配置审计

产品介绍

文档版本 01

发布日期 2023-10-25

华为技术有限公司

商标声明


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 什么是配置审计

简介

配置审计（Config）服务提供全局资源配置的检索，配置历史追溯，以及基于资源配置的持续的审计评估能力，确保云上资源配置变更符合客户预期。

须知

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，因此强烈建议您保持资源记录器的开启状态。如何开启并配置资源记录器请参见**配置资源记录器**。

产品架构

您可以使用Config查看您所拥有的资源有哪些；可以查看资源详情、资源之间的关系、资源历史；Config会在资源变更时发送消息通知给您，并定期（6小时）对您的资源变更消息进行存储；Config还会定期（24小时）对您的资源进行存储；您还可以通过配置合规规则来对您的资源进行合规性检查。

- **查看资源详情：**Config会索引您在云平台上的所有资源信息，为您提供丰富的检索功能。
- **查看资源关系：**Config会建立资源之间的关系状态，帮助您查看资源之间的关联关系。
- **查看资源历史：**您可以通过开启、配置资源记录器，来持续跟踪资源的变更历史。
- **发送消息通知：**您在开启资源记录器并成功配置消息通知（SMN）后，Config会推送资源变更的消息给您。
- **资源变更消息存储：**您在开启资源记录器并成功配置消息通知（SMN）和对象存储桶（OBS）后，Config会定期（6小时）对您的资源变更消息进行存储。
- **资源快照文件存储：**您在开启资源记录器并成功配置对象存储桶（OBS）后，Config会定期（24小时）对您的资源进行快照并对快照文件存储。
- **资源评估：**Config提供合规扫描，帮助您自动化地检查资源的合规性。

- **高级查询：**Config提供高级查询能力，通过使用ResourceQL语法来自定义查询云资源。
- **资源聚合器**：Config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。
- **合规规则包**：Config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。

访问方式

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问配置审计服务。

- **管理控制台方式**

  管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录**管理控制台**，单击主页左上角的  ，选择“管理与监管 >配置审计 Config”。
- **API方式**

  如果用户需要将云平台上的配置审计服务集成到第三方系统，用于二次开发，请使用API方式访问配置审计服务，具体操作请参见**《配置审计API参考》**。

2 功能总览

表2-1列出了配置审计服务的常用功能。

在使用配置审计服务之前，建议您先了解配置审计服务的基本概念，以便更好地理解本服务提供的各项功能。

表 2-1 配置审计服务常用功能

功能分类	功能名称	功能描述
资源清单	查看所有资源列表	查看当前账号下的全部资源。包含资源的名称、所在区域、所属服务、资源类型、所属企业项目。
	查看单个资源详情	查看当前账号下某个具体资源的资源详情。包含资源的名称、创建时间、规格等。
	筛选资源	通过设置筛选条件（资源名称、资源ID、标签、企业项目）快速筛选出所需要的资源。
	导出资源列表	导出所需资源列表的Excel格式文档。
	查看资源合规	查看单个资源的合规性数据。
	查看资源关系	查看资源之间的关联关系。
	查看资源历史	查看资源的变更历史。
资源合规	添加规则	添加资源合规规则后，方可进行资源合规评估。可设置合规策略类型、合规策略的规则参数等。
	立即评估	如果您需要立即启动规则评估，可以使用“立即评估”功能。
	停用规则	如果您不再需要某项资源合规规则，您可停用此规则。
	启用规则	如果您需要使用某项已被停用的资源合规规则，您可启用此规则。
	编辑规则	如果当前合规规则不再适用，您可以编辑此规则，修改规则参数等。

功能分类	功能名称	功能描述
	删除规则	如果当前合规规则不再适用，您可以删除此规则。
	不合规资源	您可以查看和导出当前账号下全部不合规资源的信息。
	组织合规规则	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。
	修正配置	针对合规规则评估出的不合规资源，您可以基于合规规则创建修正配置，按照您自定义的修正逻辑对不合规资源进行快速修正，确保您的云上资源持续合规。
资源记录器	开启资源记录器	开启资源记录器后，才可以跟踪资源的变更情况。
	配置资源记录器	配置资源监控范围、消息通知主题、资源转储，并授权资源记录器调用消息通知服务（SMN）发送通知的权限和对象存储服务（OBS）的写入权限。
	修改资源记录器	可以修改资源记录器的相关配置。如：监控范围、资源转储、数据保留周期、消息通知主题、授予的权限等。
	关闭资源记录器	如您不再需要使用资源记录器记录资源变更情况，您可以随时关闭它。
高级查询	使用高级查询	使用ResourceQL自定义查询用户当前的资源配置状态。
	新建查询	可以添加自定义查询，方便之后直接调用该模板使用高级查询。
	查看查询	查看某个查询的名称、描述和查询语句。
	修改查询	如果当前自定义查询不再适用，您可以修改已创建的自定义查询的名称、描述和查询语句。
	删除查询	如果当前自定义查询不再适用，您可以删除已创建的自定义查询。
资源聚合器	创建资源聚合器	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。
	查看资源聚合器	查看所有已创建的资源聚合器列表和详情。
	修改资源聚合器	修改资源聚合器聚合的源账号。
	删除资源聚合器	如不再需要某个资源聚合器，可以删除此资源聚合器。

功能分类	功能名称	功能描述
	查看聚合的合规规则	在规则列表中查看资源聚合器聚合的全部合规规则及其合规性数据。
	查看聚合的资源	在资源列表中查看资源聚合器聚合的全部资源。
	授权资源聚合器账号	源账号向聚合器账号授予收集资源配置和合规性数据的权限。
	资源聚合器高级查询	资源聚合器提供高级查询能力，通过使用ResourceQL自定义查询单个或多个聚合源账号的资源配置状态。
合规规则包	创建合规规则包	通过示例模板或用户自定义的模板创建合规规则包，用于统一创建和管理合规规则。
	查看合规规则包	查看已创建的合规规则包列表和详情。
	删除合规规则包	如果当前合规规则包不再适用，您可以删除已创建的合规规则包，由其管理的合规规则会自动删除。
	组织合规规则包	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合规规则包，直接作用于您组织内的成员账号中。
云审计-记录配置审计	支持云审计的关键操作	通过云审计服务，您可以记录与配置审计服务相关的操作事件，便于后续的查询、审计和回溯。
	如何查看审计日志	介绍如何在云审计服务管理控制台查看或导出最近7天的配置审计操作记录。

3 计费说明

如果您配置了资源记录器，那么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**。

如果您配置了自定义合规规则，那么自定义合规规则使用的函数工作流（FunctionGraph）可能会产生相应的费用，具体请参见**FunctionGraph计费说明**。

如果您为合规规则创建了修正配置，修正配置通过关联RFS服务的私有模板或FunctionGraph服务的函数实例来对不合规资源执行修正，因此可能会产生相应的费用，具体请参见**FunctionGraph计费说明**。使用RFS服务本身不收取费用，但通过RFS私有模板如创建了付费资源，其相关费用请参见相应服务的计费说明。

配置审计服务商用后会按资源记录器记录的资源变化次数，合规规则的执行次数收费。

配置审计服务在2024年会继续免费，后续存在收费可能，如果后续启动收费，我们会提前通知您。

4 权限管理

如果您需要针对配置审计服务，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制员工对华为云资源的访问范围。例如您希望部分员工拥有配置资源记录器的权限，那么您可以使用IAM为员工创建用户，通过授予配置资源记录器的权限策略，控制员工对配置审计服务的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用配置审计服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

Config 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

Config部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问Config时，不需要切换区域。

具有Config服务只读权限的用户具有查看“资源清单”页面的权限，可以查看用户账号下的全部资源，不需要用户具有相应云服务的只读权限。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action），Config支持的API授权项请参见《配置审计API参考》中的“权限策略及授权项说明”章节。

如表1 Config系统权限所示，包括了Config的所有系统权限。

表 4-1 Config 系统权限

系统策略名称	描述	依赖关系
RMS ConsoleFullAccess	配置审计服务控制台使用所有权限，包含查看资源，以及资源记录器、资源合规、高级查询、资源聚合器、合规规则包的查看和操作权限。	RF FullAccess
RMS FullAccess	配置审计服务所有权限，包含查看资源，以及资源记录器、资源合规、高级查询、资源聚合器、合规规则包的查看和操作权限。	RF FullAccess
RMS ReadOnlyAccess	配置审计服务只读权限，包含查看资源，以及资源记录器、资源合规、高级查询、资源聚合器、合规规则包的查看权限。	无

说明

当添加了RMS ConsoleFullAccess权限的IAM用户或IAM身份中心用户在控制台对资源记录器、合规规则和合规规则包进行操作时仍提示没有操作权限，是因为相关功能需要特定权限的IAM委托，因此需要您单独添加操作IAM委托的权限。具体详情如下：

您在对资源记录器、合规规则和合规规则包进行操作时会提示需要创建委托并添加相应权限，创建委托需要您先添加iam:agencies:createAgency（创建委托），iam:permissions:grantRoleToAgency（为委托授予指定权限）权限，其中iam:permissions:grantRoleToAgency需根据不同的操作授予指定权限。

表4-2列出了Config常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。“√”表示支持，“×”表示暂不支持。

表 4-2 常用操作与系统权限的关系

操作	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
查看所有资源列表	√	√	√
查看单个资源详情	√	√	√
筛选资源	√	√	√
导出资源列表	√	√	√
查看资源合规	√	√	√
查看资源关系	√	√	√
查看资源历史	√	√	√

操作	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
查看资源记录器	√	√	√
开启/配置/修改资源记录器	√	√	x
关闭资源记录器	√	√	x
查看合规策略定义	√	√	√
更新合规规则	√	√	x
创建合规规则	√	√	x
查看合规规则	√	√	√
删除合规规则	√	√	x
创建组织合规规则	√	√	x
修改组织合规规则	√	√	x
查看组织合规规则	√	√	√
删除组织合规规则	√	√	x
查看合规规则结果	√	√	√
触发合规规则评估	√	√	x
更新合规评估结果	√	√	x
创建合规修正配置	√	√	x
查看合规修正配置	√	√	√
修改合规修正配置	√	√	x
删除合规修正配置	√	√	x
查看合规修正执行状态	√	√	√
执行合规修正	√	√	x
添加合规修正例外	√	√	x
删除合规修正例外	√	√	x
查看合规修正例外列表	√	√	√
运行高级查询	√	√	x
新建高级查询	√	√	x
查看高级查询	√	√	√

操作	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
列举高级查询	√	√	√
更新高级查询	√	√	x
删除高级查询	√	√	x
创建资源聚合器	√	√	x
查看资源聚合器	√	√	√
修改资源聚合器	√	√	x
删除资源聚合器	√	√	x
查看聚合的合规规则	√	√	√
查看聚合的资源	√	√	√
授权资源聚合器账号	√	√	x
删除资源聚合器账号授权	√	√	x
删除资源聚合器的待授权请求	√	√	x
查看资源聚合器的待授权列表	√	√	√
运行资源聚合器高级查询	√	√	x
查看授权列表	√	√	√
创建合规规则包	√（依赖RF FullAccess）	√（依赖RF FullAccess）	x
查看合规规则包	√	√	√
列举合规规则包	√	√	√
删除合规规则包	√（依赖RF FullAccess）	√（依赖RF FullAccess）	x
更新合规规则包	√（依赖RF FullAccess）	√（依赖RF FullAccess）	x
列举合规规则包示例模板	√	√	√
创建组织合规规则包	√	√	x

操作	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
查看组织合规规则包	√	√	√
列举组织合规规则包	√	√	√
删除组织合规规则包	√	√	x
更新组织合规规则包	√	√	x

5 基本概念

资源

资源是用户可以在云平台上使用的一种实体。例如：弹性云服务器（ECS）实例、云硬盘（EVS）磁盘、虚拟私有云（VPC）实例等。

配置审计（Config）支持的资源类型和区域请参阅**支持的服务和区域**。

资源关系

资源关系记录了您在云平台上的不同资源之间的关联情况。例如：云硬盘与云服务器之间的绑定关系，云服务器与虚拟私有云之间的归属关系等。

您可以参阅**支持的资源关系**来了解目前支持的云资源关系的完整列表。

资源历史

资源历史是过去某段时间内资源不同状态的集合。

资源发生属性的变化和资源关系的变化，都会在资源历史中生成一条记录，该记录会包含此时资源的属性和资源的关系。

资源属性是用于描述资源特征的一组属性值，例如ECS资源的CPU核数信息、EVS磁盘的大小、IAM用户的密码强度等，具体请参见**如何获取各对接云服务上报Config的资源属性？**。

资源记录器

资源记录器是用来跟踪您在云平台上且Config支持的云服务资源变更情况，具体跟踪的资源变更范围取决于云服务上报Config的内容。

开启并配置资源记录器的资源转储和主题功能后，当在资源记录器监控范围内的资源被创建、修改、删除以及资源关系发生变化时，向您发出通知，同时资源记录器还可以将您的资源变更消息和资源快照进行定期存储。

资源合规性

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。您还可以查看和导出全部不合规资源的信息。

高级查询

高级查询特性提供快速查询特定资源的能力，帮助您掌握资源详情、多维度分析资源、快速导出数据报表等。

资源聚合器

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。

合规规则包

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。

6 与其他服务的关系

配置审计服务与周边服务的关系如下表所示。

表 6-1 配置审计服务与其他服务的关系

服务名称	说明	交互功能	相关内容
消息通知服务（SMN）	在配置资源记录器时，可以根据需要选择配置消息通知主题。 **说明** 如您先配置了资源存储（OBS桶），则SMN主题可以不配置。	Config支持服务的资源发生变更时，向用户发送消息通知。	**配置资源记录器**
对象存储服务（OBS）	在配置资源记录器时，可以根据需要选择配置资源存储（OBS桶）。 **说明** 如您先配置了SMN主题，则资源存储（OBS桶）可以不配置。	资源记录器会定期（6小时）将资源变更的消息存储到您配置的OBS桶中（同时需配置SMN主题）。 资源记录器会定期（24小时）将资源快照文件存储到您配置的OBS桶中。	**配置资源记录器**
统一身份认证服务（IAM）	在配置资源记录器时，需要委托授权。	快速授权包含授予Config调用SMN发送通知权限，以及OBS的写入权限。如需控制权限范围，请使用自定义授权。	**配置资源记录器**

服务名称	说明	交互功能	相关内容
	创建合规规则包时，可根据需要进行自定义委托授权。	创建合规规则包时，当您不选择自定义授权时，Config将通过服务关联委托的方式自动获取RFS的相关权限。如您需要自行控制委托权限的范围，可选择进行自定义授权，提前在统一身份认证服务（IAM）中创建委托，并进行自定义授权，但必须包含可以让合规规则包正常工作的权限（授权资源编排服务创建、更新和删除合规规则的权限）。	**创建合规规则包**
	通过IAM控制用户访问Config的权限。	通过IAM服务为用户授予不同的Config系统权限或自定义策略，以控制用户在Config中可执行的操作。	**权限管理**
云审计服务（CTS）	记录和查看Config相关的关键操作事件。	通过云审计服务，可以记录与配置审计服务相关的操作事件，便于日后的查询、审计和回溯。	**云审计-记录配置审计**
函数工作流（FunctionGraph）	通过发布在FunctionGraph上的函数，执行用户自定义的资源合规评估逻辑。	添加自定义合规规则时，将合规规则和FunctionGraph函数相关联，函数接收Config发布的事件，从事件中接收到规则参数和Config服务收集到的资源属性；函数评估该规则下资源的合规性并通过Config的OpenAPI回传Config服务合规评估结果。	**添加自定义合规规则**
	合规修正配置功能通过关联FunctionGraph服务的函数实例，对不合规资源进行快速修正。	为合规规则创建修正配置，通过关联FunctionGraph服务的函数实例，按照您在函数中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。	-
资源编排服务（RFS）	合规规则包下发的合规规则的创建、更新和删除行为最终是通过RFS服务的资源栈来实现的。	合规规则包是多个合规规则的集合，其下发的合规规则是基于RFS服务的资源栈统一进行创建、更新和删除操作。	**合规规则包**

服务名称	说明	交互功能	相关内容
	合规修正配置功能通过关联RFS服务的私有模板，对不合规资源进行快速修正。	为合规规则创建修正配置，通过关联RFS服务的私有模板，按照您在私有模板中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。	-
资源访问管理（RAM）	添加组织自定义合规规则时，需通过RAM服务将FunctionGraph函数共享给组织成员账号。	自定义策略是一个用户开发并发布在FunctionGraph上的函数，当创建组织类型的自定义合规规则时，需要通过RAM服务将FunctionGraph函数共享给组织成员账号，用于在组织成员账号下部署规则和执行合规评估。	添加自定义组织合规规则
组织Organizations	Config支持基于组织创建合规规则、合规规则包、资源聚合器等功能，组织管理员或Config服务的委托管理员可以统一进行配置并直接作用于组织内的所有成员账号中。	组织管理账号在组织中开启Config为可信服务后，Config可以获取组织中的组织单元及成员账号信息，并基于此信息使用组织级的相关能力。	• 组织合规规则 • 组织合规规则包 • 资源聚合器
云监控服务（CES）	通过CES的事件监控能力，可将Config的相关事件数据收集到云监控服务，并在事件发生时进行告警。	您可以在CES服务查看Config的系统事件监控数据，用于了解用户在什么时间对Config进行了什么操作；还可以创建事件监控的告警通知，在相关事件发生时进行告警通知。	事件监控

7 约束与限制

以下为使用配置审计（Config）服务的主要约束与限制：

表 7-1 Config 约束与限制

描述	限制值
资源数据同步周期 **说明** 已对接Config的服务的资源数据同步到Config存在延迟，不同服务的延迟时间并不相同。 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。	24小时
资源快照存储周期	24小时
资源变更消息存储周期	6小时
单个账号每天最多能开启和修改资源记录器的次数	10次
每个账号最多可以添加的合规规则数（包括由组织合规规则和合规规则包创建的托管规则）	500个
每个账号最多可以添加的合规规则包数（包括组织合规规则包）	50个
每个账号最多能创建的账号类型的资源聚合器数	30个
单个资源聚合器最多能聚合的源账号数	30个
单个账号类型资源聚合器每7天添加、更新和删除的最大源账号数	1000个
单个账号最多能创建的组织类型的资源聚合器数	1个

描述	限制值
单个账号每天最多能创建的组织类型资源聚合器次数	1次
每个账号最多能创建的高级查询数	200个
单个高级查询语句返回的结果条数	4000条
资源记录器收集到的资源配置信息数据的默认保留周期	7年（2557天）

须知

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，因此强烈建议您保持资源记录器的开启状态。如何开启并配置资源记录器请参见**配置资源记录器**。