漏洞管理服务

常见问题

文档版本	01
发布日期	2024-10-24

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 产品咨询类

1.1 什么是区域和可用区?

什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图1-1阐明了区域和可用区之间的关系。

图 1-1 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。

  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

1.2 漏洞管理服务的扫描 IP 有哪些?

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：

119.3.232.114，119.3.237.223，124.70.102.147，121.36.13.144，124.70.109.117，139.9.114.20，119.3.176.1，121.37.207.185，116.205.135.49，110.41.36.44，139.9.57.171，139.9.1.44，121.37.200.40

说明

漏洞管理服务会模拟客户端使用随机端口连接被测试设备，建议放通来自漏洞管理服务这些ip的全量端口。

1.3 漏洞管理服务可以免费使用吗?

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。

基础版配额内提供的网站漏洞管理服务（域名个数：5个，扫描次数：每日5次）是免费的。

1.4 扫描任务有哪些状态?

扫描任务的状态如表1-1所示。

表 1-1 扫描任务状态

状态	含义
已完成	任务扫描完成。
进行中	任务正在进行扫描。
排队中	任务正在等待执行。 **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“排队中”。
已失败	任务扫描失败。
未扫描	任务还未执行扫描。
已取消	任务被取消。 **说明** 任务在“进行中”或“排队中”才可以被取消。

任务可能经历的状态历程。

- 排队中→进行中→已完成
- 排队中→已取消
- 排队中→进行中→已取消

1.5 漏洞管理服务到期后还能继续使用吗?

漏洞管理服务到期后，可以继续使用基础版的所有功能。

1.6 扫描任务的得分是如何计算的?

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：

- 高危漏洞，一个扣10分，最多扣60分（6个）。
- 中危漏洞， 一个扣3分，最多扣45分（15个）。
- 低危漏洞， 一个扣1分，最多扣30分（30个）。
- 无漏洞或提示漏洞不扣分。
- 扫描分数最低为10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。

1.7 按需计费扫描失败怎么办?

用户选择“按需计费”的方式，在进行扫描时，如果扫描任务失败，不会扣费。

在解决失败问题后，如配置网站WAF白名单、修改扫描配置等，用户可以重新发起按需扫描，扫描成功后才会扣费。

1.8 为什么购买漏洞管理服务失败了?

购买失败，可能是权限不足，请检查用户权限。

用户需要拥有te_admin、bss_adm、bss_pay或bss_ops权限才能购买漏洞管理服务。如需开通该权限，请联系拥有Tenant Administrator权限的用户，开通权限，详细内容请参见《 统一身份认证服务用户指南 》。

1.9 漏洞管理服务能修复扫描出来的漏洞吗?

漏洞管理服务不能修复扫描出来的漏洞。

漏洞管理服务是一款漏洞扫描工具，能为您发现您的资产存在的漏洞，不能进行资产漏洞修复，但漏洞管理服务会为您提供详细的扫描结果以及修复建议，请您自行选择修复方法进行修复。

1.10 漏洞管理服务和传统的漏洞扫描器有什么区别?

漏洞管理服务和传统的漏洞扫描器的区别如**表1-2**所示。

表 1-2 漏洞管理服务和传统的漏洞扫描器的区别

对比项	传统的漏洞扫描器	漏洞管理服务
使用方法	使用前需要安装客户端。	不需要安装客户端，在管理控制台创建任务（输入域名或IP地址）就可以进行漏洞扫描，节约运维成本。
更新漏洞库方式	手动更新漏洞库，更新不及时。	云端同步更新漏洞库，涵盖最新漏洞，可以及时检测用户的网站是否有最新爆发的漏洞威胁。

1.11 漏洞管理服务支持扫描哪些漏洞?

漏洞管理服务支持扫描的漏洞有：

- 弱口令检测
  SSH、Telnet、FTP、MySQL、PostgreSQL、Redis、SMB、WinRM、Mongo、MSSQL Server、Memcached、SFTP。
- 前端漏洞
  SQL注入、XSS、CSRF、URL跳转等。
- 信息泄露
  端口暴露，目录遍历，备份文件，不安全文件，不安全HTTP方法，不安全端口。
- Web注入漏洞
  命令注入，代码注入，XPATH注入，SSRF注入，反序列化等注入漏洞。
- 文件包含漏洞
  任意文件读取、任意文件包含、任意文件上传、XXE。

1.12 如何查看漏洞修复建议?

网站扫描查看漏洞修复建议的方法。

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 在“资产列表 > 网站”页签，进入网站列表入口。

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 选择“漏洞列表”页签，查看漏洞信息，如图1-2所示。

图 1-2 漏洞列表

步骤6 单击漏洞名称，查看相应漏洞的“漏洞详情”、“漏洞简介”、“修复建议”，如图1-3所示，用户可以根据修复建议修复漏洞。

图 1-3 网站漏洞详情

----结束

1.13 漏洞管理服务可以跨区域使用吗?

漏洞管理服务是全局服务，不区分区域（Region），因此可以跨区域使用。

1.14 漏洞管理服务支持跨云扫描吗?

漏洞管理服务支持跨云扫描。

漏洞管理服务是通过公网访问域名/IP地址进行扫描的，只要确保该目标域名/IP地址能通过公网正常访问，就可以进行跨云扫描。

1.15 漏洞管理服务支持多个账号共享使用吗?

漏洞管理服务支持多个账号或多个IAM用户共享使用，说明如下：

- 多个账号共享使用

  例如，您通过注册华为云创建了2个账号（“domain1”和“domain2”），如果您将“domain1”的权限委托给“domain2”，则“domain2”可以使用“domain1”的漏洞管理服务。

  有关委托管理的详细操作，请参见**创建委托**。

- 多个IAM用户共享使用

  例如，您通过注册华为云创建了1个账号（“domain1”），且由“domain1”账号在IAM中创建了2个IAM用户（“sub-user1a”和“sub-user1b”），如果您授

权了“sub-user1b”用户漏洞管理服务的权限策略，则“sub-user1b”用户可以使用“sub-user1a”用户的漏洞管理服务。

有关漏洞管理服务权限管理的详细操作，请参见**创建用户并授权使用漏洞管理服务**。

1.16 单次扫描是否提供扫描报告和修复建议?

基础版漏洞管理服务提供以下单次扫描功能：将扫描任务升级为专业版规格进行扫描。扫描开始后进行一次性扣费。

单次扫描成功后，您可以查看修复建议并下载扫描报告。

- 有关查看修复建议的详细操作，请参见**如何查看漏洞修复建议?** 。
- 有关下载扫描报告的详细操作，请参见**如何下载网站扫描报告?** 。

1.17 漏洞管理服务可以对网站文字和图片改变进行检测吗?

漏洞管理服务支持对网页的内容合规进行检测，不支持对网站文字和图片改变进行检测。

1.18 使用漏洞管理服务前需要备份数据吗?

使用漏洞管理服务前不需要备份数据。

漏洞管理服务是无侵入式的服务，所以不需要备份数据。

1.19 漏洞管理服务如何判定 SQL 注入风险?

对于存在运算或判断等表达式的请求，当扫描结果与原请求相似度大于90%时，漏洞管理服务就会判定存在SQL注入风险。

1.20 漏洞管理服务支持扫描 SQL 注入吗?

漏洞管理服务支持扫描前端漏洞（SQL注入、XSS、CSRF、URL跳转等）。

1.21 Apache Log4j2 漏洞检测相关问题

1. 网站漏洞扫描和主机扫描是否支持Apache Log4j2漏洞检测？检测原理有何不同?

   答：网站漏洞扫描和主机扫描支持Apache Log4j2漏洞检测，但检测原理不同。网站漏洞扫描的检测原理是基于漏洞POC验证，如果没有攻击入口或路径，或已经开启了Web应用防火墙等防护措施，则无法扫出来；主机扫描的检测原理是登录操作系统之后探测JAR包版本，匹配是否在受影响的版本范围之内，相对高效。

   建议有条件的话，使用网站漏洞扫描和主机扫描远程扫描，若发现问题请尽快按**处置办法**进行操作。

2. Apache Log4j2漏洞之前能扫出来，后来扫不出来，不稳定是什么原因?

   答：只要扫出来过Apache Log4j2漏洞，建议马上排查相应网站或主机，尽快按**处置办法**进行操作。

后面扫不出来的原因，可能是网站已修复，或已通过Web应用防火墙等防护措施解决，另外由于该漏洞POC验证相对复杂，涉及较多网络交互，网络环境因素如安全组策略加固等变动，也可能导致漏洞不能稳定扫出来，但建议客户还是尽快排查处置，彻底规避风险。

3. 哪些版本支持Apache Log4j2漏洞检测?

   答：当前包括基础版（可免费开通）在内的所有版本均支持，但由于基础版规格有较多限制，如不支持主机漏洞扫描、Web漏洞扫描的扫描时长和次数受限，可能存在扫描不全面的问题。建议有条件的话，根据业务需求购买专业版及以上版本进行全面扫描。

   不同版本规格说明请参见**服务版本**。

1.22 漏洞管理服务与 HSS、WAF 有什么区别?

漏洞管理服务支持主机和Web漏洞扫描，从攻击者的视角扫描漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。HSS是提升主机整体安全性的服务，通过安装在主机上的Agent守护主机安全，全面识别并管理主机中的信息资产。漏洞管理服务中的主机漏扫和HSS的区别如下：

- 漏洞管理服务功能：远程漏洞扫描工具，不用部署在主机上，包括Web漏洞扫描、操作系统漏洞扫描、资产及内容合规检测、安全配置基线检查。从类似黑盒的外部视角，对目标主机网站等进行扫描，发现暴露在外的安全风险。
- HSS功能：终端主机安全防护工具，部署在主机上，包括资产管理、漏洞管理、基线检查、入侵检测、程序运行认证、文件完整性校验、安全运营、网页防篡改等功能，注重的是运行在主机上的业务的安全防护。

WAF是对网站业务流量进行多维度检测和防护，降低数据被篡改、失窃的风险。

华为云提供的漏洞管理服务、HSS服务、WAF服务，帮助您全面从网站、主机、Web应用等层面防御风险和威胁，提升系统安全指数。建议三个服务搭配使用。

表 1-3 漏洞管理服务、HSS、WAF 的区别

服务名称	所属分类	防护对象	功能差异
漏洞管理服务（CodeArts Inspector）	应用安全、主机安全	提升网站、主机整体安全性。	• 多元漏洞检测 • 网页内容检测 • 网站健康检测 • 基线合规检测 • 主机漏洞扫描
企业主机安全（HSS）	主机安全	提升主机整体安全性。	• 资产管理 • 漏洞管理 • 入侵检测 • 基线检查 • 网页防篡改

服务名称	所属分类	防护对象	功能差异
Web应用防火墙（WAF）	应用安全	保护Web应用程序的可用性、安全性。	• Web基础防护 • CC攻击防护 • 精准访问防护

1.23 漏洞扫描时会影响现有运行服务吗?

漏洞扫描是无侵入式的服务，不会对现有运行的服务产生影响。

1.24 漏洞管理服务的漏洞库是基于什么的?

主机扫描的漏洞库信息主要基于操作系统厂商公开发布的安全公告，二进制扫描的漏洞库主要是基于NVD漏洞库。

1.25 漏洞管理服务从哪些漏洞源获得已知漏洞信息?

漏洞管理服务的已知漏洞信息来源主要为各操作系统厂商的安全公告、NVD公开漏洞库等。漏洞信息来源及修复建议中可能会包含一些公网域名，主要提供用户漏洞的官方参考链接，便于用户参考，具体如下所示：

en.wikipedia.org、wiki.debian.org、lkml.iu.edu、www.huaweicloud.com、github.com、lists.apache.org、spring.io、oval.mitre.org、usn.ubuntu.com、ubuntu.com、lists.suse.com、bugzilla.suse.com、www.suse.com、lists.centos.org、access.redhat.com、bugzilla.redhat.com、lists.debian.org、salsa.debian.org、security-tracker.debian.org、bugs.debian.org、packages.debian.org、developer.huaweicloud.com、api.msrc.microsoft.com、support.microsoft.com、portal.msrc.microsoft.com、lists.fedoraproject.org、bodhi.fedoraproject.org、www.kylinos.cn、repo.huaweicloud.com、src.uniontech.com、nvd.nist.gov、git.launchpad.net、people.ubuntu.com、cve.mitre.org、secdb.alpinelinux.org、cve.mitre.org、www.hweuleros.com等公网域名。

2 网站扫描类

2.1 使用“一键认证”有什么要求?

在选择“一键认证”方式对域名进行认证前，请您请确保待检测站点的服务器搭建在华为云的以下区域，且该服务器是您当前登录账号的资产：

- 华北-北京一
- 华北-北京四
- 华东-上海一
- 华东-上海二
- 华南-广州
- 华南-深圳
- 东北-大连
- 西南-贵阳一

图 2-1 一键认证方式

2.2 如何快速发现网站漏洞?

漏洞扫描的原理是，通过爬虫获取用户网站的URL列表，然后对列表中所有URL进行扫描。

如果用户需要快速扫描，可以在创建扫描任务时，“扫描策略”选择“极速策略”，如图2-2所示。

说明

扫描策略分为：极速策略、标准策略、深度策略。选择深度扫描可以更深层次的发现漏洞，建议您优先选择“深度策略”。

图 2-2 设置扫描模式

2.3 网站登录需要动态验证码，可以使用漏洞管理服务的自动登录功能吗?

如果网站登录需要动态验证码，可以使用漏洞管理服务的自动登录功能。

只需在网站登录设置页面**配置网站的Cookie值**。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?**

2.4 为什么扫描任务自动登录失败了?

漏洞管理服务在扫描过程中，会在用户提交的登录页面上查找登录输入框，以及登录按钮，登录成功后，还会在页面上识别退出登录的触发链接，避免登出。查找这些元素的成功率受影响于用户站点页面元素的复杂程度。

如果扫描任务自动登录失败，可能是因为您的网站需要登录才能访问，请检查您是否通过漏洞管理服务对您的网站进行了正确的网站登录信息配置，请参照以下操作步骤设置网站登录方式或者修改网站登录配置信息。

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 在“资产列表 > 网站”页签，进入网站列表入口。

步骤4 在目标网站的“操作”列，单击“编辑”，进入网站编辑页面，根据需要修改“网站登录设置”，如**图2-3**所示。

图 2-3 编辑页面

步骤5 单击“确认”。

----结束

2.5 创建网站扫描任务或重启任务不成功时如何处理?

请执行**添加网站**操作重新创建网站。

2.6 网站漏洞扫描一次需要多久?

网站漏洞扫描的时长，跟多种因素相关，包括网站规模（即自动爬取的页面数）、网站响应速度、页面复杂度、网络环境等，通常扫描时长为小时级别，最长不超过24小时。

测试环境下，200个页面的网站完成一次全量扫描耗时约1个小时，这里仅供参考，请以实际扫描时间为准。

另外扫描的过程中会向网站发送一定数量的检测请求，可能会导致网站的负载小幅度增大。

2.7 为什么任务扫描中途就自动取消了?

如果一个任务扫描到一半被系统自动取消了，可能有以下两个原因：

- 没有配置“网站登录设置”信息。

  用户没有配置“网站登录设置”信息，漏洞管理服务无法进行深入的访问，任务就会自动取消。 建议设置“网站登录设置”信息后，重新扫描。
- 扫描过程中，出现了网络问题。

  网络异常，漏洞管理服务将无法访问网站，任务就会自动取消。建议网络正常后，重新扫描。

2.8 如何设置定时扫描?

在创建任务时，设置“开始时间”，设置好启动时间后，系统会在用户设置的时间点启动该任务，如**图2-4**所示。

说明

启动时间必须在一周之内。

图 2-4 定时开始

2.9 域名认证完成后网站根目录下面的认证文件可以删除吗?

不可以。漏洞管理服务在后续扫描过程中会读取该文件，验证网站的所有权是否仍然有效。

如果认证文件被删除，当再次对该域名进行扫描时，会提示失败。

2.10 为什么执行下载认证文件操作后没有看到下载的认证文件?

文件认证功能已下线，请参考**添加网站**使用免认证或一键认证方式。

2.11 创建任务时为什么总是提示域名格式错误?

创建任务时，为了让漏洞管理服务识别出网站使用的协议（http或https），需要在输入的时候填写此信息。

正确的域名格式为：“http(s)://域名或IP”。

例如：一个使用https协议，IP地址为10.10.10.1的网站，在创建任务时应输入的“目标网址”为“https://10.10.10.1”。

2.12 认证文件有什么用途?

文件认证功能已下线，请参考**添加网站**使用免认证或一键认证方式。

2.13 为什么域名一键认证失败?

为什么要进行域名认证

华为云漏洞管理服务不同于一般的扫描工具，因为漏洞管理服务的扫描原理是基于自动化渗透测试（对被扫描的对象发送非恶意的“攻击报文”），因此需要确保用户扫描的网站的所有权是用户自己。

漏洞管理服务支持的认证方式

- “免认证”方式。
- 华为云租户“一键认证”。

华为云“一键认证”失败的原因

华为云一键认证的功能只针对两种用户：

- 使用了华为云WAF的用户。
- 客户要扫描的网址对应的EIP是华为云华北、华东、华南、东北局点的EIP。

因此认证失败可能有以下原因：

- 用户不是上述的两种用户。
- 用户是华为云WAF的用户，但该WAF和漏洞管理服务不在一个账户下，则认证会失败，因为只有购买WAF的账户才能查看WAF的回源IP。
- 用户要扫描的EIP不是在该账户下购买的，因为系统是根据该账户去查询用户已经购买的EIP，然后和输入的EIP进行比对，所以不在同一个账号下无法一键认证。
- 域名信息跟规范不符

  该类网站不能使用漏洞管理服务。

2.14 如何将认证文件上传到网站根目录?

文件认证功能已下线，请参考**添加网站**使用免认证或一键认证方式。

2.15 如何对网站进行认证?

请参考**添加网站**对网站进行认证。

2.16 如何解决漏洞管理服务中已添加网站的“网站地址”错误的问题?

开通漏洞管理服务后，首先您需要将网站资产以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。

将网站添加到漏洞管理服务时，您需要配置网站的地址信息。由于漏洞管理服务中不支持修改网站的地址信息，如果已添加的网站地址错误，须在漏洞管理服务“资产列表”中将已添加的网站删除，再重新添加并配置网站，操作步骤如下所示。

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 在“资产列表 > 网站”页签，单击操作列的“删除”，弹出确认删除提示框。

步骤4 单击“确认”，即可删除网站。

步骤5 删除网站后，请重新添加网站，详细操作请参见添加网站。

步骤6 添加网站完成后，您可创建扫描任务，使用漏洞管理服务扫描网站漏洞，详细操作请参见创建扫描任务。

----结束

2.17 如何解决网站扫描失败，报连接超时的问题?

网站扫描任务失败，报错为连接超时，可能原因与解决办法如下。

1. 您的被测网站不稳定或无法通过互联网访问，请使用Chrome等浏览器访问网站，确认是否正常访问。
2. 您的网站设置了防火墙或其他安全策略，导致漏洞扫描的引擎IP被当成恶意攻击而拦截。请参见**漏洞管理服务的扫描IP有哪些?** 为漏洞扫描引擎设置访问白名单。

2.18 漏洞管理服务支持 web_CMS 漏洞吗?

漏洞管理服务暂不支持web_CMS漏洞扫描功能。

2.19 标准策略、极速策略和深度策略有哪些区别?

漏洞管理服务提供支持以下3种网站扫描模式：

- “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。

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。

2.20 已添加的域名是否可以删除?

可以删除，但域名删除后，该资产的历史扫描数据将被删除，不可恢复。

2.21 如何查看漏洞管理服务扫描出的网站结构?

执行完漏洞扫描任务后，进入“总览”页面，在“最近扫描任务列表”中，单击目标扫描对象，进入任务详情页面，单击“站点结构”页签，查看网站结构。

说明

站点结构展示的是任务扫描出的漏洞对应的网页地址及整体结构，如果任务暂未扫描出漏洞，站点结构无数据显示。

图 2-5 查看站点结构

2.22 如何获取网站 cookie 值?

如果您的网站除了需要账号密码登录，还有其他的访问机制（例如，需要输入动态验证码），则建议您设置cookie登录方式进行网站漏洞扫描，以便漏洞管理服务能为您发现更多安全问题。

设置cookie登录方式时需要输入网站的cookie值。

须知

获取cookie值后，在创建扫描任务时，请您保持网站的登录状态，以免cookie失效。

手动获取网站 cookie 值

以Google Chrome浏览器为例说明，获取网站（例如，www.example.com）的cookie值的步骤如下：

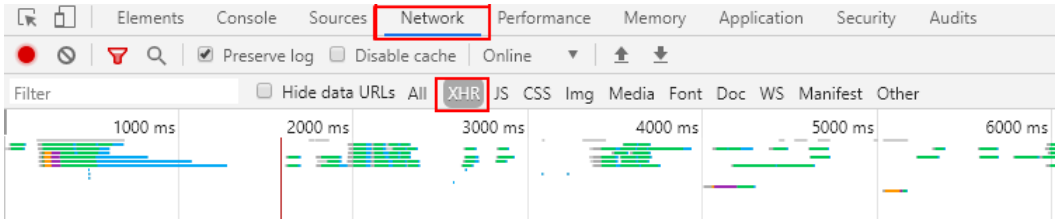
步骤1 打开Google Chrome浏览器。

步骤2 按“F12”，进入浏览器的开发者模式。

步骤3 在地址栏中输入目标网站地址“www.example.com”。

步骤4 在调试页面中，选择“Network > XHR”，如图2-6所示。

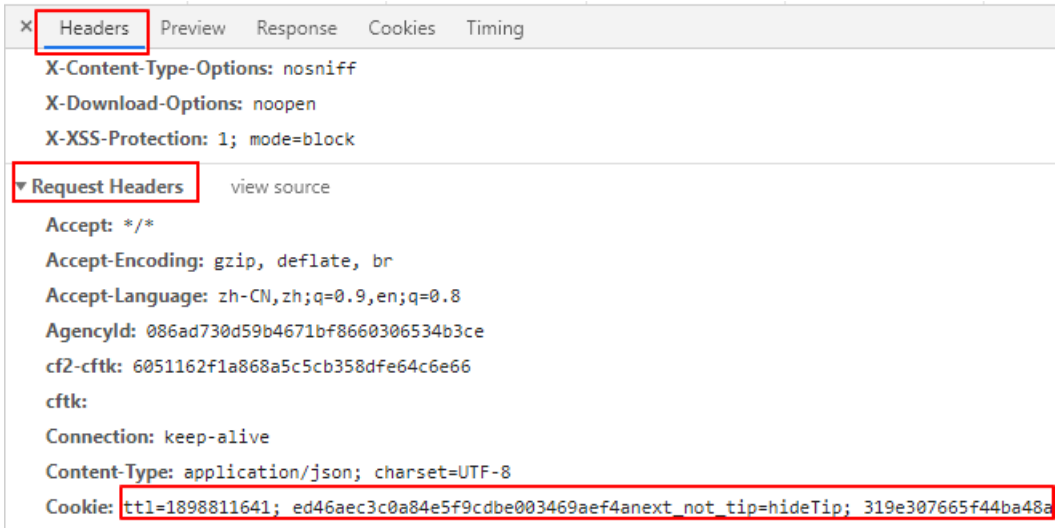
图 2-6 Network 页面



步骤5 在左侧导航树中，选择一个http请求。

步骤6 在“Headers”页面的“Request Headers”区域框，获取当前网站页面的“Cookie”字段值，如图2-7所示。

图 2-7 获取 cookie 值



----结束

使用浏览器插件获取网站 cookie 和 storage 值

如果您的网站登录之后不仅设置了cookie，还设置了storage，只提供cookie无法使漏洞管理服务正常登录网站，建议您通过浏览器插件获取网站cookie、local storage和session storage值，以Google Chrome浏览器为例，步骤如下：

步骤1 下载浏览器插件Cookie Getter并解压缩。

表 2-1 下载列表

支持浏览器	下载地址	SHA-256文件校验
Google Chrome、Microsoft Edge	Cookie Getter	7C35DC34F732B4B3F2B89C3B8ADAEE6ECE3079B991718AAB10B963F7D15B1468

步骤2 打开Google Chrome浏览器，单击“设置”，单击“扩展程序”，打开“开发者模式”开关。

步骤3 单击“加载已解压的扩展程序”，选择解压后的文件根目录，加载浏览器插件。

步骤4 打开并登录网站。

步骤5 单击扩展程序-浏览器插件Cookie Getter图标，获取浏览器插件展示的JSON格式cookie和storage值全文。

----结束

须知

- 漏洞管理服务的Cookie登录支持设置“以分号分隔的键值对”和“JSON”两种格式cookie值。
- 您可以按需裁剪或修改浏览器插件获取的数据，保持正确的JSON格式并提供必要的cookie和storage值即可。

2.23 网站 cookie 值发生变化时，如何进行网站漏洞扫描?

当某个网站挂载多个子网站，且需要对这些网站都进行漏洞扫描（使用cookie登录方式）时，如果您从网站主入口登录后，再进入其他子网站，网站的cookie值可能会发生改变。对于cookie值发生改变的子网站，您需要为这些子网站单独完成扫描任务的创建。

您也可采用共用cookie方式，来避免cookie值发生变化。被扫描站点的多个页面之间，是否会共用cookie，取决您的web站点是否支持此功能。

- 有关设置网站cookie登录方式的详细操作，请参见**网站登录设置**。
- 有关创建扫描任务的详细操作，请参见**创建扫描任务**。

2.24 如何处理域名认证时提示“域名已被其他人使用”？

对域名进行认证时，如果提示域名已被其他人使用，说明该域名已被其他账号进行认证。一般情况下，能够认证该域名的账号应隶属于您的单位，请咨询您的同事是否用了其他账号认证了该域名，或者您也可以提工单咨询域名认证情况。

2.25 漏洞管理服务可以扫描域名下的项目吗?

漏洞管理服务采用网页爬虫的方式全面深入地爬取网站url，然后针对爬取出来的页面模拟黑客进行试探攻击，帮助您发现网站潜在的安全隐患。如果域名下的项目没有被漏洞管理服务爬取出来，则该项目不会被漏洞管理服务扫描到。您可以通过网站扫描详情，查看域名下的项目是否被漏洞管理服务扫描到。

有关查看网站扫描详情的操作，请参见**查看网站扫描详情**。

2.26 如何扫描弱密码?

漏洞管理服务不支持对弱密码单独进行扫描。您可以通过查看网站扫描详情，了解弱密码的扫描情况。

有关查看网站扫描详情的操作，请参见**查看网站扫描详情**。

2.27 网站扫描是否可以加/web 访问?

可以。创建扫描任务页面，填写目标网址时可以加上网页路径。

例如：目标网址是“https://www.example.com”，扫描的网址加上具体的网页路径后“https://www.example.com/login.php”。

2.28 可以扫描产品上线前的局域网站点吗?

漏洞管理服务是通过公网扫描的，局域网内站点可以配置公网代理机，使其可通过公网访问。

2.29 可以在弱密码库中添加弱密码吗?

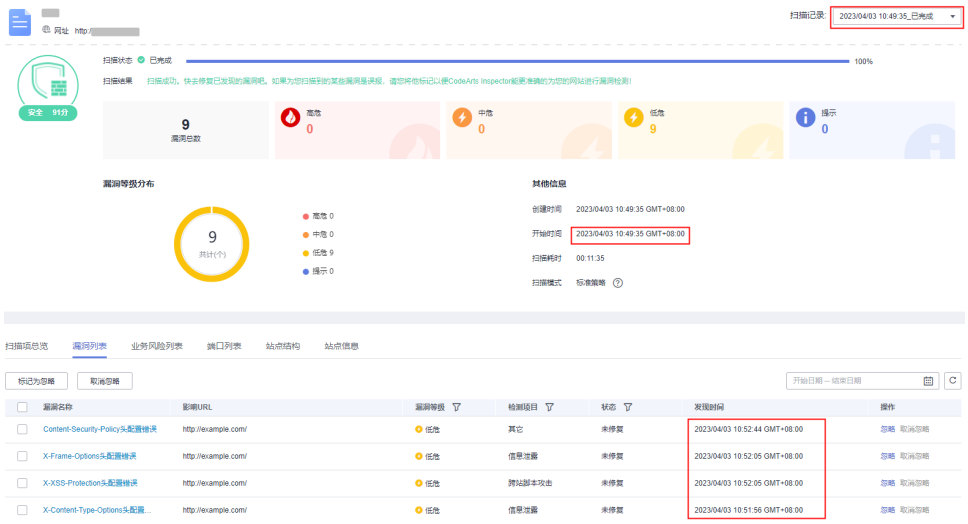
不可以在弱密码库中添加弱密码。

2.30 为什么漏洞发现时间早于扫描开始时间?

当漏洞管理服务扫描完成后，您没有及时处理发现的漏洞。若您再次开始扫描，扫描完成后，漏洞列表中会展示该漏洞，且发现时间为初次发现该漏洞的时间，如图2-8所示。

您可以在“历史扫描报告”下拉列表中，选择与该漏洞“发现时间”相同日期的扫描任务，并在该扫描任务的“漏洞列表”中查询到该漏洞。

图 2-8 漏洞列表



2.31 使用了 Web 应用防火墙，对网站扫描时 SSL/TLS 存在 bar mitzvah attack 漏洞?

使用了Web应用防火墙（WAF）对网站扫描时SSL/TLS存在bar mitzvah attack漏洞，需要设置TLS配置。

步骤1 登录Web应用防火墙控制台。

步骤2 进入网站设置页面入口。

步骤3 在目标网站所在行的“防护网站”列中，单击目标网站，进入网站基本信息页面。

步骤4 在“TLS配置”所在行，单击 修改TLS配置。

步骤5 选择“TLS v1.2”和“加密套件2”，加密算法为EECDH+AESGCM:EDH+AESGCM。

图 2-9 TLS 配置

步骤6 单击“确定”。

步骤7 重新对网站进行扫描即可正常。

----结束

2.32 专业版是否支持一级域名的扫描?

专业版限制一个二级域名扫描，兼容用户把一级域名当做二级域名来使用的场景，这时添加一级域名，配额仍然算作二级域名的，即不能再新加二级域名了。例如用户买了专业版一个配额，可以添加example.com一级域名进行扫描，也算作二级域名的配额，如果想添加www.example.com就必须增加购买配额了。

2.33 如何修复 TLS 弱加密套件?

基本概念

加密套件是TLS/SSL协议中的一个概念，是指服务器和客户端所使用的加密算法组合。在TLS握手阶段，客户端将自身支持的加密套件列表告诉服务器，服务器根据自己支持的所有套件中选择一个作为之后所使用的加密方式。这些算法包括**密钥交换算法**、**批量加密算法**和**消息认证码**（MAC）算法，组合起来有数百种不同的密码套件。这些密码套件中有的安全性较差，称为弱加密套件，例如：TLS_DHE_RSA_WITH_AES_128_GCM_SHA256。

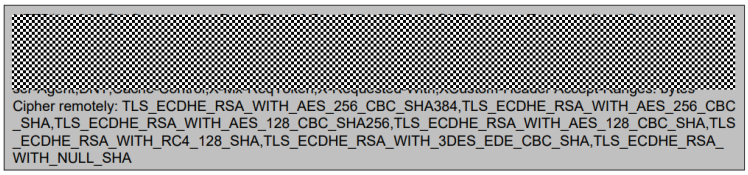
安全标准与兼容性

什么加密套件会被判定为弱加密套件，不同标准有着不同的判定方案，如PCI DSS的FS要求。不同厂商也会根据自身业务规定不同标准，如漏洞管理服务就参考了《华为密码算法应用规范》来判定弱加密套件。

业务需要根据自身实际情况来调整加密套件，例如某些业务（如**电商网站**）为了追求最大兼容性也会舍弃一定的安全性、**华为云WAF**也为不同用户提供了多套加密套件的组合。

修复

在 TLS/SSL配置项中去除漏洞管理服务扫描出的弱加密套件(详细请参见扫描报告漏洞信息“响应详情”中的内容)。



当用户判断弱加密套件为业务需要且风险可控时，则可忽略该漏洞。

配置修改方法

通常Web应用的TLS/SSL协议由Web容器配置（常见的Tomcat/Nginx/Apache），或者通过云服务供应商提供的服务配置（WAF/Https）。开发人员需要根据自身业务情况确认配置位置，并了解TLS/SSL相关配置项。常见的参考：

- **Apache Tomcat 8 (8.5.73) - SSL/TLS Configuration How-To**
- **SSL/TLS Strong Encryption: How-To - Apache HTTP Server Version 2.4**
- **Nginx Configuring HTTPS servers**

也可以参考**Mozilla SSL Configuration Generator**自动生成的TLS/SSL配置来修改。

修复验证

用户可以自行通过在线检测网站或开源工具验证（搜索引擎搜索SSL检测）。

2.34 为什么漏洞管理服务多次扫描结果不一致?

动态扫描（DAST）的结果由多种因素决定，多次扫描结果可能存在不一致的情况，如某类漏洞的数量存在差异，在扫描结果相差不大的情况下，结合多份扫描结果的内容进行分析，关注漏洞是否存在即可。

下面将解释扫描结果不一致的原因。

漏洞管理服务工作机制

漏洞管理服务从客户端的角度，模拟黑客向测试目标发起攻击，根据网站的响应（内容、时间等信息）来判断是否存在漏洞。

- 根据登录信息登录测试目标

- 主动爬虫爬取相关目标
- 发送攻击报文进行测试
- 根据响应内容判断漏洞存在

影响因素

结合漏洞管理服务工作机制，我们可以得出影响扫描结果的以下几个关键因素，这些因素在多次扫描中的差异，会最终导致多次扫描结果的不一致。

- **会话维持**

  如果登录信息存在问题，漏洞管理服务将无法登录进目标系统，只能进行测试目标外围的信息探测，从而影响扫描结果。常见的可能原因有：

  - 用户名密码被更改
  - Cookie/Token 等信息失效，结合业务本身的Cookie/Token等会话机制判断
  - 业务自身的会话机制
    - 多因子认证：验证码、短信等等。
    - 异地登录限制。
    - 登录频率限制。
    - 异常请求等强制中断会话。
    - 单用户登录（不允许多个客户端同时登录）。
    - 登录失败次数限制。
- **扫描范围**

  漏洞管理服务主动爬虫会通过自动填充form表单等策略来尝试发现更多页面。

  业务对随机值响应不一致导致了扫描范围不一致。
- **响应信息**

  响应信息是漏洞管理服务判断漏洞是否存在的决定性因素。网络状况、动态内容、WAF机制、测试目标本身稳定性都会影响漏洞的判定，常见的可能原因有：

  - 网络状况
    - 网络链接本身：网络延迟、网络波动。
    - 业务策略：访问过快、攻击报文、异常报文等直接将客户端加入黑名单。
    - 业务稳定性：在大量请求下的稳定性（响应时间）。
  - 业务逻辑
    - 响应内容不一致
      - 攻击报文中存在大量异常、随机值，业务对不同内容响应不同。
      - 对不同客户端（ip/user-agent/...）响应不同。
    - 响应时间不一致

      攻击报文中存在大量异常、随机值，业务处理方式不一致，耗时不同。

- WAF机制
  - 限制访问频率
  - 限制攻击来源访问

2.35 新网站资产管理方式会存在什么影响?

背景

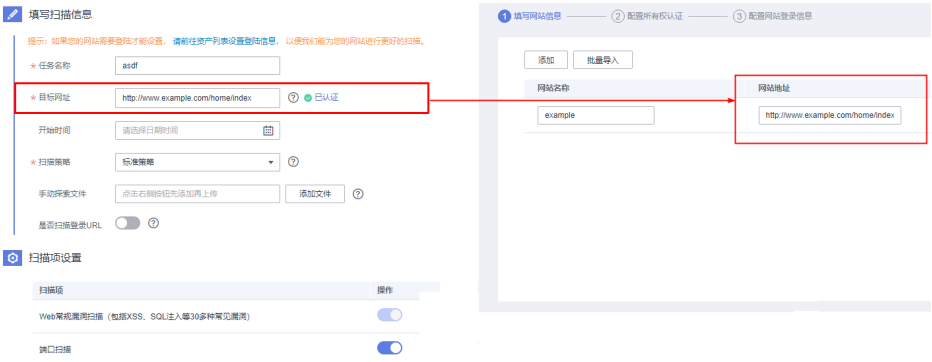
2023年8月1日后，漏洞管理服务Web扫描的资产管理方式由域名管理扩展至网站管理。

影响

- 扫描任务操作逻辑变化。

  之前“创建任务”界面的“目标网址”中填写的网站URL，直接在新界面的“网站地址”处填写即可。

  图 2-10 填写网站地址

- 历史任务处理。

  对于已存在的历史任务，有两种方式进行扫描。

  a. 在“查看报告”界面，单击“重新扫描”，对上一次扫描的网站重新进行扫描。

  图 2-11 重新扫描历史任务

  b. 通过“新建网站”资产，指定具体网站URL。

  假如历史任务的目标网址为：http://www.example.com/home/index，则新建网站时，“网址地址”与该历史任务的目标网址保持一致。

图 2-12 网站地址

新增网站的具体操作请参考**添加网站**。

3 主机扫描类

3.1 漏洞管理服务的主机扫描 IP 有哪些?

如果设置了访问限制，请添加策略允许漏洞管理服务的IP地址可以访问您的主机。如果您使用了主机安全防护软件，请将漏洞管理服务访问主机的IP地址添加到该软件的白名单中，以免该软件拦截了漏洞管理服务访问用户主机的IP地址。

119.3.232.114，119.3.237.223，124.70.102.147，121.36.13.144，124.70.109.117，139.9.114.20，119.3.176.1，121.37.207.185，116.205.135.49，110.41.36.44，139.9.57.171，139.9.1.44，121.37.200.40

3.2 漏洞管理服务的弱口令检测，支持的常见协议、中间件有哪些?

漏洞管理服务的弱口令检测功能支持的常见协议、中间件如下：

SSH、Telnet、FTP、SFTP、Mysql、MariaDB、PostgreSQL、Redis、SMB、WinRM、MongoDB、Memcached、SqlServer

3.3 为什么主机添加成功后不能在主机列表中查找到?

由于漏洞管理服务系统处理任务需要一段时间，因此主机添加成功后您不能在主机列表中马上查找到该添加的主机。请您等待一段时间，刷新主机列表再查找添加的主机。

3.4 主机扫描支持哪些区域?

目前，主机扫描支持所有区域，公网可达。

3.5 如何对 Linux 主机进行授权?

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，如何授权请参照**编辑Linux主机授权**。

3.6 如何对 Windows 主机进行授权?

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主机进行扫描授权。如何授权请参照**编辑Windows主机授权**。

Windows主机漏洞扫描依赖于winrm服务开启，如何开启请参照**如何开启WinRM服务?** 。

3.7 为什么在扫描时会提示授权委托失败?

授权委托失败可以根据以下方法进行排查与解决。

- 使用子账号进行扫描

  如果您登录华为云使用的是子账号，请确保该子账号所在的用户组拥有Agent Operator和Security Administrator这两个权限，否则扫描时会提示委托授权失败。

- 使用企业账号（主账号进行扫描）（推荐）

  如果用户使用的是主账号扫描还是提示委托失败，可能是因为委托数量到达了上限。

  查询委托数量是否达到上限：

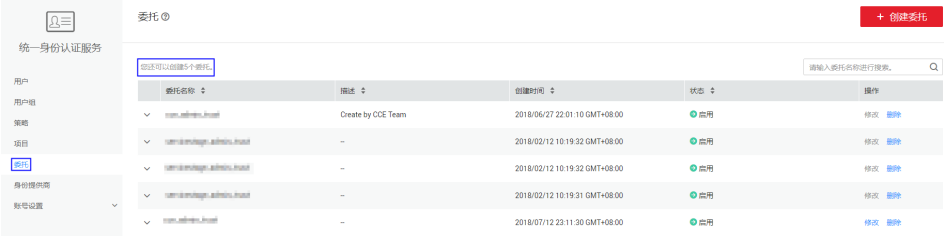
  a. 将鼠标移动至用户名，单击“统一身份认证”，如**图3-1**所示，进入“用户”页面。

  图 3-1 统一身份认证

  b. 单击“委托”，进入“委托”页面查看委托数量，如**图3-2**所示，最多可委托10个。

图 3-2 委托数量



3.8 如何解决主机不能访问?

可能原因

在使用主机扫描时会显示扫描失败，无法访问您的主机，可能有如下两个原因。

1. 网络故障。
2. 开启了主机安全防护软件。

解决方法

1. 如果是网络故障的原因导致主机不能访问，请在网络恢复后重新进行主机扫描。
2. 如果是因为开启了主机安全防护软件导致主机不能访问，则区分如下两种情况：
   - 如果未使用主机安全防护软件的“SSH登录IP白名单”功能，则请参考**如何手动解除误拦截IP?**，先检查IP是否被拦截，若已被拦截需要解除误拦截IP再重新进行主机扫描。若没有被拦截则请联系华为云技术支持工程师处理。

     该操作仅指导购买并开启了华为云企业主机安全（HSS）的客户。
   - 如果使用了主机安全防护软件的“SSH登录IP白名单”功能，则请参考**开启了主机安全（HSS）如何配置SSH登录IP白名单**将如下这些漏洞管理服务的扫描IP添加至主机访问的白名单中，再重新进行主机扫描。

     119.3.232.114，119.3.237.223，124.70.102.147，121.36.13.144，124.70.109.117，139.9.114.20，119.3.176.1，121.37.207.185，116.205.135.49，110.41.36.44，139.9.57.171，139.9.1.44，121.37.200.40

开启了主机安全（HSS）如何配置 SSH 登录 IP 白名单

须知

- 该示例仅指导购买并开启了华为云企业主机安全（HSS）且未配置过白名单的客户，如何将漏洞管理服务扫描IP添加至白名单。
- 如果您使用的是其他主机安全防护产品，请自行添加。
- 使用鲲鹏计算EulerOS（EulerOS with ARM）和Centos 8.0及以上版本的主机，SSH登录IP白名单功能对其不生效。
- 配置了SSH登录IP白名单的服务器，只允许白名单内的IP通过SSH登录，启用该功能时请确保将所有需要发起SSH登录的IP地址都加入白名单中。

步骤1 登录**企业主机安全控制台**，参考**图3-3**，单击“添加白名单IP”。

图 3-3 添加白名单 IP

步骤2 在配置框中输入白名单IP，在“可选云服务器”列表中选择云服务器，如图3-4所示：

图 3-4 添加 SSH 登录 IP 白名单

----结束

3.9 主机扫描为什么会扫描失败?

主机扫描失败的主要原因有主机未进行授权、主机不可达，请参考以下方法排查您的主机扫描失败的原因并解决问题。

- 排查主机是否完成了授权，如果未授权，请参见**如何对主机进行授权**完成主机授权。
- 排查主机是否能正常访问，主机不能访问可能有以下几个原因：
  - 主机所在的安全组或网络ACL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。
  - 主机IP被当成不信任IP被**主机安全服务**拦截，请参见**解除拦截受信任的IP**解除主机IP封禁，并参见**配置SSH登录IP白名单**将您的主机IP配置为白名单。
  - 使用了nat绑定主机进行扫描，建议您使用跳板机以及绑定公网的扫描方式进行主机扫描，具体操作请参见**如何配置跳板机进行内网扫描?** 。
  - 主机IP被加入了CFW防护阻断策略或黑名单，访问被阻断，导致漏洞管理服务节点访问失败。您需要执行**添加防护规则**或**添加白名单**放行被阻断的IP，添加白名单时，“端口”是指源端口，“协议类型”选择“Any”。

3.10 主机扫描支持非华为云主机吗?

主机扫描支持非华为云主机。

目前支持linux主机和Windows主机。

3.11 漏洞管理服务支持哪些操作系统的主机扫描?

漏洞管理服务支持扫描的主机操作系统版本如下：

支持的Linux操作系统版本，如**表3-1**所示。

支持的Windows操作系统版本，如**表3-2**所示。

表 3-1 Linux 操作系统版本

分类	支持的OS类型
EulerOS	EulerOS 2.2, 2.3, 2.5, 2.8 and 2.9 64bit
CentOS	CentOS 6.10, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, and 8.2 64 bit **说明** CentOS 8基于RedHat 8公开的补丁信息做检查。
RedHat	Red Hat Enterprise Linux 6.10, 7.5, and 8 64bit
Ubuntu	Ubuntu 16.04, 18.04, 20.04, and 22.04 server 64bit
SUSE	SUSE Enterprise 11 SP4 64bit, SUSE Enterprise 12 SP1/SP2/SP3/SP4 64bit, SUSE Enterprise 15 SP1/SP2 64bit

分类	支持的OS类型
OpenSUSE	OpenSUSE 13.2 and 42.2 64bit
Debian	Debian 8.2.0, 8.8.0, 9.0.0, 10.0.0, and 11.1.0 64bit
Kylin OS	Kylin OS V10 SP1 64bit
统信UOS	V20
Huawei Cloud EulerOS	HCE 2.0
openEuler	openEuler 20.03
AlmaLinux	AlmaLinux 8/9
Rocky Linux	Rocky Linux 8/9

表 3-2 Windows 操作系统版本

分类	支持的Windows系统版本
Windows Server	Windows Server 2012 R2，Windows Server 2016，Windows Server 2019

3.12 如何修复扫描出来的主机漏洞?

不同的主机系统修复漏洞的方法有所不同，软件漏洞的修复需要具有一定专业知识的人员进行操作，根据服务器的情况进行漏洞修复，可参考漏洞管理服务给出的修复建议，修复漏洞时应按照如下的操作步骤进行修复。

步骤1 对需要修复的服务器实例进行备份，防止出现不可预料的后果。

步骤2 对需要修复的资产和漏洞进行多次确认。根据业务情况以及服务器的使用情况等综合因素，确认自己的资产是否需要做漏洞修复，并形成漏洞修复列表。

步骤3 在模拟测试环境中部署待修复漏洞的相关补丁，从兼容性和安全性方面进行测试，并输出补丁漏洞修复测试报告，报告内容应包含补丁漏洞修复情况、漏洞修复的时长、补丁本身的兼容性、以及漏洞修复可能造成的影响。

步骤4 进行漏洞修复时，最好多人在场，边操作边记录，防止出现误操作。

步骤5 漏洞修复完成后，在测试环境对目标服务器系统上的漏洞进行修复验证，确保服务器没有异常，输出详细的修复记录进行归档，方便日后遇见相关问题可快速反应。

----结束

总之，为了防止在漏洞修复过程中出现问题，在漏洞修复前要及时备份、制定方案、在测试环境进行模拟测试验证可行性，在修复过程中要小心并及时记录，在修复后及时生成完备的修复报告进行归档。

如果以上方案仍未能解决您的问题，建议您使用华为云“管理检测与响应”的安全加固功能，一站式完成漏洞修复。

3.13 漏洞管理服务可以扫描本地的物理服务器吗?

漏洞管理服务可以扫描本地的物理服务器。若需要扫描本地的物理服务器，需要满足以下条件。

- 本地网络可通外网。
- 本地物理服务器为Linux操作系统，且满足以下版本要求：
  - EulerOS：支持的最低系统版本为EulerOS 2.2。
  - CentOS：支持的最低系统版本为CentOS 6.5。
  - RedHat：支持的最低系统版本为Red Hat Enterprise Linux 6.10。
  - Ubuntu：支持的最低系统版本为Ubuntu 16.04 server。
  - SUSE：支持的最低系统版本为SUSE Enterprise 11 SP4。
  - OpenSUSE：支持的最低系统版本为OpenSUSE 13.2。
  - Debian：支持的最低系统版本为Debian 8.2.0。
  - Kylin OS：支持的系统版本为Kylin OS V10 SP1。
  - 统信UOS：支持的系统版本为统信UOS V20。
  - Huawei Cloud EulerOS：支持的系统版本为HCE 2.0。
  - openEuler：支持的系统版本为openEuler 20.03。
- 可以远程登录到本地物理服务器。

本地物理服务器满足以上条件后，可以在漏洞管理服务界面通过添加跳板机的方式，使用漏洞管理服务扫描本地的物理服务器。

有关物理服务器使用漏洞管理服务的详细介绍，请参见**物理服务器可以使用漏洞管理服务吗?** 。

3.14 物理服务器可以使用漏洞管理服务吗?

当您的物理服务器为Linux操作系统，且满足以下版本要求时，如果您的物理服务器可以远程登录，则可以通过**添加跳板机**的方式使用漏洞管理服务。

- EulerOS：支持的最低系统版本为EulerOS 2.2。
- CentOS：支持的最低系统版本为CentOS 6.5。
- RedHat：支持的最低系统版本为Red Hat Enterprise Linux 6.10。
- Ubuntu：支持的最低系统版本为Ubuntu 16.04 server。
- SUSE：支持的最低系统版本为SUSE Enterprise 11 SP4。
- OpenSUSE：支持的最低系统版本为OpenSUSE 13.2。
- Debian：支持的最低系统版本为Debian 8.2.0。
- Kylin OS：支持的系统版本为Kylin OS V10 SP1。
- 统信UOS：支持的系统版本为统信UOS V20。
- Huawei Cloud EulerOS：支持的系统版本为HCE 2.0。
- openEuler：支持的系统版本为openEuler 20.03。

3.15 如何创建 SSH 授权?

Linux主机支持“SSH授权登录”授权方式。

添加Linux主机后，请参照**编辑Linux主机授权**中的操作步骤创建SSH授权。

3.16 配置主机授权时，必须使用加密密钥吗?

在创建SSH授权登录（Linux主机）时，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。

有关配置主机授权的详细操作，请参见**如何对Linux主机进行授权?** 。

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

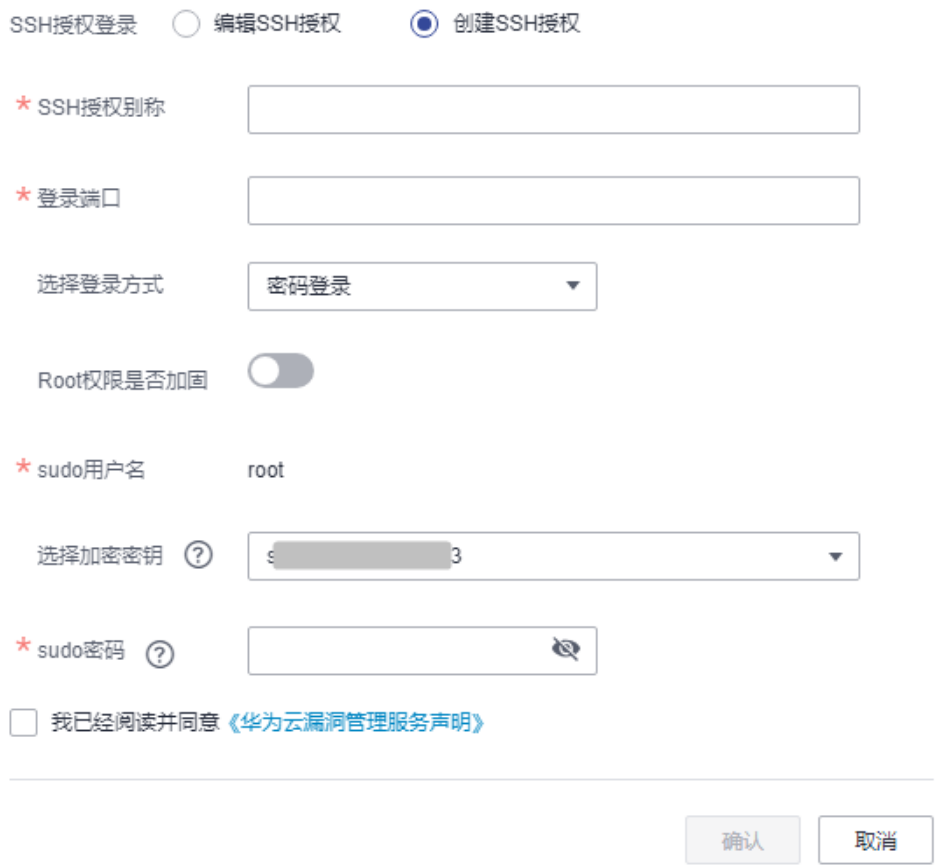
  有关创建密钥的详细操作，请参见**创建密钥**。
- 使用数据加密服务需要单独计费，详细的服务资费和费率标准，请参见**价格详情**。

3.17 创建 SSH 授权时，如何设置登录端口?

在为Linux主机创建SSH授权登录时，需要设置登录端口，如**图3-5**所示。

在设置登录端口时，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。

图 3-5 设置登录端口



3.18 如何扫描修改了 IP 地址的主机?

如果您的主机已在本地配置了账号和密码，当您修改该主机的IP地址后，请先在本地重新配置该主机的账号和密码，然后在漏洞管理服务中添加该主机并授权漏洞管理服务可以访问该主机。

有关对主机进行授权的详细操作，请参见**如何对Linux主机进行授权?** 。

3.19 对主机扫描出的漏洞执行“忽略”操作有什么影响?

在扫描详情页面中，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。后续执行扫描任务会扫描出该漏洞，但相应的漏洞统计结果将发生变化，扫描报告中也不会出现该漏洞。

3.20 主机扫描可以关闭基线检查吗?

主机扫描不能关闭基线检查。

如果您确认基线检查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，相应的检查项统计结果将发生变化，扫描报告中也不会出现该检查项。

3.21 基线检查的风险个数是如何统计的?

基线检查结果中“未通过”的检查项的总数即为基线检查的风险个数。

3.22 等保合规的检查项可以忽略吗?

可以。

- 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，后续执行扫描任务会扫描出该漏洞，但相应的检查项统计结果将发生变化，扫描报告中也不会出现该检查项。
- 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。

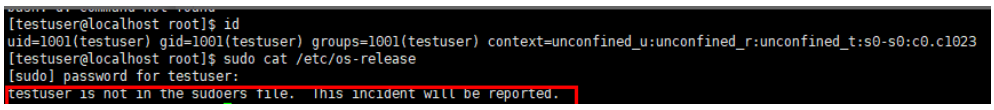
3.23 基线检查总数与检查项数不一致，为什么?

漏洞管理服务目前仅支持扫描一个tomcat进程，当目标主机有多个tomcat进程时，基线检查的总扫描数与检查项显示的个数不一致。

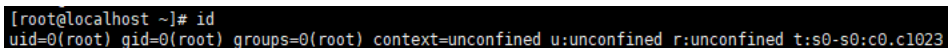
请您保留一个tomcat进程后，重新对该目标主机进行扫描。

3.24 配置普通用户和 sudo 提权用户漏洞扫描操作案例

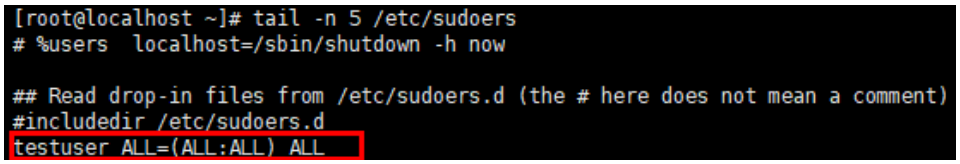
默认情况下，Linux系统没有将普通用户列入到sudoer列表中（普通用户 is not in the sudoers file. This incident will be reported.）:



1. 登录系统并切换到root权限。

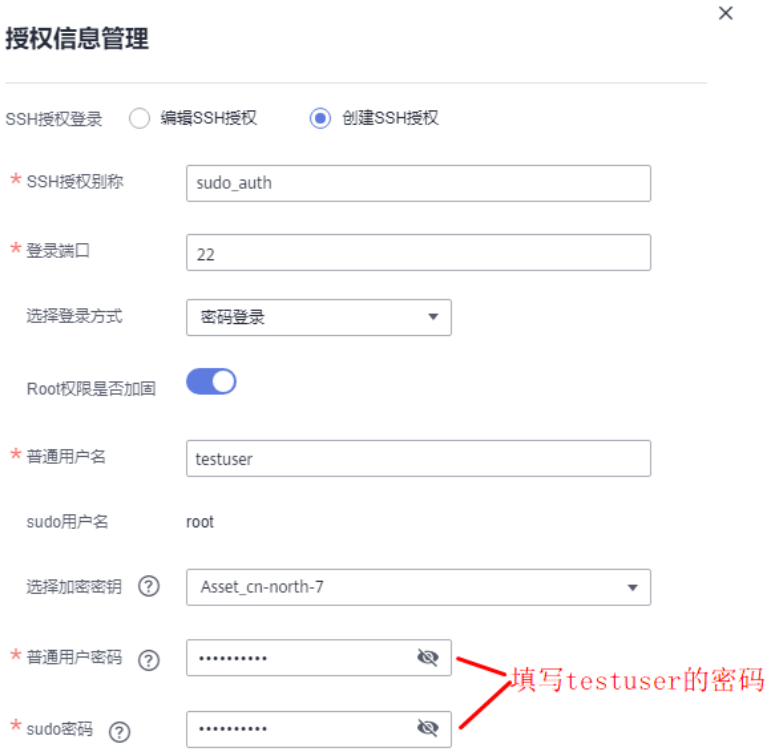
2. 输入#vi /etc/sudoers，就会打开sudoers配置文件。
3. 在配置文件末尾添加：普通用户名 ALL=(ALL:ALL) ALL，输入 :wq! ，保存修改。

说明

```
[testuser@localhost root]$ sudo cat /etc/os-release
[sudo] password for testuser:
NAME="EulerOS"
VERSION="2.0 (SP5)"
```

- 使用漏洞管理服务的sudo提权扫描功能时，认证凭据输入位置的“普通用户密码”和“sudo密码”请保持一致，均为“普通用户”的密码。



对于在“/etc/sudoers”中配置了“Defaults targetpw”的操作系统，需要输入root密码才能提权执行命令，因此建议暂时先将“Defaults targetpw”相关配置注释掉，扫描完成后再恢复原配置。

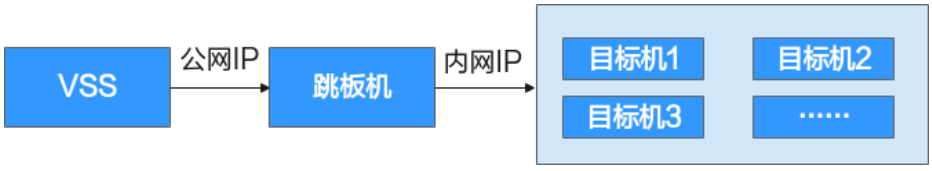
```
linux-1lll:~ # cat /etc/sudoers | grep Default.*targetpw
Defaults targetpw   # ask for the password of the target user i.e. root
ALL     ALL=(ALL) ALL   # WARNING! Only use this together with 'Defaults targetpw'!
```

- 扫描完成后，请还原配置。

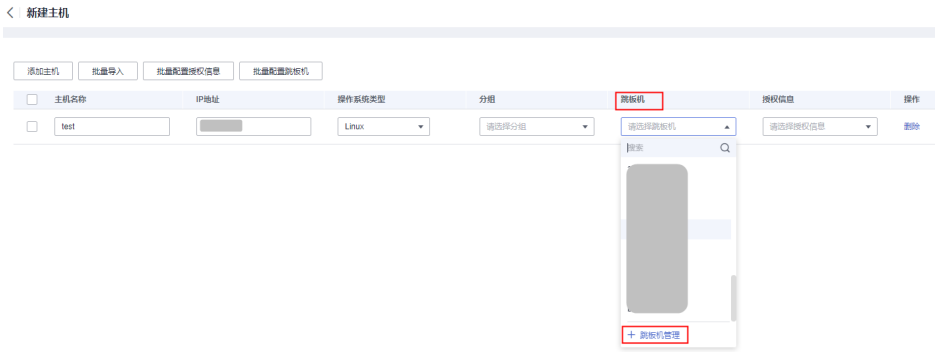
3.25 如何配置跳板机进行内网扫描?

使用跳板机进行内网扫描的网络示意图如图3-6所示。

图 3-6 网络示意图



1. 创建主机扫描任务，IP地址栏填写目标主机的内网IP。
2. 添加跳板机配置。
   配置的跳板机“公网IP”需与被测目标机的内网环境互通。



添加跳板机后，还需在该跳板机的ssh配置文件“/etc/ssh/sshd_config”中添加：AllowTcpForwarding yes，用于支持SSH授权登录转发。修改配置后需重启sshd服务。

3.26 主机互通性测试异常如何处理?

通过互通性测试可以测试待扫描的主机与扫描环境的连通性是否正常。

主机互通性测试不同异常提示的处理方法如下：

- 目标机或跳板机的SSH服务未开启，无法登录，请开启SSH服务。

- 目标机或跳板机的SSH服务连接超时，请确认网络是否可连通或是否有防火墙阻隔。

  待扫描的主机或跳板机的IP地址网络不通，解决办法请参见**如何解决主机不能访问?** 。

- 目标机或跳板机的系统账户密码错误，认证失败，请确认授权信息是否正确。

  主机授权信息中用户密码不正确，解决办法请参见**配置Linux主机授权**。

- 目标机或跳板机的系统账户密钥错误，认证失败，请确认授权信息是否正确。

  主机授权信息中用户密钥不正确，解决办法请参见**配置Linux主机授权**。

- 目标机的系统账户登录成功但权限不足，无法得到最完整、准确的扫描结果，请确认是否增加系统账户的权限。

主机授权信息中root权限加固场景下，用户密码不正确，解决办法请参见**配置普通用户和sudo提权用户漏洞扫描失败案例**。

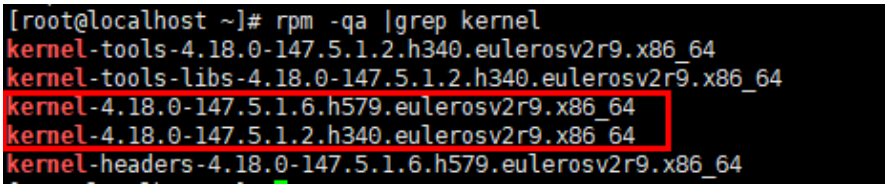
- Windows系统暂不支持互通性测试，请使用Linux系统主机进行互通性测试。

3.27 为什么安装了最新 kernel 后，仍报出系统存在低版本 kernel 漏洞未修复?

使用yum update kernel将kernel更新至最新版本后，漏洞管理服务扫描EulerOS仍报出大量kernel漏洞。这种情况不属于漏洞管理服务工具误报，而是由于升级kernel之后未及时重启并使用最新版本的kernel运行。kernel升级到最新版本后未重启并运行，实际上仍然使用未升级前的kernel扫描系统，所以漏洞仍然存在。

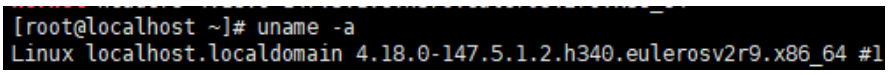
- 执行 如下命令可以查看当前系统安装了哪些版本的 kernel。

```
rpm -qa | grep kernel
```



- 执行如下命令可以查看当前系统实际使用的是什么版本的kernel。

```
uname -a
```



⚠ 注意

- 上面例子中就是实际使用的是低版本的存在大量CVE漏洞的kernel，因此使用漏洞管理服务扫描仍会报kernel存在CVE-2020-0465等漏洞。
- 此案例对于使用了CentOS、EulerOS、Red Hat、SUSE的用户均适用。
- 此外还有某些情况下，用户使用的yum源并不是操作系统官方最新的源，也即yum源中没有操作系统最新的安全补丁，此种情况下也可能报出kernel漏洞未修复的问题。此种情况下需要更新yum源为操作系统官方源或者向操作系统提供方寻求安全补丁的支持。总之，需要基于漏洞管理服务扫描报告中的“修复建议”中的installed version和fixed version的内容，进行分析和修复。

3.28 如何开启 WinRM 服务?

WinRM（Windows 远程管理，Windows Remote Management）是WEB服务管理在微软的Microsoft Windows中的实现，它允许处于一个共同网络内的Microsoft Windows计算机彼此之间互相访问和交换信息。在一台机器启用WinRM后，另一台机器就能通过Windows PowerShell对开启WinRM的机器进行远程管理。

> **⚠ 注意**
>
> 目前对Windows系统的认证扫描支持基于HTTPS的WinRM（5986端口）和基于HTTP的WinRM（5985端口），建议用户配置使用更安全的基于HTTPS的WinRM。
>
> 如果仅为了做漏洞扫描而修改WinRM配置的，建议在扫描完成后，恢复系统原先的配置。

开启基于 HTTPS 的 WinRM 服务

基于HTTPS的WinRM只支持Windows Server 2016及以上版本。

步骤1 以Windows系统管理员身份运行PowerShell。

步骤2 执行如下命令查看基于HTTPS的WinRM是否开启。

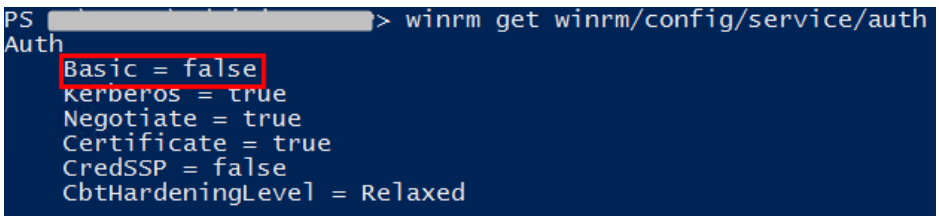
```
winrm e winrm/config/listener
```

输出结果有HTTPS的“Listener”且“Enabled”为“true”，则为开启状态。如果未开启，则请直接执行**步骤4**。

步骤3 校验WinRM是否使用用户名密码验证及使用的证书是否正确。

1. 执行如下命令查看是否使用用户名密码验证。
   a. 执行如下命令查看Auth信息。

   ```
   winrm get winrm/config/service/auth
   ```

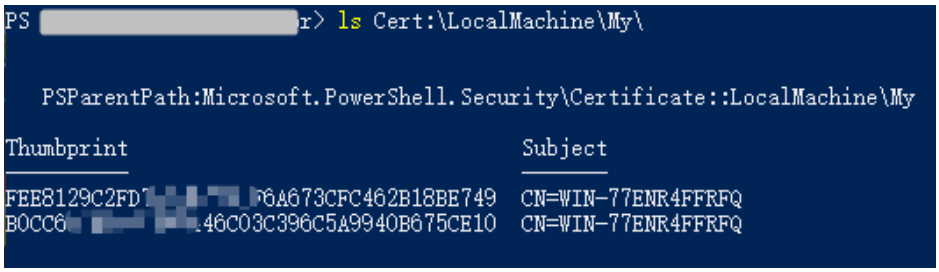
   b. 执行如下命令修改“Basic”的值为“true”。

   当返回值中“Basic”为“true”时，无需执行该步骤。

   ```
   winrm set winrm/config/service/auth '@{Basic="true"}'
   ```

2. 执行如下命令校验WinRM使用的证书是否正确。

   ```
   ls Cert:\LocalMachine\My\
   ```

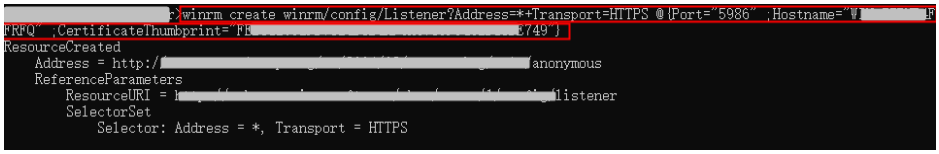



- 如果有输出，且“Thumbprint”与**步骤2**的Thumbprint对应，“CN”名与主机名对应，则基于HTTPS的WinRM已配置完成。
- 如果不满足上面任意一条则请直接执行**步骤5**替换HTTPS WinRM使用的证书。

步骤4 以Windows系统管理员身份运行cmd，并执行如下命令创建基于HTTPS的WinRM服务。

该步中需要使用CN与主机名相同的证书，如果不同，请先执行**步骤5.1**生成证书。

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Port="5986" ;Hostname="" ;CertificateThumbprint=""}
```



执行成功结果如上图。其中，“Port”为监听端口（建议不做更改），“CertificateThumbprint”为证书的Thumbprint，“Hostname”为主机名，可通过在PowerShell中输入如下命令获取：

```
hostname
```

可再通过**步骤2**～**步骤3**验证HTTPS WinRM配置是否正确。

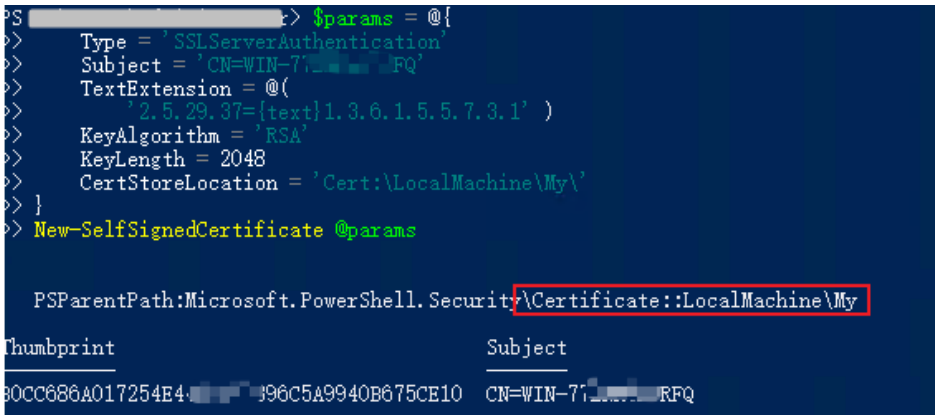
步骤5 替换HTTPS WinRM使用证书。

1. 生成CN与主机名相同的自签名证书。

   在PowerShell中输入如下命令创建证书：

   ```
   $params = @{
      Type = 'SSLServerAuthentication'
      Subject = 'CN='
      TextExtension = @(
         '2.5.29.37={text}1.3.6.1.5.5.7.3.1' )
      KeyAlgorithm = 'RSA'
      KeyLength = 2048
      CertStoreLocation = 'Cert:\LocalMachine\My\'
   }
   New-SelfSignedCertificate @params
   ```

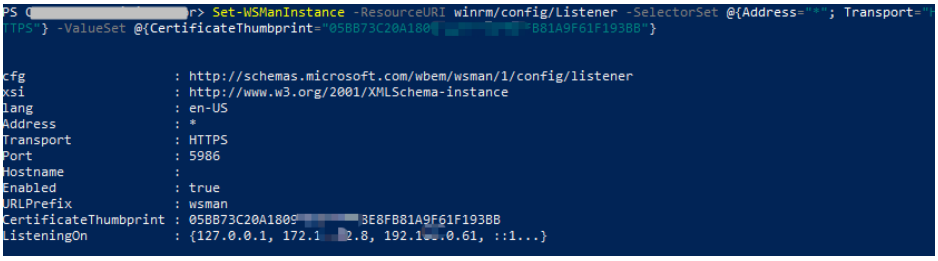
   其中，除“Subject”的值外，其他值请和上述命令保持一致，“Subject”值的格式为“CN=hostname”，hostname的获取见**步骤4**。



生成成功会输出证书的Subject和Thumbprint。

2. 执行如下命令替换证书。

```
Set-WSManInstance -ResourceURI winrm/config/Listener -SelectorSet @{Address="*";
Transport="HTTPS"} -ValueSet @{CertificateThumbprint=""}
```



其中，“CertificateThumbprint”为证书的Thumbprint，可再通过**步骤2**～**步骤3**验证HTTPS WinRM配置是否正确。

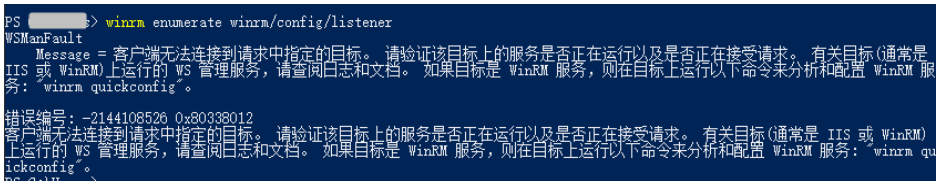
----结束

开启基于 HTTP 的 WinRM 服务

步骤1 以Windows系统管理员身份运行PowerShell。

步骤2 执行如下命令查看基于HTTP的WinRM是否开启。

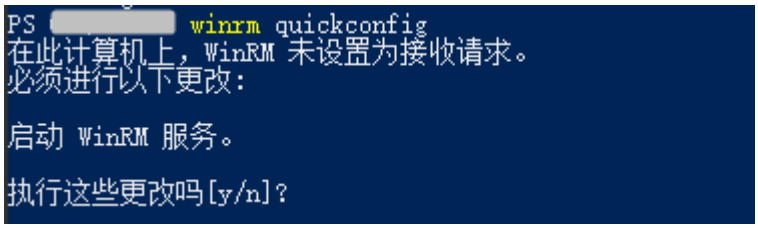
```
winrm enumerate winrm/config/listener
```



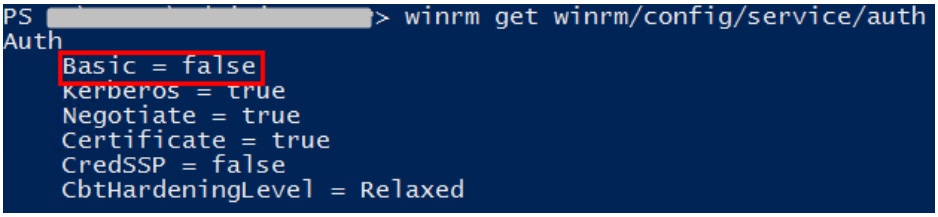
- 如果存在报错信息，则表示WinRM服务未开启，请执行**步骤3**。
- 如果不存在报错信息，则表示WinRM服务已开启，请执行**步骤4**。

步骤3 执行如下命令开启WinRM，选择y完成设置。

```
winrm quickconfig
```

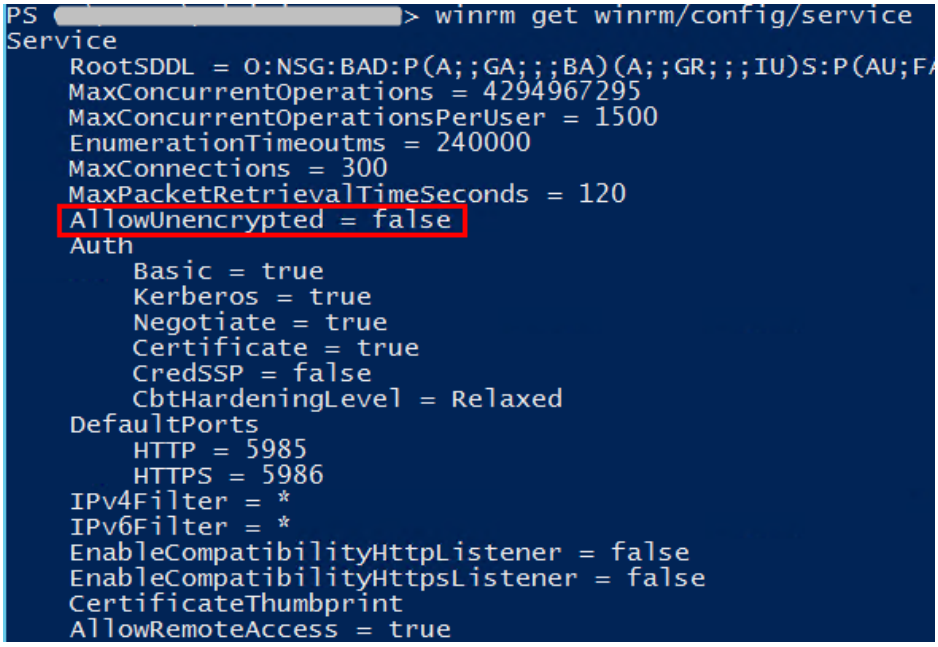



步骤4 配置Auth。

1. 执行如下命令查看Auth信息。
   ```
   winrm get winrm/config/service/auth
   ```
   

2. 执行如下命令修改“Basic”的值为“true”。
   当返回值中“Basic”为“true”时，无需执行该步骤。
   ```
   winrm set winrm/config/service/auth '@{Basic="true"}'
   ```

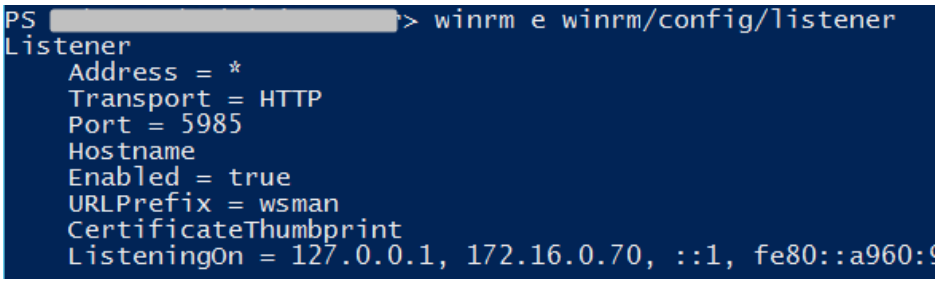
步骤5 配置加密方式为允许非加密。

1. 执行如下命令查看Service信息。
   ```
   winrm get winrm/config/service
   ```
   

   当返回值中“AllowUnencrypted”为“false”时，请执行**步骤5.2**。
2. 执行如下命令修改“AllowUnencrypted”的值为“true”。
   ```
   winrm set winrm/config/service '@{AllowUnencrypted="true"}'
   ```

步骤6 执行如下命令检查基于HTTP的WinRM服务是否开启成功。

```
winrm e winrm/config/listener
```

查看返回值，输出结果有HTTP的“Listener”且“Enabled”为“true”，则为开启状态。

----结束

关闭 WinRM 服务

步骤1 以管理员身份运行Powershell并执行如下命令。

```
winrm set winrm/config/service/auth '@{Basic="false"}'
winrm set winrm/config/service '@{AllowUnencrypted="false"}'
```

步骤2 执行如下命令关闭WinRM服务。

```
net stop winrm
```

----结束

3.29 使用跳板机扫描内网主机和直接扫描公网主机，在扫描能力方面有什么区别?

使用跳板机扫描内网主机和直接扫描公网主机，在扫描能力方面区别如表3-3所示。

表 3-3 扫描能力差异介绍

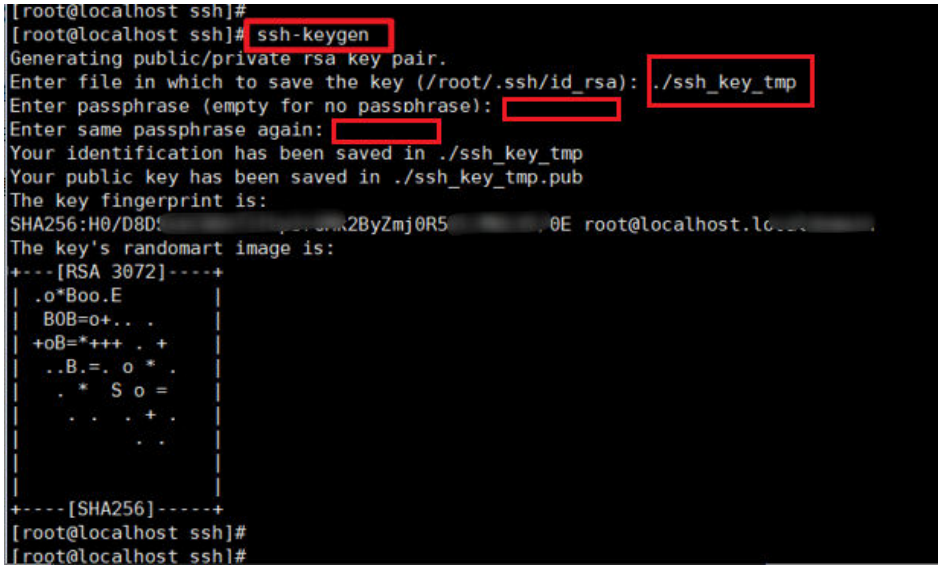
扫描能力	通过公网IP直接扫描公网主机	通过跳板机扫描内网主机
操作系统安全补丁扫描	支持	支持
远程服务/协议漏洞扫描	支持	不支持 **说明** 远程服务/协议类漏洞的扫描依赖于扫描器与被测目标的相关端口直接交互，因此不能通过跳板机完成测试验证。
操作系统安全配置扫描	支持	支持
Web中间件安全配置扫描	支持	支持
等保合规扫描	支持	支持

3.30 如何生成私钥和私钥密码?

当主机扫描通过密钥的方式来登录目的主机时，会涉及到私钥和私钥密码的填写。

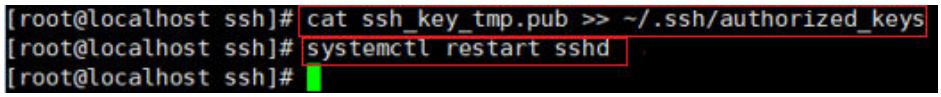
私钥和私钥密码的生成方式如下：

步骤1 在目的主机上执行**ssh-keygen**命令生成公钥和私钥，按照提示信息输入生成密钥的文件路径，并输入2次私钥密码。

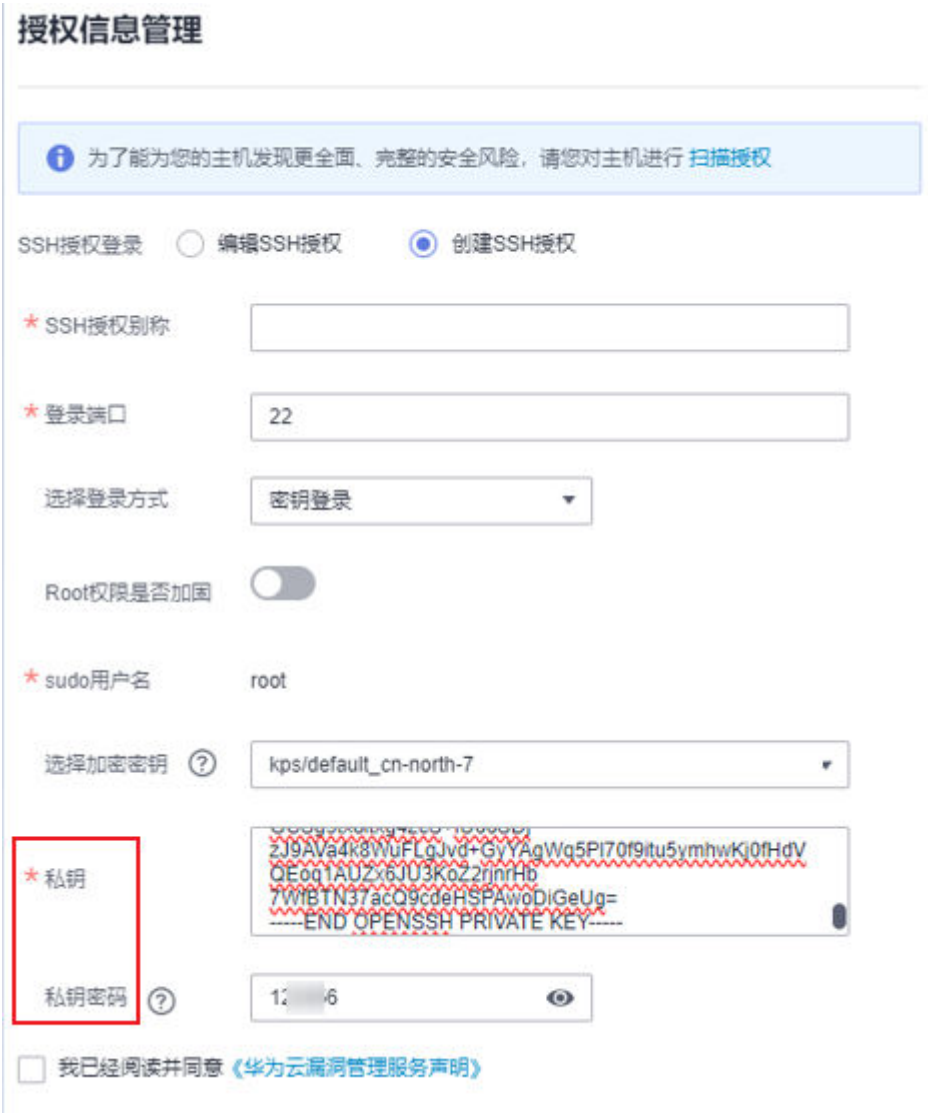


执行**ls**命令可查看在设置的文件路径下生成的公钥和私钥文件。

步骤2 将公钥配到目的主机的sshd服务认证配置里面，然后执行**systemctl restart sshd**命令重启ssh服务。



步骤3 执行**cat**命令查看私钥文件内容，并将私钥内容进行复制，拷贝至“**授权信息管理**”页面的私钥文本框中，并输入私钥密码。

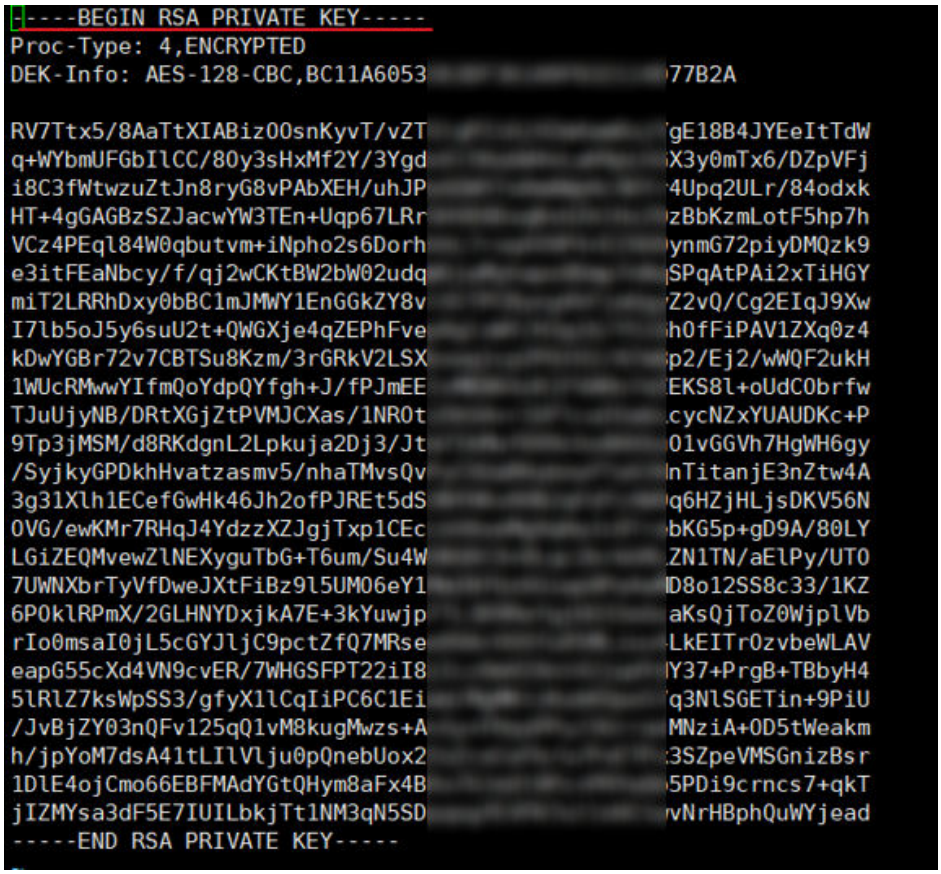


到此，源主机就有了私钥，目的主机就有了公钥，源主机发起连接请求到目的主机时，目的主机会随机发送一个字符串给源主机，源主机利用私钥加密该字符串，然后发送给目的主机，目的主机利用公钥解密该字符串，如果和发送时匹配，则认证通过。

----结束

3.31 ssh 版本较低，生成的密钥以“BEGIN RSA PRIVATE KEY”开头，无法登录怎么办?

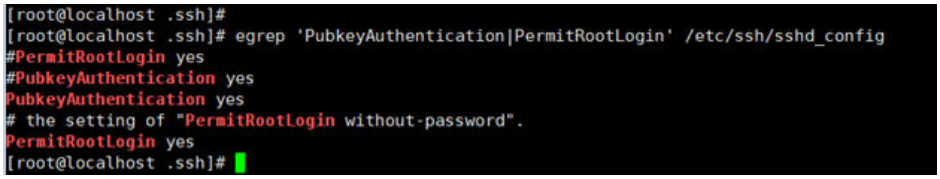
若该版本ssh无法登录，则需要将ssh升级到高版本，高版本生成的私钥是以“BEGIN OPENSSH PRIVATE KEY”开头的，OpenSSH从7.8版本开始改用了OpenSSH密钥格式。



3.32 如何确认目的主机是否支持公钥认证登录和 root 登录?

执行如下命令查看配置文件是否开启公钥认证和root登录：

egrep 'PubkeyAuthentication|PermitRootLogin' /etc/ssh/sshd_config



- 若出现如下回显则表示开启了公钥认证方式。
  PubkeyAuthentication yes
- 若出现如下回显则表示允许root登录。
  PermitRootLogin yes

3.33 主机扫描权限异常如何处理?

当使用主机扫描功能遇到如下报错时，

CodeArts Inspector.00050001: The user role has no permission to access the interface.

User: AAA:user:BBB is not authorized to perform: kms:cmk:decryptData.

需登录AAA账号，检查BBB用户是否含有**kms:cmk:decryptData**权限。

如果没有**kms:cmk:decryptData**权限，可参考**IAM指导文档**手动添加相应的权限再进行互通性测试。

4 移动应用安全类

4.1 漏洞管理服务支持哪些安全漏洞检测?

安卓应用支持七大类漏洞检测：配置安全、加密安全、组件安全、签名证书安全、存储安全、权限安全、网络安全。

鸿蒙应用及服务支持七大类安全漏洞检测：权限安全、网络安全、签名证书安全、公共事件安全、Ability安全、存储安全、加密安全。

4.2 隐私合规检测支持哪些场景?

覆盖工信部、网信办、公安部等监管机构标准及要求，通过动态、静态及动静结合的方式，自动化检测隐私声明和行为的一致性。

覆盖应用及使用SDK的隐私合规检测，包括但不限于：不规范隐私声明使用、违规使用用户个人信息、不给权限不让用、过度索取权限、强制用户使用定向推送、误导下载APP。

4.3 任务状态显示失败如何处理?

任务扫描失败可能由多种原因造成，需要针对具体情况进行分析，常见的失败原因如下：

表 4-1 常见失败原因分析

失败原因分析	解决方案
应用文件解析异常	应用文件本身存在不完整、结构异常等问题，导致服务无法正常解析。提供正确的应用文件重新创建扫描任务即可。
应用文件上传中损坏	应用文件在传送过程中损坏，导致无法正确解析，重新创建扫描任务进行扫描即可。

失败原因分析	解决方案
其它原因导致任务失败	多次重复创建任务后扫描任务仍然失败，可联系

说明

失败任务不会产生扣费，可重新创建任务进行扫描。

4.4 扫描的安全漏洞告警如何分析定位?

针对移动扫描的安全漏洞，如何通过报告提供的信息进行分析、定位、修复？检测结果提供了如下信息：

1. 报告提供了问题代码信息，包括文件名及其路径，可以通过该信息快速定位到问题文件。

   说明

   针对部分检测问题，如签名安全检测告警，无具体问题文件显示。

2. 漏洞特征信息，主要为安全漏洞所涉及的函数代码。
3. 安全漏洞修复建议，结合上述代码信息确定具体告警位置，分析漏洞告警是否确认为安全漏洞。

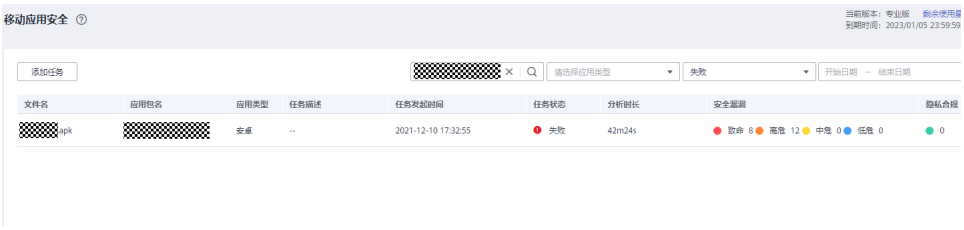
4.5 扫描的隐私合规问题如何分析定位?

针对扫描结果中的隐私合规问题告警，可以通过以下几个信息进行分析定位，并整改处理。

1. 截图：在动态运行APP过程中，对部分涉及界面的合规问题进行截图举证，在最终扫描结果中提供截图展示，用户可根据截图进行告警分析。
2. 调用栈：涉及收集个人数据类告警，包括第三方SDK收集，扫描结果中会提供代码调用栈信息，帮助应用开发人员快速查找问题点。
3. 隐私申明片段：对于应用实际行为与隐私声明不一致的合规问题，扫描结果中会提取相应的隐私审批片段，能快速从应用隐私申明、第三方SDK隐私申明中定位问题点。
4. 相应政策规范：该项告警违反的哪些规范条目，在扫描报告中详细列举，用户可以针对性的进行分析整改。

4.6 任务部分检测项有数值，但任务状态显示失败?

如下图显示，任务检测结果中安全漏洞检测有告警，隐私合规问题数为0，任务状态为“失败”。



每个任务会进行多个检测项的检查，如基础安全检测、违规收集信息检测、隐私声明一致性检测等，整个检测过程分为应用解析、静态分析、动态运行三个阶段，因为应用自身原因，如闪退、无法解析、无法安装等原因导致其中某个阶段出现异常的时候任务会中止。这时候已经有了一部分检测结果，但为了保证整体任务检测完整性，我们会判定当前任务失败，且报告不可查看，扫描失败的任务不扣费。

4.7 安全漏洞报告中问题文件或者漏洞特征信息为空?

安全漏洞扫描结果中，我们会展示相关的问题文件及特征信息，但是在实际报告会发现存在问题文件或者漏洞特征信息为空的情况，如下图所示：

这是因为部分检查项是针对全局性的，不针对某个文件，所以存在问题文件跟漏洞特征信息为空情况，属于正常现象。

4.8 任务扫描超 1 小时仍然未结束?

根据样本统计，单任务平均扫描耗时约1小时，扫描时长跟以下几个因素有关：

- 文件大小，文件越大扫描越耗时。
- 代码量，代码量越多扫描越耗时。
- 代码复杂程度，因为业务、代码实现的原因导致代码实现相对较复杂，调用链长，这些都会导致扫描耗时增加。

故部分应用扫描时长会高于平均耗时，如超过12小时仍未结束，可能是因为某些异常原因导致任务无法正常结束，我们会判定该类任务未超时，终止任务执行、设置任务状态为“超时”。

4.9 哪些场景下检测结果可能会存在漏报?

- 加固加壳的应用，例如通过爱加密加固。
- 使用不支持无障碍服务UI框架开发的应用，例如游戏。
- SDK版本低于18。

4.10 如何在应用检测过程中输入用户凭证登录应用?

应用在“分析中”状态，如果当前处于隐私合规检测阶段，可单击状态列的“分析中”链接打开详情窗口，应用动态运行界面会投屏至网页端。

当应用出现登录界面时，界面自动停止运行，此时用户可通过本地键盘输入登录凭证，完成登录操作。

4.11 检测过程中，无法打开详情查看手机实时检测界面怎么解决?

手机检测界面仅在隐私合规检测阶段可查看，其他检测阶段不可见，通常在任务启动5分钟左右会进行隐私合规检测操作，此时才可以查看。

4.12 隐私声明 URL 地址、个人信息第三方共享目录 URL 地址如何获取?

打开App时会弹出隐私声明对话框，对话框里包含了隐私声明以及第三方SDK隐私声明的链接，可以单击链接获取详细地址。

5 二进制成分分析类

5.1 成分分析的扫描对象是什么?

成分分析的扫描对象为产品编译后的二进制软件包或固件：Linux安装包、Windows安装包、Web部署包、安卓应用、鸿蒙应用、IOS应用、嵌入式固件等；不支持扫描源码类文件；详细操作参见**添加二进制成分分析任务**。

5.2 成分分析的主要扫描规格有哪些?

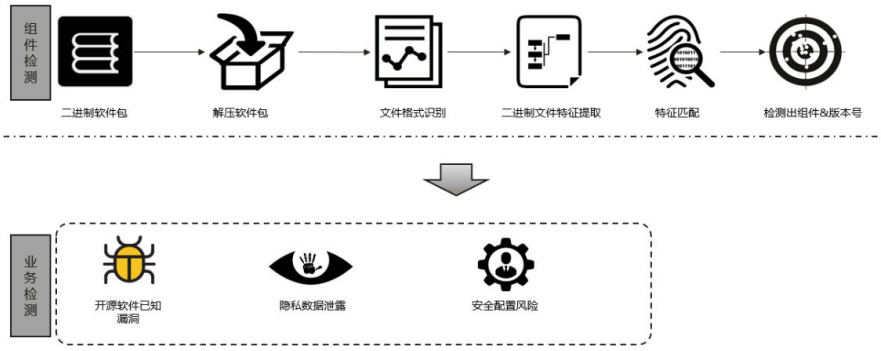
- 支持的编程语言类型：C/C++/Java/Go/JavaScript/Python/Rust/Swift/C#/PHP。
- 支持的文件：.7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war等格式文件，及Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot等固件。
- 支持上传的文件大小：不超过5GB。
- 平均扫描时间预估：根据不同的压缩格式或者文件类型扫描时长会有一定的差异，平均100MB/6min。
- 服务采用基于软件版本的方式检测漏洞，不支持补丁修复漏洞场景的检测。

5.3 成分分析的扫描原理是什么，主要识别哪些风险?

对用户提供的软件包/固件进行全面分析，通过解压获取包中所有待分析文件，基于组件特征识别技术以及各种风险检测规则，获得相关被测对象的组件BOM清单和潜在风险清单。主要包括以下几类：

- **开源软件风险：**检测包中的开源软件风险，如已知漏洞、License合规等。
- **安全配置风险：**检测包中配置类风险，如硬编码凭证、敏感文件（如密钥、证书、调试工具等）问题、OS认证和访问控制类问题等。
- **信息泄露风险：**检测包中信息泄露风险，如IP泄露、硬编码密钥、弱口令、GIT/SVN仓泄露等风险。
- **安全编译选项：**支持检测包中二进制文件编译过程中相关选项是否存在风险。

图 5-1 风险项



5.4 成分分析的开源软件风险如何分析?

成分分析基于静态风险检测，会对用户上传的软件包/固件进行解压并分析其中的文件，识别包中文件包含的开源软件清单，并分析是否存在已知漏洞、License合规等风险。用户扫描完成后，建议按照以下步骤进行分析排查：

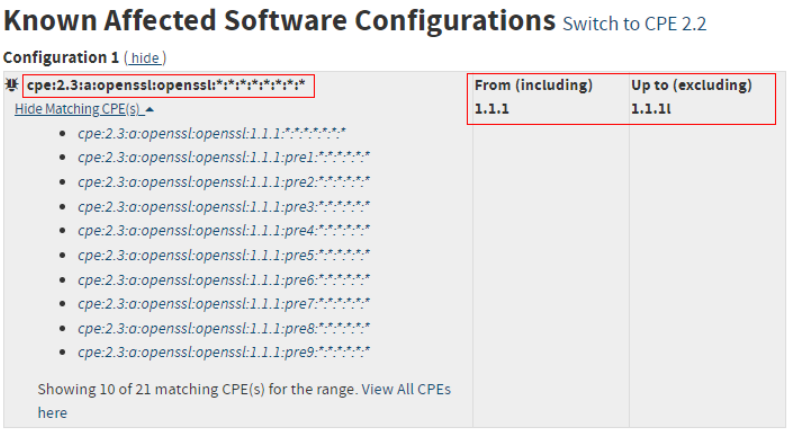
1. 开源软件分析，分析开源软件是否存在以及软件版本是否准确。

   基于报告详情页面或导出的报告中开源软件所在文件全路径找到对应文件，然后分析该文件中开源软件是否存在或准确（可由相关文件的开发或提供人员协助分析），如果否，则无需后续分析。

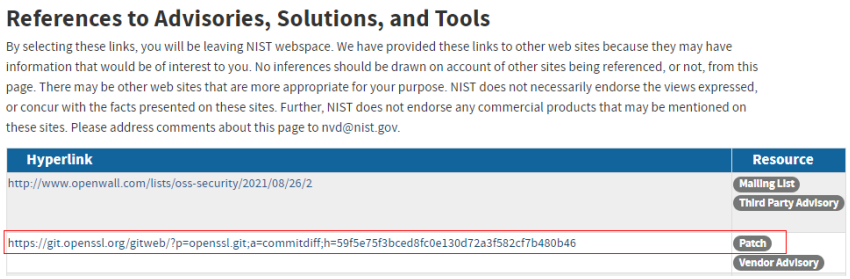
2. 已知漏洞分析，分析已知漏洞是否准确。

   通过NVD、CVE、CNVD等社区搜索相关CVE已知漏洞编号，获取漏洞详情

   - **概要分析：**查看影响的软件范围，如CVE-2021-3711在NVD社区中的Known Affected Software Configurations，如下图，确认漏洞是否影响当前使用的软件版本，如果当前使用的软件版本不在影响范围内，则初步说明漏洞可能不涉及/影响。



- **精细化分析**：漏洞通常存在于某些函数中，可以通过社区中的漏洞修复补丁确认漏洞详情、涉及函数以及修复方式，如下图，用户可以结合自身软件对于相关开源软件功能的使用是否涉及相关漏洞



3. License合规分析。基于报告中开源软件及对应的License分析软件是否合规，满足公司或准入要求。
4. 风险解决方式：
   - **已知漏洞**：如果当前使用的软件版本存在漏洞，可通过升级软件版本至社区推荐版本解决。紧急情况下也可以通过社区推荐的patch修复方式临时解决。
   - **License合规**：如果使用的软件存在合规风险，则需要寻找相似功能且合规的开源软件进行替代。

5.5 成分分析的安全配置类问题如何分析?

1. 成分分析会检测用户包中一些安全配置项是否合规，主要如下：
   - 用户上传的软件包/固件中存在的敏感文件，如（密钥文件，证书文件，源码文件, 调试工具等）。
   - 用户上传的软件包/固件中操作系统中的用户与组配置、硬编码凭证、认证和访问控制等配置类问题。若不存在操作系统，则不涉及。
2. 安全配置类检查问题分析指导：

   导出PDF报告，搜索【安全配置检查概览】关键字，可以看到各检查项的结果，pass表示通过，failed表示未通过，NA表示不涉及（若无操作系统，则针对操作系统配置检查项为不涉及）。搜索【安全配置检查】关键字，可以查看具体每项的检查结果。

   检查结果说明：
   - 审视项：检查的方式/方法。
   - 问题：存在问题的文件列表，若无问题则显示暂无问题。
   - 建议值：针对检查出的问题给出的修改建议。
   - 描述：审视项描述。

5.6 成分分析的信息泄露问题如何分析?

成分分析基于静态风险检测，会对用户上传的软件包/固件进行解压并分析其中的文件，识别包中是否存在信息泄露类风险，如敏感IP、GIT/SVN仓、弱口令、硬编码密钥等风险。

针对已识别的信息泄露类风险，可以通过查看导出报告中的告警详情，如PDF报告，可以在结果概览中确认是否有信息泄露风险。如果有，则可以查看相应信息泄露明细，每个告警都会包含以下几个说明，针对工具扫描出的风险清单，用户可以基于自

身实际使用情况判断是否有信息泄露风险，如存在，则采取不同措施屏蔽或修改即可。

- 问题类型：IP泄露/硬编码密码/Git地址泄露等。
- 文件路径：发现信息泄露的文件在包中的全路径。
- 上下文内容：发现风险的文本行内容，包含风险内容和上下文内容。
- 匹配内容：实际发现的风险内容。
- 匹配位置：在文件中x行，x位置发现的信息泄露风险。

5.7 组件版本为什么没有被识别出来或识别错误?

成分分析扫描无法识别组件版本常见原因有：

1. 成分分析特征库不支持该开源软件版本。
2. 用户引用的开源软件修改过源码，或使用时部分引用该软件功能，导致实际编译/发布文件中相关软件特征未达到工具识别阈值，造成开源软件无法识别或版本识别异常。
3. 用户使用的开源软件包含被动依赖软件，该依赖软件可能为部分引用，造成软件无法识别或版本识别异常。

5.8 成分分析如何购买?

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。

5.9 成分分析的资源包为什么购买失败了?

可能是因为权限不足导致购买失败，请检查用户权限。

用户需要拥有te_admin、bss_adm、bss_pay或bss_ops权限才能购买漏洞管理服务。如需开通该权限，请联系拥有Tenant Administrator权限的用户，开通权限，详细内容请参见《**统一身份认证服务用户指南**》。

5.10 成分分析的开源漏洞文件路径如何查看?

有多种方式可查看开源漏洞分析结果的文件路径：

- 方式一：进入报告详情页面，在“开源软件漏洞”中，单击“组件名称”可查看包含组件的文件对象，鼠标放在相应“对象路径”，即可查看该对象路径，也可单击右侧按钮复制。

- 方式二：打开报告详情页面，单击“下载报告 > 生成PDF报告”，待文件生成后单击“下载报告 > 导出PDF”下载报告至本地，查阅PDF报告中第3章节，即可查看相应组件文件路径。

  3 组件列表

  3.1 boost-1.68.0

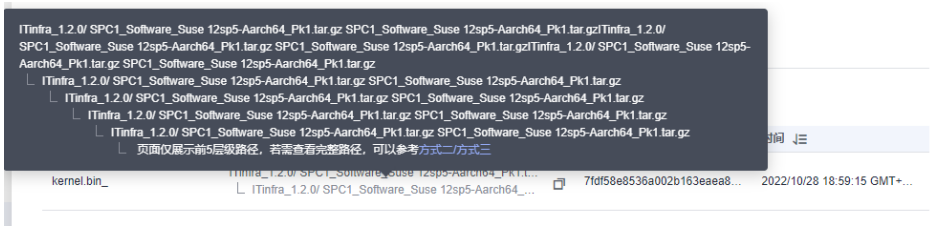
名称	boost
版本	1.68.0
发布日期	2018-08-01
许可协议	e V1.0

文件路径
34 sr/lib/lib bo
34. uashfs_/usr/lib/lib boo
34._ usr/lib/lib boo
34 /lib/lib b

- 方式三：打开报告详情页面，单击“下载报告 > 生成Excel报告”，待文件生成后单击“下载报告 > 导出Excel”下载报告至本地，查阅Excel报告中“组件报告”或“漏洞报告”sheet页，即可查看相应组件文件路径。

  对象路径以“/”标识目录结构，其中“_/”表示服务对该层文件进行解析，进而分析其子目录文件。比如：scrm-service-weixin.jar_/BOOT-INF/classes/libWeWorkFinanceSdk_Java.so，您可以对scrm-service-weixin.jar进行解压缩，查看其子目录BOOT-INF/classes/libWeWorkFinanceSdk_Java.so文件，进而分析该文件中开源软件是否存在或准确。

  若文件有多个层级，则表示服务对父层级文件进行解析，进而分析子层级文件是否引用开源软件。对于方式一，多层级效果以换行缩进形式呈现，如下图所示；对于方式二或方式三，多层级路径以“:”连接展示。

5.11 成分分析的任务扫描失败怎么办？

任务扫描失败可能由多种原因造成，需要针对具体情况进行分析，常见的失败原因如下：

表 5-1 常见失败原因分析

失败原因	解决方案
文件解析异常	文件本身存在不完整、结构异常等问题，导致服务无法正常解析。提供通用的压缩、固件、包格式文件重新创建扫描任务即可。
文件上传中损坏	文件在传送过程中损坏，导致无法正确解析。重新创建扫描任务进行扫描即可。
其它原因导致任务失败	多次重复创建任务后扫描任务仍然失败，可联系服务运维团队。

⚠ 注意

若用户使用“按需套餐包”创建正式版任务，如果任务扫描失败，不会扣除套餐包配额；若用户使用免费版配额创建免费版任务，如果任务扫描失败，不会扣除免费版配额。

5.12 如何查看用户组是否具有 Tenant Administrator 或 VSS Administrator 权限，及如何对用户组角色授权?

1. 登录华为云，在右上角单击“控制台”。
2. 单击右上角的*个人账号*下的“统一身份认证”，进入“统一身份认证服务”页面。
3. 选择“用户组”，单击用户组名称即可查看角色授权记录。

图 5-2 查看用户组授权记录

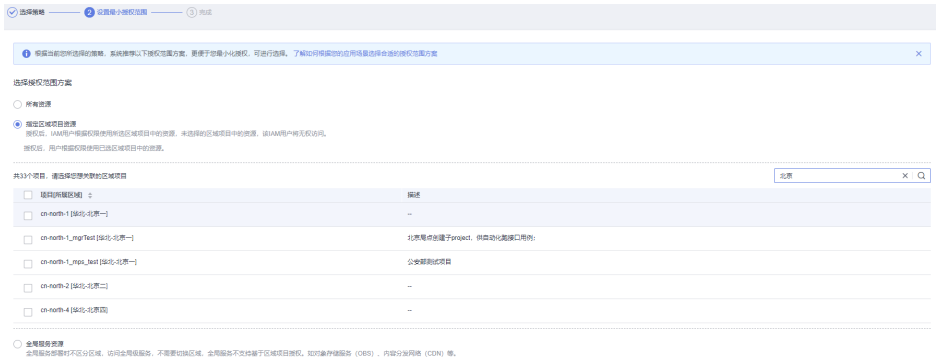
说明

切换至“用户管理”页签，可以查看该用户组下的所有用户，也可以将其他用户添加至该用户组。

4. 如果该用户组缺少相应角色权限，单击“授权”，进入“选择策略”步骤，模糊搜索“Tenant Administrator”或“VSS Administrator”权限的关键字，勾选相应策略。

5. 单击“下一步”，设置最小授权范围。

图 5-3 设置最小授权范围



6. 单击“确定”，即可完成用户组角色授权。

5.13 如何解决 Roles with READONLY_USER 或其他角色权限报错问题?

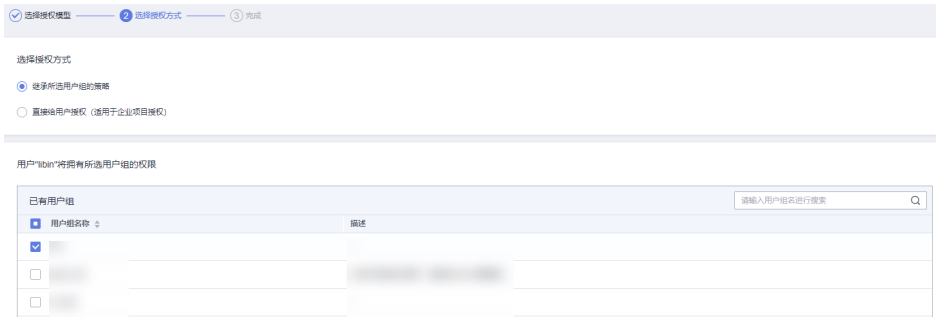
用户需要具有Tenant Administrator或VSS Administrator权限才能使用二进制成分分析相关业务。如需开通该权限，请联系具有Tenant Administrator或VSS Administrator权限的用户进行授权，可参考**如何查看用户组是否具有Tenant Administrator或VSS Administrator权限，及如何对用户组角色授权?** 查看具有权限的用户。

1. 使用具有Tenant Administrator或VSS Administrator权限的账号登录华为云，在右上角单击“控制台”。
2. 单击右上角的***个人账号***下的“统一身份认证”，进入“统一身份认证服务 > 用户”页面。
3. 在用户列表中，单击需要授权用户所在行的“授权”，进入“授权”页面。

图 5-4 用户授权

4. 授权方式选“继承所选用户组的策略”，用户组勾选具有Tenant Administrator或VSS Administrator权限的用户组。

图 5-5 选择授权方式



5. 单击“确定”，完成授权。

6 计费类

6.1 漏洞管理服务如何收费?

计费项

漏洞管理服务根据您的服务版本，扫描配额包的个数和购买时长计费。

表 6-1 计费项信息

计费项目	计费说明
服务版本（必选）	按购买的服务版本（基础版、专业版、高级版或企业版）计费。
扫描配额包	按购买的个数计费。
购买时长	提供包年/包月和按需计费的购买模式。

计费模式

漏洞管理服务提供按需计费和包年/包月两种计费模式，用户可以根据实际需求选择计费模式。

表 6-2 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：每日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。不限制扫描次数。	
高级版			
企业版			

变更配置

- 域名配额扩容：当您的业务需求增加，可在计费周期内“扩容”域名的扫描配额包。支持扩容**专业版配额**、**高级版配额**以及**企业版配额**。不支持多个版本同时存在。
- 专业版升级为高级版：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**。
- 退订：购买漏洞管理服务的扫描配额包后，如需停止使用，请到费用中心执行**退订**操作。

续费

扫描配额包到期后，您可以进行续费以延长扫描配额包的有效期，也可以设置到期自动续费。请参见**续费管理**。

到期与欠费

包周期资源开通成功后，如果没有按时续费，公有云平台会提供一定的保留期，详细信息请参见“**保留期**”。

欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，账号将进入欠费状态，需要在约定时间内支付欠款，详细操作请参考**欠费还款**。

6.2 如何为漏洞管理服务续费?

操作场景

该任务为您介绍当漏洞管理服务即将到期时，您如何续费。续费后，您可以继续使用漏洞管理服务的专业版、高级版或者企业版功能。

前提条件

已获取管理控制台的登录账号与密码。

说明

如果您使用的是子账号，需要主账号对子账号赋予BSS Administrator操作权限后，才可以使用子账号执行续费操作。

操作步骤

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 在“总览”页面，单击“续费”。

步骤4 进入续费管理入口，如图6-1所示。

图 6-1 进入续费管理入口

步骤5 在需要续费的漏洞管理服务所在行的“操作”列，单击“续费”。

步骤6 在对应页面根据页面提示完成续费。

详细续费操作请参见续费管理。

----结束

6.3 如何退订漏洞管理服务?

操作场景

该任务为您介绍如何退订漏洞管理服务的专业版、高级版和企业版功能。

前提条件

已获取管理控制台的登录账号与密码。

说明

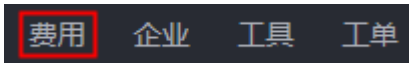
如果您使用的是子账号，需要主账号对子账号赋予BSS Administrator操作权限后，才可以使用子账号执行退订操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击界面右上方的“费用”，进入“费用中心”界面，如图6-2所示。

图 6-2 费用中心入口



步骤3 在左侧导航树上，选择“退订与变更 > 退订管理”。

步骤4 在对应页面根据页面提示完成退订。

详细退订操作请参见**退订管理**。

----结束

6.4 购买专业版漏洞管理服务的注意事项?

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。

6.5 如何减少漏洞管理服务配额?

购买漏洞管理服务或配额后不能减少配额，仅支持升级规格。

如果用户需要减少配额，需要等之前购买的套餐到期或者退订当前套餐后，重新购买。退订和购买漏洞管理服务请参考**如何退订漏洞管理服务?** 和**购买漏洞管理服务**。

7 报告类

7.1 如何下载网站扫描报告?

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。

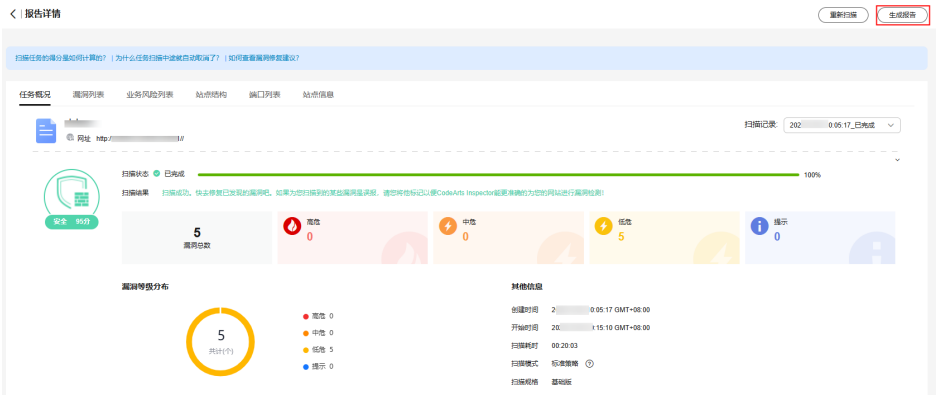
步骤3 在“资产列表 > 网站”页签，进入网站列表页面。

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 7-1 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 修改“报告名称”，“报告名称”自动生成，可修改。

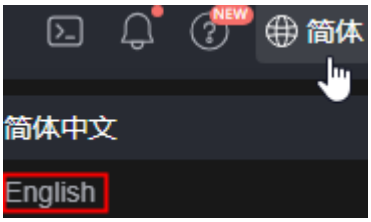
步骤7 单击“确定”，弹出前往报告中心下载报告的提示框。

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

7.2 漏洞扫描报告模板包括哪些内容?

当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。

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 7-2 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 29 个，漏洞类型 4 种。其中高危漏洞有 1 个。

任务名称	ecshop3
扫描对象	http://
开始时间	2020-09-22 11:04:50
结束时间	2020-09-22 11:13:01
扫描耗时	1.34小时

1.2 网站指纹信息

IP	
服务器	OPENRESTY[ ];NGINX
编程语言	PHP[5.6.37];LUA
开放端口	8080, 8081

- 漏洞分析概览
  统计漏洞类型及分布情况。

图 7-3 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					
4 分	总漏洞数 29	高危漏洞 1	中危漏洞 1	低危漏洞 27	提示威胁 0

2.2 漏洞类型分布

分类	漏洞类型	检测结果
恶意内容	恶意外链	安全
	挖矿后门	安全
	网页木马	安全
潜在风险	网站请求头	4个风险项
	Https协议	安全
网站安全漏洞	跨站请求伪造	安全
	应急漏洞	安全
	信息泄露	16个漏洞 查看详情
	注入攻击	安全
	其它	4个漏洞 查看详情
	路径遍历	安全
	授权问题	安全
	弱密码	1个漏洞 查看详情
	跨站脚本攻击	8个漏洞 查看详情

- 服务端口列表
  查看目标网站的所有端口信息。

图 7-4 网站的端口列表

3 端口列表

端口	状态	协议	服务
8,081	Open	TCP	QuickTime Streaming Server
8,080	Open	TCP	QuickTime Streaming Server | Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications

- 漏洞根因及详情
  您可以根据修复建议修复漏洞。

图 7-5 漏洞根因及详情

5.2 应急漏洞

序号	漏洞名称	漏洞级别	漏洞个数
1	Fastjson远程代码执行漏洞	高危	1

5.2.1 Fastjson远程代码执行漏洞

漏洞级别 高危

漏洞简介

关注到Fastjson 存在反序列化远程代码执行漏洞，可导致直接获取服务器权限，且此漏洞为 17 年 Fastjson 1.2.24 版本反序列化漏洞的延伸利用，危害严重。此漏洞影响版本 < 1.2.51，请受影响的用户尽快升级至安全版本。

修复建议

1)方案一：升级 fastjson，升级到最新版本1.2.58，下载地址：https://github.com/[redacted]/fastjson/releases/tag/1.2.58;
2)方案二：移除 fastjson，如需使用 json 解析库建议使用 gson 或 jackson-databind 等组件最新版本替换。

问题URL列表

序号	影响URL	发现时间
1	http://[redacted]	2019-07-12 22:11:29

5.2.1.1 http://[redacted]

发现时间 2019-07-12 22:11:29

命中详情 "{[redacted]}"

请求详情

[redacted]

响应详情

[redacted]

7.3 如何实现漏洞扫描报告中不展示基线检查结果?

当您将主机的Tomcat、Nginx和Apache都关闭后，漏洞管理服务对该主机不能进行基线检查，生成的漏洞扫描报告中将不展示基线检查结果。

您可以参照基线检查结果的修复建议修复基线漏洞，有关查看漏洞修复建议的详细操作，请参见**如何查看漏洞修复建议?** 。

7.4 漏洞管理服务提供的扫描报告加盖华为公章吗?

漏洞管理服务提供的漏洞扫描报告不可以加盖华为公章。

7.5 为什么不能进行通知设置?

通知设置功能暂时下线整改，不可用。功能下线后，您将不能再进行通知设置。

已经设置通知的用户可以正常接收漏洞管理服务发送的通知消息。若您需要更改接收通知的手机号，请提交工单，由华为云技术支持工程师进行更改。

7.6 漏洞管理服务支持查看并下载英文报告吗?

漏洞管理服务仅网站漏洞扫描、主机扫描功能支持查看并下载英文报告，其他功能如移动应用安全、二进制成分分析、安全监测仅支持查看和下载中文报告。

说明

网站漏洞扫描、主机扫描功能支持查看并下载英文报告，需切换控制台语言为英文后，参考**下载网站扫描报告**、**下载主机扫描报告**进行英文版报告生成和下载。