漏洞管理服务

用户指南

文档版本 01

发布日期 2024-06-12

华为云计算技术有限公司

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 操作指引

漏洞管理服务使用概览如**表1-1**所示。

表 1-1 漏洞管理服务使用流程概览

子流程	说明
购买漏洞管理服务	漏洞管理服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。 具体操作请参见**购买漏洞管理服务**。
创建扫描任务	创建扫描任务即可对网站进行扫描，具体操作请参见**创建扫描任务**。
开启主机扫描	开启主机扫描即可对主机进行扫描，具体操作请参见**开启主机扫描**。
新增监测任务	新增监测任务即可对资产进行监测，具体操作请参见**新增监测任务**。
查看扫描结果	扫描完成后可以通过“任务详情”页面查看扫描结果。 ● 网站扫描结果，请参见**查看网站扫描详情**。 ● 主机扫描结果，请参见**查看主机扫描详情**。

2 开通漏洞管理服务

2.1 产品规格差异

漏洞管理服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。

各服务版本支持的计费方式、功能和规格说明如下所示，您可以根据业务需求选择相应的服务版本。

表 2-1 各服务版本计费方式

服务版本	支持的计费方式	说明	价格详情
基础版	• 配额内的服务免费 • 按需计费	• 基础版配额内仅支持Web网站漏洞扫描（域名个数：5个，扫描次数：5个域名每日总共可以扫描5次）是免费的。 • 基础版提供的以下功能按需计费： 1. 可以将Web漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持20台主机。	产品价格详情
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。	
高级版	包年/包月		
企业版	包年/包月		

表 2-2 各服务版本功能说明

功能	基础版	专业版	高级版	企业版
常见Web漏洞检测	√	√	√	√
端口扫描	√	√	√	√
自定义登录方式	√	√	√	√
Web 2.0高级爬虫	√	√	√	√
网站指纹识别	√	√	√	√
扫描任务管理	√	√	√	√
漏洞查看及管理	√	√	√	√
CVE漏洞扫描	×	√	√	√
弱密码检测	×	√	√	√
网页内容合规检测（文字）	×	√	√	√
操作系统漏洞扫描	×	√	√	√
操作系统基线检查	×	√	√	√
中间件基线检查	×	√	√	√
云原生基线扫描	×	√	√	√
查看漏洞修复建议	×	√	√	√
下载扫描报告	×	√	√	√
安全监测（定时扫描）	×	√	√	√
网页内容合规检测（图片）	×	×	×	√
网站挂马检测	×	×	×	√
链接健康检测（死链、暗链、恶意外链）	×	×	×	√
操作系统等保合规检查	×	×	×	√
支持手动探索文件导入	×	×	×	√

表 2-3 各服务版本支持的扫描配额说明

版本	域名/IP个数	扫描次数	单个任务时长	任务优先级	单用户并发扫描数
基础版	Web漏扫：包含5个二级域名或IP:端口。	Web漏扫：5个域名每日总共可以扫描5次	2小时	低	默认Web漏扫最大并发为1个域名。

版本	域名/IP个数	扫描次数	单个任务时长	任务优先级	单用户并发扫描数
专业版	Web漏扫：包含1个二级域名或IP:端口。 主机漏扫：包含20个IP地址。		无限制	高	默认Web漏扫最大并发为3个域名。 默认主机漏扫最大并发为5个IP。
高级版	Web漏扫：默认包含1个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制IP地址个数。		无限制	高	默认Web漏扫最大并发为5个域名。 默认主机漏扫最大并发为10个IP。
企业版	Web漏扫：默认包含5个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制IP地址个数。 **说明** 当默认的扫描配额不能满足您的需求时，您可以通过购买扫描配额包增加扫描配额（一个扫描配额包中包含一个一级域名扫描配额）。		无限制	高	默认Web漏扫最大并发为10个域名。 默认主机漏扫最大并发为20个IP。 **说明** 更高并发需要，请提交工单联系专业工程师为您服务。

2.2 购买漏洞管理服务

操作场景

该任务指导用户首次使用漏洞管理服务时，如何购买漏洞管理服务的专业版、高级版和企业版扫描功能。

须知

- 仅支持从专业版升级至高级版，当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额升级为一级域名配额，可以直接将专业版升级到高级版。
- 不支持多个版本同时存在。如果是老客户，已购买的版本下存在基础版和专业版，基础版全部免费升级为专业版，版本到期时间以订单到期时间最长的为准。
- 不支持从专业版或高级版直接升级至企业版，当您是专业版或高级版用户时，如果需要使用企业版，请直接购买企业版。为保证您的权益，请您购买企业版后，提工单退订专业版或高级版。
- 购买漏洞管理服务或配额后，不支持直接修改配额，仅支持升级规格，请谨慎操作。如需减少配额请参考**如何减少漏洞管理服务配额？**。

前提条件

已获取管理控制台的登录账号（拥有VSS Administrator与BSS Administrator权限）与密码。

购买步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择区域或项目后，单击 ☰，选择“开发与运维 > 漏洞管理服务”，进入漏洞管理服务管理界面。

步骤3 单击页面右上角的“升级规格”，进入漏洞管理服务购买页面。

如果您已经体验了漏洞管理服务基础版，可以选择购买专业版、高级版和企业版的扫描功能。

步骤4 在购买漏洞管理服务界面，进行服务选型配置。

- “计费模式”选择“包年/包月”，如图2-1、图2-2和图2-3所示，参数说明如表2-4所示，参数配置完成后，请执行步骤5。

  说明

  - 使用基础版的用户，可以继续使用基础版的功能，每个用户可添加的域名个数不超过5个。
  - 当用户在使用中需要增加专业版/高级版/企业版域名扫描配额，购买的数量不能小于已购买的数量，到期时间不变。

图 2-1 计费模式-包年/包月（专业版）

图 2-2 计费模式-包年/包月（高级版）

图 2-3 计费模式-包年/包月（企业版）

表 2-4 服务选型参数说明

参数	参数说明
规格选择	漏洞管理服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。
规格说明	对应版本支持的功能介绍。
购买时长	- 专业版 可以选择1个月～3年的时长。 - 高级版 可以选择1个月～3年的时长。 - 企业版 支持“1个月”、“3个月”、“1年”的购买时长。

参数	参数说明
扫描配额包	– 选择“专业版”时，需要配置购买的域名扫描配额包数量。 Web漏扫：包含1个二级域名或IP:端口，每个公网IP支持的端口号不限 主机漏扫：包含20个IP地址。 购买的“扫描配额包”不能少于资产列表的网站数量。 **须知** ■ 如果您在购买专业版之前使用过免费体验版（即基础版）进行扫描，在购买专业版时，“扫描配额包”的选择必须等于或者大于当前资产列表已添加的网站个数。 ■ 如果当前资产列表的某个基础版域名，您不想升级为专业版为其付费，请您在购买专业版之前对其进行删除。 ■ 如果您只需要将当前基础版域名全部升级为专业版规格，“扫描配额包”的选择等于当前资产列表已添加的网站个数。 ■ 如果您需要增加域名配额，即增加扫描的网站个数，“扫描配额包”的选择大于当前资产列表已添加的网站个数，且“扫描配额包”的选择值为您期望的域名配额值。 ■ 购买专业版成功后，当前资产列表所有基础版域名默认升级为专业版，享受专业版规格。 – 选择“高级版”时，需要配置购买的域名扫描配额包数量。 Web漏扫：默认包含1个一级域名（不限制二级域名个数）/IP（不限制端口个数），每个公网IP支持的端口号不限。 主机漏扫：不限制IP地址个数。 – 选择“企业版”时，每个配额包包含如下： Web漏扫：默认包含5个一级域名（不限制二级域名个数）/IP（不限制端口个数），每个公网IP支持的端口号不限。 主机漏扫：不限制IP地址个数 若默认的域名配额数量不能满足您的要求，您可以通过配置扫描配额包的数量，增加域名配额。

- 计费模式选择“按需计费”，如图2-4所示。
  - 创建任务时，保持升级开关关闭，开始扫描后默认享受单次基础版扫描服务。
  - 创建任务时，开启升级开关，开始扫描后享受单次专业版扫描服务。扫描开始后进行一次性扣费，请保障您的账户余额充足。
  - 基于基础版创建主机扫描时，每次扫描最多20台主机，扫描开始后进行一次性扣费，请保障您的账户余额充足。

图 2-4 计费模式-按需计费

请参照以下操作步骤完成一次扫描任务：

a. 单击“立即体验”回到“资产列表”界面。

说明

如果没有网站，请先添加网站，再在创建任务界面进行单次按需购买。

b. 单击“扫描”，进入“创建任务”界面，相关设置如图2-5所示。

图 2-5 扫描设置

您可以打开“是否将本次扫描升级为专业版规格”开关，将本次扫描升级为专业版。

设置完成后，用户可以根据需要选择定时扫描或者立即扫描，在弹出的“付费提醒”界面，单击“同意并扫描”。

说明

- 在您扫描成功后，该费用将从您的账户余额中扣取。在页面右上角，单击“费用”，进入费用中心，可以查看余额变动。漏洞管理服务默认每隔1小时统计一次按需扫描的次数，进行费用扣取。
- 用户选择“按需计费”的方式进行扫描时，如果扫描任务失败，则本次扫描不扣费。

步骤5 参数设置完毕后，在页面右下角，单击“立即购买”。

说明

如果您对价格有疑问，可以单击“了解计费详情”了解产品价格。

步骤6 确认订单详情无误并阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

2.3 域名配额扩容

操作场景

该任务指导已购买专业版、高级版或者企业版的用户增加扫描的域名配额。

须知

- 若用户以前使用过基础版（免费体验版）进行扫描，在升级为专业版时，基础版所有的已有域名会占用专业版配额。
- 当前不支持从专业版或者高级版直接升级至企业版，若您是专业版或者高级版用户，并想要使用企业版，请直接购买企业版，为保证您的权益，请您购买企业版后，提工单退订专业版或者高级版。
- 当前不支持仅购买企业版（不购买配额）后再次升级增加配额。如果要想增加配额，请先退订企业版，重新购买。

前提条件

- 已获取管理控制台的登录账号（拥有VSS Administrator与BSS Administrator权限）和密码。
- 已购买专业版、高级版或者企业版的漏洞管理服务。

扩容专业版配额

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表”，单击右上角的“升级规格”，进入升级专业版规格入口。

步骤4 在升级规格界面设置配额，如图2-6所示。

图 2-6 专业版配额扩容

在“扫描配额包”栏，单击 + 增加域名扫描配额包数量。

说明

- “扫描配额包”即配置的域名/IP地址个数，目前支持的范围为1-100。
- 选择的“扫描配额包”必须大于当前拥有的域名配额。
- 每个扫描配额包默认包含1个二级域名或公网IP:端口。

步骤5 在页面右下角，单击“立即购买”。

说明

如果您对价格有疑问，可以单击“了解计费详情”了解产品价格。

步骤6 确认订单详情无误并阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

扩容高级版配额

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表”，单击右上角的“升级规格”，进入升级高级版规格入口。

步骤4 在升级规格界面设置配额，如图2-7所示。

图 2-7 高级版配额扩容

在“扫描配额包”栏，单击 + 增加域名扫描配额包数量。

说明

- “扫描配额包”即配置的域名/IP地址个数，目前支持的范围为1-100。
- 选择的“扫描配额包”必须大于当前拥有的域名配额。
- 每个扫描配额包默认包含1个一级域名（不限制二级域名个数）/IP（不限制端口个数）。

步骤5 在页面右下角，单击“立即购买”。

说明

如果您对价格有疑问，可以单击“了解计费详情”了解产品价格。

步骤6 确认订单详情无误并阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

扩容企业版配额

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表”，单击右上角的“升级规格”，进入升级企业版规格入口。

步骤4 在升级规格界面设置配额，如图2-8所示。

图 2-8 企业版配额扩容

在“扫描配额包”栏，单击 增加扫描配额包 。

说明

- “扫描配额包”即配置的域名/IP地址个数，目前支持的范围为1～100。
- 每个扫描配额包默认包含1个一级域名（不限制二级域名个数）/IP（不限制端口个数）。

步骤5 在页面右下角，单击“立即购买”。

说明

如果您对价格有疑问，可以单击“了解计费详情”了解产品价格。

步骤6 确认订单详情无误并阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

2.4 升级为高级版

当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额全部升级为一级域名配额，可以直接将专业版升级为高级版。

该任务指导专业版用户将漏洞管理服务升级为高级版。

前提条件

- 已获取管理控制台的登录账号（拥有VSS Administrator与BSS Administrator权限）和密码。
- 已购买专业版的漏洞管理服务。

升级为高级版

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 单击“升级规格”，进入升级规格界面。

步骤4 在升级规格界面，单击“高级版”，设置配额，如图2-9所示。

图 2-9 升级为高级版配额

在“扫描配额包”栏，单击 + 增加域名扫描配额包数量。

说明

- “扫描配额包”即配置的域名/IP地址个数，目前支持的范围为1-100。
- “扫描配额包”栏的数量默认为专业版配额的数量。
- “扫描配额包”可以选择大于或等于当前拥有的专业版配额，漏洞管理服务仅支持专业版配额全部升级，不支持专业版配额部分升级。
- 每个扫描配额包默认包含1个一级域名（不限制二级域名个数）/IP（不限制端口个数）。

步骤5 确认订单详情无误并阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤6 在“付款”页面，选择付款方式进行付款。

----结束

3 网站漏洞扫描

3.1 添加网站

开通漏洞管理服务后，您首先需要将网站资产以IP或域名的形式添加到漏洞管理服务中并完成网站认证，才能进行漏洞扫描。

如果您的网站中存在需要登录才能访问的网页，还需要配置网站登录信息（支持“Web页面登录”、“Cookie登录”和“Header登录”三种登录方式），漏洞管理服务才能为您更好的检测网站安全问题。

说明

如果您在添加网站时，提示“当前套餐可新增域名已达到上限”，无法添加网站时，可参照以下方法进行处理：

- 参照**域名配额扩容**进行域名配额扩容，购买“扫描配额包”，“扫描配额包”必须大于当前版本已有的配额。
- 如果您的资产列表有不需要防护的网站，建议删除后再添加新的网站。

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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在“资产列表 > 网站”页签，单击“新建网站”，进入“新建网站 > 填写网站信息”页面。

步骤4 添加网站。

须知

漏洞管理服务是通过公网访问域名/IP地址进行扫描的，请确保该目标域名/IP地址能通过公网正常访问。

- 单个添加网站
  a. 单击左上角“添加”，如图3-1所示，参数说明如表3-1所示。

  图 3-1 添加网站

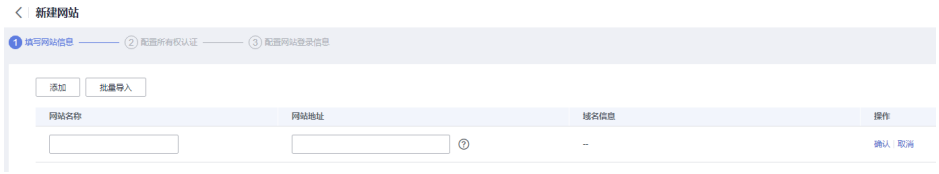
  

  表 3-1 添加网站配置参数说明

参数名称	参数说明
网站名称	用户需要添加的网站名称。
网站地址	添加网站的地址。 正确格式为：http://域名或IP地址、https://域名或IP地址。
域名信息	无需配置。

  b. 单击新增网站所在行的“确认”，添加网站成功。
  添加网站成功后，“域名信息”自动获取“网站地址”中的信息生成。
- 批量导入网站
  a. 单击“批量导入”，弹出“批量新增域名”对话框。如图3-2所示。

  图 3-2 批量添加网站

b. 配置一个及以上网站地址。

网站地址格式为：http://域名或IP地址、https://域名或IP地址。多个网站地址使用换行分开。

c. 单击“添加网站”。

“网站名称”和“域名信息”根据“网站地址”自动生成。

说明

添加网站信息成功后，支持编辑和删除网站信息。

步骤5 单击“下一步”，进入“配置所有权认证”页面。

步骤6 选择认证类型。

说明

如果待检测站点的服务器搭建在华为云上，且该服务器是您当前登录账号的资产，才可以选择“一键认证”的方式进行快速认证，否则只能选择“免认证”的方式进行认证。

- 免认证，仔细阅读图3-3中的“使用须知”，确认符合条件后，勾选“我已阅读并了解上述使用要求”，进行网站认证。

图 3-3 免认证方式

- 一键认证，如图3-4所示。

图 3-4 一键认证方式

步骤7 单击“下一步”，进入“配置网站登录信息”页面。

步骤8 （可选）配置网站登录信息。

如果网站中存在需要登录才能访问的网页，进行登录设置后，漏洞管理服务能够为您更好的检测网站安全问题。如果此处未配置网站登录信息，则网站添加成功后，可参考**网站登录设置**进行网站信息的配置。

1. 在目标网站所在行的“操作”列，单击“配置网站登录信息”，页面右侧弹出“配置网站登录信息”窗口。
2. 参照表3-2完成网站信息配置，如图3-5所示。

图 3-5 网站登录设置

说明

漏洞管理服务提供了“Web页面登录”、“Cookie登录”和“Header登录”三种登录方式，三种登录方式的开关默认为关闭。请按照业务认证逻辑，启用对应配置。

表 3-2 网站登录页面参数说明

参数名称	参数说明	样例
“Web页面登录”		
登录页面	网站登录页面的地址。	https://auth.example.com/

参数名称	参数说明	样例
用户名	登录网站的用户名。	test
密码	对应用户名的密码。	--
确认密码	再次输入用户名的密码。	--
“Cookie登录” 当配置的“Web页面登录”无法成功登录进业务系统时，可以尝试通过配置原始Cookie的方式进行扫描。		
cookie值	输入登录网站的cookie值。 若没有cookie，请在“Header登录”中，通过添加自定义Header的方式进行登录扫描。 有关获取登录网站的cookie值的详细操作，请参见**如何获取网站cookie值?**	domain_tag
“Header登录”		
自定义Header	配置HTTP请求头部。最多可添加5个自定义HTTP请求头。 当待扫描的网站需要请求中附带特殊的HTTP请求头时，可以通过自定义Header进行设置。 HTTP请求头常见的如：带有Token或Session字样。	--
“网站登录验证”		
验证登录网址	登录成功后才能访问的网址，便于漏洞管理服务快速判断您的登录信息是否有效。	https://console.example.com/

3. 单击“确认”，完成网站登录信息的配置。

步骤9 阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”。

步骤10 单击“确定”，添加网站成功。

----结束

后续操作

网站登录方式设置完成，您还需要创建扫描任务，详细操作请参见**创建扫描任务**。

相关操作

- **如何修改漏洞管理服务已添加的域名?**
- **为什么域名认证失败?**
- **已添加的域名是否可以删除?**

3.2 网站登录设置

操作场景

该任务指导用户通过漏洞管理服务进行网站登录设置，修改网站信息。

如果您的网站页面需要登录才能访问，必须进行网站登录设置，以便漏洞管理服务能为您发现更多安全问题。漏洞管理服务提供了三种登录方式，请您根据您的网站访问限制条件选择登录方式：

- Web页面登录。

  如果您的网站仅需要账号密码就可以登录访问，设置该方式即可。
- Cookie登录。

  建议优先配置“Web页面登录”方式。如果发现通过“Web页面登录”仅能扫描到登录界面，无法成功扫描到内部业务系统时，可以根据业务实际认证方式配置“Cookie登录”进行扫描。
- Header登录。

  建议优先配置“Web页面登录”方式。如果发现通过“Web页面登录”仅能扫描到登录界面，无法成功扫描到内部业务系统时，可以根据业务实际认证方式配置“Header登录”进行扫描。

以上登录方式根据网站访问情况选择。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加网站。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在“资产列表 > 网站”页签，单击对应的网站信“操作”列的“编辑”，页面右侧弹出“编辑网站”窗口。

步骤4 根据需要修改网站登录信息，如**图3-6**所示，参数说明如**表3-3**所示。

图 3-6 编辑网站登录信息页面

表 3-3 编辑网站登录信息参数说明

参数名称	参数说明	样例
网站信息		
网站地址	漏洞管理服务不支持修改“网站地址”，如需修改，请删除该网站后，再重新创建新的网站。	http://www.domain.com

参数名称	参数说明	样例
网站名称	自定义的网站名称，可修改。	test
“Web页面登录”		
登录页面	网站登录页面的地址。	https://auth.example.com/
用户名	登录网站的用户名。	test01
密码	对应用户名的密码。	--
确认密码	再次输入用户名的密码。	--
“Cookie登录” 当配置的“Web页面登录”无法成功登录进业务系统时，可以尝试通过配置原始Cookie的方式进行扫描。		
cookie值	输入登录网站的cookie值。 若没有cookie，请在“Header登录”中，通过添加自定义Header的方式进行登录扫描。 有关获取登录网站的cookie值的详细操作，请参见**如何获取网站cookie值?**	domain_tag
“Header登录”		
自定义Header	配置HTTP请求头部。最多可添加5个自定义HTTP请求头。 当待扫描的网站需要请求中附带特殊的HTTP请求头时，可以通过自定义Header进行设置。 HTTP请求头常见的如：带有Token或Session字样。	--
“网站登录验证”		
验证登录网址	登录成功后才能访问的网址，便于漏洞管理服务快速判断您的登录信息是否有效。	https://console.example.com/

步骤5 单击“确认”，网站登录信息设置成功。

----结束

3.3 创建扫描任务

操作场景

该任务指导用户通过漏洞管理服务创建扫描任务。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加网站。
- 如果您的网站设置了防火墙或其他安全策略，将导致漏洞管理服务的扫描IP被当成恶意攻击者而误拦截。因此，在使用漏洞管理服务前，请您将以下漏洞管理服务的扫描IP添加至网站访问的白名单中：

  119.3.232.114，119.3.237.223，124.70.102.147，121.36.13.144，124.70.109.117，139.9.114.20，119.3.176.1

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在“资产列表 > 网站”页签，单击对应的网站信息“操作”列的“扫描”，页面右侧弹出“创建任务”窗口。

说明

用户可以同时扫描多个网站。勾选多个网站后，单击列表左上方的“批量扫描”，在页面右侧弹出的“创建任务”窗口中单击“确认”，即可批量扫描网站。

步骤4 请根据表3-4进行扫描设置，设置后如图3-7所示。

图 3-7 创建扫描任务

表 3-4 扫描设置参数说明

参数	参数说明
开始时间	可选参数，设置开始扫描的时间，不设置默认立即扫描。

参数	参数说明
扫描策略	三种扫描策略： • 极速策略：扫描耗时最少，能检测到的漏洞相对较少。 • 标准策略：扫描耗时适中，能检测到的漏洞相对较多。 • 深度策略：扫描耗时最长，能检测到最深处的漏洞。 有些接口只能在登录后才能访问，建议用户配置对应接口的用户名和密码，漏洞管理服务才能进行深度扫描。 **说明** • “极速策略”：扫描的网站URL数量有限且漏洞管理服务会开启耗时较短的扫描插件进行扫描。 • “深度策略”：扫描的网站URL数量不限且漏洞管理服务会开启所有的扫描插件进行耗时较长的遍历扫描。 • “标准策略”：扫描的网站URL数量和耗时都介于“极速策略”和“深度策略”两者之间。
手动探索文件	仅企业版（单个域名扫描）涉及该参数的配置。 单击“添加文件”可添加需要扫描的探索文件。手动探索文件的获取方式，请参考**手动探索指导**，文件大小不要超过30M。 使用手动探索文件时，将不启用自动爬虫，仅扫描探索文件中指定的URL。
是否扫描登录URL	默认不扫描登录URL，开启扫描登录URL前请先评估业务影响。
是否将本次扫描升级为专业版规格	仅基础版涉及该参数的配置。 基础版用户开启此功能后，扫描过程中会按需扣费： • 鼠标移动至了解升级后影响。 • 打开此功能时，扫描时会自动升级为专业版按需扣费，关闭该功能时，扫描时不会升级。
扫描项设置	漏洞管理服务支持的扫描功能参照**表3-5**。 • ：开启。 • ：关闭。

表 3-5 扫描项设置

扫描项名称	说明
Web常规漏洞扫描（包括XSS、SQL注入等30多种常见漏洞）	提供了常规的30多种常见漏洞的扫描，如XSS、SQL等漏洞的扫描。默认为开启状态，不支持关闭。
端口扫描	检测主机打开的所有端口。
弱密码扫描	对网站的弱密码进行扫描检测。

扫描项名称	说明
CVE漏洞扫描	CVE，即公共暴露漏洞库。漏洞管理服务可以快速更新漏洞规则，扫描最新漏洞。
网页内容合规检测（文字）	对网站文字的合规性进行检测。
网页内容合规检测（图片）	对网站图片的合规性进行检测。
网站挂马检测	挂马：上传木马到网站上，使得网站在运行的时候执行木马程序，被黑客控制，遭受损失。漏洞管理服务可以检测网站是否存在挂马。
链接健康检测（死链、暗链、恶意外链）	对网站的链接地址进行健康性检测，避免您的网站出现死链、暗链、恶意链接。

说明

- 如果您当前的服务版本已经为专业版，不会提示升级。
- 基础版支持常见漏洞检测、端口扫描。
- 专业版支持常见漏洞检测、端口扫描、弱密码扫描。
- 高级版支持常见漏洞检测、端口扫描、弱密码扫描。
- 企业版支持常见网站漏洞扫描、基线合规检测、弱密码、端口检测、紧急漏洞扫描、周期性检测。

步骤5 设置完成后，单击“确认”，进入扫描任务页面。

创建扫描任务后，会先进入“排队中”状态，满足运行条件后任务状态变为“进行中”。

说明

当网站列表中有“扫描状态”为“排队中”或“进行中”的任务时，可以单击网站列表上方的“批量取消”，在弹出的窗口中勾选需要取消扫描操作的网站进行批量取消。

----结束

后续处理

扫描任务完成，您可以查看网站详情并下载网站扫描报告，详细操作请参见**查看网站扫描详情**、**生成并下载网站扫描报告**。

相关操作

如果您在创建扫描任务过程中遇到问题，请参考以下方法解决：

- **如何快速发现网站漏洞?**
- **为什么扫描任务自动登录失败了?**
- **为什么任务扫描中途就自动取消了?**
- **创建任务时为什么总是提示域名格式错误?**

- 网站漏洞扫描一次需要多久？
- 如何解决网站扫描失败报连接超时的问题？
- 创建网站扫描任务或重启任务不成功时如何处理？

3.4 查看网站扫描详情

该任务指导用户通过漏洞管理服务查看网站扫描结果，可以查看扫描项总览、业务风险列表、漏洞列表、端口列表、站点结构。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加网站。
- 已执行扫描任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在“资产列表 > 网站”页签，进入网站列表页面。

网站资产列表相关参数说明如表3-6所示。

表 3-6 网站资产列表参数说明

参数	参数说明
网站名称	网站的名称。
网站地址	网站的地址。
登录认证	根据网站配置的登录方式自动生成。 取值包括： ● Web登录 ● Cookie认证 ● Header认证 如果未配置登录方式，则显示为“--”。

参数	参数说明
扫描状态	网站的扫描状态。 取值包括： ● 全部状态 ● 进行中 ● 已完成 ● 已取消 ● 排队中 ● 已失败 ● 未扫描
安全等级	网站的安全等级。 取值包括： ● 全部等级 ● 安全 ● 低危 ● 中危 ● 高危 ● 未知
上一次扫描时间	网站最近一次扫描任务的时间。

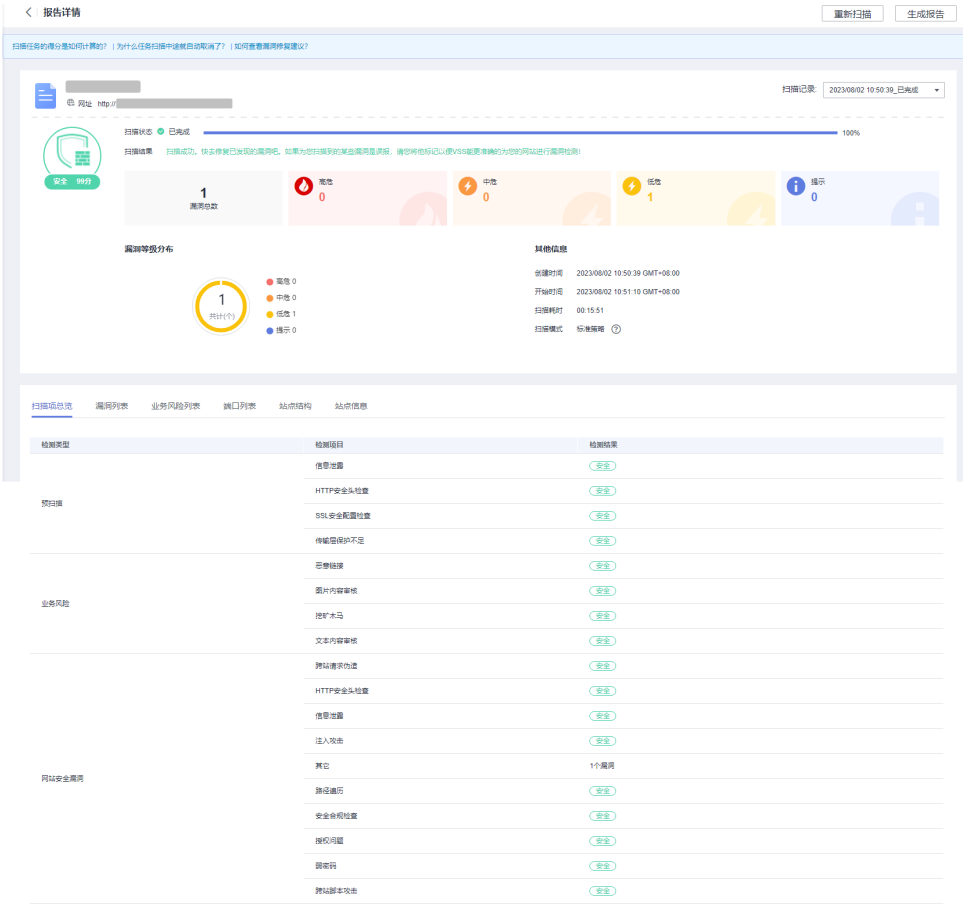
步骤4 在目标网站所在行的“安全等级”列，单击“查看报告”，进入扫描任务详情页面，如图3-8所示。

说明

- 扫描任务详情界面默认显示最近一次的扫描情况，如果您需要查看其他时间的扫描情况，在“扫描记录”下拉框中，选择扫描时间点。

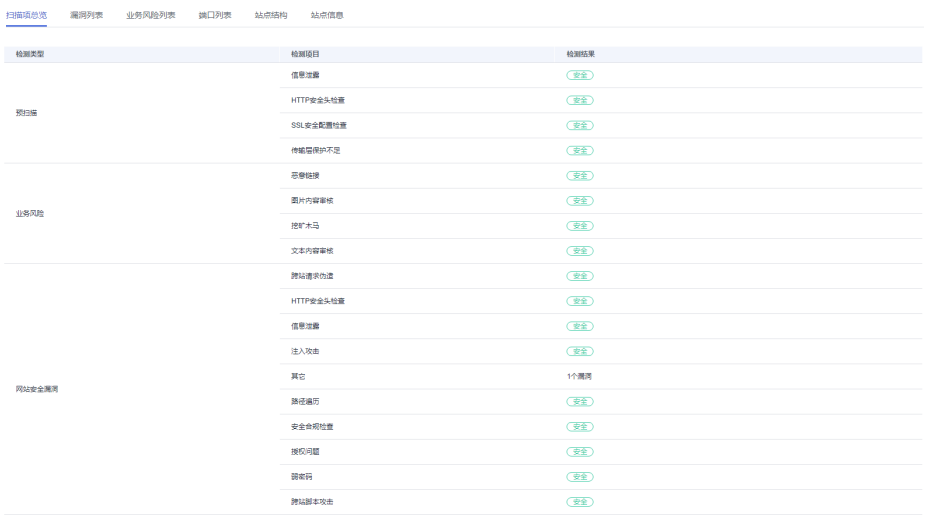
  扫描报告只会保留最近10次的记录，之前的历史数据会保留一年，如果需要获取请联系华为云技术支持工程师处理。
- 单击右上角的“重新扫描”，可以重新执行扫描任务。
- 当扫描任务成功完成后，单击右上角的“生成报告”，生成网站扫描报告。

图 3-8 查看扫描任务详情



步骤5 选择“扫描项总览”页签，查看扫描项的检测结果，如图3-9所示。

图 3-9 扫描项总览



步骤6 选择“漏洞列表”页签，查看漏洞信息，如图3-10所示。

图 3-10 漏洞列表

说明

- 单击漏洞名称可以查看相应漏洞的“漏洞详情”、“漏洞简介”、“修复建议”。
- 如果您确认扫描出的漏洞不会对网站造成危害，请在目标漏洞所在行的“操作”列，单击“忽略”，忽略该漏洞，后续执行扫描任务会扫描出该漏洞，但扫描结果将不会统计忽略的漏洞。例如，如果您对2个低危漏洞执行了“忽略”操作，则再次执行扫描任务，扫描结果显示的低危漏洞个数将减少2。

  您可以勾选多个漏洞，单击漏洞列表左上方的“标记为忽略”进行批量忽略。
- 如果想对已忽略的漏洞恢复为风险类型，在目标漏洞所在行的“操作”列，单击“取消忽略”，恢复检测此漏洞。

  您可以勾选多个漏洞，单击漏洞列表左上方的“取消忽略”进行批量取消。

步骤7 选择“业务风险列表”页签，查看业务风险信息，如图3-11所示。

图 3-11 业务风险列表

步骤8 选择“端口列表”页签，查看目标网站的端口信息，如图3-12所示。

图 3-12 端口列表

步骤9 选择“站点结构”页签，查看目标网站的站点结构信息，如图3-13所示。

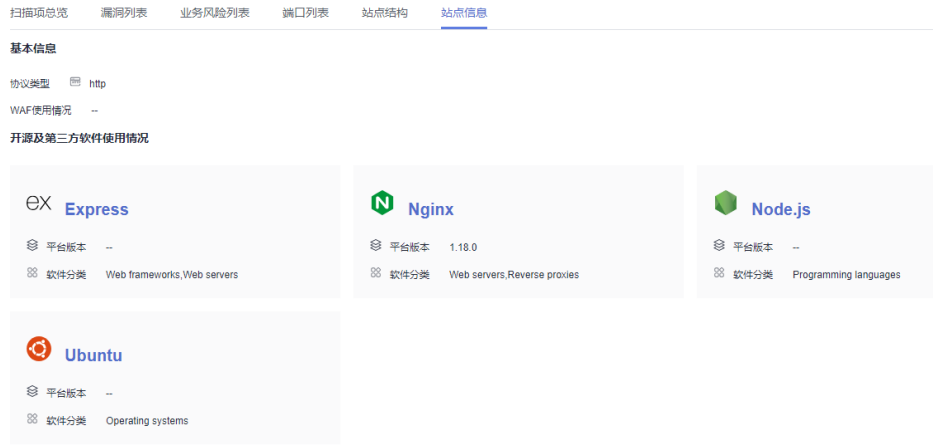
说明

站点结构显示的是目标任务的漏洞的具体站点位置，如果任务暂未扫描出漏洞，站点结构无数据显示。

图 3-13 站点结构

步骤10 选择“站点信息”页签，查看目标网站的站点信息，如图3-14所示。

图 3-14 站点信息



----结束

后续处理

当您修复网站漏洞后，在扫描详情界面右侧单击“重新扫描”，重新扫描网站后，请在网站扫描详情界面查看该漏洞是否已修复。

相关操作

- 有关网站扫描得分的计算方法参考如下：

  扫描任务被创建后，初始得分是一百分，任务扫描完成后，根据扫描出的漏洞级别会扣除相应的分数。

  网站扫描：高危减10分，中危减5分，低危减3分，无漏洞则不扣分。

说明

- 得分越高，表示漏洞数量越少，网站越安全。
- 如果得分偏低，请根据实际情况对漏洞进行忽略标记，或根据修复建议修复漏洞，或使用Web应用防火墙服务为您的网站保驾护航。
- 漏洞修复后，建议重新扫描一次查看修复效果。

- 有关修复漏洞的详细介绍，请参见**漏洞管理服务能修复扫描出来的漏洞吗?**

3.5 生成并下载网站扫描报告

操作场景

当网站扫描任务成功完成后，您可以下载任务报告，报告目前只支持PDF格式。

前提条件

已成功完成网站扫描任务，即目标网站的“扫描状态”为“已完成”。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

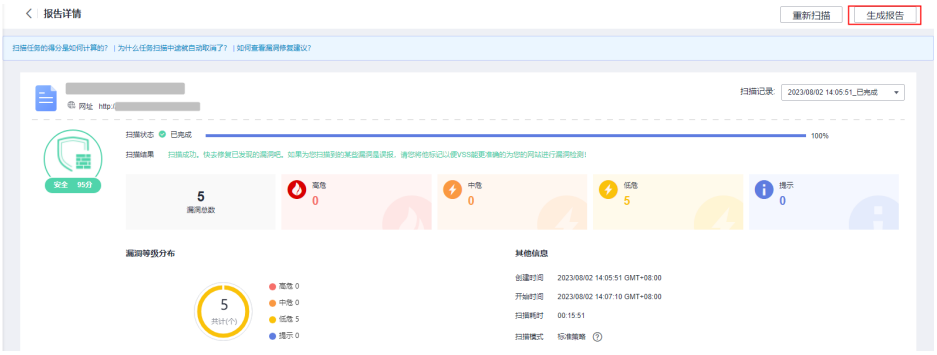
步骤3 在“资产列表 > 网站”页签，进入网站列表页面。

步骤4 在目标网站所在行的“安全等级”列，单击“查看报告”，进入扫描任务详情页面。

步骤5 单击“生成报告”，弹出“生成报告配置”窗口。

扫描报告仅支持专业版及以上版本扫描任务下载，请升级到专业版及以上版本体验。

图 3-15 生成扫描报告



说明

生成的扫描报告会在24小时后过期。过期后，若需要下载扫描报告，请再次单击“生成报告”，重新生成扫描报告。

步骤6 （可选）修改“报告名称”。

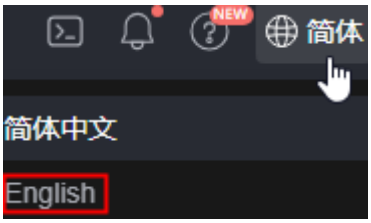
步骤7 单击“确定”，弹出前往报告中心下载报告的提示框。

步骤8 单击“确定”，进入“报告中心”页面。

步骤9 单击生成报告所在行的“下载”，可将报告下载到本地。

说明

网站漏洞扫描报告支持生成并下载英文版，需切换控制台语言为英文后，按照上述指导进行英文版报告生成和下载。



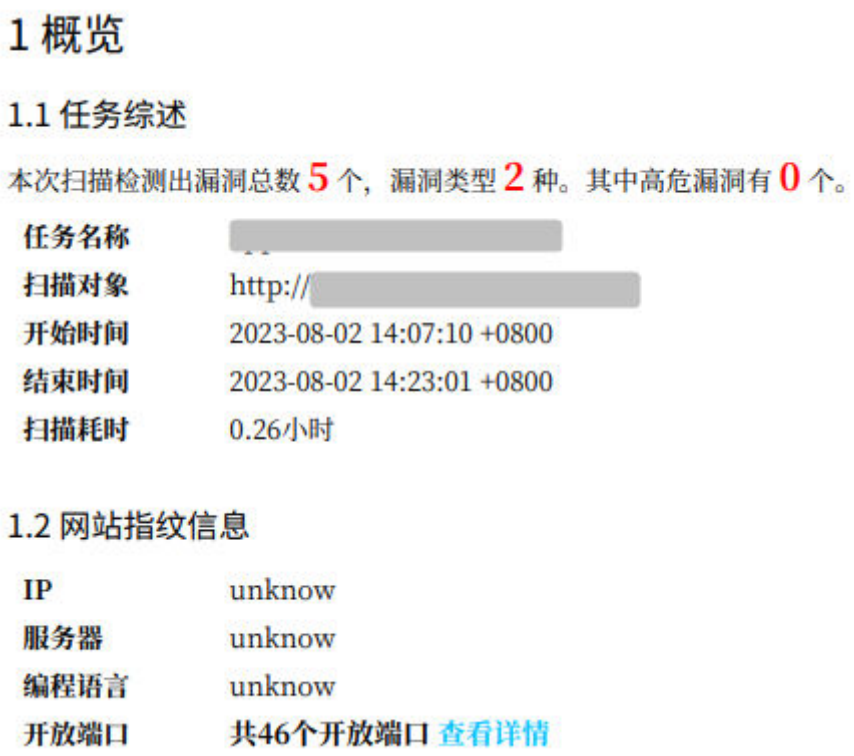
----结束

网站漏洞扫描报告模板说明

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：

- 概览
  查看目标网站的扫描漏洞数。

  图 3-16 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 5 个，漏洞类型 2 种。其中高危漏洞有 0 个。

任务名称	[redacted]
扫描对象	http://[redacted]
开始时间	2023-08-02 14:07:10 +0800
结束时间	2023-08-02 14:23:01 +0800
扫描耗时	0.26小时

1.2 网站指纹信息

IP	unknow
服务器	unknow
编程语言	unknow
开放端口	共46个开放端口 查看详情

- 漏洞分析概览
  统计漏洞类型及分布情况。

图 3-17 漏洞类型分析

2 漏洞分析概览

2.1 扫描概览

扫描分数&漏洞个数					
95 分	总漏洞数	高危漏洞	中危漏洞	低危漏洞	提示威胁
	5	0	0	5	0

2.2 漏洞类型分布

分类	漏洞类型	检测结果
网站安全漏洞	跨站请求伪造	安全
	HTTP安全头检查	4个漏洞 查看详情
	信息泄露	安全
	注入攻击	安全
	其它	1个漏洞 查看详情
	路径遍历	安全
	安全合规检查	安全
	授权问题	安全
	弱密码	安全
	跨站脚本攻击	安全

- 服务端口列表
  查看目标网站的所有端口信息。

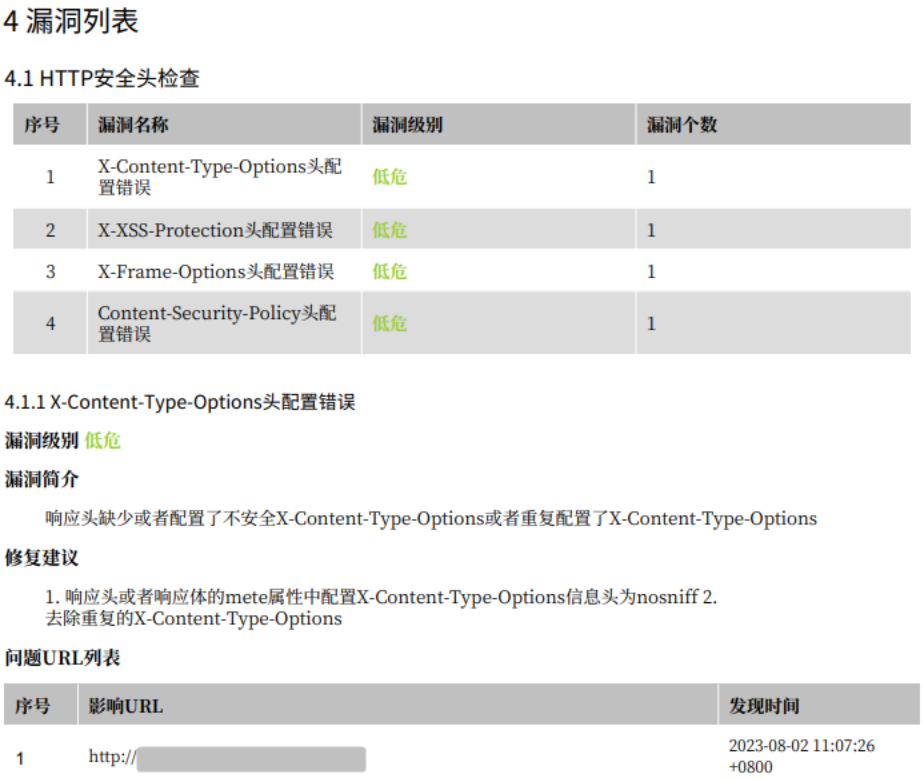
图 3-18 网站的端口列表

3 端口列表

端口	状态	协议	服务
22	Open	TCP	OpenSSH 7.4
30,000	Open	TCP	ndmps
30,001	Open	TCP	Apache httpd 2.4.49
30,002	Open	TCP	Apache httpd 2.4.38
30,003	Open	TCP	rtsp
30,004	Open	TCP	Nagios NSCA
30,005	Open	TCP	Apache httpd 2.4.6
30,006	Open	TCP	Oracle WebLogic Server 10.3.6.0
30,010	Open	TCP	Oracle WebLogic admin httpd 12.2.1.3
30,011	Open	TCP	Oracle WebLogic admin httpd 12.2.1.3

- 漏洞根因及详情
  您可以根据修复建议修复漏洞。

图 3-19 漏洞根因及详情



4 漏洞列表

4.1 HTTP安全头检查

序号	漏洞名称	漏洞级别	漏洞个数
1	X-Content-Type-Options头配置错误	低危	1
2	X-XSS-Protection头配置错误	低危	1
3	X-Frame-Options头配置错误	低危	1
4	Content-Security-Policy头配置错误	低危	1

4.1.1 X-Content-Type-Options头配置错误

漏洞级别 低危

漏洞简介

响应头缺少或者配置了不安全X-Content-Type-Options或者重复配置了X-Content-Type-Options

修复建议

1. 响应头或者响应体的mete属性中配置X-Content-Type-Options信息头为nosniff 2. 去除重复的X-Content-Type-Options

问题URL列表

序号	影响URL	发现时间
1	http://	2023-08-02 11:07:26 +0800

3.6 删除网站

操作场景

该任务指导用户通过漏洞管理服务来删除网站。

须知

域名删除后，该资产的历史扫描数据将被删除，不可恢复。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加网站。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在“资产列表 > 网站”页签，单击对应的网站信息“操作”列的“删除”。

说明

用户可以同时删除多个网站。勾选多个网站后，单击列表左上方的“批量删除”，在弹出的确认对话框单击“确认”，即可批量删除网站。

步骤4 在弹出的确认对话框中，单击“确认”。

在页面右上角弹出“域名删除成功”，则说明网站删除成功。

----结束

相关操作

有关添加域名的详细操作，请参见**添加网站**。

4 主机扫描

4.1 添加主机

该任务指导用户通过漏洞管理服务添加主机。

须知

漏洞管理服务的基础版不支持主机扫描功能，如果您是基础版用户，请通过以下方式使用主机扫描功能：

- 购买专业版、高级版或企业版。
- 按需计费，每次最多可以扫描20台主机。

操作场景

漏洞管理服务支持添加Linux操作系统和Windows操作系统的主机。

- Linux主机扫描支持主机漏洞扫描、基线检测、等保合规检测。
- Windows主机扫描目前仅支持主机漏洞扫描。

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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 单击“新建主机”，进入“新建主机”页面。

步骤5 在“新建主机”页面，执行以下操作。

- 单个添加主机

  单击“添加主机”，如图4-1所示，参数说明如表4-1所示。

  图 4-1 添加主机

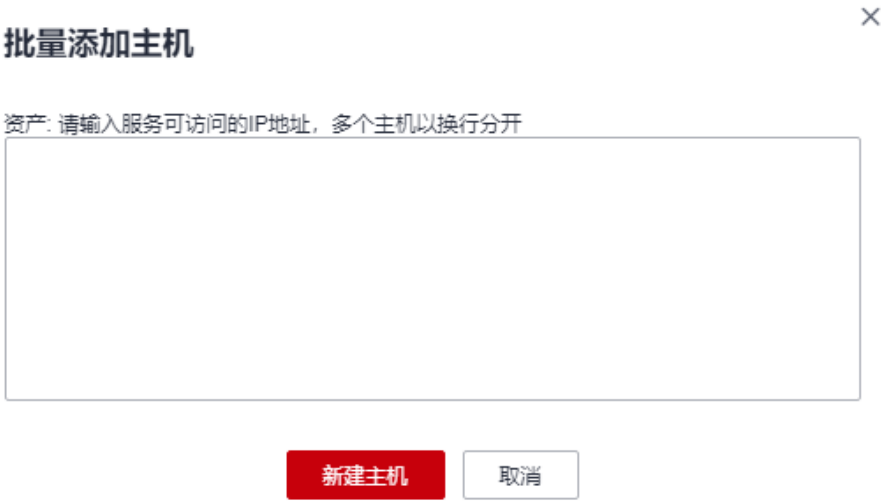
  表 4-1 添加主机配置参数说明

参数名称	参数说明
主机名称	用户需要添加的主机名称，必填参数。
IP地址	添加主机的公网IP地址，必填参数。
操作系统类型	主机的操作系统类型，支持Linux操作系统和Windows操作系统。
分组	主机的分组。 用户可根据实际情况选择已有分组或者是新建分组，新建分组的步骤如下： 1. 单击“新建分组”，弹出“新增主机组”窗口。 2. 输入“主机组名称”。 主机组名称不能与已有的重复。 3. 单击“确认”。
跳板机	主机的跳板机，可在下拉框中选择已有跳板机，或者单击“跳板机管理”，编辑或创建跳板机。 Windows主机暂不支持跳板机。 编辑或创建跳板机的操作请参见步骤6。 支持勾选多个主机批量配置跳板机。
授权信息	主机的授权信息。必填参数，可在下拉框中选择已有授权信息，或者单击“授权信息管理”，编辑或创建授权信息。 – 当“操作系统类型”为“Linux”时，编辑或创建授权信息的操作请参见步骤6。 – 当“操作系统类型”为“Windows”时，编辑或创建授权信息的操作请参见步骤6。 支持勾选多个主机批量配置授权信息。
操作	单击“删除”可删除主机信息。

- 批量添加主机

a. 单击“批量导入”，弹出“批量添加主机”对话框中。如图4-2所示。

图 4-2 批量添加主机



b. 配置IP地址。
多个IP地址，使用换行分开。

c. 单击“新建主机”。
新建成功的“主机名称”根据输入的IP地址自动生成，可修改。

步骤6 配置完主机信息后，阅读页面下方的“使用须知”并勾选“我已阅读并了解上述使用要求”。

步骤7 单击“确定”，添加主机完成。

----结束

相关操作

- 为什么主机添加成功后不能在主机列表中查找到?
- 主机扫描支持哪些区域?

4.2 编辑主机授权

4.2.1 编辑 Linux 主机授权

操作场景

该任务指导用户通过漏洞管理服务对已添加的Linux主机授权信息进行编辑。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加Linux主机。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 在目标Linux系统主机的“操作”列，单击“编辑”，页面右侧弹出“编辑主机”窗口。

步骤5 在“授权信息”区域，单击“选择SSH授权”下拉框，选择“授权信息管理”，显示“授权信息管理”页面。

步骤6 选择编辑已有SSH授权或创建新的SSH授权。

- 选择“编辑SSH授权”，如图4-3所示。

图 4-3 编辑 SSH 授权

选择需要编辑的SSH授权信息，单击图标，即可修改SSH授权的信息。配置说明如表4-2所示。

- 选择“创建SSH授权”，如图4-4所示。

图 4-4 创建 SSH 授权

设置配置参数，配置说明如表4-2所示。

表 4-2 参数说明

参数名称	参数说明
SSH授权别称	自定义SSH授权名称。
登录端口	SSH授权登录的端口号。 请确保安全组已添加该端口，以便主机可通过该端口访问漏洞管理服务。
选择登录方式	SSH授权的登录方式。 取值范围： - 密码登录 - 密钥登录
Root权限是否加固	打开该权限后，不可以用root账号直接登录，而只能通过普通用户登录，然后才能切换到root用户。
sudo用户名	默认为root，不可修改。

参数名称	参数说明
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建漏洞管理服务专用的默认主密钥。 **须知** – 您也可以在数据加密服务的以下区域创建密钥： ■ 华北-北京一 ■ 华北-北京四 ■ 华南-广州 ■ 华东-上海一 ■ 华东-上海二 ■ 西南-贵阳一 ■ 华南-深圳 有关创建密钥的详细操作，请参见**创建密钥**。 – 使用数据加密服务需要单独计费，详细的服务资费和费率标准，请参见**价格详情**。
sudo密码	当“选择登录方式”为“密码登录”时，才显示该参数。 设置sudo用户对应的密码，为了您的账号安全，您的密码会加密保存。
私钥	当“选择登录方式”为“密钥登录”时，才显示该参数。
私钥密码	当“选择登录方式”为“密钥登录”时，才显示该参数。 设置私钥用户对应的密码，为了您的账号安全，您的密码会加密保存。
普通用户名	当开启“Root权限是否加固”时，才显示该参数。
普通用户密码	当开启“Root权限是否加固”，且“选择登录方式”为“密码登录”时，才显示该参数。 设置普通用户名对应的密码，为了您的账号安全，您的密码会加密保存。

阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“确认”，完成Linux主机授权信息的创建。

步骤7 单击“确认”，完成Linux主机授权信息的编辑。

步骤8 单击“确认”，编辑Linux主机授权信息成功。

----结束

相关操作

配置主机授权后，您可以取消主机授权，取消主机授权后，将不能完全扫描出主机的安全风险。有关取消主机授权的详细操作，请参见**取消主机授权**。

4.2.2 编辑 Windows 主机授权

操作场景

该任务指导用户通过漏洞管理服务对已添加的Windows主机授权信息进行编辑。

前提条件

- 已获取管理控制台的登录账号与密码。
- 登录用户只支持Administrator。
- 已添加Windows主机。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

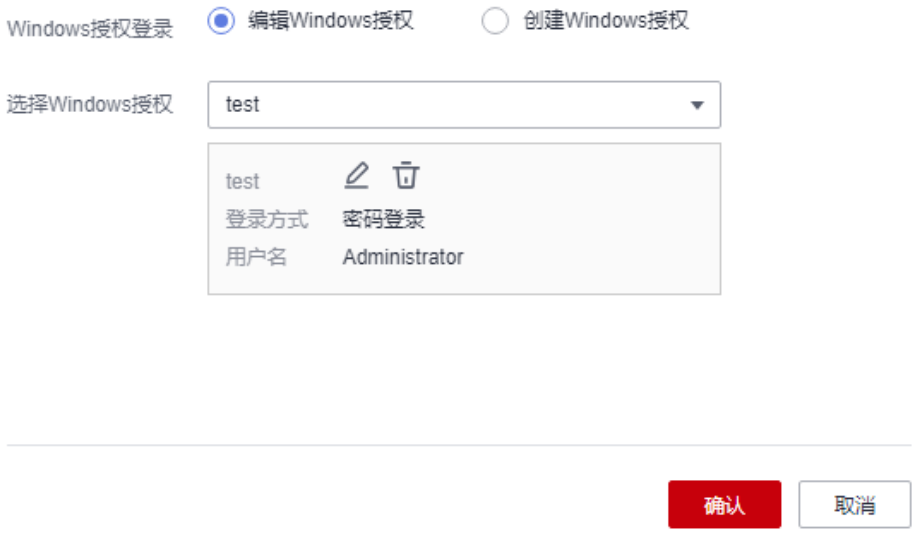
步骤4 在目标Windows系统主机的“操作”列，单击“编辑”，页面右侧弹出“编辑主机”窗口。

步骤5 在“授权信息”区域，单击“选择Windows授权”下拉框，选择“授权信息管理”，显示“授权信息管理”页面。

步骤6 选择编辑已有Windows授权或创建新的Windows授权。

- 选择“编辑Windows授权”，如**图4-5**所示。

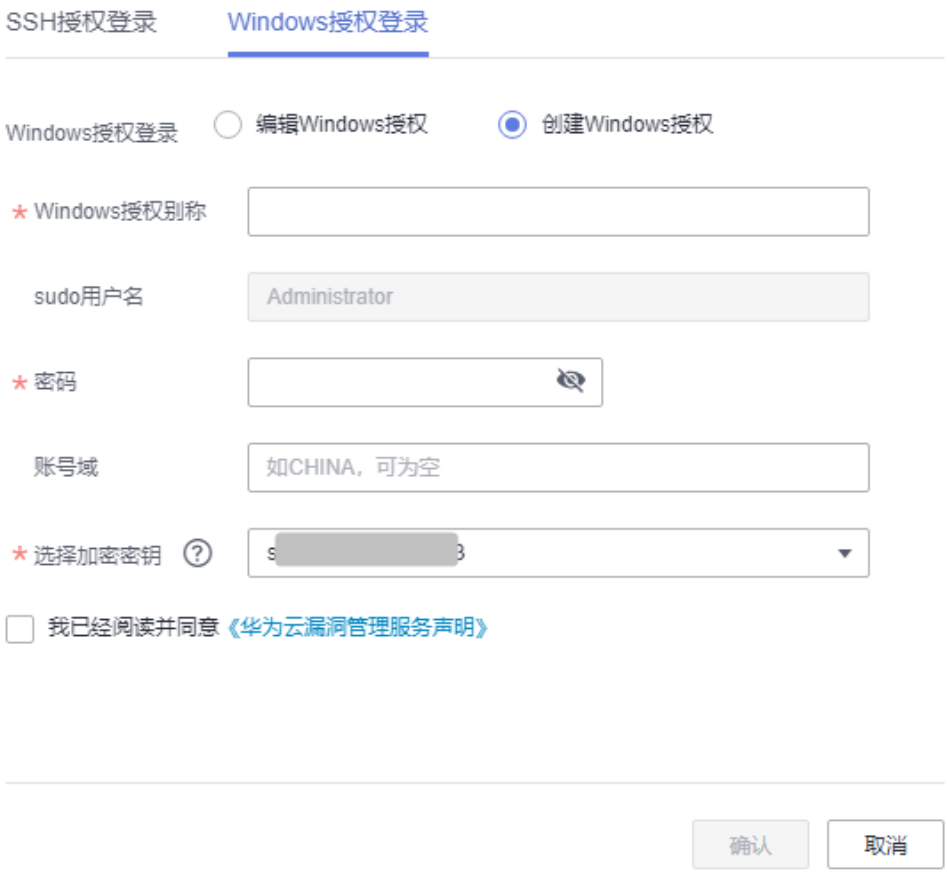
图 4-5 编辑 Windows 授权



选择需要编辑的Windows授权信息，单击图标，即可修改Windows授权的信息。配置说明如**表4-3**所示。

- 选择“创建Windows授权”，如**图4-6**所示。

图 4-6 创建 Windows 授权



设置配置参数，配置说明如**表4-3**所示。

表 4-3 参数说明

参数名称	参数说明
windows授权别称	自定义windows授权名称。
用户名	默认为Administrator。
密码	windows系统登录密码。
账号域	查看该windows系统的账号域并填写到此处，该参数也可以为空，不填写。
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建漏洞管理服务专用的默认主密钥。 **须知** – 您也可以在数据加密服务的以下区域创建密钥： ■ 华北-北京一 ■ 华南-广州 ■ 华东-上海二 有关创建密钥的详细操作，请参见**创建密钥**。 – 使用数据加密服务需要单独计费，详细的服务资费和费率标准，请参见**价格详情**。

阅读《华为云漏洞管理服务声明》后，勾选“我已阅读并同意《华为云漏洞管理服务声明》”，单击“确认”，完成Windows主机授权信息的创建。

步骤7 单击“确认”，完成Windows主机授权信息的编辑。

步骤8 单击“确认”，编辑Windows主机授权信息成功。

----结束

相关操作

配置主机授权后，您可以取消主机授权，取消主机授权后，将不能完全扫描出主机的安全风险。有关取消主机授权的详细操作，请参见**取消主机授权**。

Windows主机漏洞扫描依赖于WinRM服务开启，如何开启请参见**如何开启WinRM服务**。开启WinRM服务后，请将如下IP加入可访问您主机上WinRM（HTTPS是5986端口，HTTP是5985端口）的白名单列表中：

- 119.3.232.114
- 119.3.237.223
- 124.70.102.147
- 121.36.13.144

- 124.70.109.117
- 139.9.114.20
- 119.3.176.1

4.3 开启主机扫描

操作场景

该任务指导用户通过漏洞管理服务开启主机扫描。

开启主机扫描后，漏洞管理服务将对主机进行漏洞扫描与基线检测。

须知

漏洞管理服务的基础版不支持主机扫描功能，如果您是基础版用户，请通过以下方式使用主机扫描功能：

- 购买专业版、高级版或企业版。
- 按需计费，每次最多可以扫描20台主机。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

说明

为了确保扫描成功，在开启主机扫描前，请先完成以下操作。

1. 参照**编辑Linux主机授权**和**编辑Windows主机授权**完成主机授权。
2. 如果主机所在的安全组设置了访问限制，请参见**如何解决主机不能访问**添加策略允许漏洞管理服务的IP网段访问您的主机。
3. 如果用户同时使用了**主机安全服务**，参见**配置SSH登录IP白名单**将漏洞管理服务的IP配置为白名单。否则，漏洞管理服务的IP会被当成不信任IP被**主机安全服务**拦截，造成扫描任务失败。
4. 参照**测试互通性**完成主机与扫描环境的连通性测试。

开启主机扫描（专业版/企业版）

步骤1 **登录管理控制台**。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 单击主机信息“操作”列的“扫描”，进入主机扫描入口，如**图4-7**所示。

图 4-7 进入主机扫描入口

说明

您可以选中需要扫描的主机，在主机列表上方单击“批量操作 > 批量扫描”，对选中的多台主机批量进行扫描。

- 当“主机连接状态”为“未知”时，需先单击目标主机所在行的“互通性”进行测试。
- 当“主机连接状态”为“IP不可达”或“连接失败”时，单击“扫描”后，会弹出主机连接状态确定提示框，请根据提示选择是否继续扫描。

步骤5 在弹出的对话框中，单击“确认”。

说明

当主机列表中有“扫描状态”为“排队中”或“进行中”的任务时，可以单击主机列表上方的“批量操作 > 批量取消”，在弹出的窗口中勾选需要取消扫描操作的主机进行批量取消。

----结束

开启主机扫描（基础版）

漏洞管理服务的基础版不支持主机扫描功能，如果您是基础版用户，请通过以下方式使用主机扫描功能：

- 购买专业版、高级版或企业版。
- 按需计费，每次最多可以扫描20台主机。

请参照以下操作步骤，按需购买主机扫描功能。

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 单击主机信息“操作”列的“扫描”，进入主机扫描入口。

说明

您可以选中需要扫描的主机，在主机列表上方单击“批量操作 > 批量扫描”，对选中的多台主机批量进行扫描。

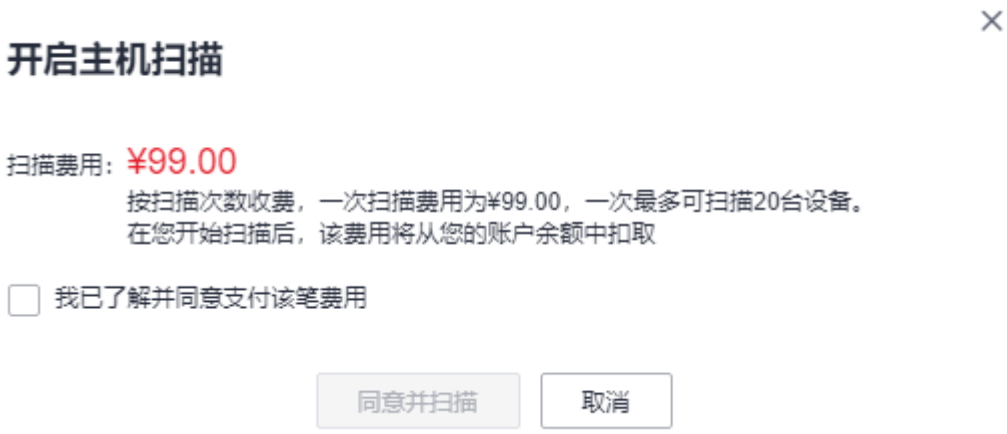
- 当“主机连接状态”为“未知”时，需先单击目标主机所在行的“互通性”进行测试。
- 当“主机连接状态”为“IP不可达”或“连接失败”时，单击“扫描”后，会弹出主机连接状态确定提示框，请根据提示选择是否继续扫描。

步骤5 在右侧弹出的页面中，如图4-8所示，单击“确定”。

图 4-8 创建任务

步骤6 在弹出的对话框中，如图4-9所示，勾选“我已了解并同意支付该笔费用”，单击“同意并扫描”。

图 4-9 开启主机扫描



- 在您扫描成功后，该费用将从您的账户余额中扣取。在页面右上角，单击“费用”，进入费用中心，可以查看余额变动。漏洞管理服务默认每隔1小时统计一次按需扫描的次数，进行费用扣取。
- 用户选择“按需计费”的方式进行扫描时，如果扫描任务失败，则本次扫描不扣费。

须知

- 当主机扫描任务成功时，请查看主机扫描详情，详细操作请参见**查看主机扫描详情**。
- 当主机扫描任务失败时，本次扫描不扣费。
- 当主机列表中有“扫描状态”为“排队中”或“进行中”的任务时，可以单击主机列表上方的“批量操作 > 批量取消”，在弹出的窗口中勾选需要取消扫描操作的主机进行批量取消。

----结束

相关操作

如果主机授权后仍扫描失败，请参照以下方法处理：

- **如何解决主机不能访问?**
- **主机扫描为什么会扫描失败?**
- **为什么在扫描时会提示授权委托失败?**

4.4 查看主机扫描详情

操作场景

该任务指导用户通过漏洞管理服务查看主机扫描详情。

说明

- Linux主机扫描支持主机漏洞扫描、基线检测、等保合规检测。
- Windows主机扫描目前仅支持主机漏洞扫描。

前提条件

- 已获取管理控制台的登录账号和密码。
- 主机扫描任务已成功完成。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 查看主机信息，相关参数说明如**表4-4**所示。

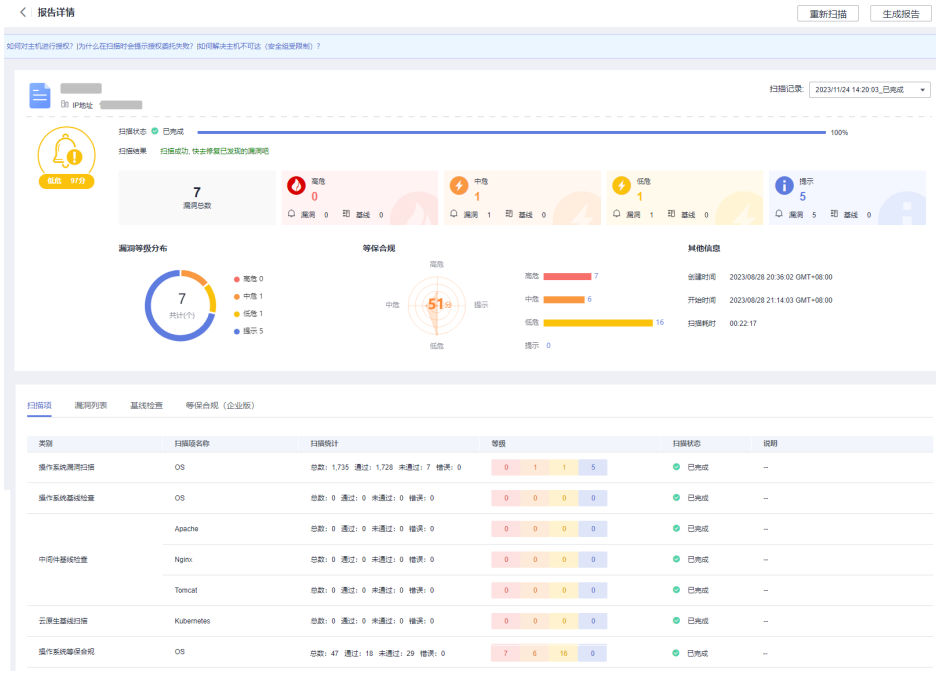
表 4-4 主机资产列表参数说明

参数	参数说明
主机名称	主机的名称。
IP地址	主机的IP地址。
授权信息	主机授权的具体操作请参见**编辑Linux主机授权**和**编辑Windows主机授权**。
操作系统	主机的操作系统，包含Linux和Windows操作系统。 该参数默认不显示，单击主机列表右上方的  ，可选择显示该参数。
跳板机	添加跳板机的具体操作请参见**添加跳板机**。
分组	主机所在的分组。 单击主机列表上方的“批量操作 > 更换分组”，可更换主机组。
主机连接状态	主机的连接状态。 取值包括： ● 全部状态 ● 连接成功 ● IP不可达 ● 登录失败 ● 未知
扫描状态	主机的扫描状态。 取值包括： ● 全部状态 ● 进行中 ● 已完成 ● 已取消 ● 排队中 ● 已失败 ● 未扫描

参数	参数说明
安全等级	主机的安全等级。 取值包括： • 全部等级 • 安全 • 低危 • 中危 • 高危 • 未知
上一次扫描时间	主机最近一次扫描任务扫描时间。

步骤5 在目标主机所在行的“安全等级”列，单击“查看报告”，查看相应任务的“扫描项总览”，如图4-10所示，各栏目说明如表4-5所示。

图 4-10 查看主机扫描详情



说明

- 扫描任务详情界面默认显示最近一次的扫描情况，如果您需要查看其他时间的扫描情况，在“扫描记录”下拉框中，选择扫描时间点。

  扫描报告只会保留最近10次的记录，之前的历史数据会保留一年，如果需要获取请联系华为云技术支持工程师处理。
- 单击右上角的“重新扫描”，可以重新执行扫描任务。
- 当扫描任务成功完成后，单击右上角的“生成报告”，可以生成相应的主机扫描报告。

表 4-5 详情总览说明

栏目	说明
目标IP	主机IP。
任务信息	显示目标任务的基本信息，包括： • 得分：任务被创建后，初始得分是一百分，任务扫描完成后，根据扫描出的漏洞个数和漏洞级别会扣除相应的分数，提示漏洞和无漏洞则不扣分。 • 漏洞总数：包含高危、中危、低危和提示中漏洞及基线的总数。 • 漏洞等级分布：以饼状图的形式展示漏洞等级数分布，漏洞等级包括高危、中危、低危和提示。 • 等保合规：为您提供本地化、系统化、专业的等保测评服务，为您提供一站式安全产品及服务，帮助您测评整改，提升安全防护能力，快速满足国家实行的网络安全等级保护制度，Windows扫描暂不支持此项检测。 等保合规的漏洞数和分数会单独展示。 **须知** 仅企业版可查看“等保合规”功能的检测结果。 • 其他信息：创建时间、开始时间以及任务的扫描耗时。 • 扫描结果：扫描任务的执行结果，有“扫描成功”和“扫描失败”两种结果。
扫描项	显示扫描任务的类别、扫描项名称、扫描统计、等级和扫描状态。

步骤6 选择“扫描项”页签，查看目标主机的扫描项信息，如图4-11所示。

图 4-11 扫描项

步骤7 选择“漏洞列表”页签，查看目标主机的漏洞信息，如图4-12所示。

图 4-12 漏洞列表界面

说明

- 如果您确认扫描出的漏洞不会对主机造成危害，您可以在目标漏洞所在行的“操作”列，单击“忽略”，忽略该漏洞。漏洞被忽略后，相应的漏洞统计结果将发生变化，在扫描报告中也不会出现该漏洞，并且在后续的扫描任务中，漏洞忽略的结果会被继承。
- 单击漏洞名称，进入“漏洞详情”页面，根据修复建议修复漏洞。

步骤8 选择“基线检查”页签，查看主机扫描的基线检查信息，如图4-13所示。

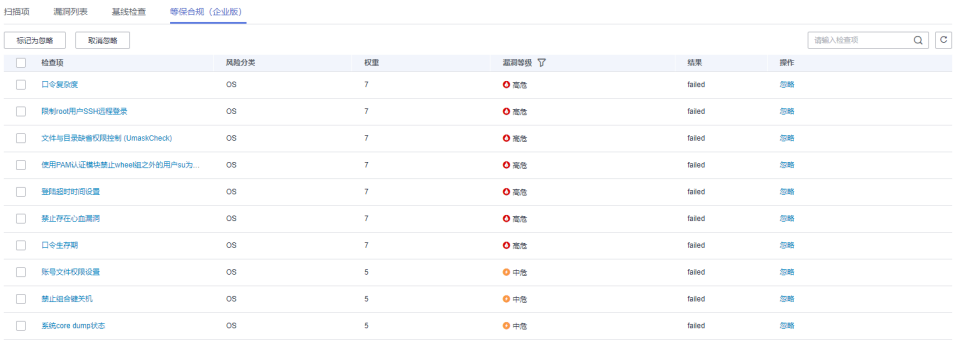
图 4-13 基线检查

说明

- 如果您确认扫描出的检查项不会对主机造成危害，您可以在目标检查项所在行的“操作”列，单击“忽略”，忽略该检查项。检查项被忽略后，相应的检查项统计结果将发生变化，在扫描报告中也不会出现该检查项，并且在后续的扫描任务中，检查项忽略的结果会被继承。
- Windows扫描暂不支持基线检测扫描。

步骤9 单击“等保合规（企业版）”页签，进入“等保合规（企业版）”的详情列表界面，显示目标主机的等保合规检测信息，如图4-14所示。

图 4-14 等保合规



须知

- 如果您确认扫描出的检查项不会对主机造成危害，您可以在目标检查项所在行的“操作”列，单击“忽略”，忽略该检查项。检查项被忽略后，相应的检查项统计结果将发生变化，在扫描报告中也不会出现该检查项，并且在后续的扫描任务中，检查项忽略的结果会被继承。
- 漏洞管理服务目前仅企业版用户支持等保合规检测，如果您需要对您的主机进行等保合规检测，请购买企业版。

----结束

相关操作

- 有关主机扫描得分的计算方法参考如下：

  扫描任务被创建后，初始得分是一百分，任务扫描完成后，根据扫描出的漏洞级别会扣除相应的分数。

  主机评分 = 100分 – 高危漏洞数 * 3分/个 – 中危漏洞数 * 2分/个 – 低危漏洞数 * 1分/个。每类漏洞最多计算20个。

  说明

  - 得分越高，表示漏洞数量越少，主机越安全。
  - 如果得分偏低，请根据实际情况对漏洞进行忽略标记，或根据修复建议修复漏洞。
  - 漏洞修复后，建议重新扫描一次查看修复效果。
- 有关修复主机漏洞的详细介绍，请参见**如何修复扫描出来的主机漏洞？**。

4.5 生成并下载主机扫描报告

操作场景

当主机扫描任务成功完成后，您可以生成漏洞扫描报告和等保合规配置报告，报告目前支持PDF格式和Excel格式。

须知

漏洞管理服务目前仅企业版用户支持等保合规检测，如果您需要下载等保合规配置报告，请购买企业版。

前提条件

已成功完成主机扫描任务，即目标主机的“扫描状态”状态为“已完成”。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 选择主机，单击“生成报告”，弹出“生成报告配置”窗口，如图4-15所示。

图 4-15 生成主机报告配置

步骤5 修改“报告名称”，选择“报告类型”。

“报告名称”自动生成，可修改。

步骤6 单击“确定”，弹出前往报告中心下载报告的提示框。

步骤7 单击“确定”，进入“报告中心”页面。

步骤8 单击生成报告所在行的“下载”，可将报告下载到本地。

说明

在目标主机所在行的“安全等级”列，单击“查看报告”，进入报告详情页面后，也支持生成报告。

主机扫描报告支持生成并下载英文版，需切换控制台语言为英文后，按照上述指导进行英文版报告生成和下载。

----结束

主机漏洞扫描报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板说明如下：

- 主机概览

  查看目标主机的基本信息。

  图 4-16 查看主机概览信息

  1 主机概览

主机风险	低危 97分
IP地址	[redacted]
主机名	[redacted]
操作系统	Linux
插件版本	VSS-PLUGIN-1691132582
扫描起始时间	2023/08/03 18:59:58
扫描结束时间	2023/08/03 19:05:04

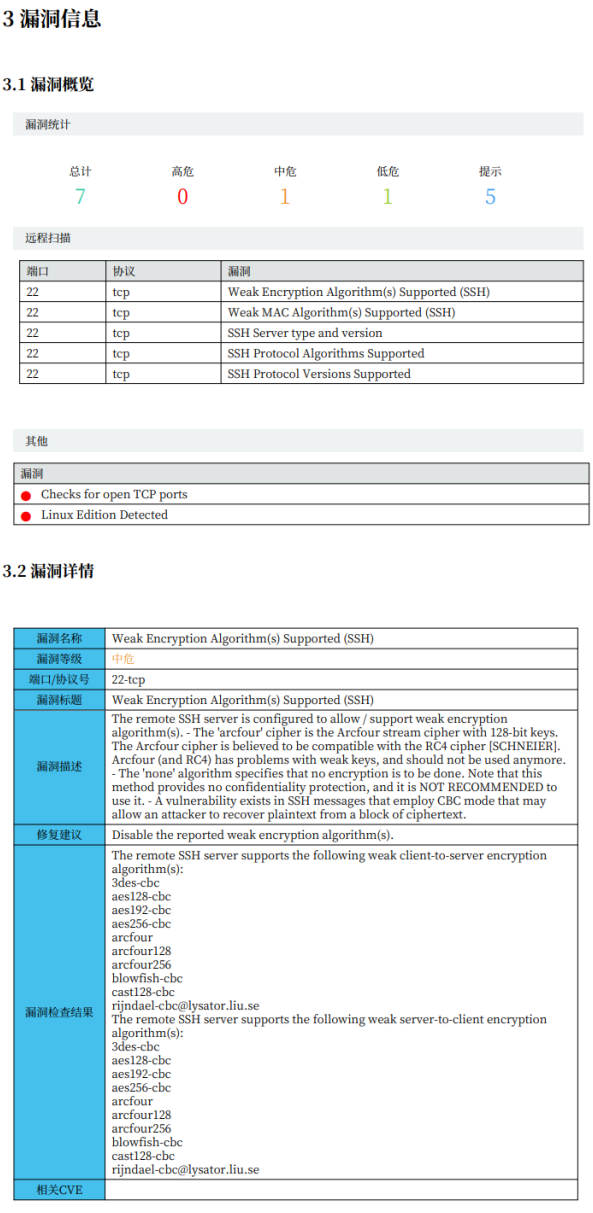
- 扫描信息概览

  查看目标主机的扫描总览信息。

图 4-17 查看扫描概览信息

- 系统漏洞扫描详情
  您可以根据修复建议修复系统漏洞。

图 4-18 查看漏洞详情以及修复建议



3 漏洞信息

3.1 漏洞概览

漏洞统计

总计	高危	中危	低危	提示
7	0	1	1	5

远程扫描

端口	协议	漏洞
22	tcp	Weak Encryption Algorithm(s) Supported (SSH)
22	tcp	Weak MAC Algorithm(s) Supported (SSH)
22	tcp	SSH Server type and version
22	tcp	SSH Protocol Algorithms Supported
22	tcp	SSH Protocol Versions Supported

其他

漏洞
Checks for open TCP ports
Linux Edition Detected

3.2 漏洞详情

漏洞名称	Weak Encryption Algorithm(s) Supported (SSH)
漏洞等级	中危
端口/协议号	22-tcp
漏洞标题	Weak Encryption Algorithm(s) Supported (SSH)
漏洞描述	The remote SSH server is configured to allow / support weak encryption algorithm(s). - The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.
修复建议	Disable the reported weak encryption algorithm(s).
漏洞检查结果	The remote SSH server supports the following weak client-to-server encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The remote SSH server supports the following weak server-to-client encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se
相关CVE	

- 基线检查详情

  您可以根据修复建议修复基线漏洞。

图 4-19 查看基线检查结果以及修复建议

4 基线检查信息

4.1 基线检查概览

总计	高危	中危	低危	提示
26	0	14	12	0

4.2 基线检查详情

检查项	规则：禁用IP转发功能
风险分类	OS
等级	中危
结果	未通过
子检查项1	**检查结果:** 未通过 **检查描述:** 执行命令sysctl net.ipv4.ip_forward，检查net.ipv4.ip_forward的值是否为0 **当前值:** net.ipv4.ip_forward=1 **建议值:** net.ipv4.ip_forward = 0
修复建议	修改/etc/sysctl.conf中参数 net.ipv4.ip_forward=0 执行以下命令保存配置 #sysctl -p

说明

当“基线检查”页签无数据显示时，则不会在报告中体现基线检查的信息。

等保合规配置报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板说明如下：

- 概览
  查看等保合规配置报告的概览信息。

图 4-20 查看等保合规概览信息

1. 概览

48	总计	高危	中危	低危	提示
	29	8	7	14	0

- 等保合规检查详情
  您可以根据修复建议修复等保合规漏洞。

图 4-21 查看等保合规检查详情

2. 等保合规检查详情

检查项	禁止存在心血漏洞
权重	7
等级	高危
结果	未通过
子检查项1	**检查结果:** 未通过 **检查描述:** 确保openssl版本符合要求:openssl version | egrep "(1\.0\.0)|(1\.0\.1f)|(1\.0\.1e)|(1\.0\.1d)|(1\.0\.1c)|(1\.0\.1b)|(1\.0\.1a)|(1\.0\.1)|(1\.0\.2-beta)|(1\.0\.2-beta1)" **当前值:** OpenSSL 1.0.1f 6 Jan 2014 **建议值:** 输出为空
修复建议	

表3.1 禁止存在心血漏洞

4.6 其他操作

4.6.1 添加跳板机

操作场景

该任务指导用户通过漏洞管理服务为Linux系统的主机配置跳板机。

说明

当前仅支持添加Linux系统跳板机。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加Linux系统的主机。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 在目标Linux系统主机的“操作”列，单击“编辑”，页面右侧弹出“编辑主机”窗口。

步骤5 在“授权信息”区域，单击“选择跳板机”下拉框，选择“跳板机管理”，显示“跳板机管理”页面。

步骤6 选择编辑已有跳板机或创建新的跳板机。

- 选择“编辑跳板机”，如图4-22所示。

图 4-22 编辑跳板机

选择需要编辑的跳板机，单击图标，即可修改跳板机的信息。配置说明如**表4-6**所示。

修改完跳板机信息后，单击“确认”，完成跳板机的修改。

- 选择“创建跳板机”，如**图4-23**所示。

图 4-23 创建跳板机

设置配置参数，配置说明如**表4-6**所示。

表 4-6 跳板机配置参数说明

参数名称	参数说明
主机名称	跳板机的主机名称。
公网IP	跳板机的公网IP。
登录端口	跳板机的登录端口。

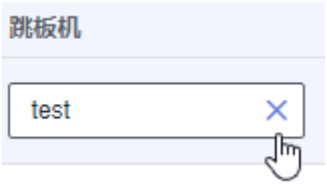
参数名称	参数说明
选择登录方式	登录跳板机的方式。 – 选择“密码登录”时，需要配置登录跳板机的“用户名”和“密码”。 – 选择“密钥登录”时，需要配置登录跳板机的“用户名”、“私钥”和“私钥密码”。
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建漏洞管理服务专用的默认主密钥。 **须知** – 您也可以在数据加密服务的以下区域创建密钥： ■ 华北-北京一 ■ 华北-北京四 ■ 华南-广州 ■ 华东-上海一 ■ 华东-上海二 ■ 西南-贵阳一 ■ 华南-深圳 有关创建密钥的详细操作，请参见**创建密钥**。 – 使用数据加密服务需要单独计费，详细的服务资费和费率标准，请参见**价格详情**。

配置完跳板机信息后，单击“确认”，完成跳板机的创建。

步骤7 单击“确认”，完成跳板机的选择。

步骤8 （可选）单击跳板机后的×，可以删除跳板机。

图 4-24 删除跳板机



----结束

4.6.2 取消主机授权

操作场景

该任务指导用户通过漏洞管理服务取消主机授权。

取消主机授权后，将不能完全扫描出主机的安全风险，请谨慎操作。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加主机。
- 已开通预置账号。
- 已在创建任务时授权华为云通过网络连接到对应的主机，即已进行主机授权。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

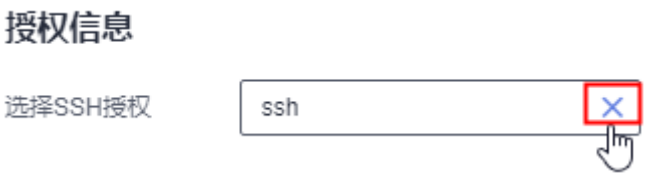
步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 在目标主机的“操作”列，单击“编辑”，页面右侧弹出“编辑主机”窗口。

步骤5 删除授权信息。

- 当目标主机操作系统为Linux时，在“授权信息”区域，单击“选择SSH授权”后的×，即可删除授权信息。

  图 4-25 删除 Linux 操作系统主机授权

- 当目标主机操作系统为Windows时，在“授权信息”区域，单击“选择Windows授权”后的×，即可删除授权信息。

  图 4-26 删除 Windows 操作系统主机授权

步骤6 单击“确认”，取消主机授权成功。

----结束

4.6.3 测试互通性

操作场景

该任务指导用户测试待扫描的主机与扫描环境的连通性是否正常。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 在目标主机的“操作”列，单击“互通性”，即可进行测试。

----结束

相关操作

主机互通性测试异常如何处理?

4.6.4 更换分组

操作场景

该任务指导用户通过漏洞管理服务为已添加的主机更换分组。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 勾选一个或多个目标主机，单击“更换分组”，弹出“更换分组”窗口。

- 在已有“主机组”下拉列表中，选择已有的主机组，如图4-27所示。

图 4-27 更换分组

- 单击“新建分组”页签，输入“主机组名称”，创建新的主机组，如图4-28所示。

图 4-28 新建分组

说明

在目标主机的“操作”列，单击“编辑”，在“编辑主机”窗口中也可新建或更换主机组。

步骤5 单击“确认”，主机更换分组成功。

----结束

4.6.5 删除主机

操作场景

该任务指导用户通过漏洞管理服务删除已添加的主机。

删除主机后，该主机的所有扫描历史报告将会被删除，请谨慎操作。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤4 在目标主机的“操作”列，单击“删除”，在弹出的对话框中，单击“确定”。

说明

用户可以同时删除多个主机。勾选多个主机后，单击“批量操作 > 删除”，在弹出的对话框单击“确定”，批量删除主机。

----结束

5 安全监测

5.1 新增监测任务

操作场景

漏洞管理服务支持网站扫描，网站是您的“资产”，您可以在“安全监测”界面对您的资产进行安全扫描与编辑操作。

该任务指导用户通过漏洞管理服务新增监测任务，监测任务新增成功后，自动开启监测。

须知

漏洞管理服务的基础版不支持安全监测功能，如果您是基础版用户，请您通过购买专业版、高级版或企业版使用该功能。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加网站。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在“安全监测”页面，单击“新增监测任务”，进入新增监测任务入口。

步骤4 在“新增监测任务”界面，请根据表5-1进行扫描设置，设置后如图5-1所示。

图 5-1 监测任务的扫描设置

表 5-1 扫描设置参数说明

参数	参数说明
任务名称	用户自定义。
目标网址	待扫描的网站地址或IP地址。 通过下拉框选择已认证通过的域名。
扫描周期	单击下拉框选择任务扫描周期。 • 每天 • 每三天 • 每周 • 每月
开始时间	设置监测任务开始的时间。
扫描模式	三种扫描模式： • 极速策略：扫描耗时最少，能检测到的漏洞相对较少。 • 标准策略：扫描耗时适中，能检测到的漏洞相对较多。 • 深度策略：扫描耗时最长，能检测到最深处的漏洞。
是否扫描登录URL	默认不扫描登录URL，开启扫描登录URL前，请务必确认不会影响正常业务
是否将每次扫描升级为专业版规格	基础版用户开启此功能后，扫描过程中会按需扣费： • 鼠标移动至 了解升级后影响。 • 打开此功能时，扫描时会自动升级为专业版按需扣费，关闭该功能时，扫描时不会升级。

参数	参数说明
扫描项设置	漏洞管理服务支持的扫描项参照表5-2。 •  ：开启 •  ：关闭

表 5-2 扫描项设置

扫描项名称	说明
Web常规漏洞扫描（包括XSS、SQL注入等30多种常见漏洞）	提供了常规的30多种常见漏洞的扫描，如XSS、SQL等漏洞的扫描。默认为开启状态，不支持关闭。
端口扫描	检测主机打开的所有端口。
弱密码扫描	对网站的弱密码进行扫描检测。
CVE漏洞扫描	CVE，即公共暴露漏洞库。漏洞管理服务可以快速更新漏洞规则，扫描最新漏洞。
网页内容合规检测（文字）	对网站文字的合规性进行检测。
网页内容合规检测（图片）	对网站图片的合规性进行检测。
网站挂马检测	挂马：上传木马到网站上，使得网站在运行的时候执行木马程序，被黑客控制，遭受损失。漏洞管理服务可以检测网站是否存在挂马。
链接健康检测（死链、暗链、恶意外链）	对网站的链接地址进行健康性检测，避免您的网站出现死链、暗链、恶意链接。

步骤5 设置完成后，单击“确认”。

说明

如果没有设置开始扫描时间，且此时服务器没有被占用，则创建的任务可立即开始扫描，任务状态为“进行中”；否则进入等待队列中等待，任务状态为“等待中”。

----结束

5.2 暂停监测任务

操作场景

该任务指导用户通过漏洞管理服务停止资产的监测。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已开启资产的监测任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面。

步骤4 在目标监测任务所在行的“操作”列中，单击“暂停监测”，在弹出的对话框中，单击“确认”。

说明

如果用户需要再次开启监测任务，在目标监测任务所在行的“操作”列中，单击“开启监测”，开启监测任务。

----结束

5.3 编辑监测任务

操作场景

该任务指导用户通过漏洞管理服务编辑资产的监测任务。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已创建监测任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面。

步骤4 在目标监测任务所在行的“操作”列中，单击“编辑任务”，如图5-2所示。

图 5-2 编辑监测任务

步骤5 根据需求，重新配置监控信息和扫描项设置。

----结束

5.4 删除监测任务

操作场景

该任务指导用户通过漏洞管理服务删除已创建的监测任务。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已创建监测任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面。

步骤4 在目标监测任务所在行的“操作”列中，单击“删除任务”，在弹出的对话框中，单击“确认”。

----结束

5.5 查看安全监测列表

操作场景

该任务指导用户通过漏洞管理服务查看安全监测列表。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已新增监测任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面，如图5-3所示，相关参数说明如表5-3所示。

图 5-3 查看安全监测列表

表 5-3 安全监测列表参数说明

参数	参数说明
任务名称	创建监测任务时用户自定义的任务名称。
监测周期	监测任务开始执行的周期。 • 每天 • 每三天 • 每周 • 每月
监测资产	创建监测任务时填写的目标网址。
扫描模式	扫描模式分为“极速策略”、“标准策略”和“深度策略”，建议选择“深度策略”模式。
上一次扫描时间	最近一次扫描的时间。
最近一次扫描情况	最近一次扫描任务的信息，包括得分和各等级的漏洞数量。单击*分数*或者“查看详情”，进入“扫描详情”界面查看扫描概况。

----结束

5.6 查看任务详情

操作场景

该任务指导用户通过漏洞管理服务查看任务详情。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已开启了资产的监测任务。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面。

步骤4 在目标监测任务所在行的“最近一次扫描情况”列，单击*分数*或者“查看详情”，进入“任务详情”界面，可以查看扫描任务的详情。

扫描任务详情的内容说明请参见**查看网站扫描详情**。

----结束

6 移动应用安全

6.1 支持的服务版本

移动应用安全扫描仅支持基础版和专业版，详细内容请参见表6-1。

表 6-1 版本说明

服务版本	支持的计费方式	说明
基础版	免费	基础版主要为用户提供体验机会，仅支持安全漏洞扫描。基础版同样提供在线报告查看功能，查看内容仅限安全漏洞项，不包括隐私合规项。每个用户默认拥有5次基础版额度，扫描失败不扣费。
专业版	包年，按需套餐包计费 套餐包规格为10次或1次，可增加扫描配额包。	专业版为付费版本，提供全量功能，包含安全漏洞、隐私合规检测。隐私合规紧跟工信部164号发文，针对违规收集个人信息、超范围收集个人信息、频繁索权、过度索权等通报问题进行检测。用户可在线查看扫描报告，并导出PDF格式离线报告。

6.2 添加任务

用户添加任务成功后即开始自动扫描，中间不可停止，不可重复触发扫描，任务扫描成功后才会扣款。

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文件。
- 扫描文件需存在UI界面且无需登录。

操作步骤

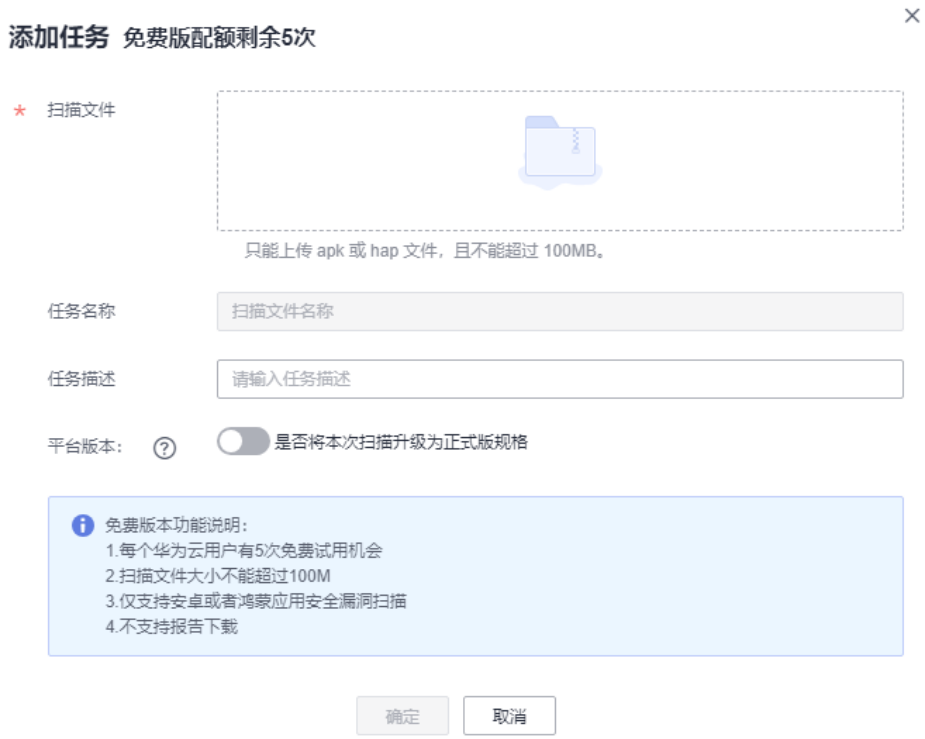
步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，单击“移动应用安全”。

步骤4 在“移动应用安全”页面，单击“添加任务”，在弹出的对话框中，单击“添加文件”选择本地的软件包，导入扫描对象，如图6-1所示。

图 6-1 添加扫描对象



说明

- 支持上传hap、apk类型的文件。
- 若用户未购买套餐包添加任务时提示扣费，已购买套餐包的用户即可可以直接创建任务，无需单次扣费。
- “是否将本次扫描升级为正式版本规格”默认关闭。如果打开，表示将本次扫描升级为正式版本规格。

步骤5 单击“确定”，开始扫描，请等待1小时左右，当任务状态显示“完成”，即可完成扫描。

说明

- 单击“停止”，可停止正在执行的任务。
- 单击“查看进度”，可查看正在执行的任务进度。

----结束

6.3 管理任务

操作场景

该任务指导用户通过漏洞管理服务查找、删除应用安全任务。

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 在左侧导航树中，单击 ，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，单击“移动应用安全”。

步骤4 在“移动应用安全”页面，查看应用安全任务列表，相关参数说明如表6-2所示。

图 6-2 应用安全任务列表

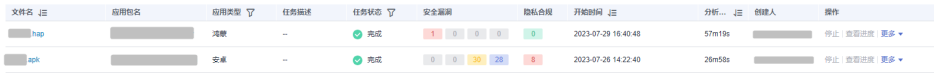


表 6-2 应用安全任务列表参数说明

参数	参数说明
文件名	扫描文件名称。
应用包名	应用包名称。
应用类型	应用类型为安卓或鸿蒙。
任务描述	对任务信息进行说明。

参数	参数说明
任务状态	• “排队中”：上传扫描对象后开始等待扫描。 • “分析中”：任务正在进行扫描。 当任务处于“分析中”状态大约5分钟时，可以单击任务状态进入检测详情界面。 – 详情界面左侧实时显示应用运行过程。 – 当出现登录界面时，暂停运行，此时支持用户操作手机界面输入登录凭证，输入完成后可单击右侧“完成”继续自动化检测。如果用户选择“跳过”，界面忽略登录操作，继续运行剩余检测任务。 **说明** 如果用户选择“跳过”，移动应用安全服务无法检测需要登录才能访问的页面，最终检测结果也不会包含需要登录才能访问的页面检测结果。 – 隐私合规检测完成后，会自动断开手机投屏界面。 • “完成”：任务已完成扫描。 • “失败”：任务扫描失败。 • “超时”：任务扫描超时。
安全漏洞	扫描结果的漏洞分布情况。
隐私合规	隐私合规的扫描结果。
开始时间	任务开始时间。
分析时长	分析上传文件的时间。
创建人	任务的创建人。

步骤5 在下拉框 

下拉选择应用类型，可根据应用类型筛选查看任务。

步骤6 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7 在输入框 

中输入任务名称关键字，可根据任务名称关键字筛选查看。可以和任务状态联合使用。

步骤8 单击 
刷新任务列表。

----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 > 漏洞管理服务”，进入漏洞管理服务管理控制台。

步骤3 在左侧导航栏，单击“移动应用安全”。

步骤4 在“移动应用安全”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“更多 > 删除”，根据系统提示执行删除操作。

----结束

6.4 查看扫描详情

该任务指导用户通过漏洞管理服务查看移动应用安全扫描结果。

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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，单击“移动应用安全”。

步骤4 在“移动应用安全”页面，单击对应任务的“文件名”。

步骤5 进入扫描报告查看页面，如图6-3所示，各栏目说明如表6-3所示。

图 6-3 查看应用安全扫描报告详情

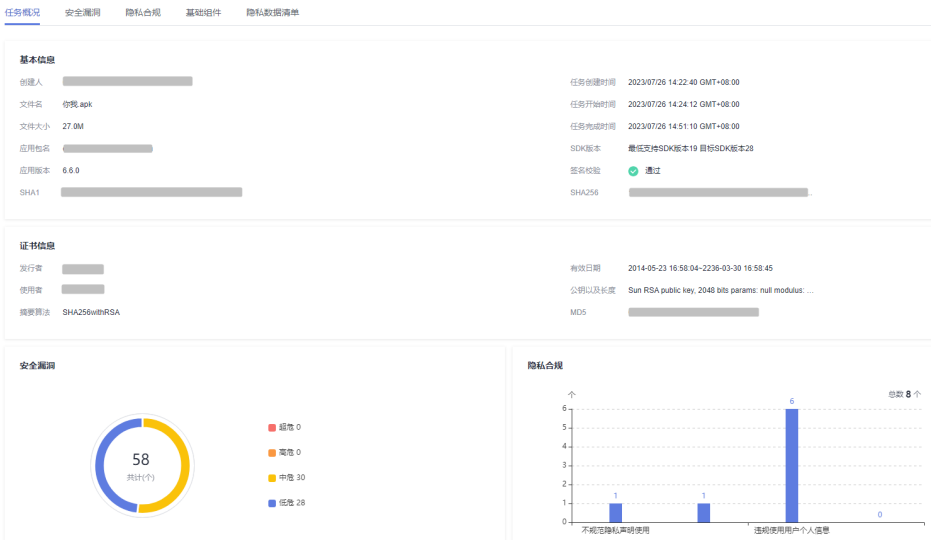


表 6-3 详情总览说明

栏目	说明
任务概况	显示目标任务的基本信息，包括： 基本信息：查看扫描文件大小、版本、特征库版本等基本信息。 证书信息：证书的发行者、使用者、摘要算法等信息。 安全漏洞：致命、高危、中危、低危各个级别漏洞数量占比。 隐私合规：不规范隐私声明使用、不合理权限申请、违规使用用户个人信息、其他侵害用户权益行为的使用情况。
安全漏洞	安全漏洞的风险描述和修复建议。
隐私合规	显示不规范隐私的详细数据分析，包括： ● 不规范隐私声明使用 – 无隐私策略声明 – 同意不清晰 – 隐私声明默认勾选同意 – 用户同意隐私政策之前申请隐私权限 – 用户同意隐私政策之前收集敏感信息 ● 不合理权限申请 – 不给权限不让用 – 过度索取权限 ● 违规使用用户个人信息 – 超频率读取用户数据 – 应用在后台读取用户隐私数据 – 第三方SDK采集用户隐私数据 – APP未经用户同意或超范围使用用户个人信息 – 与第三发共享并使用用户个人信息 ● 其他侵害用户权益行为 – 强制用户使用定向推送 – 误导下载APP
基础组件	被扫描的软件包所有的组件信息，例如名称、描述、保护级别等。
隐私数据清单	被扫描的软件包所有的个人信息，及个人信息对应的隐私政策声明和应用实际收集的信息。

----结束

6.5 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，报告目前只支持PDF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“完成”。

操作步骤

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击  ，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

步骤3 在左侧导航栏，单击“移动应用安全”。

步骤4 在“移动应用安全”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“更多 > 导出报告”。

步骤6 报告生成后，即可在本地打开查看。

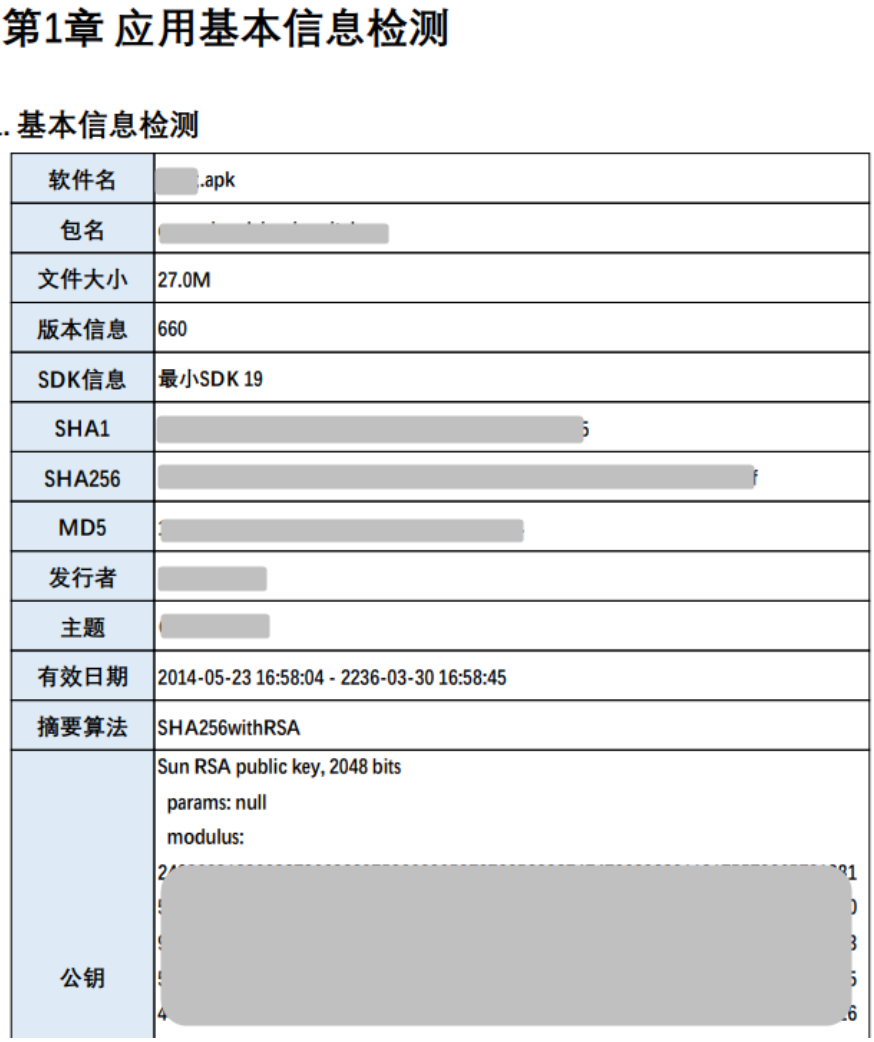
----结束

移动应用安全扫描报告模板说明

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）

- 应用基本信息检测
  应用检测的基本信息和检测概况。

图 6-4 应用基本信息



1. 第1章 应用基本信息检测

1.1. 基本信息检测

软件名	.apk
包名	
文件大小	27.0M
版本信息	660
SDK信息	最小SDK 19
SHA1	
SHA256	
MD5	
发行者	
主题	
有效日期	2014-05-23 16:58:04 - 2236-03-30 16:58:45
摘要算法	SHA256withRSA
公钥	Sun RSA public key, 2048 bits params: null modulus:

- 应用漏洞检测
  您可以参考每个组件扫描出的漏洞详细信息修复漏洞。

图 6-5 应用漏洞检测

2. 第2章 应用漏洞检测

2.1. 配置安全

2.1.1. 注册设备管理器

检测项目	存在[redacted]的行为，该行为未经交互。风险等级：高。
风险等级	高危
问题描述	存在[redacted]行为，该行为经常在恶意软件中出现，风险较高
检测场景	存在[redacted]行为，该行为未经交互。风险等级：高。
检测结果	安全
风险详情	无
修复建议	无需修复

- 应用隐私合规检测

图 6-6 应用隐私合规检测

3. 第3章 应用隐私合规检测

3.1. 无隐私策略声明

检测项目	首次启动无隐私声明
检测目的	164号文->APP、SDK违规处理用户个人信息方面->违规收集个人信息。重点整治APP、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。
是否存在风险	不存在
风险行为描述	不涉及
整改建议	不涉及
调用栈	不涉及
隐私策略声明	不涉及

- 应用权限信息检测

图 6-7 应用权限信息

4. 第4章 应用权限信息检测

权限名	描述	保护级别	权限类型
[redacted]ON			其他
a[redacted]O			其他
[redacted]			其他
[redacted]O			其他
a[redacted]T			其他
c[redacted]E			其他
c[redacted]GE			其他
c[redacted]E			其他
[redacted]T_			其他
[redacted]E			其他
c[redacted]E			其他
[redacted]MS G			其他
c[redacted]R			其他

- 应用组件信息检测
  查看软件的所有组件信息。

图 6-8 应用组件信息

5. 第5章 应用组件信息检测

5.1. Activity信息

名称	动作	类别	主要活动	导出
cr[redacted]vity	cn.[redacted]ten t.DActivity	c[redacted]sit yloan	否	是
cr[redacted]ti vity	cn.j[redacted]nten t.JNotifyActivity	c[redacted]it yloan	否	是
cr[redacted]ty	cn.j[redacted] op[redacted]y	a[redacted]r y.DEFAULT, co[redacted]rsit yloan	否	是
[redacted]ity	cn.[redacted] ush[redacted]y	a[redacted]or y.DEFAULT, c[redacted] yloan	否	是

- 移动应用安全评测依据

图 6-9 移动应用安全评测信息

- 隐私数据清单

图 6-10 隐私数据清单

7. 第7章 隐私数据清单

序号	个人信息类型	隐私政策声明	应用实际收集
1	联系人	√	√
2	短信		√
3	通话记录		√
4	浏览器书签信息		
5	浏览器访问历史		
6	日程表		
7	照片		
8	音视频		
9	位置信息		√
10	设备ID信息		
11	IMEI		√
12	本机电话号码	√	√
13	基站定位信息		√
14	IMSI		√
15	Android_ID		√
16	设备MAC地址		√
17	应用安装包信息		√

7 二进制成分分析

7.1 支持的服务版本

漏洞管理服务侧已正式停售二进制成分分析功能，用户无法新购，已购买二进制成分分析相关规格的用户不受影响，可继续使用至套餐包到期。

如您需要继续使用同款产品，请在**开源治理服务CodeArts Governance**中重新购买使用。

二进制成分分析扫描仅支持基础版和专业版，详细内容请参见**表7-1**。

表 7-1 版本说明

服务版本	支持的计费方式	说明
基础版	免费	基础版主要为用户提供体验机会，仅支持开源软件漏洞扫描，扫描文件大小不能超过100M。基础版提供在线报告查看功能，不支持报告下载。每个用户默认拥有5次基础版额度，扫描失败不扣配额。
专业版	包年，按需套餐包计费 套餐包规格为20次或1次，可增加扫描配额包。	专业版为付费版本，提供全量功能，包含开源软件漏洞、安全配置、密钥和信息泄露、安全编译选项，扫描文件大小不能超过5G。用户可在线查看扫描报告，并导出PDF格式或Excel格式离线报告。 扫描失败时，不扣配额。

7.2 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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

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”，在弹出的对话框中，单击“添加文件”选择本地的软件包，导入扫描对象，如图7-1所示。

图 7-1 添加扫描对象

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

7.3 管理任务

操作场景

该任务指导用户通过漏洞管理服务查找、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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

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7-2所示。

图 7-2 成分分析任务列表

表 7-2 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。

参数	参数说明
任务状态	• “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 > 漏洞管理服务”，进入漏洞管理服务管理控制台。

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 > 漏洞管理服务”，进入漏洞管理服务管理控制台。

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

7.4 查看扫描详情

该任务指导用户通过漏洞管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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

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“报告”，如图7-3所示。

说明

单击“任务名称”也可以进入扫描报告页面。

图 7-3 进入成分分析扫描报告入口

步骤6 进入扫描报告查看页面，各栏目说明如表7-3所示。

说明

当扫描任务成功完成后，单击右上角的“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。

表 7-3 详情总览说明

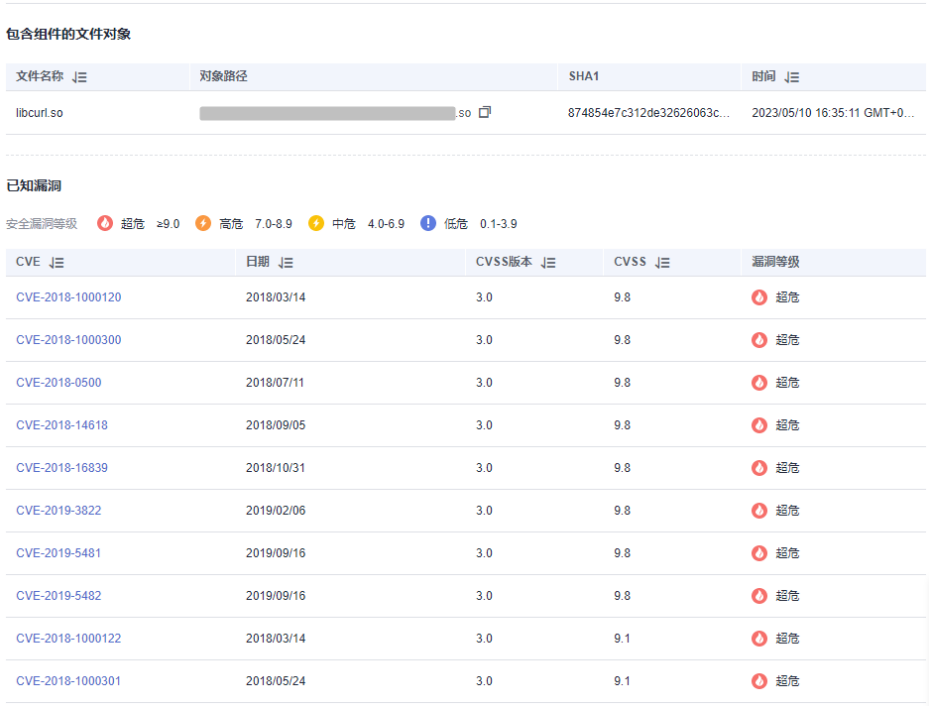
栏目	说明
任务概况	显示目标任务的基本信息，包括： ● 查看文件名、文件大小、平台版本、特征库版本等基本信息。
	显示目标任务的组件检测、安全漏洞、安全配置、许可协议、信息泄露等检测概况，包括： ● 组件检测：被扫描的软件包所有的组件数量，有漏洞、未知版本和无漏洞组件数量占比。 ● 安全漏洞：超危、高危、中危、低危各个级别漏洞数量占比。 ● 安全配置：展示通过、失败、不涉及的检测结果数量占比。 ● 许可协议：展示数量排名前六的漏洞使用许可。 ● 信息泄露：展示各检测结果数量分布。
开源漏洞分析	显示扫描任务中的每个组件的组件名、组件版本、许可协议、包含文件数以及存在漏洞数。 组件名称和漏洞数可按升降序查看。 可按组件类别、组件名称对组件列表进行筛选查看。
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。
密钥和信息泄露	显示IP、硬编码密码、弱口令、Git地址、SVN地址和硬编码密钥的检测结果。
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。

步骤7 在“开源漏洞分析”页签查看软件包的每个组件的漏洞。

说明

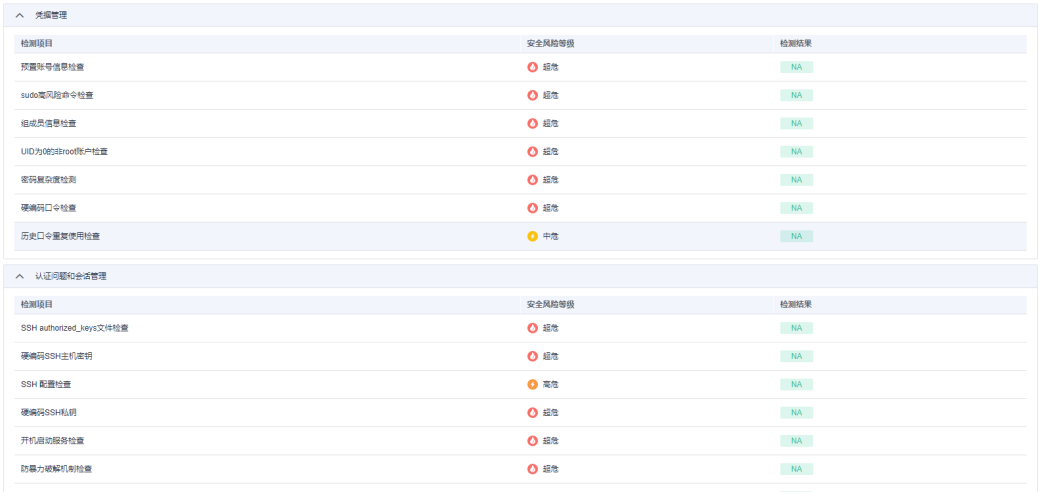
如果检测结果存在漏洞或者风险，可单击“组件名称”列，查看详细信息。

- 鼠标移至“对象路径”列，可查看文件完整路径；单击右侧复制按钮，可拷贝文件完整路径信息。
- 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”。



步骤8 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 7-4 安全配置检查结果



步骤9 在“密钥和信息泄露”页签查看对应检测项目的检测结果。

图 7-5 密钥和信息泄露检测结果

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

步骤10 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 7-6 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	0.00%	27
NX	堆栈不可执行	92.59%	2
PIC	地址无关	100.00%	0
PIE	随机化	N/A	0
RELRO	GOT表保护	59.26%	11
SP	栈保护	74.07%	7
NO Rpath/Runpath	动态库搜索路径（禁选）	100.00%	0
FS	Fortify Source	3.70%	26
Ftrapv	整数溢出检查	N/A	0
Strip	删除符号表	100.00%	0

----结束

7.5 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 在左侧导航树中，单击 ☰，选择“服务列表 > 开发与运维 > 漏洞管理服务”，进入漏洞管理服务页面。

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“报告”。

说明

单击“任务名称”也可以进入下载报告页面。

图 7-7 进入成分分析扫描报告入口

步骤6 单击右上角的“生成PDF报告”或“生成Excel报告”。

图 7-8 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”，可以下载报告。

图 7-9 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 7-10 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 /sbcScanList?recordId=
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 7-11 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 7-12 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 7-13 查看漏洞列表信息

4 漏洞列表

4.1.1. ffmpeg-3.1.2

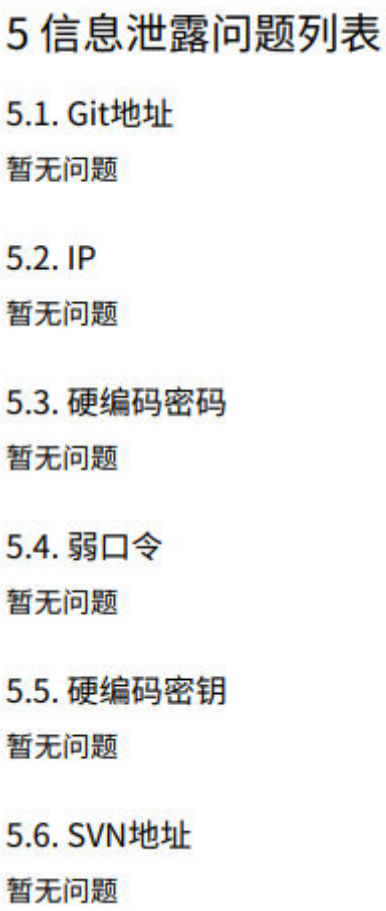
4.1.1.1. CVE-2016-6881

CVE编号	CVE-2016-6881
漏洞描述	The zlib_refill function in libavformat/swfdec.c in FFmpeg before 3.1.3 allows remote attackers to cause an infinite loop denial of service via a crafted SWF file.
影响组件名称	ffmpeg
影响组件版本	3.1.2
漏洞发布时间	2016-12-23
漏洞CVSS分数	5.5
漏洞风险等级	中危
解决方案	It has been reported that this has been fixed. Please refer to the product listing for upgraded versions that address this vulnerability.

文件路径
com.huawei.himovie.test.apk_/lib/armeabi/libweiboffmpeg.so

- 密钥和信息泄露问题列表

图 7-14 查看密钥和信息泄露信息



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 7-15 查看安全编译选项信息

6 安全编译选项问题列表

6.1. BIND_NOW (共计27个文件未通过该检查项)

编号	问题所在文件路径
1	com.huawei.himovie.test.apk_/lib/armeabi/libffmpeg_neon.so
2	com.huawei.himovie.test.apk_/lib/armeabi/libpdc.so
3	com.huawei.himovie.test.apk_/lib/armeabi/libOttCaInterface.so
4	com.huawei.himovie.test.apk_/lib/armeabi/libc++_shared.so
5	com.huawei.himovie.test.apk_/lib/armeabi/libutility.so
6	com.huawei.himovie.test.apk_/lib/armeabi/libcurl.so
7	com.huawei.himovie.test.apk_/lib/armeabi/libweiboffmpeg.so
8	com.huawei.himovie.test.apk_/lib/armeabi/libweibocache.so
9	com.huawei.himovie.test.apk_/lib/armeabi/libCDNSelector.so
10	com.huawei.himovie.test.apk_/lib/armeabi/libaegissec.so

- 安全配置检查列表

图 7-16 查看安全配置检查列表

7 安全配置检查列表

7.1. 预置账号信息检查

7.1.1

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

7.1.1 详细信息

问题
[There is no operate system in the package]

7.6 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。

8 总览

操作场景

该任务指导用户通过“总览”查看网站和主机扫描概况，主要展示资产信息和漏洞信息。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加网站和主机。

查看扫描概况

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“开发与运维 > 漏洞管理服务”，进入“总览”界面。

步骤3 查看扫描概况。

- 查看资产总数，如图8-1所示。
  资产总数是高危资产、中危资产、低危资产和安全资产的总和。

  图 8-1 资产总数

- 查看资产信息，如图8-2所示，资产信息参数说明如表8-1所示。

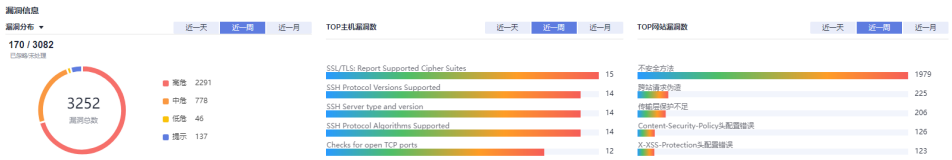
图 8-2 资产信息

表 8-1 资产信息参数说明

参数	说明	操作
资产分布	显示已扫描和未扫描的资产的总数。	当资产的个数为0时，单击“添加资产”，进入到资产列表界面添加网站或主机。
资产	显示TOP风险前五位的网站或主机的资产。	- 单击“资产信息”区域右上角的“网站”或“主机”，可查看对应资产的信息。 - 单击资产可以进入到相应的资产报告详情页。
资产别称	显示网站或主机的名称。	--
漏洞总数	统计漏洞的总数，包括高危、中危、低危和提示的总数之和。	--
漏洞等级	显示资产不同等级的风险个数，包括高危、中危、低危和提示。	--
得分	- 得分最低的网站为最危险的网站，如果得分一样，则比较高危漏洞个数、中危漏洞个数.....依次类推。 - 如果用户添加了资产且所有资产的扫描得分是100分，则没有最危险网站，展示“--”。	--
扫描时间	显示资产扫描的时间。	--

- 查看近一天、近一周或近一月资产的漏洞信息，如图8-3所示。
  漏洞分布情况支持指定网站、主机或所有资产进行查看。

图 8-3 查看扫描情况



----结束

9 报告中心

操作场景

该任务指导用户通过“报告中心”生成、下载或删除报告。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已生成网站或主机报告。

查看扫描概况

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“开发与运维 > 漏洞管理服务”，进入“总览”界面。

步骤3 单击“报告中心”，在“报告中心”页面可执行如下操作：

- 下载报告
  - 勾选“已生成”状态的报告，单击“批量下载”，可下载多个报告到本地。
  - 单击“已生成”状态的报告所在行的“下载”，可下载单个报告到本地。
- 生成报告

  单击“已过期”状态的报告所在行的“生成”，若报告记录未被清理，则会产生一条新的记录。

  如果报告生成失败，可以尝试重新生成一次。如果无法解决，请联系华为云技术支持工程师处理。
- 删除报告
  - 勾选需要删除的报告，单击“批量删除”，可根据提示信息删除多个报告。
  - 单击报告所在行的“删除”，可根据提示信息删除单个报告。

  删除操作无法恢复，请谨慎操作。

----结束

10 云审计服务支持的关键操作

10.1 云审计服务支持的漏洞管理服务操作列表

通过云审计服务，用户可以记录与漏洞管理服务相关的操作事件，便于日后的查询、审计和回溯。

开启了云审计服务后，系统开始记录漏洞管理服务资源的操作。

云审计服务管理控制台保存最近7天的操作记录，查看云审计日志操作请参考**查看审计事件**。

云审计服务支持的漏洞管理服务操作列表如**表10-1**所示。

表 10-1 云审计服务支持的漏洞管理服务操作列表

操作名称	资源类型	事件名称
网站		
创建域名	domain	createDomain
删除域名	domain	deleteDomain
编辑域名	domain	editDomain
免认证/一键认证	domain	authenticateDomain
快捷认证	domain	authorizeDomain
创建漏洞扫描任务	scan	createScanTask
创建内部漏洞扫描任务	scan	createInnerScanTask
重启漏洞扫描任务	scan	restartScanTask
取消漏洞扫描任务	scan	cancelScanTask
编辑漏洞扫描任务	scan	editScanTask
创建订阅套餐	resource	createPurchaseOrder

操作名称	资源类型	事件名称
更新订阅套餐	resource	createAlterOrder
批量更新订阅套餐	resource	createBatchAlterOrder
新用户注册	resource	createVSSResource
删除监测任务	monitor	deleteMonitorJob
暂停监测任务	monitor	pauseMonitorJob
恢复监测任务	monitor	resumeMonitorJob
忽略漏洞	vuln	addVulnFalsePositive
取消忽略漏洞	vuln	deleteVulnFalsePositive
生成网站扫描报告	report	generateWebScanReport
下载网站扫描报告	report	downloadWebScanReport
主机		
添加主机	host	addHost
删除主机	host	deleteHost
编辑主机	host	editHost
更换分组	host	changeHostGroup
新增主机组	host	addHostGroup
编辑主机组	host	editHostGroup
删除主机组	host	deleteHostGroup
创建主机扫描任务	scan	createHostScanTask
取消主机扫描任务	scan	cancelHostScanTask
添加跳板机	jumper	saveJumperServer
编辑跳板机	jumper	editJumperServer
删除跳板机	jumper	deleteJumperServer
添加smb授权	credential	saveSmbCredential
编辑smb授权	credential	editSmbCredential
删除smb授权	credential	deleteSmbCredential
添加ssh授权	credential	saveSshCredential
编辑ssh授权	credential	editSshCredential
删除ssh授权	credential	deleteSshCredential
添加租户委托	tenant	addTenantAgency

操作名称	资源类型	事件名称
删除租户委托	tenant	deleteTenantAgency
清空资源	cleanup	resourcesCleanUp
忽略漏洞	vuln	addVulnFalsePositive
取消忽略漏洞	vuln	deleteVulnFalsePositive
生成主机扫描报告	report	generateHostScanReport
下载主机扫描报告	report	downloadHostScanReport

11 权限管理

11.1 创建用户并授权使用漏洞管理服务

如果您需要对您所拥有的漏洞管理服务进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用漏洞管理服务资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将漏洞管理服务资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

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，您可以跳过本章节，不影响您使用漏洞管理服务的其它功能。

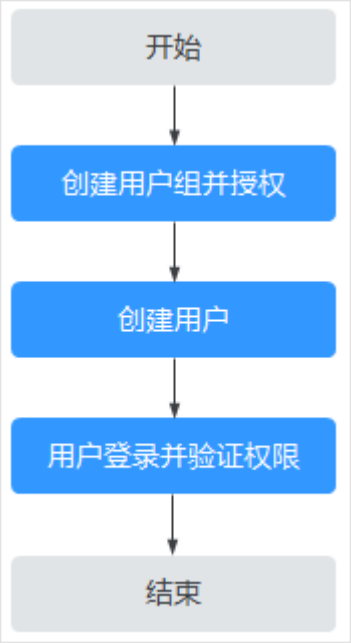
本章节为您介绍对用户授权的方法，操作流程如**图11-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的漏洞管理服务权限，并结合实际需求进行选择，漏洞管理服务支持的系统权限，请参见：**漏洞管理服务系统权限**。若您需要对除漏洞管理服务之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 11-1 给用户授权服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予漏洞管理服务权限“VSS Administrator”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   在“服务列表”中选择除漏洞管理服务外（假设当前策略仅包含“VSS Administrator”）的任一服务，若提示权限不足，表示“VSS Administrator”已生效。