

开源治理服务

用户指南

文档版本 01
发布日期 2024-03-13



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 控制台总览	1
2 二进制成分分析	4
2.1 添加任务.....	4
2.2 管理任务.....	5
2.3 查看扫描详情.....	7
2.4 下载扫描报告.....	12
2.5 相关术语说明.....	17
3 License 管理	19
4 审计	21
4.1 支持云审计的关键操作.....	21
4.2 如何查看审计日志.....	21

1 控制台总览

开源治理服务（CodeArts Governance）是针对软件开发提供的一站式开源软件治理服务，凝聚华为在开源治理上的优秀实践经验，提供开源软件元数据及软件成分分析、恶意代码检测等能力，从合法合规、网络安全、供应安全等维度消减开源软件使用风险，助力企业更加安全、更加高效地使用开源软件。


本节为您介绍开源治理服务控制台登录方式及菜单页。

登录方式

1. 登录华为云官网，单击页面右上角“控制台”，如图1-1所示。

图 1-1 华为云官网



2. 将鼠标移至页面左上角，在滑出的服务列表中选择“开源治理服务”，即可进入开源治理服务控制台。

总览页

开源治理服务控制台总览页主要展示：资产信息和最近一次检测情况。

- 我的资产
展示最近30天被扫描的软件包个数，以及有风险和未完成的软件包个数。
- 风险信息 TOP5
展示前五项组件风险信息，可查看组件名称、组件版本、语言类型、版本时间、漏洞数、高危漏洞数、License风险等级和引用数量。
- 最近一次二进制成分分析扫描
展示最近一次扫描详细情况，如所示，参数说明如所示。

图 1-2 最近一次二进制成分分析扫描



表 1-1 二进制成分分析扫描参数说明

参数	说明
扫描对象	被扫描的软件包/固件，单击可进入本次任务的扫描详情。
文件大小	被扫描的文件的大小。
开始时间	开始扫描的时间。
扫描耗时	扫描花费的时长。
任务状态	任务扫描状态，包括：排队中、分析中、完成、失败。
检测结果风险统计	显示各检查项的检测项目风险文件总数。
安全漏洞风险项	显示不同风险等级的漏洞个数，风险等级包括：超危、高危、中危、低危。
检测项目合规统计	显示各检查项的检测项目的合规占比。
许可协议 TOP6	显示数量排名前六的漏洞使用许可。
恶意软件扫描	显示各检查项的检测项目风险总数。

单服务页面

单服务包括：二进制成分分析、License管理和专家咨询服务，其中，专家咨询服务包括研发安全SDL培训、隐私合规咨询和移动应用安全专家服务。

表 1-2 单服务页面列表

服务名称	说明
二进制成分分析	添加二进制成分分析任务，上传.zip、.rar、.tar、.tar.gz、.jar、.apk、.hap、.so、.gz、.gzip等格式文件，扫描其中的开源软件、信息泄露、安全配置、安全编译选项等存在的潜在风险， 了解更多 。
License管理	根据企业开源软件使用要求，管理和设置开源许可证的风险等级。

服务名称	说明
专家咨询服务	<ul style="list-style-type: none">● 研发安全SDL培训 SDL (Security Development Lifecycle, 安全开发生命周期) 是为了应对愈发严峻的网络安全挑战而建立、发展的一系列方法论与最佳实践。华为SDL更是与IPD紧密结合, 从公司政策、组织、流程、供应链、服务等方面建立和完善可持续、可信赖的覆盖产品研发全流程的安全保障体系。华为研发安全SDL实践高研班已上线云商店, 面向研发高管, 提供华为研发安全SDL概述、R&D安全保障体系、网络安全技术能力建设等培训课程。● 隐私合规咨询 隐私合规咨询, 针对于欧盟GDPR、中国隐私保护法、数据安全法的法律法规咨询, 以及如何落地研发流程的咨询服务能力。● 移动应用安全专家服务 移动应用安全咨询, 针对于安卓、鸿蒙应用的移动应用安全检测咨询服务, 提供人工检测、修复指导和复测服务, 可满足中国四部委针对于移动应用隐私合规的强制性标准要求。<ul style="list-style-type: none">- 全面覆盖安全合规业务范畴, 包含各个环节的指导、落实、督查、整改。- 确保合规落实有效, 囊括所有安全合规要求, 以及落实这些要求对应的实施措施、检查方法。- 快速准确直观地展示安全合规问题, 并寻找对应解决方案, 使安全合规工作标准化、专业化。

2 二进制成分分析

2.1 添加任务

提供软件包/固件全面分析功能，基于各类检测规则，获得相关被测对象的开源软件、信息泄露、安全配置、安全编译选项等存在的潜在风险。

用户只需上传产品软件包或固件文件提交扫描任务，服务即可输出详尽专业的测试报告。

前提条件

- 已获取管理控制台的登录账号与密码。
- 本地已准备好待扫描的二进制软件包。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。
- 步骤3** 在左侧导航栏，单击“二进制成分分析”。
- 步骤4** 在“二进制成分分析”页面，单击“添加任务”，弹出“添加任务”对话框，单击“扫描对象”旁的文件框，选择本地的软件包，导入扫描对象。

添加任务 温馨提示：免费版配额剩余3次 ?



* 扫描对象



1. 支持 .zip、.rar、.tar、.tar.gz、.jar、.apk、.hap、.so、.gz、.gzip 等10+格式的文件
2. 文件名只能包含：中文、字母、数字、空格、下划线 (_)、破折号 (-) 或点 (.)
3. 文件名最大长度为100字符
4. 文件大小不能超过5GB(免费试用任务限制100MB)

任务名称

扫描文件名称

任务描述

请输入任务描述



是否将本次扫描升级为正式版规格 ?

二进制成分分析 免费版功能特点

1. 每个用户有5次免费体验额度
2. 扫描文件大小不能超过100M
3. 仅支持开源软件漏洞扫描
4. 不支持报告下载

注：本次任务扫描将从您的免费扫描次数中扣除一次扫描配额！扫描失败不扣除！

数据资产严格保密

1. 服务将对您上传的文件及测试报告等严格保密；
2. 只有您 (相应华为云账号) 有权访问和处理以上数据资产；
3. 服务对您上传的文件扫描分析后会立即删除；

确定

取消

说明

- 支持上传 .7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war 等格式文件，及 Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot 等固件。
- 当前仅提供正式版按需套餐扫描计费模式。

步骤5 单击“确定”，开始扫描。

----结束

2.2 管理任务

操作场景

该任务指导用户通过开源治理服务查找、删除或停止正在扫描的成分分析任务。

前提条件

已获取管理控制台的登录账号与密码。

查看任务

步骤1 登录管理控制台。

步骤2 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。

步骤3 在左侧导航栏，单击“二进制成分分析”。

步骤4 在“二进制成分分析”页面，查看成分分析任务列表，相关参数说明如图2-1所示。

图 2-1 成分分析任务列表

文件名	任务描述	任务状态	安全漏洞	开始时间	任务时长	操作
par14.rar	-	已完成	0 0 0 0	2022/07/29 15:44:52 GMT+	58 s	查看报告 停止 删除
nacos-client-1.4.0.jar	-	已完成	1 2 0 0	2022/07/29 10:03:31 GMT+	49 s	查看报告 停止 删除

表 2-1 成分分析任务列表参数说明

参数	参数说明
文件名	软件包名称。
任务描述	自定义描述。
任务状态	<ul style="list-style-type: none"> “等待中” 导入扫描对象后开始等待扫描。 “进行中” 任务正在进行扫描。 “已完成” 任务已完成扫描。 “已停止” 任务扫描中单击了操作栏的“停止”。 “已失败” 任务扫描失败。
安全漏洞	成分分析扫描出的漏洞分布情况。
开始时间	成分分析开始的时间。
任务时长	成分分析扫描完成、失败或停止的所用时长。
操作	查看报告、停止、删除按钮。


步骤5 在下拉框 下拉选择任务状态，可根据任务状态筛选查看任务。

步骤6 在输入框 中输入文件名关键字或任务描述，可根据文件名关键字或任务描述筛选查看，可以和任务状态联合使用。

步骤7 单击  刷新任务列表。

步骤8 （可选）报告比对。

1. 勾选两份任务状态无异常的报告。

2. 单击 ，选择“报告比对”，进入报告对比详情页面，可查看比对结果。

----结束

删除任务

步骤1 [登录管理控制台](#)。

步骤2 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。

步骤3 在左侧导航栏，单击“二进制成分分析”。

步骤4 在“二进制成分分析”页面，可看到全部添加过的任务。

步骤5 单击待删除任务后操作列的“删除”。

根据系统提示执行删除操作。

----结束

停止任务

步骤1 [登录管理控制台](#)。

步骤2 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。

步骤3 在左侧导航栏，单击“二进制成分分析”。

步骤4 在“二进制成分分析”页面，可看到全部添加过的任务。

步骤5 单击待停止任务后操作栏的“停止”，在弹出的对话框中单击“确认”。

说明

只有任务状态为进行中才可操作停止任务。

----结束

2.3 查看扫描详情

该任务指导用户通过开源治理服务查看成分分析扫描结果。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已执行扫描任务。

操作步骤

- 步骤1** 登录管理控制台。
- 步骤2** 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。
- 步骤3** 在左侧导航栏，单击“二进制成分分析”。
- 步骤4** 在“二进制成分分析”页面，可看到全部添加过的任务。
- 步骤5** 单击对应任务操作列的“查看报告”，如图2-2所示。

图 2-2 进入成分分析扫描报告入口



说明

单击“任务名称”也可以进入扫描报告页面。

- 步骤6** 进入扫描报告查看页面，各栏目说明如表2-2所示。

表 2-2 详情总览说明

栏目	说明
任务概况	<p>显示目标任务的基本信息，包括：文件名、文件大小、特征库版本、平台版本等基本信息。</p> <p>显示目标任务的组件检测、安全漏洞、安全配置、许可协议、信息泄露、安全编译选项、恶意软件扫描等检测概况，包括：</p> <ul style="list-style-type: none"> ● 组件检测：展示被扫描的软件包所有的组件数量，有漏洞、未知版本和无漏洞组件数量占比。 ● 安全漏洞：展示超危、高危、中危、低危各个级别漏洞数量占比。 ● 安全配置：展示通过、失败、不涉及的检测结果数量占比。 ● 许可协议：展示数量排名前六的漏洞使用许可。 ● 信息泄露：展示信息泄露各检测项结果分布。 ● 安全编译选项：展示安全编译各检测项结果分布。 ● 恶意软件扫描：展示病毒和恶意代码扫描结果分布。
开源软件漏洞	<p>显示扫描任务中每个组件的组件名称、组件版本、许可协议、包含文件数以及存在漏洞数。</p> <ul style="list-style-type: none"> ● 组件名称、组件版本和文件数可按升降序查看。 ● 可按许可协议对组件列表进行筛选查看。

栏目	说明
License详情	显示开源软件的License检测结果，包括License使用的风险等级和License间的兼容性风险。 <ul style="list-style-type: none">License信息：二进制文件包License检测结果，包含License名称、风险等级、涉及组件和License描述和风险分析。License兼容性：二进制文件包中各目录的License间兼容性风险检测。
密钥和信息泄露	显示Git地址、IP、硬编码密码、弱口令、硬编码密钥和SVN地址的检测结果。
安全编译选项	显示BIND_NOW、NX、PIC等检测项目的描述、检测结果、不符合文件数。
安全配置	显示凭据管理、认证问题和会话管理的检测项目、级别、检测结果。
恶意软件扫描	显示病毒扫描和恶意代码扫描的结果。

📖 说明

当扫描任务成功完成后，单击右上角的“下载报告”，选择“生成PDF报告”或“生成Excel报告”，生成扫描报告后，单击右上角的“导出PDF”，可以下载报告。

步骤7 在“开源软件漏洞”页签可查看软件包各个组件的漏洞。

如果检测结果存在漏洞或者风险，可单击“组件名称”列，查看详细信息。

- 单击“对象路径”，可以查看文件对象路径详细信息。
- 单击“CVE”漏洞名称可以查看相应漏洞的“漏洞详情”、“漏洞简介”、“解决方案”、“漏洞修复参考”、“参考链接”。

curl 组件详情

包含组件的文件对象

文件名称	对象路径	SHA1	时间
libtunnelapi.so	Vastbase		2022/08/03 02:52:54 GMT+...

已知漏洞

安全漏洞等级 🔴 超危 ≥9.0 🟡 高危 7.0-8.9 🟠 中危 4.0-6.9 🟡 低危 0.1-3.9

CVE	日期	CVSS版本	CVSS	漏洞等级
CVE-2021-22945	2021/09/23	3.0	9.1	🔴 超危
CVE-2021-22901	2021/06/11	3.0	8.1	🟡 高危
CVE-2022-22576	2022/05/26	3.0	8.1	🟡 高危
CVE-2021-22926	2021/08/05	3.0	7.5	🟡 高危
CVE-2021-22946	2021/09/29	3.0	7.5	🟡 高危
CVE-2022-27775	2022/06/02	3.0	7.5	🟡 高危
CVE-2022-27780	2022/06/02	3.0	7.5	🟡 高危
CVE-2022-27781	2022/06/02	3.0	7.5	🟡 高危
CVE-2022-27782	2022/06/02	3.0	7.5	🟡 高危
CVE-2021-22922	2021/08/05	3.0	6.5	🟠 中危

步骤8 在“密钥和信息泄露”页签查看对应检测项目的检测结果。

图 2-3 密钥和信息泄露检测结果

检测项目	检测结果
Git地址	0
IP	0
硬编码密码	24
弱口令	0
硬编码密钥	0
SVN地址	0

步骤9 在“安全编译选项”页签查看编译选项对应检测项目的检测结果。

图 2-4 安全编译选项检测结果

检测项目	描述	检测结果	不符合文件数 (个)
BIND_NOW	立即绑定	91.18%	3
NX	堆栈不可执行	100.00%	0
PIC	地址无关	70.97%	9
PIE	随机化	100.00%	0
RELRO	GOT表保护	91.18%	3
SP	栈保护	76.47%	8
NO Rpath/Runpath	动态库搜索路径 (禁选)	100.00%	0
FS	Fortify Source	0.00%	34
Ftrapv	整数溢出检查	N/A	0
Strip	删除符号表	100.00%	0

步骤10 在“安全配置”页签查看凭据管理、认证问题和会话管理对应检测项目的检测结果。

图 2-5 安全配置检查结果

^ 凭据管理		
检测项目	安全风险等级	检测结果
预置帐号信息检查	🔴 高危	NA
sudo规则命令检查	🔴 高危	NA
组成员信息检查	🔴 高危	NA
UID为0的非root帐户检查	🔴 高危	NA
密码复杂度检测	🔴 高危	NA
硬编码口令检查	🔴 高危	NA
历史口令重复使用检查	🟡 中危	NA
^ 认证问题和会话管理		
检测项目	安全风险等级	检测结果
SSH authorized_keys文件检查	🔴 高危	NA
硬编码SSH主机密钥	🔴 高危	NA
SSH 配置检查	🟡 高危	NA
硬编码SSH私钥	🔴 高危	NA
开机启动服务检查	🔴 高危	NA
防暴力破解机制检查	🔴 高危	NA

步骤11 在“恶意软件扫描”页签查看病毒扫描和恶意代码扫描的检测结果。

文件名称	文件位置	病毒名称
有病毒和恶意软件的文件.zip	-	Downloader.Win.Kulucz.9097a1f3
有病毒和恶意软件的文件.zip	-	Downloader.Win.Paoh.710a5081
有病毒和恶意软件的文件.zip	-	Blackbox.Win32.FBI+CD.A
有病毒和恶意软件的文件.zip	-	Trojan.Agent.06d98788
有病毒和恶意软件的文件.zip	-	Downloader.Win.Kulucz.9097a1f3

文件名称	恶意类别	恶意类型	恶意类型内类	威胁等级	置信度	检测结果
有病毒和恶意软件的文件.zip	Python	恶意指令	系统命令替换	高危	高	疑似存在【系统命令替换】问题
有病毒和恶意软件的文件.zip	Python	恶意指令	木马下载执行	高危	高	疑似存在【木马下载执行】问题
有病毒和恶意软件的文件.zip	Python	恶意指令	恶意指令执行	中危	中	疑似存在【恶意指令执行】问题
有病毒和恶意软件的文件.zip	Python	恶意指令	恶意指令执行	高危	高	疑似存在【恶意指令执行】问题
有病毒和恶意软件的文件.zip	Python	恶意指令	敏感信息外发	高危	高	疑似存在【敏感信息外发】问题

----结束

2.4 下载扫描报告

操作场景

扫描任务成功完成后，您可以下载任务报告，报告目前支持PDF和Excel格式。

前提条件

已成功完成成分分析扫描任务，即任务状态为“已完成”。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。

步骤3 在左侧导航栏，单击“二进制成分分析”。

步骤4 在“二进制成分分析”页面，可看到全部添加过的任务。

步骤5 单击对应任务操作列的“查看报告”。

📖 说明

单击“任务名称”也可以进入下载报告页面。

图 2-6 进入成分分析扫描报告入口

文件名称	任务描述	任务状态	安全漏洞	开始时间	任务时长	操作
test.zip	-	已完成		2022/08/08 17:29:10 GMT+8...	40 s	查看报告 导出 删除

步骤6 单击右上角的“生成PDF报告”或“生成Excel报告”。

图 2-7 生成扫描报告



步骤7 扫描报告生成完成后，单击右上角的“导出PDF”或“导出Excel”，可以下载报告。

图 2-8 下载扫描报告



说明

生成的扫描报告会在12小时后过期。过期后，若需要下载扫描报告，请再次单击“生成PDF报告”或“生成Excel报告”，重新生成扫描报告。

----结束

二进制成分分析扫描报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板主要内容说明如下：（以下截图中的数据仅供参考，请以实际扫描报告为准）

- **概览**
查看目标软件包的扫描漏洞数。

图 2-9 查看任务概览信息

1 概览

1.1 任务综述

本次扫描检测出漏洞总数 **84** 个。其中超危漏洞有 **9** 个。

任务名称	scrm-service-weixin.jar
报告地址	https://console[redacted]'/sbcScanList?recordId=[redacted]
开始时间	2022-07-25 20:48:56
结束时间	2022-07-25 20:51:47
扫描耗时	0.05小时
服务版本	1.1

- **结果概览**
统计漏洞类型及分布情况。

图 2-10 查看结果概览信息

2 结果概览

2.1 漏洞概览

漏洞个数				
总漏洞数	超危漏洞	高危漏洞	中危漏洞	低危漏洞
927	24	344	523	36

2.2 组件概览

组件分布			
总组件数	风险组件	无漏洞组件	未知版本组件
19	8	0	1

2.3 许可协议概览

许可协议分布	
许可协议	组件数量
Apache License V2.0	8
MIT License	2
LGPL V2.1	2
Mozilla Public License (MPL) V1.1	1
GPL V2.0	1
OpenSSL Combined License	1
GPL V3.0	1

2.4 信息泄露概览

问题分布	
检查项	问题数量
弱口令	0
硬编码密码	4
硬编码密钥	14
IP	26
Git地址	30
SVN地址	1

- 组件列表
查看软件的所有组件信息。

图 2-11 查看组件列表信息

3 组件列表

3.1. aho-corasick-0.4.0

名称	aho-corasick
版本	0.4.0
发布日期	2017-05-16
许可协议	Apache License V2.0
文件路径	
scrm-service-weixin.jar_/BOOT-INF/lib/ahocorasick-0.4.0.jar	

- 漏洞列表
您可以参考每个组件扫描出的漏洞详细信息修复漏洞。

图 2-12 查看漏洞列表信息

4 漏洞列表

4.1.1. linux_kernel-4.4.197

4.1.1.1. CVE-2011-4917

CVE编号	CVE-2011-4917
漏洞描述	Linux Kernel contains a flaw that is triggered as access to /proc/stat is world-readable and may allow disclosing mouse and keyboard activity. This may allow a local attacker to e.g. determine the length of typed passwords and in turn more easily guess a user's password.
影响组件名称	linux_kernel
影响组件版本	4.4.197
漏洞发布时间	2017-07-17 00:00:00
漏洞CVSS分数	1.2
漏洞风险等级	低危
解决方案	For details, see the reference link in the Reference Information column for vulnerability analysis and handling.[Machine Translation]
漏洞修复参考	https://lkml.org/lkml/2011/11/7/340

文件路径	
	rtds_sample.zip/_zImage

4.1.1.2. CVE-2007-3719

CVE编号	CVE-2007-3719
漏洞描述	The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes that perform voluntary sleeps, which allows local users to cause a denial of service (CPU consumption), as described in "Secretly Monopolizing the CPU Without Superuser Privileges."
影响组件名称	linux_kernel
影响组件版本	4.4.197
漏洞发布时间	2007-07-12 16:30:00
漏洞CVSS分数	2.1
漏洞风险等级	低危
解决方案	

- 信息泄露问题列表

图 2-13 查看信息泄露问题

5 信息泄露问题列表

5.1. Git地址

暂无问题

5.2. IP

暂无问题

5.3. 硬编码密码

暂无问题

5.4. 弱口令

暂无问题

5.5. 硬编码密钥

暂无问题

5.6. SVN地址

暂无问题

- 安全编译选项问题列表

图 2-14 查看安全编译选项问题列表

6 安全编译选项问题列表

6.1. BIND_NOW (共计3个文件未通过该检查项)

编号	问题所在文件路径
1	唱吧.apk/lib/armeabi/libaacdecoder.so
2	唱吧.apk/lib/armeabi-v7a/libaacdecoder.so
3	唱吧.apk/lib/x86/libaacdecoder.so

- 安全配置检查列表

图 2-15 查看安全配置检查列表

6 安全配置检查列表

6.1. 预置账号信息检查

6.1.1

扫描项	预置账号信息检查
审视项	解析 /etc/passwd 和 /etc/shadow 文件，查看其配置参数是否合规
扫描结果	不涉及
建议值	1.锁定系统账户。2.uid或用户名唯一。3.不同账户设定不同密码。4. 使用sha512加密账户密码。5. root用户密码
描述	检查预置账号如下配置信息：是否存在未锁定的系统预置账号，是否存在相同 用户名/uid 的用户，是否存在相同密码hash的账户，是否存在弱加密算法加密的密码，root用户密码是否设置了最长使用期限

6.1.1 详细信息

问题
[There is no operate system in the package]

- 恶意软件扫描问题列表

图 2-16 查看恶意软件扫描问题

8 恶意软件扫描问题列表

8.1 病毒扫描

暂无问题

8.2 恶意代码扫描

暂无问题

2.5 相关术语说明

开源(open source)

即开放一类技术或一种产品的源代码，源数据，源资产，可以是各行业的技术或产品，其范畴涵盖文化、产业、法律、技术等多个社会维度。

开源软件(open source software)

允许用户直接访问源代码，通过开源许可协议将其复制、修改、再发布的权利向公众开放的计算机软件。

开源组件(open source component)

是开源软件系统中最小可识别且本身不再包含另外组件的、组件信息可在公共网站获取且可独立分发、开发过程中带有版本号并且可组装的软件实体。

开源许可证(open source license)

开源软件的版权持有人授予用户可以学习、修改开源软件，并向任何人或为任何目的分发开源软件的权利。

软件成分分析(Software Composition Analysis)

通过分析软件包含的一些信息和特征来实现对该软件的识别、管理、追踪的技术。

PE(Portable Executable)

是Windows系统下的可执行文件的标准格式。

ELF(Executable and Linkable Format)

是一种Unix或Linux系统下的可执行文件，目标文件，共享链接库和内核转储(core dumps)的标准文件格式。

APK(Android application package)

是Android操作系统使用的一种应用程序包文件格式，用于分发和安装移动应用及中间件。

HAP(HarmonyOS application package)

是鸿蒙操作系统使用的一种应用程序包文件格式，用于分发和安装移动应用及中间件。

CVE(Common Vulnerabilities and Exposures)

又称通用漏洞披露、常见漏洞与披露，是一个与信息安全有关的数据库，收集各种信息安全弱点及漏洞并给予编号以便于公众查阅。

CVSS(Common Vulnerability Scoring System)

通用漏洞评分系统，是一个行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度，有CVSS 2.0、3.0、3.1标准。

固件(firmware)

是一种嵌入在硬件设备中的软件。

NVD

National Vulnerability Database国家安全漏洞库。

CNVD

China National Vulnerability Database国家信息安全漏洞共享平台。

CNNVD

China National Vulnerability Database of Information Security国家信息安全漏洞库。

组件依赖

保证组件正确运行所依赖的必须加载的其他组件。

3 License 管理

操作场景

用户可以查看开源License的信息和自定义开源License的风险等级。

前提条件

已获取管理控制台的登录账号与密码。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 选择“服务列表 > 开发与运维 > 开源治理服务”，进入开源治理服务管理控制台。
- 步骤3** 在左侧导航栏，单击“License管理”。
- 步骤4** 在“License管理”页面，可看到License列表，内容包含License名称、风险等级、License描述和风险分析以及重置操作。

License名称	风险等级	License描述和风险分析	操作
AGPL V3.0	高	在分发或通过web向用户提供服务场景下：1. 无论是否修改，该软件本身都必须开源。2. 允许各种链接，但与其链接的...	重置
Apache 2.0 License with Export Co...	低	风险来自于美国出口管制制度的遵循，若须使用到产品中，建议咨询公司贸易合规办公室。	重置
Apache License V2.0	低	1.允许以源代码或目标码形式复制、分许可、分发作品或其衍生作品（注：衍生作品是指任何基于或衍生自该软件的源代...	重置
Apache Software License V1.1	低	允许以源代码和目标码形式修改或不修改使用和分发，无强制代码开源义务，需要履行使用声明义务，需要在分发时附带...	重置
BSD 2-Clause License	低	同BSD LICENSE	重置
BSD 3-Clause License	低	1.允许以源代码和目标码形式修改或不修改使用和分发。2.声明要求:所使用软件的版权声明+许可证文本+不担保声明	重置
BSD 3-Clause Open MPI variant	低	1.允许以源代码和目标码形式修改或不修改使用和分发。2.声明要求:所使用软件的版权声明+许可证文本+不担保声明	重置
BSD-3-Clause-LBNL	低	无开源风险，在分发时需附上版权声明及免责声明，不允许未经授权使用加州大学、Lawrence Berkely国家实验室，美国...	重置
Common Development and Distribu...	中	Common Development and Distribution License: 2005年，SUN公司宣布将开放操作系统Solaris的源代码，并推出CDD...	重置
Common Development and Distribu...	中	许可证义务: 可以复制和分发 CDDL 许可证软件的源码，不能删除或更改软件中所包含的任何版权、专利或商标声明。...	重置

10 总条数: 37 < 1 2 3 4 >

- 单击License的风险等级下拉框可以自定义对应License的风险等级。

- 单击License的重置按钮可恢复对应License的默认风险等级。

----结束

4 审计

4.1 支持云审计的关键操作

操作场景

平台提供了云审计服务。通过云审计服务，您可以记录与云服务器相关的操作事件，便于日后的查询、审计和回溯。

前提条件

已开通云审计服务。

支持审计的关键操作列表

表 4-1 云审计服务支持的云服务器操作列表

操作名称	资源类型	事件名称
创建移动应用安全任务	task	createSecappTask
删除移动应用安全任务	task	deleteSecappTask
下载移动应用安全报告	report	downloadSecappReport
清理移动应用安全资源	resource	cleanUpSecappResources



4.2 如何查看审计日志

操作场景

开启了云审计服务后，系统开始记录开源治理服务相关的操作。云审计服务会保存最近1周的操作记录。

本小节介绍如何在云审计服务管理控制台查看最近1周的操作记录。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在左侧导航树中，单击 ，选择“管理与监控 > 云审计服务 CTS”，进入云审计服务控制台，默认展示事件列表信息页面。

事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：


- 时间范围：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。
 - 事件类型、事件来源、资源类型和筛选类型。
 - 在下拉框中选择查询条件。其中，“事件来源”选择“DevSecurity”。
 - “筛选类型”选择“按事件名称”时，还需选择某个具体的事件名称。
 - “筛选类型”选择“按资源ID”时，还需选择或者手动输入某个具体的资源ID。
 - “筛选类型”选择“按资源名称”时，还需选择或手动输入某个具体的资源名称。
 - 操作用户：在下拉框中选择某一具体的操作用户，次操作用户指用户级别，而非租户级别。
 - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
4. 选择查询条件后，单击“查询”。
 5. 在需要查看的事件左侧，单击  展开该记录的详细信息，如 [图4-1](#) 所示。

图 4-1 展开记录

事件名称	资源类型	云服务	资源ID	资源名称	事件级别	操作用户	操作时间	操作
createScaTask	task	DevSecurity	4mm...	ScaTask	normal	S...	2023/09/15 08:52:32 GMT+08:00	查看事件


```

request [{"inherit":false,"taskType":0,"callback":null,"cidr":null,"autoProdTree":false,"alias":null,"fileSize":0,"filename":null,"testScenarioId":null,"testScenarioName":null,"testCases":null,"deliver":0,"inheritMode":0,"paidType":"package","description":"","type":"devsecurity","openSourceBaseline":false,"accurate":false},{"app":"apk","true":false,"bmscope":true,"securecat":true,"seninfo":true,"secusfa":false,"cybellum":false,"cryptology":false,"qianxin":false,"ssst":false,"malware":true,"buildId":null,"rosVersion":null,"engineSelected":true}],{"me":"ibcut.so"}
trace_id 27
code 200
trace_name createScaTask
is_consistent true
resource_type task
trace_rating normal
api_version 1.0
message User S[...]@aa01[...] creates an task of DevSecurity service.
source_ip 100.79.4.139
trace_type ConsoleAction
service_type DevSecurity
event_type system
project_id $[...]
response Create task success.
resource_id 4mm[...]
track_name system
time 2023/09/15 08:52:32 GMT+08:00
resource_name ScaTask
user [{"domain":{"name":"S[...]","id":"[...]"},"name":"S[...]","id":"[...]"}]
record_time 2023/09/15 08:52:32 GMT+08:00
    
```

6. 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如 [图4-2](#) 所示，显示该操作事件结构的详细信息。

图 4-2 查看事件

```
{
  "request": "{\"inherit\":false,\"taskType\":0,\"callback\":null,\"cida\":null,\"autoProdtree\":false,\"alias\":null,
  \"trace_id\":\"2[REDACTED]\",
  \"code\":\"200\",
  \"trace_name\":\"createScaTask\",
  \"is_consistent\":true,
  \"resource_type\":\"task\",
  \"trace_rating\":\"normal\",
  \"api_version\":\"1.0\",
  \"message\":\"User S[REDACTED] d] creates an task of DevSecurity service.\",
  \"source_ip\":\"1[REDACTED]\",
  \"trace_type\":\"ConsoleAction\",
  \"service_type\":\"DevSecurity\",
  \"event_type\":\"system\",
  \"project_id\":\"8[REDACTED]\",
  \"response\":\"Create task success.\",
  \"resource_id\":\"4[REDACTED]\",
  \"tracker_name\":\"system\",
  \"time\":\"2023/09/15 08:52:32 GMT+08:00\",
  \"resource_name\":\"ScaTask\",
  \"user\":{
    \"domain\":{
      \"name\":\"S[REDACTED]\",
```