组织管理员或Config服务的委托管理员，您可以添加组织类型的资源合规规则，直接作用于您组织内的成员账号中。
- **合规规则修正配置**：当您通过系统预设策略或自定义策略创建合规规则后，您可以为合规规则创建修正配置，按照您自定义的修正逻辑对规则检测出的不合规资源进行快速修正。
- **合规规则包**：合规规则包是合规规则的集合，通过使用合规规则包可以批量部署多条合规规则，并统一查看合规性数据。