Nessus 6.3 用户指南

2015 年 03 月 24 日

柯力士信息安全 www.jw-assoc.com

目录

简介

此文档将指导您如何使用 Tenable 网络安全产品—Nessus 的用户界面（UI）”。如果您有任何意见或建议，请发电子邮件至 support@tenable.com.

Nessus 的用户界面（UI）是基于 Web 界面来访问 Nessus 漏洞扫描器的，所以，要使用 Nessus 的用户界面（UI），您就需要部署一个 Nessus 扫描器，并熟练掌握。

标准和规范

整个文档、文件名、守护进程和可执行程序需要使用 Courier 字型的粗体字，如 **gunzip**、 **httpd** 和 **/etc/passwd**。

命令行选项和关键字也要使用 Courier 字型的粗体字。命令行示例可能或不可能包含命令行提示符和命令的结果的输出文本。如下示例：命令行显示命令以 Courier 字型的粗体字正在运行，这表示用户输入的同时系统也会生成，并以 Courier 字型的非粗体字显示。以下是 Unix pwd 命令运行示例：

```
# pwd
/opt/nessus/
#
```

重要说明和注意事项都会以此符号和灰色文本框突显出来。

温馨提示、示例和最佳实践都会以此符号和蓝底白字文本突显出来。

Nessus6.3 新增内容

下列显示官方 Nessus 产品名称：

- Nessus®
- Nessus 家庭版
- Nessus 标准版
- Nessus 管理器
- Nessus 扫描器
- Nessus 企业云
- Nessus 代理

主要更新特点

下列为 Nessus6.3 中相关功能。关于完整的更新列表，请参阅“发行记录”

- 新版授权模式，其中包括 Nessus 的 Windows 代理可运行 Windows 本地检查和合规性扫描。
- 扫描仪表板会显示漏洞和合规概述
- 扫描器可由中央 Nessus 管理器来部署策略、扫描和插件和软件更新

Nessus 用户界面概述

简介

Nessus 的用户界面（UI）是基于 Web 界面来访问 Nessus 漏洞扫描器的，Nessus 扫描器包含一个简单的 HTTP 服务器和 Web 客户端，并且除了 Nessus 服务器无需安装软件，其主要特点是：

- 生成.nessus 文件，此文件为 Tenable 产品使用作为漏洞数据和扫描策略标准。
- 一个策略会话、目标清单和可全部存储在易于导出的独立.nessus 文件中的多次扫描结果。请参阅“Nessus v2 ”指南了解更多详情。
- 扫描目标可使用各种格式：IPv4 / IPv6 地址、主机名和 CIDR 标记。
- 支持 LDAP，这样 Nessus UI 帐户可对远程企业服务器进行身份验证。
- Nessus UI 可实时显示扫描结果，所以您无需等待扫描完成再查看结果。
- 无论基础平台如何，对 Nessus 扫描器提供统一的接口。Mac OS X、Windows 和 Linux 有相同功能。
- 即使 UI 以任何理由被断开，扫描仍会在服务器上继续运行。
- Nessus 的扫描报告可通过 Nessus UI 上传，并与其它报告相比较。
- 扫描仪表板能显示漏洞和合规概述，这样能让您可视化您的扫描历史趋势。
- 策略向导能帮助您快速建立高效的扫描策略，用于审核您的网络。
- 能让您设置一个扫描仪为主扫描仪，让额外的扫描仪为次要扫描仪，从而允许一个独立的 Nessus 界面来管大规模分布式扫描。
- 广泛的用户和分组系统，允许细粒度的资源共享，包括扫描仪、策略、计划和扫描结果。

支持的平台

Nessus UI 是基于 Web 的客户端，所惧它可以在任何一个现代的 Web 浏览器平台上运行。

基于 Web 的 Nessus 用户界面，通常会使用以下浏览器中指定的最低版本：Microsoft Internet Explorer 10、Mozilla Firefox 32、Google Chrome 37、Opera 24 或 Apple Safari 7.1。此外，Nessus 是与 Android 的 Chrome 29，以及 iOS7 浏览器相兼容的。

安装

Nessus 服务器的用户管理只能通过 NessusUI 或安全中心来管理。

请参阅“Nessus 6.3 安装和配置指南”中关于安装 Nessus 的说明。关于在 Linux 系统、Oracle Java（以前称为 Sun Microsystems 的 Java）的 Nessus6.3 是需要基于 Unix 的系统的 PDF 报告功能。

Nessus UI

Nessus 通过 HTTPS 端口 8834 来提供一个用户界面（UI），所以每个用户都会有一个唯一的用户名和密码。要配置的用户，请参阅“Nessus6.3 安装和配置指南”有关配置用户帐户的说明。

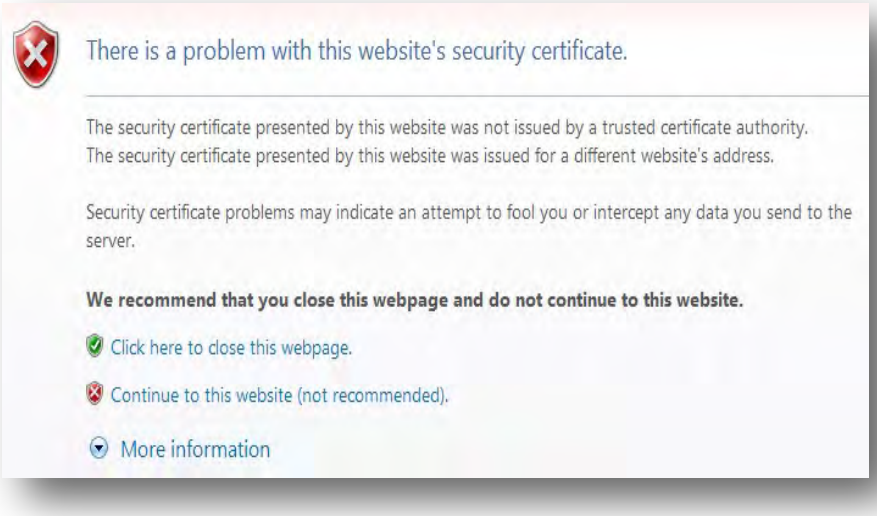
连接到 Nessus UI

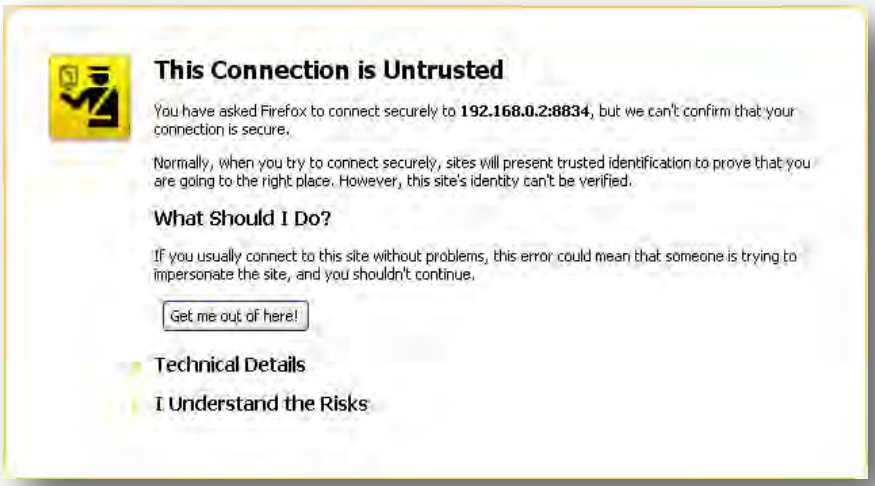
要启动 Nessus UI，执行以下操作：

- 打开您选择的 Web 浏览器。
- 在导航栏中输入：https://[server IP]:8834/

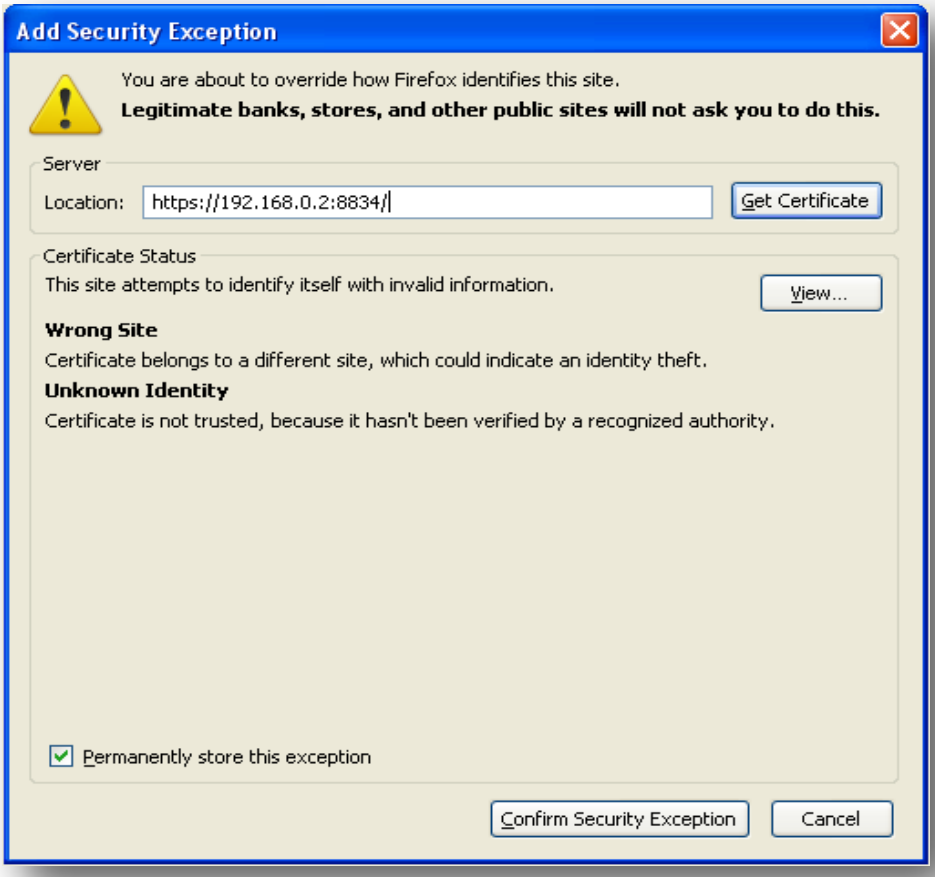
由于不支持加密的 HTTP 连接，所以请确保一定要通过 HTTPS 连接到用户界面

当您第一次尝试连接到 Nessus 的用户界面时， 大多数 Web 浏览器会提示错误，说明本网站不被信任，那是由于 Nessus 的提供自签名证书：



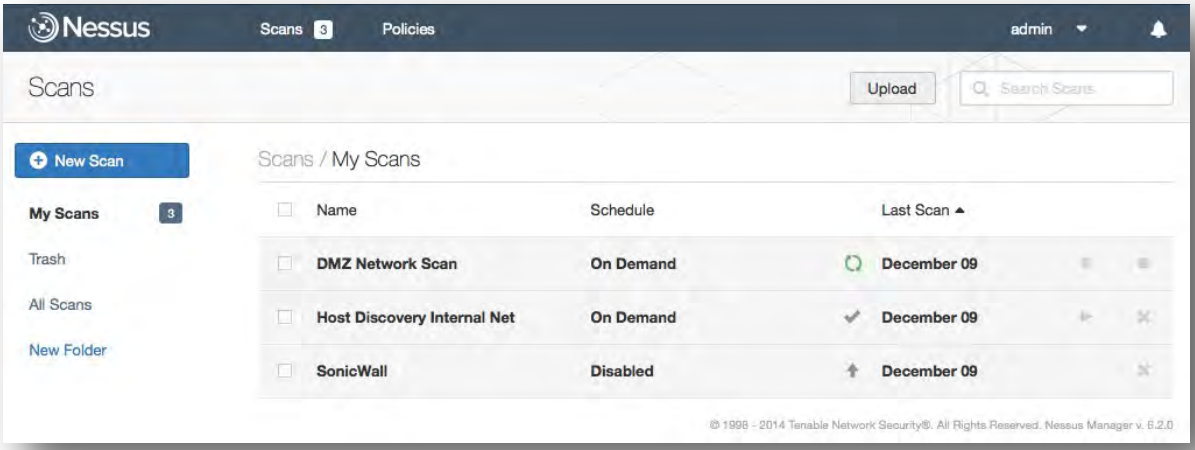


Microsoft Internet Explorer 的用户可以点击“继续浏览此网站（不推荐）”加载 Nessus 用户界面。Firefox 用户可以点击“我了解风险”，然后“添加例外...”，以显示该网站的异常对话框：

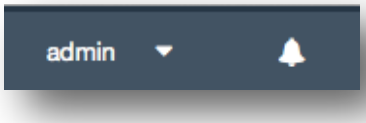


验证“位置”栏会反映 Nessus 的服务器的 URL，请点击“确认安全例外”。关于安装自定义的 SSL 证书的信息，请参阅“Nessus 6.3 安装和配置指南”。

在安装过程中，身份验证请使用之前创建的管理帐户和密码。登陆时，您可以选择让浏览器记住用户名，当然，使用此功能，您必须保证计算机始终处于安全环境中！认证成功后，用户界面会出现管理策略和扫描的菜单。管理员用户能查看用户管理选项和 Nessus 扫描仪配置选项。登陆后，您会进入 UI“Scans”.

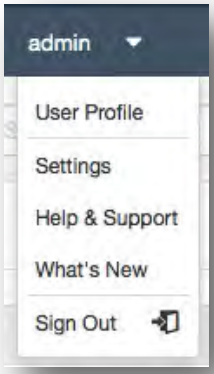


在使用 Nessus 期间，左上方的菜单会一直显示。上方截图中，右上方可查看表示当前登录的帐户的“admin” 、下拉菜单、可快速访问关于操作 Nessus 的重要通知的铃铛图标：

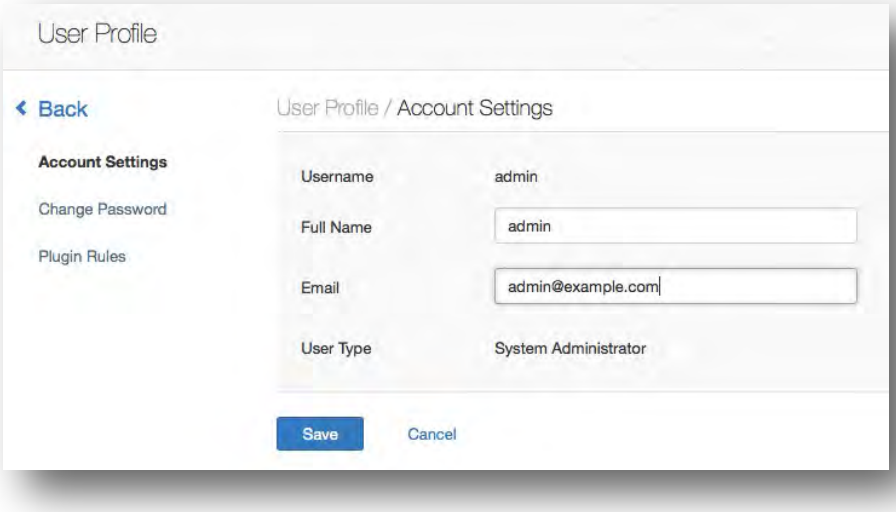


在使用 Nessus 企业云过程中，左上角的菜单选项会显示用户的邮箱地址：

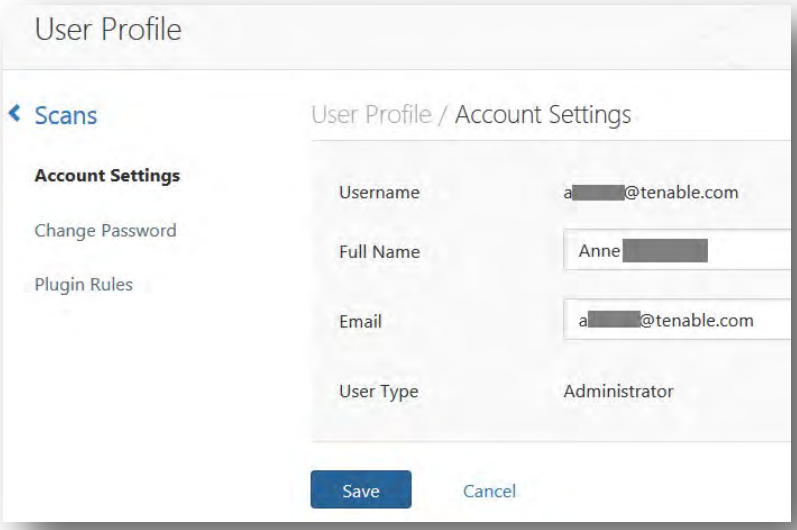
点击下拉箭头可查看用户配置文件、Nessus 常规设置、帮助与支持、最新消息，以及注销。



“用户配置文件”选项，会弹出一个菜单，其中有几项是关于用户帐户的，包括密码更改、文件夹管理、插件规则。关于这些选项的更多信息内容，在下文中您可以看到。

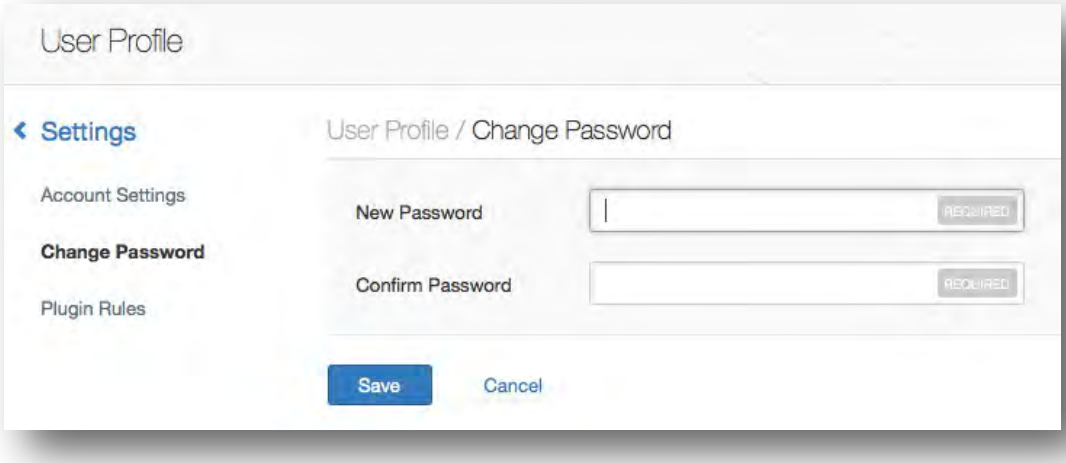


注意：Nessus 的企业云帐号的用户名是用户的注册的电子邮件地址！

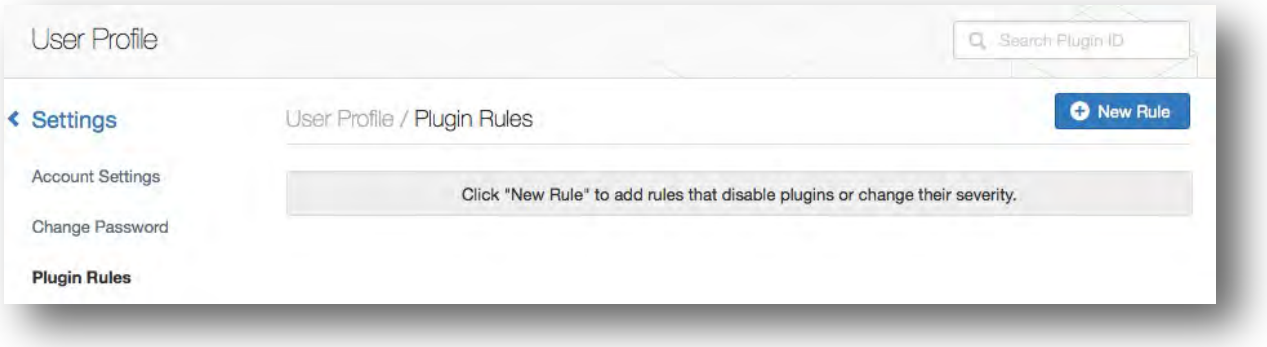


“帐户设置”会显示当前已验证的用户、全名、电子邮箱和用户类型，其中包括：系统管理员、管理员、一般用户或只读用户。点击“用户配置文件”时，显示的是默认信息。

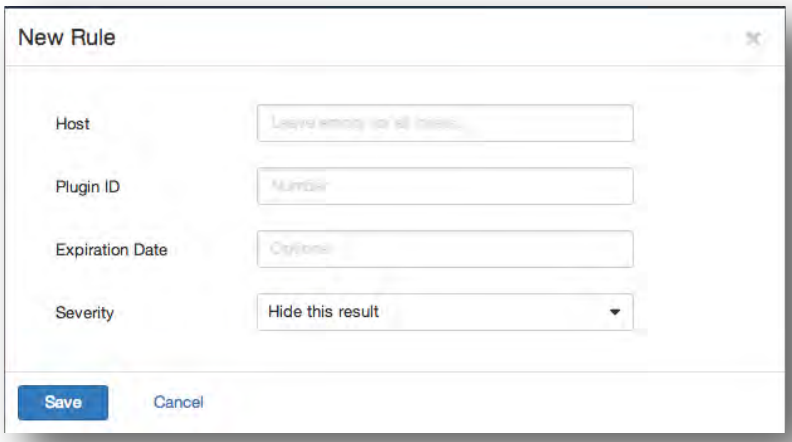
“更改密码”选项允许您更改密码，且您需要按照企业的安全策略来完成。请注意，您需要输入两次密码，以确认您的选择。



您可使用“插件规则”创建一组规则，来指示执行任何扫描的某些插件。规则可以基于主机（或所有主机）、插件 ID、一个可选的截止日期和控制程度。相同的规则可以从扫描结果页面进行设置，这样，您就能重新指定插件的控制程度，以便您更好的考量您企业的安全状态和应急预案。

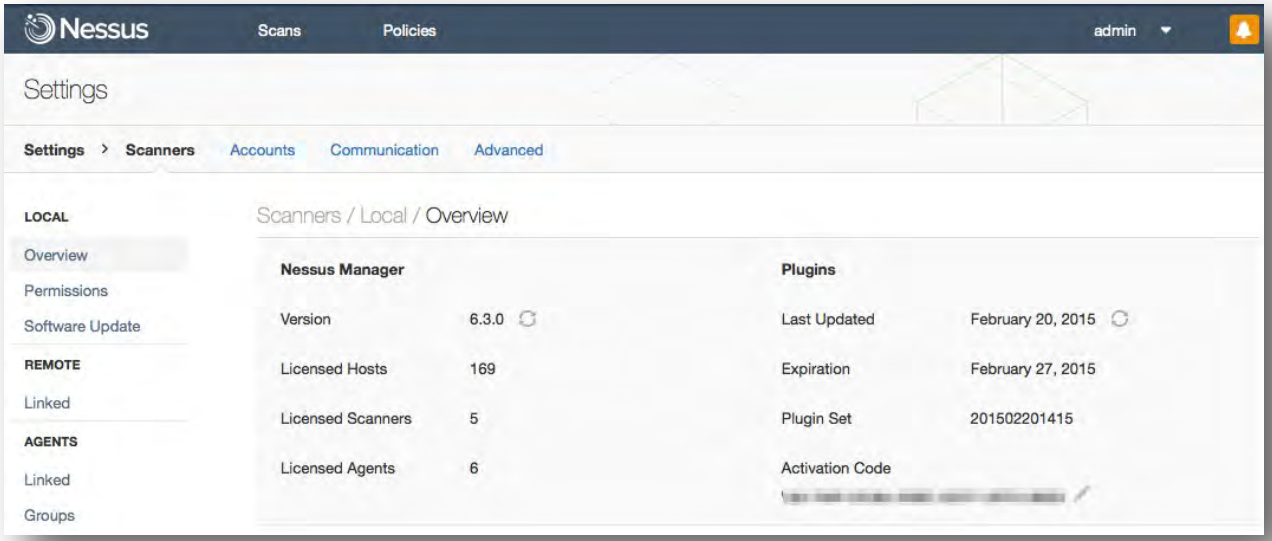


要创建一个新的规则，点击右上角的“**New Rule**”。

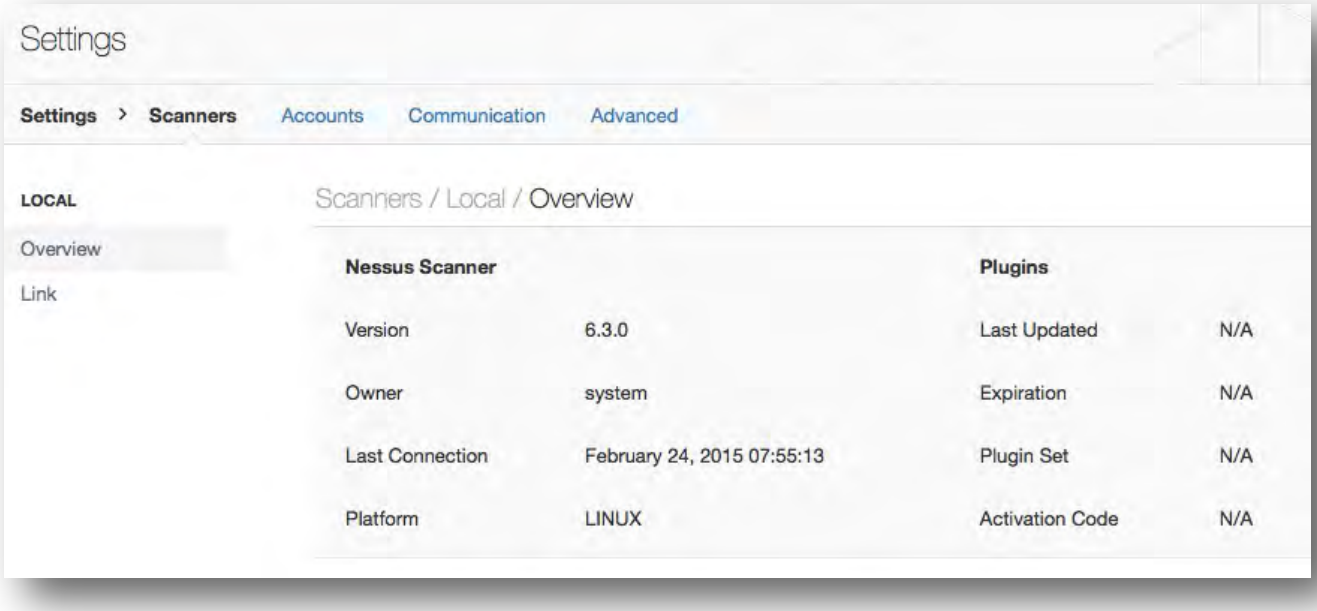


设置

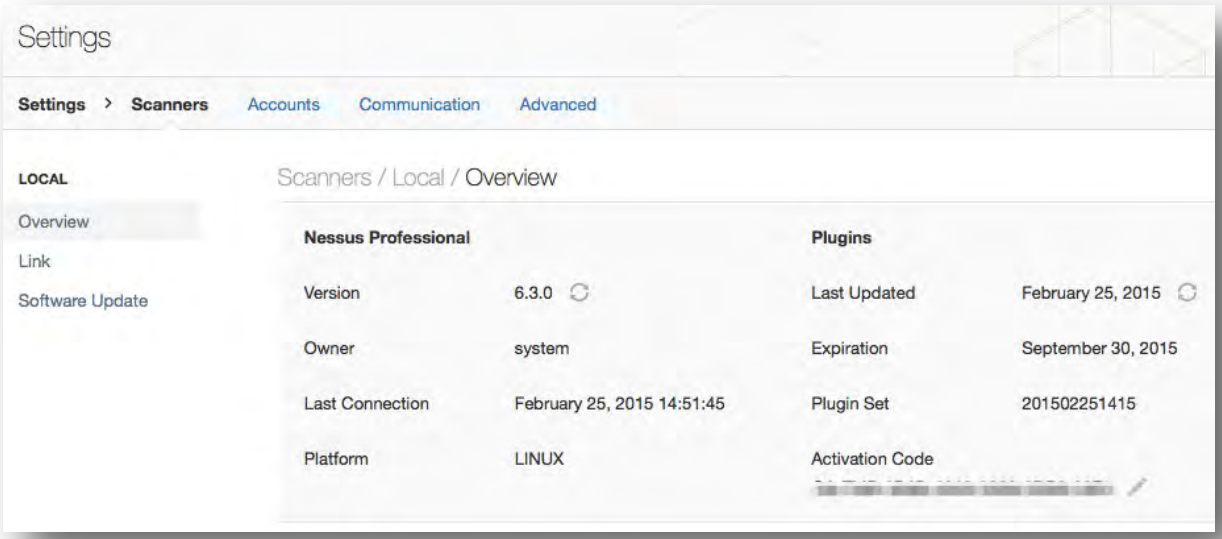
Nessus 管理器中的“**Settings**”，可访问“**Overview**”、帐户、与外部邮件和代理服务器的通信、Nessus 代理、Nessus 扫描器，以及先进的扫描选项（当前用户需要是系统管理员）。有关这些选项的详细信息，可在下文看到。



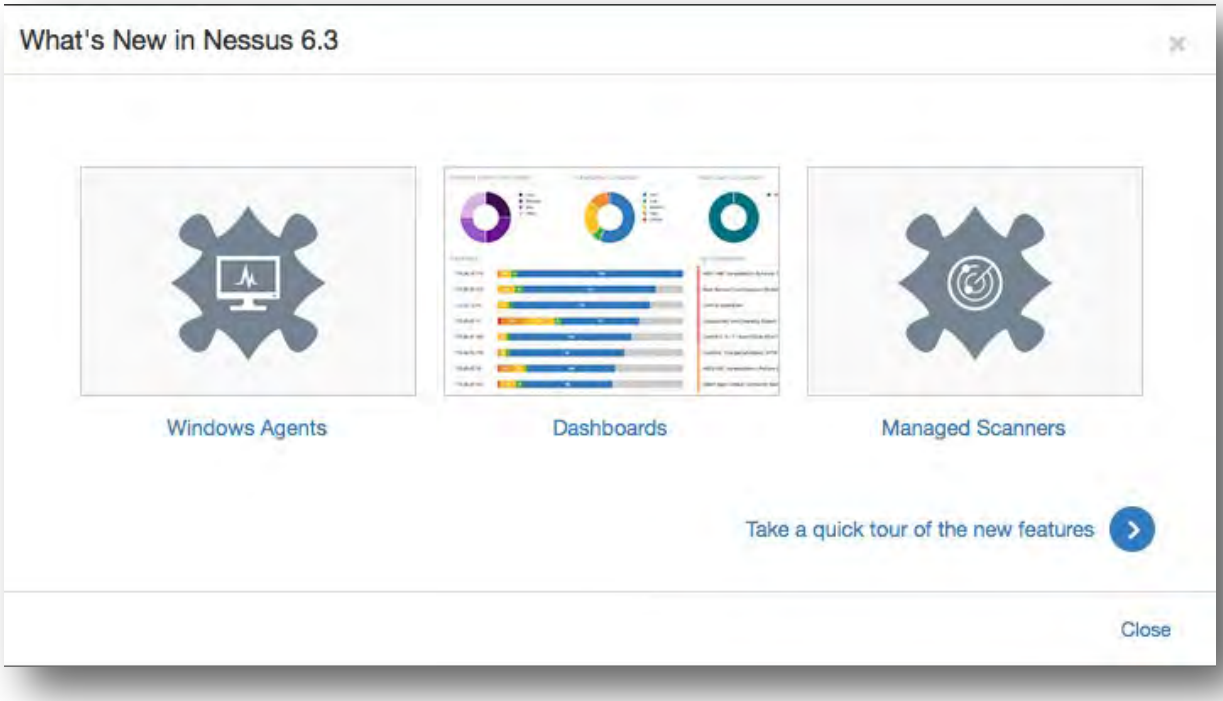
Nessus 扫描器中的“**Settings**”，只可访问“**Overview**”、帐户、与代理服务器的通讯、先进的扫描选项（当前用户需要是系统管理员）。有关这些选项的详细信息，可在下文看到



Nessus 标准版中的“**Settings**”，可访问“**Overview**”、帐户、与外部邮件和代理服务器的通信、先进的扫描选项（当前用户需要是系统管理员）。有关这些选项的详细信息，可在下文看到



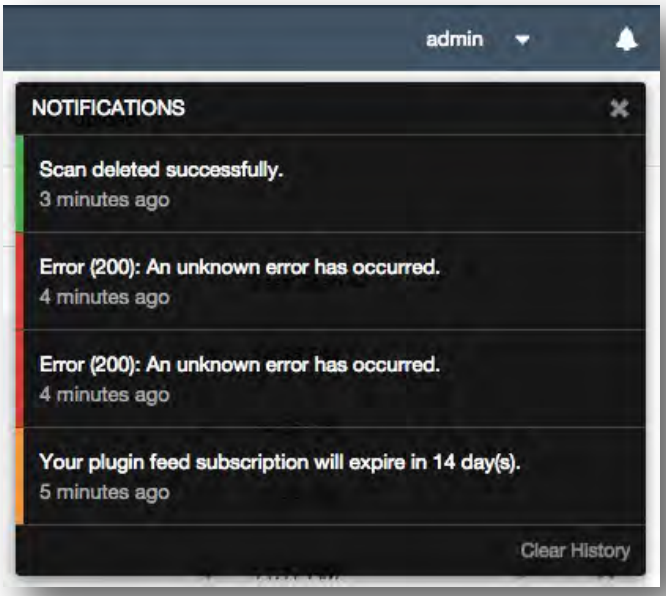
“最新消息”可快速浏览此 Nessus 新版本的新功能。每个选项的更多信息，您可以参考下图，您可以看到 Nessus 新版本的新功能



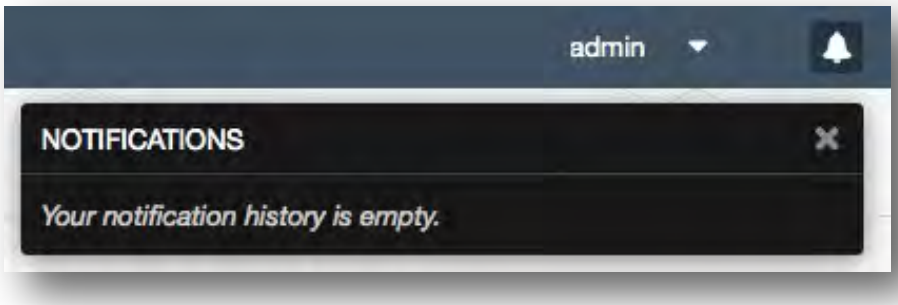
点击“帮助与支持”能在新选项卡或窗口加载 Tenable 支持门户网站。“注销”将终止当前 Nessus 的会话使用。

点击右上角的铃铛图标，可显示 Nessus 操作的任何信息，包括错误、Nessus 的新版本通知、会话事件等等。

出现任何附加的警报或错误，都会弹出窗口显示一会，然后记录会留在历史通知中，除非您将其清除掉：



如果没有通知，该通知将出现一个空的历史信息：



界面快捷键

HTML5 的接口有几种快捷键，不但可快速键盘导航到接口的主要部分，而且还可进行日常活动。这些在任何时候都可用于界面的任何地方。

界面的主要部分中，以下快捷键均可用于导航：

快捷键	描述
R	Scans 扫描
P	Policies 策略
U	Users 用户
C	Settings 设置
G	Groups (Nessus Manager and Nessus Enterprise Cloud only) 组群（权限 Nessus 管理器和
M	User Profile 用户信息

界面的主要部分中，可创建以下快捷键：

快捷键	扫描
Shift + R	New Scan 新建扫描
Shift + F	New Folder (Scan view only) 新建文件夹（仅限扫描查看）

在“扫描”中，以下快捷键可用：

快捷键	描述
N	New Scan 新建扫描

在“策略”中，以下快捷键可用：

快捷键	描述
N	New Policy 新建策略

在“用户”中，以下快捷键可用：

快捷键	描述
N	New User 新建用户

在 Nessus 管理器和 Nessus 企业去的组群中，以下快捷键可用：

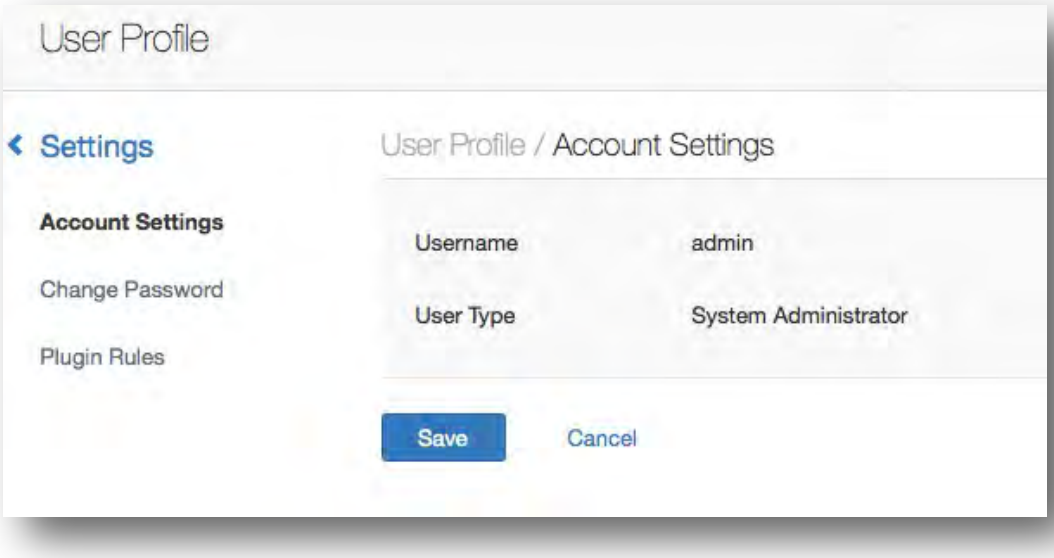
快捷键	描述
N	New User Group 新建组群

在“高级”设置中，以下快捷键可用：

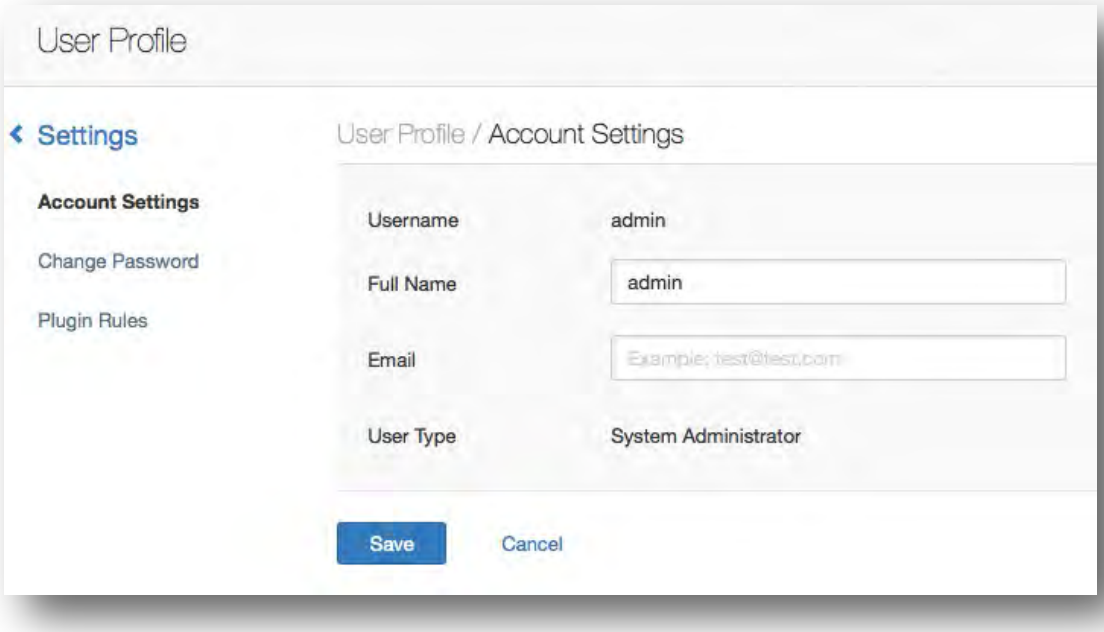
快捷键	描述
N	New Setting 新建设置

用户信息

在用户信息中，您可以对您的帐户进行相关的设置操作。



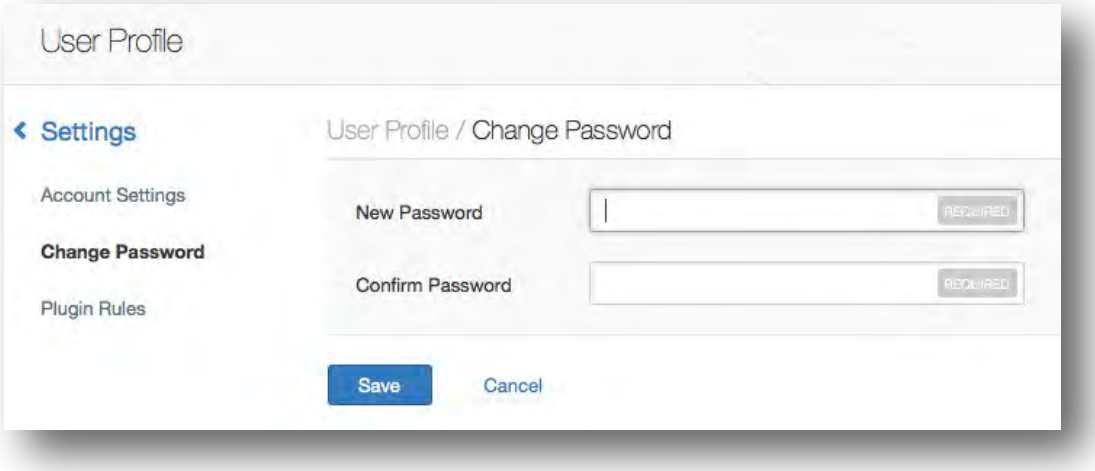
在 Nessus 管理器中，您必需更改您帐户关联的电子邮件地址：



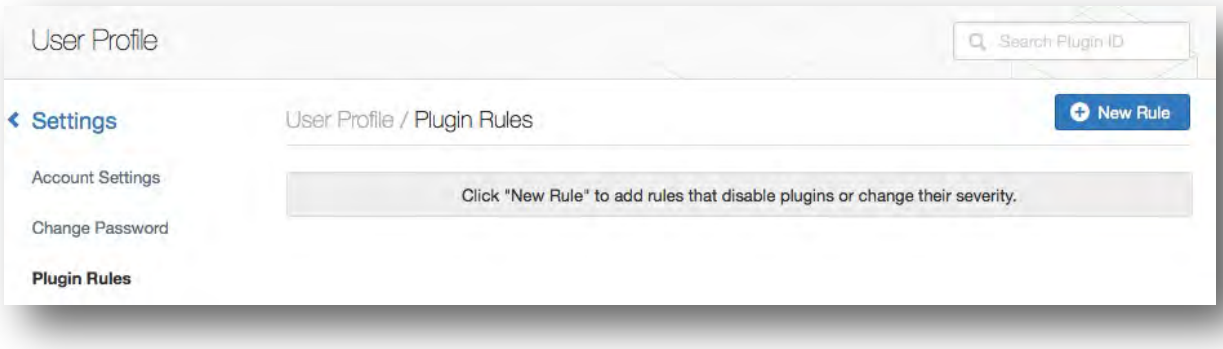
点击用户帐户更改相关帐户的选项。

无论是管理员还是用户，在“帐户设置”中会显示当前认证的用户以及用户类型。点击“用户配置文件”下拉菜单时，这是作为默认信息显示的。

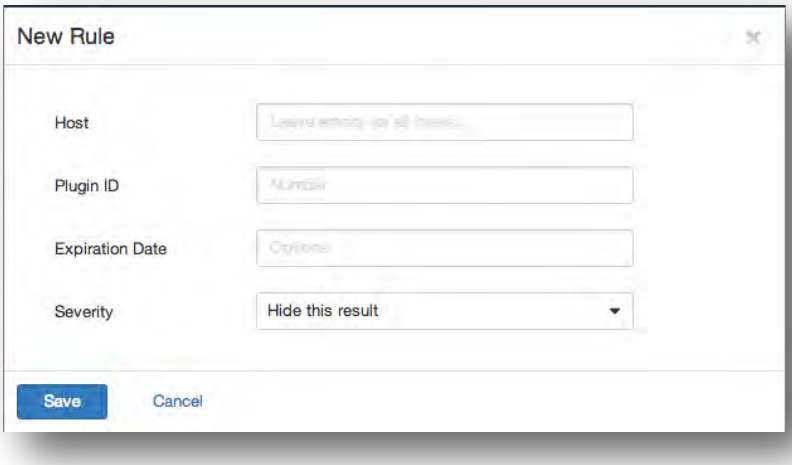
您可以在“更改密码”中更改密码，但您需要按企业的安全策略来更改。注意：您需要输入两次密码来确认您的决定。



您可使用“插件规则”创建一组规则，来指示执行任何扫描的某些插件。规则可以基于主机（或所有主机）、插件 ID、一个可选的截止日期和控制程度。相同的规则可以从扫描结果页面进行设置，这样，您就能重新指定插件的控制程度，以便您更好的考量您企业的安全状态和应急预案。



要创建新规则，请点击右上角的“**New Rule**”



策略

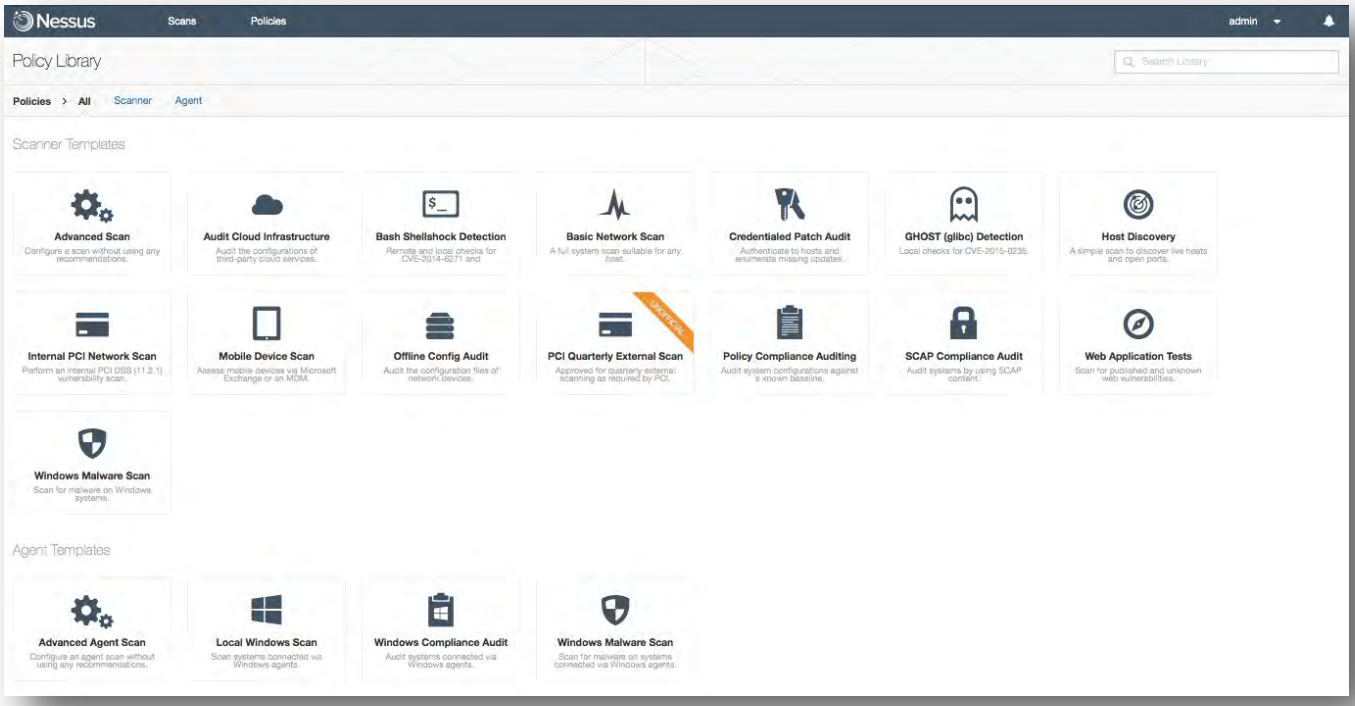
Nessus 策略是一组关于进行漏洞扫描的配置选项。

这些选项包括但不限于：

- 参数：用于控制扫描技术，如超时、主机数量、端口扫描器类型等；
- 本地证书扫描（如 Windows、SSH）：已认证的 Oracle 数据库扫描、HTTP、FTP、POP、IMAP、或基于 Kerberos 的身份验证。
- 细粒度或基于插件的扫描规格。
- 数据库合规策略检查、报告详细程度、服务检测扫描设置、Unix 的合规性检查、更多；
- 网络设备的离线配置审计：允许网络设备的安全检查，而无需直接扫描设备。
- Windows 恶意软件扫描：比较文件的 MD5 校验，同时显示良好和恶意文件。
- Nessus 6.3 将策略分为三类：扫描模板、代理模板、用户创建策略。点击在策略中的“新策略”按钮，会弹出可用的默认模板列表。默认的策略就存储在策略库中，创建于默认模板中的用户创建策略也会被存储。

创建新策略

一旦连接到一个 Nessus UI，您可以点击在顶部菜单栏的“策略”选项，创建一个自定义策略，然后将“新建策略”按键略左移动。策略库将显示如下：



您也可以策略库的右上角的搜索框搜索。

注意：策略的具体列表会根据定期或不定期添加新的策略模板而变化。例如：当“Heartbleed”和“Bash Shellshock”漏洞被披露时，为了用户更方便的使用，配置专门检测这些漏洞的策略，会被添加到列表中。

一种方法是从具有特定用途的模板中创建策略。可用模板会随时间的变化而变化。如：

策略向导名称	描述
Advanced Scan 高级扫描	需要完全控制策略配置的用户的扫描模板
Audit Cloud Infrastructure 审计云基础架构	要审计基于云的服务配置的用户，如 Amazon Web Services (AWS)和 Salesforce.com.

Bash Shellshock Detection Bash Shellshock 检测	Bash Shellshock 漏洞的远程和受信任检查。
Basic Network Scan 基础网络扫描	用于用户扫描内部或外部主机。
Credentialed Patch Audit 审计认证补丁	登录到系统中，并列举缺少的软件更新。
GHOST (glibc) Detection GHOST（glibc）检测	认证检查 GHOST 漏洞。
Host Discovery 主机发现	实时确定主机和开放的端口。
Internal PCI Network Scan 内部 PCI 网络扫描	用于管理员为支付卡行业数据安全标准（PCI DSS）内部网络的合规性审计而准备。
Mobile Device Scan 移动设备扫描	用于用户的苹果的配置文件管理器、ADSI、 MobileIron 或 Good MDM。
Offline Config Audit 离线配置审计	上传和审计网络设备的配置文件。
PCI Quarterly External Scan PCI 季度外部扫描	季度外部扫描 PCI 要求批准的策略。这仅仅是 Nessus 企业云提供
Policy Compliance Auditing 策略合规审计	审计用户提供的一个已知的基准系统配置。
SCAP Compliance Audit SCAP 合规审计	审计系统使用的是安全内容自动化协议（SCAP）的内容。
Web Application Tests Web 应用程序测试	用于用户执行一般的 Web 应用程序扫描
Windows Malware Scan Windows 恶意软件扫描	用于用户搜索 Windows 系统中的恶意软件。

如果您是从 Nessus5.x 升级到 6.3，您在策略库中的任何更改都将被覆盖。从高级模板开始，用户创建的策略将不会受到影响。

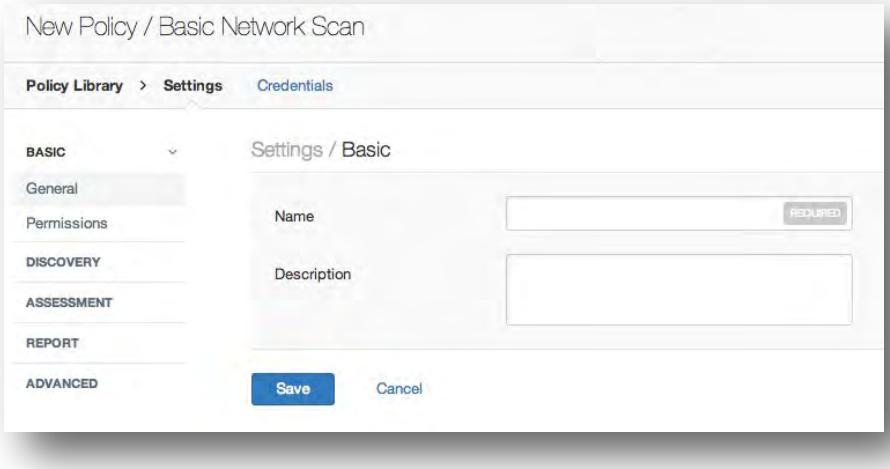
Nessus 代理扫描的模板会在““Nessus Agent Templates””章节中介绍。

策略设置

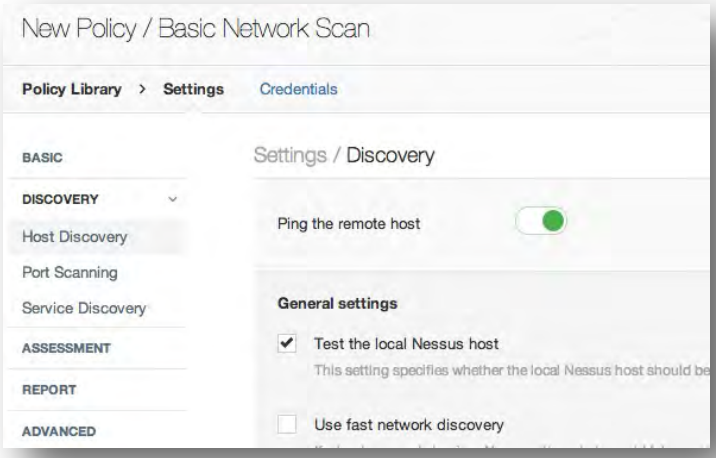
在“设置”中策略分 5 个部分：基础、发现、评估、报告和高级。通过这些部分，您可以优化您的策略设置。

根据所选择的策略模板，不是所有的部分是可配置的。

基础部分包括策略名称、描述和权限。Nessus 提供细粒度的控制策略。策略权限仅限于创建策略的用户（不能访问）或其他用户（可以使用）。

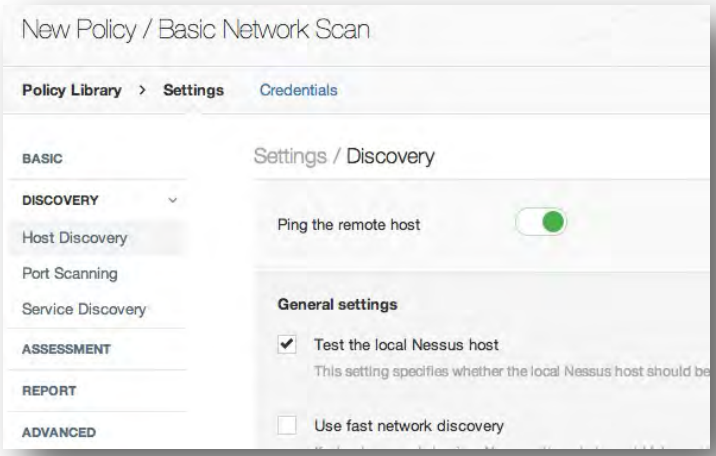


策略的发现部分可设置根据使用的策略进行控制主机发现、端口扫描、服务发现方法。



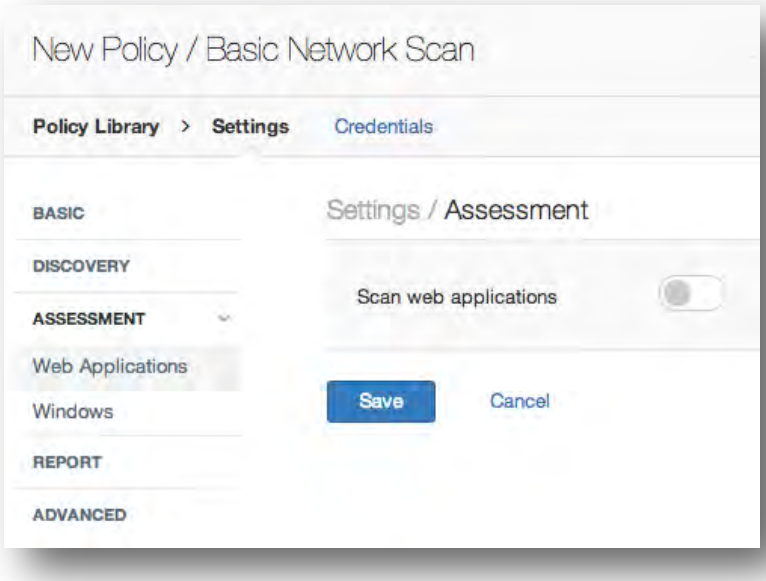
对于主机发现部分，如果未启用“Ping 远程主机”，那么 UI 上就不会看到 Ping 选项。

.根据设置，某些选项可能只在所选择的“自定义”选项中出现。

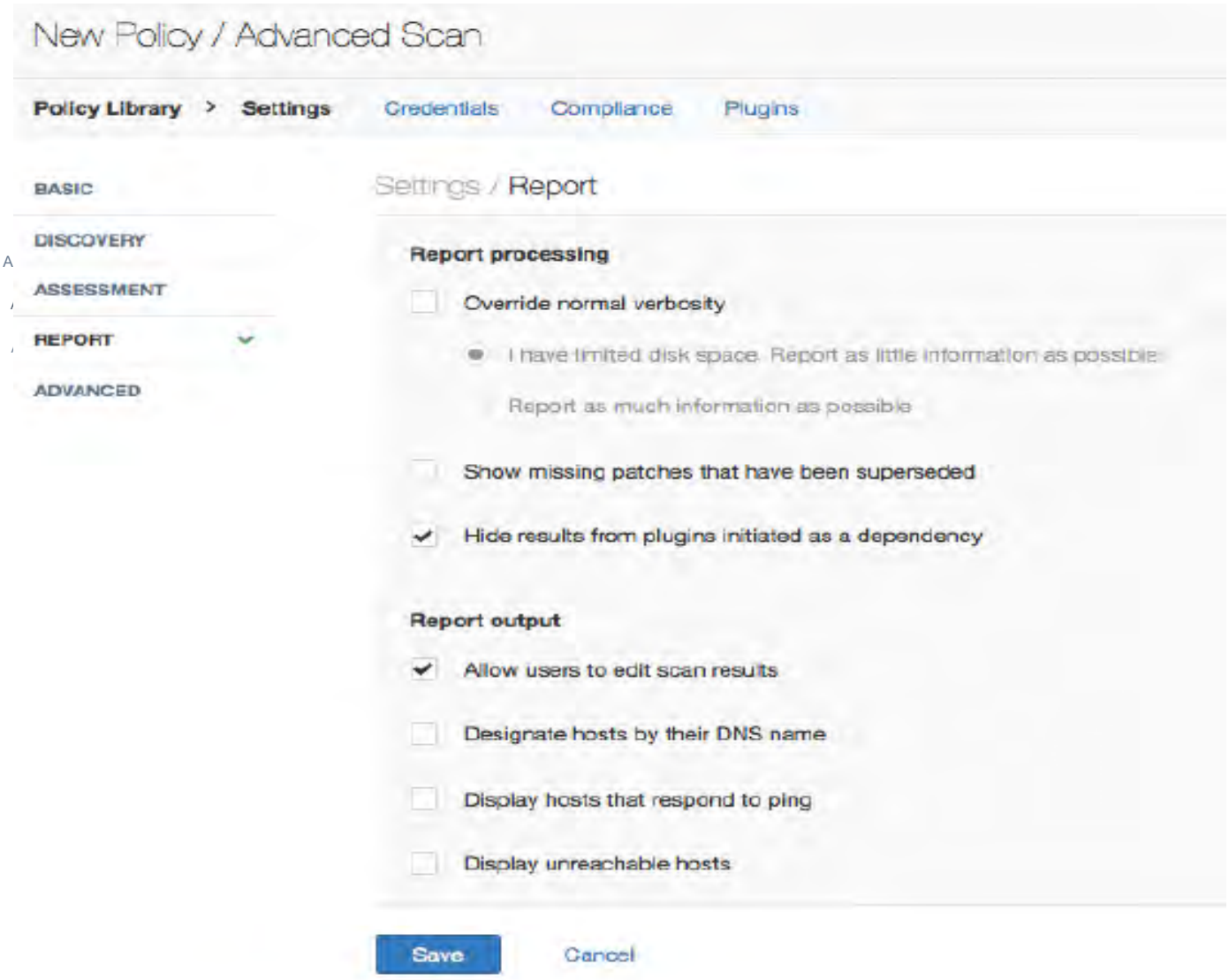


如果必要的话，可以只进行评估部分配置 web 应用程序扫描设置和 SMB 枚举的扫描

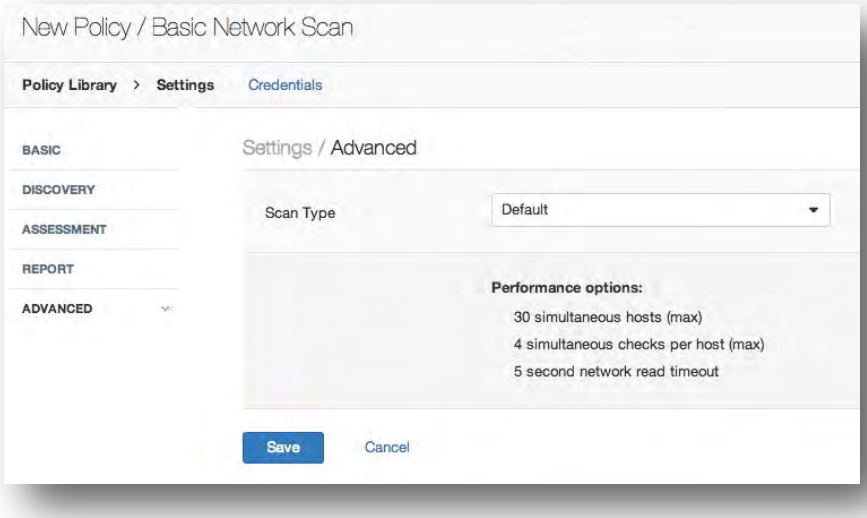
对于部分 Web 应用程序,如果扫描时不启用 Web 应用程序的话，那么部分选项将不可见



无论是否继续进行部分配置 scan 的表层报告,在扫描完成后都可以修改。



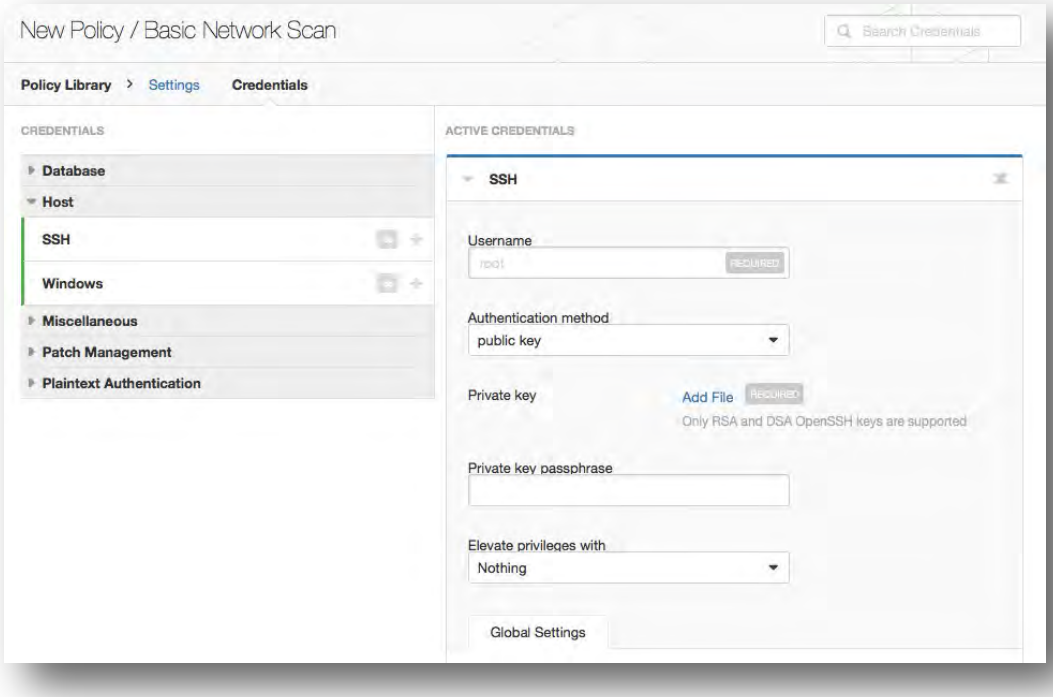
新版本的部分特性：允许配置更多的高级功能,如性能设置,额外设置的扫描检查,和日志记录功能



在高级设置策略的下级目录部分中，可以看到每个设置策略的详细情况

策略认证凭据

Tenable's Nessus scanner 是一种非常有效的检查了大量的各种漏洞的网络漏洞扫描工具，并可以被插件远程利用到综合数据库中。除了远程扫描，Nessus scanner 也可以登录到系统，并直接在主机上检查漏洞。



通过使用凭证,Nessus 可以不需要代理获得本地访问扫描目标系统的权限。这可以实现对一个非常大的网络的进行扫描来确定系统规则触发或违反合规的行为，如上所述,一些步骤创建的规则是可进行选择的。一旦创建,使用过的一些推荐设置将被保存。您可以编辑向导选项或选取保存到本地其他方面的策略

Nessus 支持有几种形式的身份验证，包括但不限于数据库、SSH、窗户、网络设备、补丁管理服务器和各种明文验证协议。例如,Nessus 利用 Unix 登录远程主机的能力，通过 Secure Shell(SSH);和 Windows 主机,Nessus 利用各种各样的微软认证技术来实现。注意,Nessus 还使用简单网络管理协议(SNMP)对路由器和交换机进行版本和信息查询。除了操作系统凭证,Nessus 支持其他形式的本地身份验证。

在 6.3 版本中 Nessus 可以对,以下类型的凭证进行策略管理

云服务，其中包括亚马逊网络服务 （AWS） 和 Salesforce.com

* 包括 MongoDB，PostgreSQL，、 Oracle、 DB2、 MySQL SQL Server 的数据库，

* 主办，其中包括 Windows 登录、 SSH 和 SNMPv3

* 移动设备管理

* 修补程序管理服务器

* 亚马逊 AWS、 VMware、 IBM iSeries，帕洛阿尔托网络泛-OS 和目录服务 （ADSI 和 X.509）

* 纯文本身份验证机制，包括 FTP、 HTTP、 POP3 和其他服务

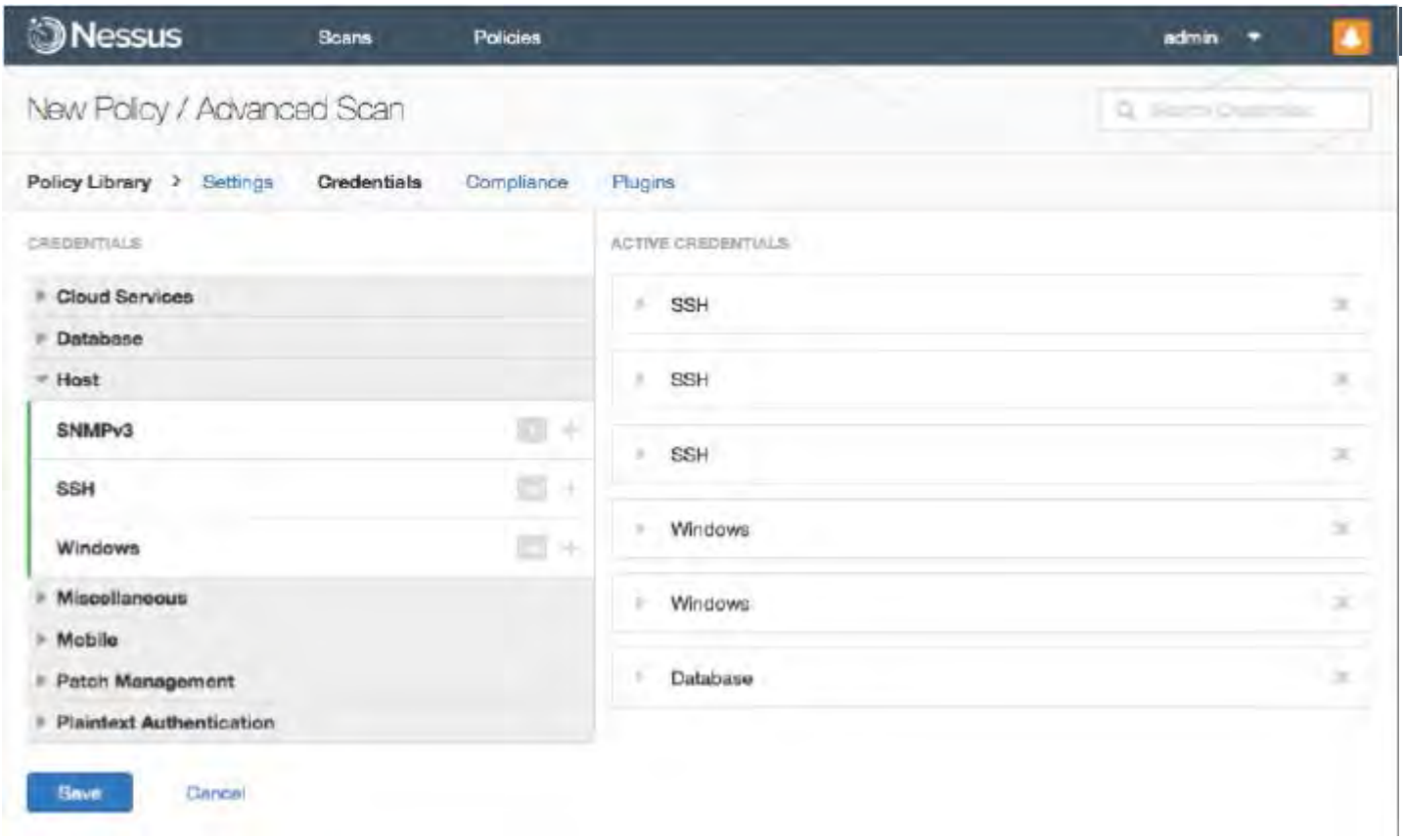
有足够权限的本地用户可以执行任何一个可以执行的权限范围内的扫描操作。扫描的程度依赖于特权授予 Nessus 配置为使用的用户帐户。更多特权扫描仪已经通过登录账户(如。根或管理员访问),更彻底的扫描结果。.

Nessus 允许多个凭证相同的策略。添加凭证,点击添加信息适当的类型的凭证。Nessus 无限制某些类型的凭证,这些在后面都会标明一个无穷大符号“∞”。而其他凭证类型将显示一个数值显示剩余数量的该类型的凭证,可以添加到政策。

“凭证”选项卡,如下图所示,允许您配置 Nessus 扫描仪扫描期间使用身份验证凭证。通过配置凭证,它允许 Nessus 执行更多种类的检查,导致更精确的扫描结果.

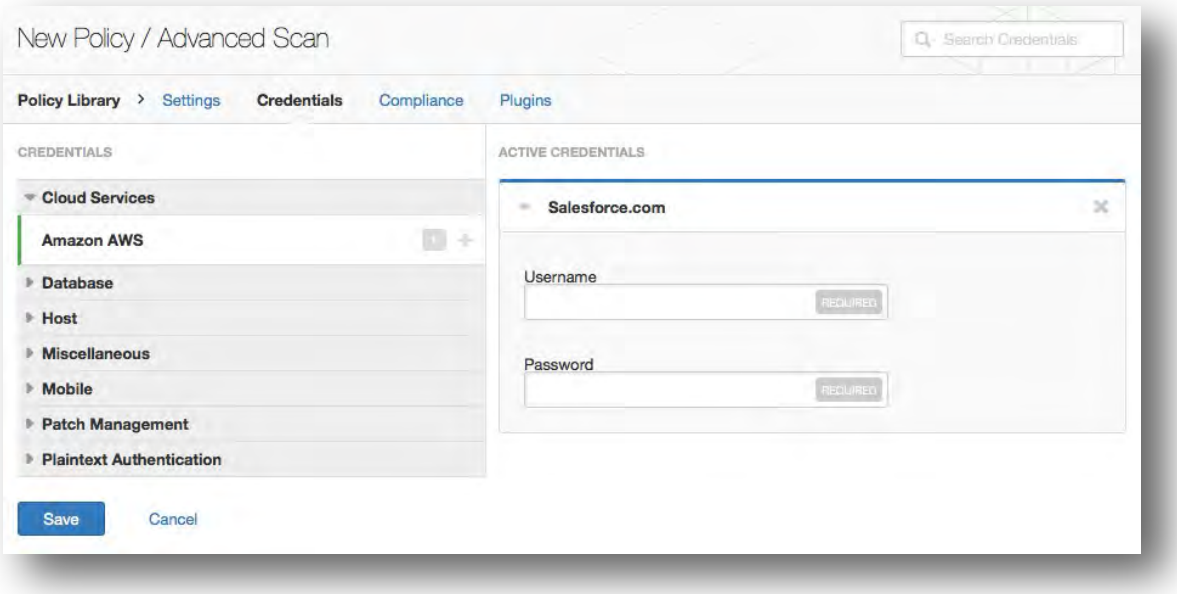
请注意 Nessus 将打开几个并发经过身份验证的连接进行有资格的审计,以确保其及时完成。确保主机被审计单位没有一个严格的帐户锁定策略基于并发会话。.

“凭证”一节在右上角有一个搜索框。如果没有匹配搜索 textthen 没有合规检查会出现在左栏。



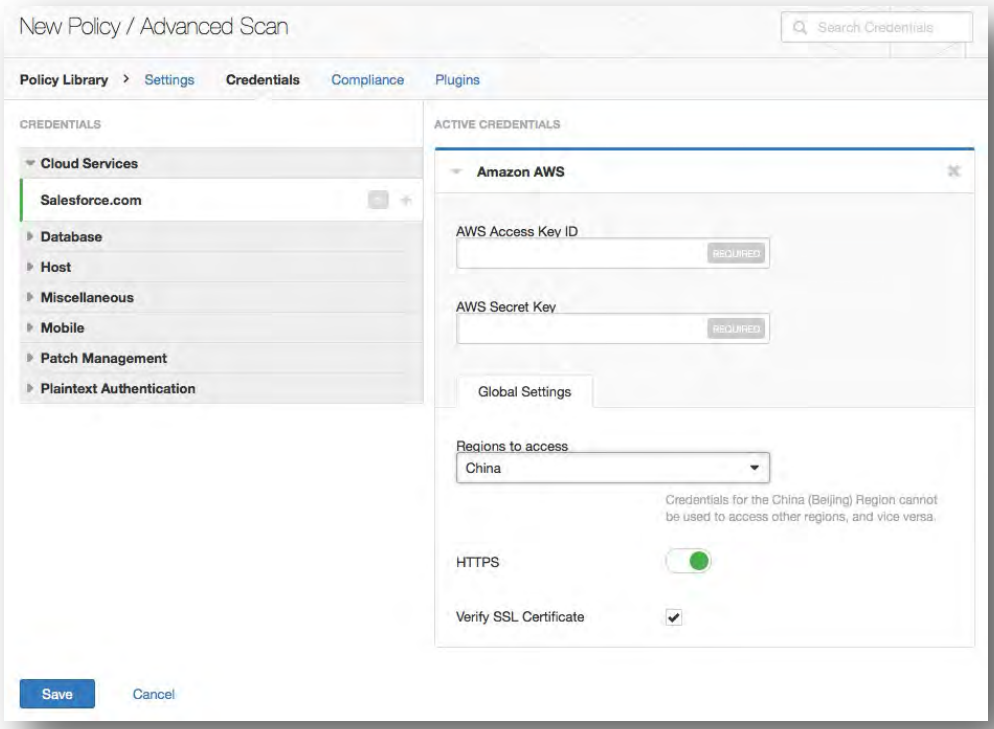
云服务

Nessus 支持两种服务:Amazon AWS 和 Saleforce.com。用户可以从凭证菜单选择“Salesforce.com”。这允许 Nessus 作为指定的用户登录到 Salesforce.com 执行合规审计。



选项	描述
Username	用户需要登录到 Salesforce.com
Password	密码与 Salesforce.com 的用户名

用户可以选择“Amazon AWS”合规审计凭证菜单和输入凭证的 AWS 帐户



选项	描述
AWS Access	AWS 访问密钥 ID 字符串.
AWS Secret Key	AWS 密钥提供身份验证 AWS 访问密钥 ID.

请参阅 Nessus 合规检查文档,在“Amazon AWS 合规能力”一节如何配置正确的权限。

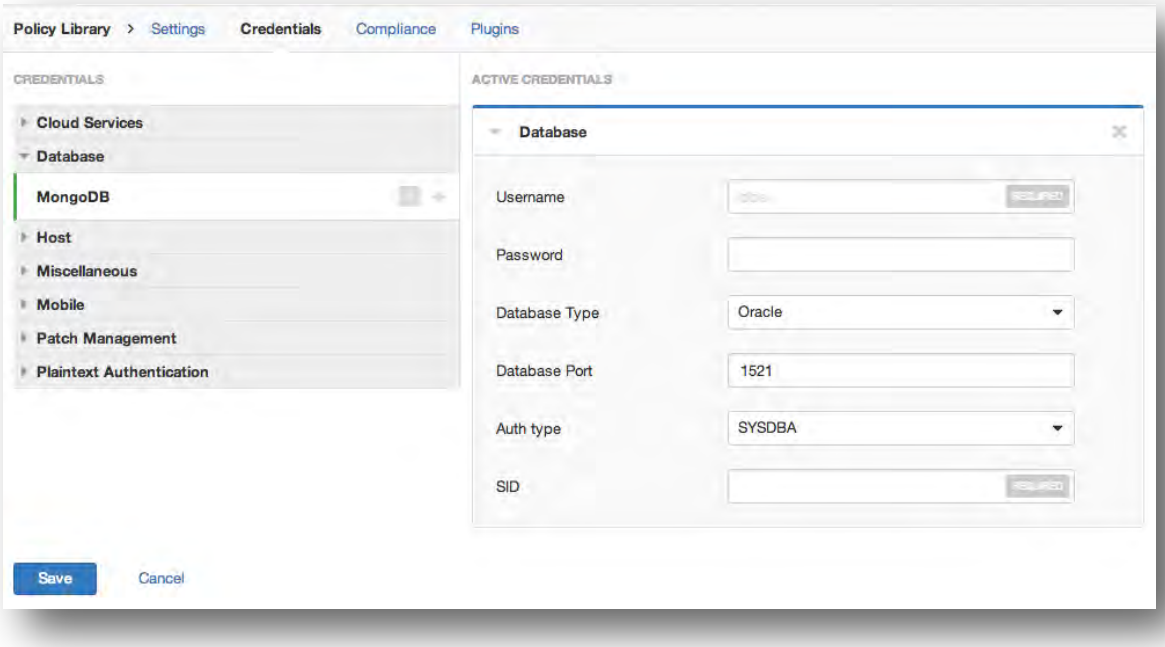
全球 Amazon AWS 设置身份验证

选项	默认	描述
Regions to access	**Rest of the World**	为了让 Nessus 审计一个 Amazon AWS 帐户,您必须定义地区你想扫描。每个亚马逊政策,您将需要不同的凭证审核帐户配置为中国地区比你将剩下的世界。选择世界其他国家将打开以下选择: •us-east-1 •us-west-1 •us-west-2 •eu-west-1 •ap-northeast-1 •ap-southeast-1

		• ap-southeast-2 • sa-east-1 • us-gov-west-1
HTTPS	**Enabled**	使用 HTTPS 访问 Amazon AWS
Verify SSL Certificate	**Enabled**	验证 SSL 数字证书的有效性。

Database

Nessus 支持身份验证和甲骨文,SQL Server,MySQL,DB2,Informix / DRDA PostgreSQL,MongoDB。凭证的所有数据库除了 MongoDB 配置通过添加“数据库”外其余的都可以从数据库凭证类别中找到.



凭据“数据库”菜单用于指定定义凭据,数据库测试的类型,和其他相关设置。

请注意,根据您的选择一些选项将会出现。

数据库用户名和密码

选项	描述
Username	数据库的用户名。
Password	提供的用户名的密码
Database Type	Nessus 支持 Oracle SQL Server, MySQL, DB2, Informix / DRDA 和 PostgreSQL.

对于 Oracle 数据库,您有以下选择.

选项	默认	描述
Database Port	1521	监听数据库端口
Auth Type	SYSDBA	支持 NORMAL, SYSOPER 和 SYSDBA
SID	none	Oracle 系统 ID，鉴别特定数据库

对于 SQL Server,您有以下选择:

选项	默认	描述
Database Port	1433	监听数据库端口
Auth Type	Windows	支持 Windows 认证或 SQL Server 认证
Instance Name	none	用来审计 SQL Server instance 的名称

对于 SQL Server,您有以下选项:

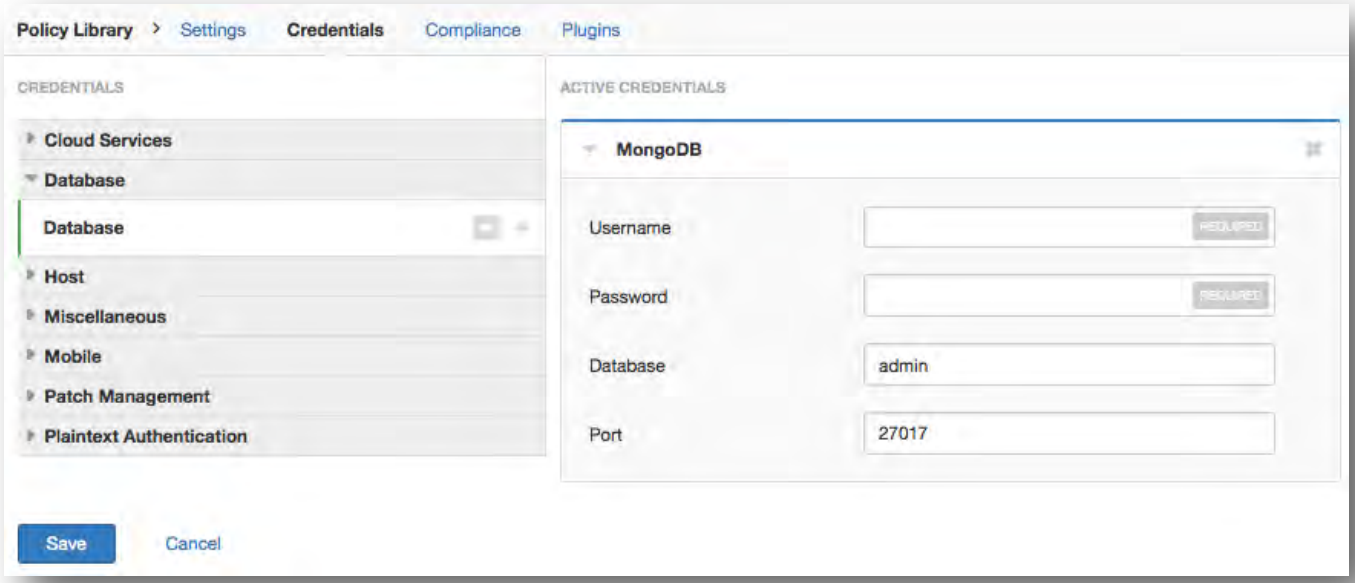
选项	默认	描述
Database Port	3306	监听数据库端口

对于 DB2,您有以下选项:

选项	默认	描述
Database Port	50000	监听数据库端口
Database Name	none	数据库名称，必须项

对于 PostgreSQL,您有以下选择:

选项	默认	描述
Database Port	5432	监听数据库端口



MongoDB"菜单用于指定合规审计 MongoDB 的策略合规:

选项	描述
Username	数据库的用户名
Password	所提供用户的密码
Database	用来审计的数据库名
Port	监听数据库端口

Host

Nessus 支持三种形式的主机认证:窗户,Secure Shell(SSH),SNMPv3。

Windows

"Windows 凭据"菜单项设置为 Nessus 提供信息,如 SMB 帐户名称,密码和域名。Nessus 支持基于 windows 系统的几种不同类型的身份验证方法:

- Lanman 身份验证方法普遍在 Windows NT 和 Windows 2000 服务器部署;早期是保留的向后兼容性。
- NTLM 身份验证方法,介绍了 Windows NT,提供了改进的安全性 Lanman 身份验证。NTLMv2 增强版,比 NTLM 密码地更安全,是默认选择的身份验证方法 Nessus 当试图登录到 Windows 服务器。NTLMv2 可以利用"SMB 签名"。

- SMB 是一个可以应用于所有 SMB 流量和 Windows 服务器签名密码校验和。许多系统管理员都启用这个特性在他们的服务器上,以确保远程用户 100%的认证和域的一部分。此外,确保执行策略,规定使用强密码,不能轻易通过字典攻击工具像 John the ripper 和 LOphtCrack 打破。这个策略是自动使用 Nessus 远程 Windows 服务器所需的。请注意,有许多不同类型的攻击利用 Windows 安全非法“散列”从电脑来重点攻击服务器。“SMB 签名”增加了一层的安全防御以防止这些中间人攻击。

- SPNEGO(简单和保护协商)协议提供单点登录(SSO)功能从一个 Windows 客户端各种保护资源通过用户的 Windows 登录凭证。Nessus 支持使用 SPNEGO 用 NTLMSSP LMv2 身份验证或 Kerberos 和 RC4 加密。SPNEGO 认证发生通过 NTLM 或 Kerberos 身份验证,没有什么需要配置 Nessus 政策。

- 如果一个扩展安全方案(例如 Kerberos 或 SPNEGO)不支持或失败,Nessus 将试图通过 NTLMSSP / LMv2 身份验证登录。如果失败,Nessus 将尝试使用 NTLM 身份验证登录。

- Nessus 还支持 Windows 域使用 Kerberos 身份验证。配置,Kerberos 域控制器的 IP 地址。(实际上,Windows Active Directory Server)必须提供。

服务器消息块(SMB)是一个文件共享协议,允许计算机通过网络分享信息。提供了这些信息 Nessus 将允许它从一个远程 Windows 主机调用发现本地信息。例如,使用凭证允许 Nessus 确定重要的应用了安全补丁。没有必要修改其他 SMB 参数默认设置。

SMB 域字段是可选的,Nessus 将能够在没有这个字段域凭据。用户名、密码和可选域指帐户的情况下登录,,发现到目标机器。“joesmith”

例如,给定一个用户名和密码的“my4x4mpl3”,一个 Windows 服务器首先查找此用户名在本地系统的用户列表,然后确定是否它是一个域的一部分。

虚拟凭证使用,Nessus 可以保持登录状态到 Windows 服务器中，但须使用以下组合:

- “Administrator” 无密码
- 一个随机测试 gust 账户用户名和密码
- 没有用户名和密码的测试空连接

所需的实际域名只是如果一个帐户名称是不同的域,在电脑上。完全有可能有一个“管理员”账户在 Windows 服务器和域内。在这种情况下,登录到本地服务器,用户名“管理员”使用该帐户的密码。登录到域,“管理员”用户名也被使用,但随着域密码和域的名称。

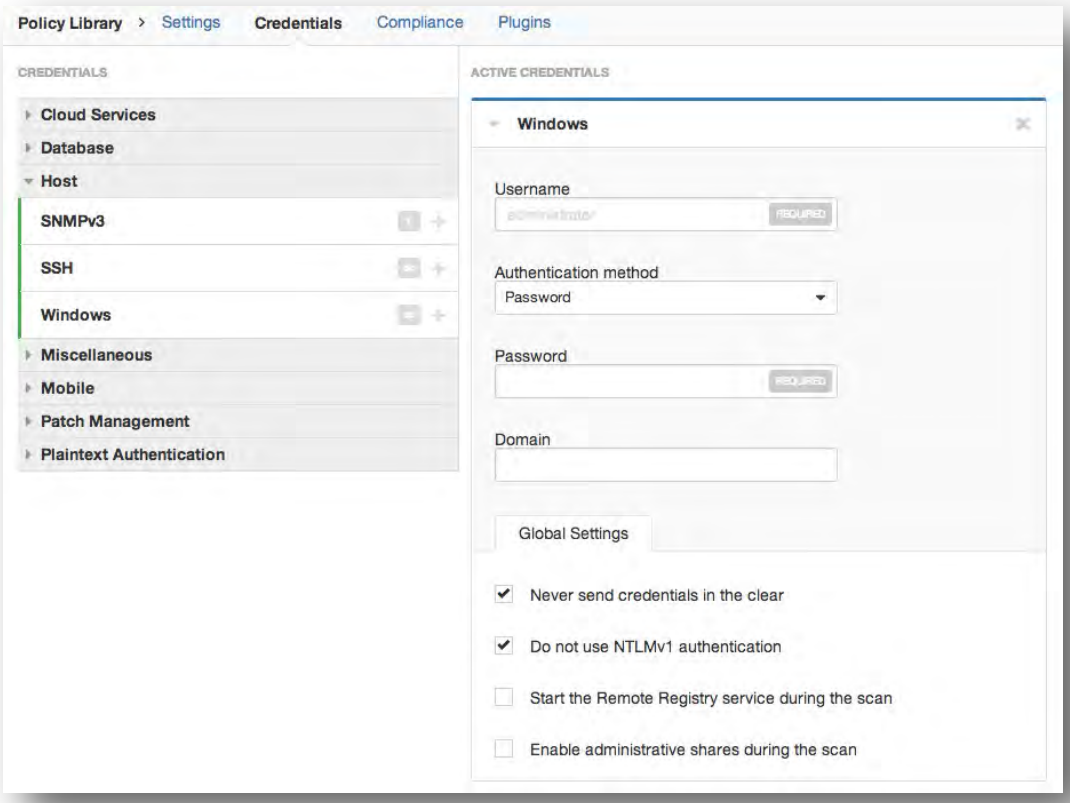
当多个 SMB 账户进行了配置,Nessus 将尝试确定登录顺序与提供的凭证。一旦 Nessus 能够验证一系列的证书,它会检查后续提供的凭证,但只有使用它们时管理权限才会授予之前的账户提供用户访问。有些版本的 Windows 允许您创建一个新的账户,将它指定为一个“管理员”。这些帐户并不总是适合实现受到信任扫描。tenable 的建议是将原办理账户,命名为“管理员”,这样使用这个账户来进行信任扫描,和完全访问是可以确保运行的。在一些版本的 Windows,这个帐户可能被隐藏。使用真正的管理员帐户运行 DOS 提示符可以开除行政特权和输入以下命令可以打开:

```
C:\> net user administrator /active:yes
```

如果 SMB 帐户创建管理员权限有限,那么 Nessus 可以很容易地和安全地扫描多个域。tenable 建议网络管理员创建特定的域账户，以便进行测试。如果提供了域帐户，Nessus 可以对 Windows Vista、Windows 7,Windows 8,Windows 2008,Windows 2008 R2,Windows 2012,Windows 2012 R2 进行更准确的安全检查。如果没有提供账户，nessus 只能尝试进行几个检查在。

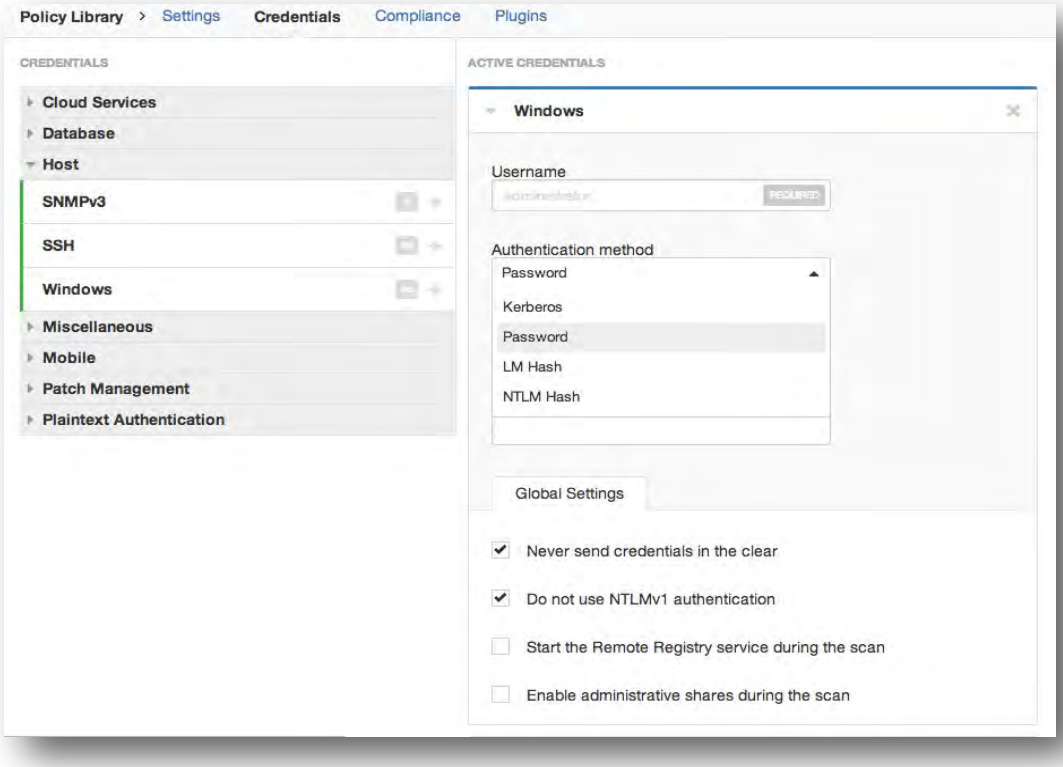
Windows 远程注册表服务允许远程计算机的凭证访问计算机的注册表时被审计。如果审计服务没有运行,是无法阅读从注册表键和值的,即使有完整的凭证。请参阅 tenable 的博客名为“动态远程注册表审计”的更多信息。但是该服务必须启动 Nessus 受到信任扫描完全审计系统的使用凭证。

在 Windows 系统中进行扫描需要一个完整的管理员账户使用等级。没有管理员权限的话，几个公告和微软软件更新的读取注册表来确定软件补丁级别是否可靠,但不是全部。Nessus 插件将提供凭证检查完全管理权限,以确保他们正确地执行。例如,完整的管理访问执行直读所需的文件系统。这允许 Nessus 附加到计算机和执行直接文件分析来确定真正的补丁级别的系统评价.



还有四个全局设置 Windows 凭据:

选项	默认	描述
Never send credentials in the clear	Enabled	出于安全原因，Windows 凭证默认不以明文发送
Do not use NTLMv1 authentication	Enabled	如果“Do not use NTLMv1 authentication”选项是关闭的，那么理论上它可能欺骗 Nessus 试图通过 NTLMv1 域凭证登陆 Windows 服务器。这提供了远程攻击者有能力使用来自 Nessus 的“hash”。这个“hash”能潜在地破解，泄露用户名或密码。这能够直接登陆服务器。通过打开扫描时的“Only use NTLMv2”强制 Nessus 使用 NTLMv2。这阻止了恶意 Windows 服务器使用 NTLM 和接受“hash”。 因为 NTLMv1 是不安全的协议，这个选项默认打开。
Start the Remote Registry service during the scan	Disabled	这个选项告诉 Nessus 启动被扫描计算机上的远程注册服务，如果它不在运行中。为了执行某些 Windows 本地检查插件，此服务必须运行
Enable administrative shares during the scan	Disabled	这个选项会允许 Nessus 访问能被管理员特选读取的注册项



windows 设置 Kerberos 身份验证方法

选项	默认	描述
Password	**none**	和其他凭证方法类似，这是目标系统上的用户密码。这是必须项
Key Distribution Center (KDC)	**none**	这主机提供用户会话工单。这是必须项。
KDC Port	**88**	如果 KDC 是跑在非 88 端口上，这个选项能直接设置 Nessus 连接上 KDC。
KDC Transport	**TCP**	注意如果你需要改变 KDC 传输值，你可能需要根据实施情况改变端口为 KDC 使用的 UDP 端口，认默 88 或者 750。
Domain	**none**	KDC 的 Windows 域管理。这是必选项。

有关如何设置 Windows 系统为当地检查,见“附录 a -建立信任的检查在 Windows 平台上”。

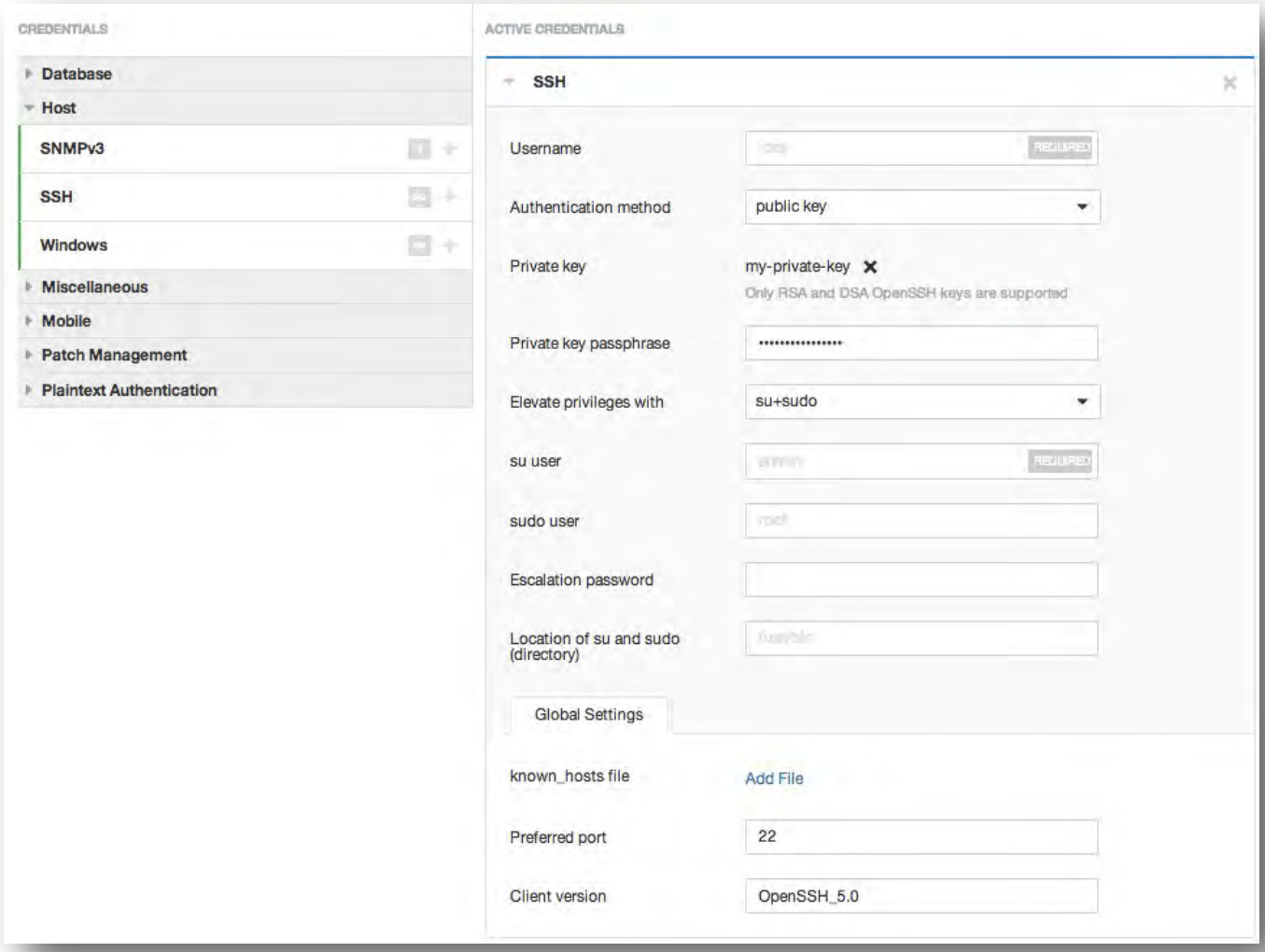
Unix

在 Unix 系统中,支持网络设备,Nessus 使用安全 Shell(SSH)协议版本 2 基于项目(如。OpenSSH,Solaris SSH 等)基于主机的检查。这种机制加密数据在运输过程中保护它免受被嗅探器程序。Nessus 支持使用 SSH 的四种类型的身份验证方法:用户名和密码,公钥/私钥,数字证书和 Kerberos。

用户可以选择“SSH 设置”菜单和输入扫描 Unix 系统的凭证凭证。这些凭证是用来获得本地信息远程 Unix 系统补丁审计和遵从性检查。有一个字段用于输入 SSH 用户帐户的名称,将执行检查目标 Unix 系统,以及 SSH 密码,SSH 公钥和私钥对,OpenSSH RSA 和 DSA 数字证书,或 Kerberos 身份验证。还有一个字段用于输入 SSH 密钥的密码或数字证书,如果这样做是有必要的.

非特权用户与本地访问在 Unix 系统中可以确定基本的安全问题,如补丁级别或/etc/passwd 文件中的条目。更全面的信息,如系统配置数据或文件权限在整个系统中,一个与“根”权限的账号是必需的.

下面的屏幕截图显示了可用的 SSH 选项。“提升特权与“拉提供了一些方法增加权限认证



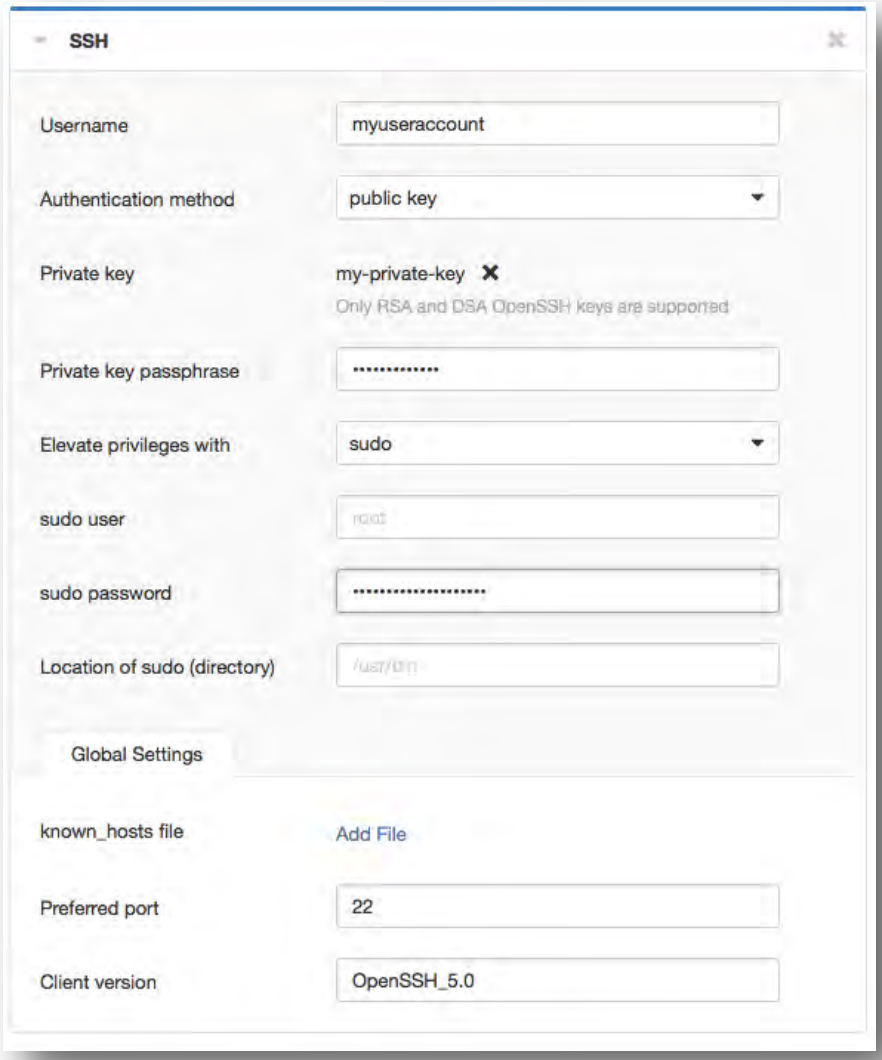
公钥加密,也称为非对称密钥加密,提供了一个更安全的身份验证机制,使用公共和私人密钥对。非对称加密的公钥用于加密数据和私钥用于解密。使用公钥和私钥是 SSH 身份验证更安全的和灵活的方法。Nessus 支持 DSA 和 RSA 密钥格式.

如公共密钥加密,Nessus 支持 RSA 和 DSA OpenSSH 证书。此外 Nessus 进行扫描还需要用户证书,签署的证书颁发机构(CA)和用户的私钥.

Nessus 支持OpenSSH SSH 公钥的格式。从其他 SSH 应用程序格式,包括腻子和 SSH 通信安全,但必须转换为 OpenSSH 公钥格式.

最有效的信任扫描时提供的凭证有“root”的权限。因为很多网站不允许远程登录如 root,Nessus 可以调用“su”、“sudo”、“su+ sudo”、“dzdo”、“。k5login”,或“pbrun”与一个单独的帐户密码,成立了“su”或“sudo”特权。此外,Nessus 可以升级特权思科设备上通过选择“思科启用”或“。k5login Kerberos 登录”。SSH Kerberos 身份验证后在本节中覆盖

下图演示了配置“sudo”结合 SSH 密钥。对于这个示例,用户帐户“审计”,它已被添加到/etc/sudoers 文件系统扫描。提供的密码是“审计”账户的密码,而不是根密码。SSH 键与键生成的“审计”账户:



Nessus 支持 blowfish-cbc aes-cbc 和 aes-ctr 密码算法。一些商业变异的 SSH 没有支持河豚算法,可能原因出口。还可以一个 SSH 服务器配置为只接受某些类型的加密。检查您的 SSH 服务器,以确保正确的算法支持。

Nessus 加密所有密码并存储在策略中。然而,使用的是 SSH 密钥身份验证,而不是 SSH 密码建议。这有助于确保您正在使用相同的用户名和密码审计不使用已知的 SSH 服务器试图登录到一个系统,可能不会在你的控制之下的。

对于网络设备支持,Nessus 将只支持 SSH 连接的网络设备的用户名和密码

如果一个帐户以外的根必须用于特权升级,它可以指定“升级账户”下的“升级密码”.

也有三个全局设置 SSH 凭证:

选项	默认	描述
known_hosts file	none	如果 SSH known_hosts 文件是可达的，且已被提供为扫描策略 Global Settings 的一部分，Nessus 仅尝试登陆这个文件的主机。这个能保证你用来审计 SSH 服务器的用户名密码不在不可控范围内被用来尝试登陆系统。
Preferred port	22	如果 SSH 跑在非 22 端口上，这个选项能直接设置 Nessus 连上 SSH
Client version	OpenSSH_5.0	指定 Nessus 在扫描中模仿哪个 SSH 客户端类型

Kerberos,由麻省理工学院开发的雅典娜项目,是一个客户机/服务器应用程序,使用对称密钥加密协议。对称加密的密钥用于加密数据的密钥用于解密数据。组织部署一个 KDC(密钥分发中心),包含了所有需要 Kerberos 身份验证的用户和服务。Kerberos 用户进行身份验证的请求一个 TGT(票据授予票)。一旦用户被授予一个 TGT,它可以用来从 KDC 请求服务票证能够利用其他 Kerberos 基础服务。Kerberos 使用 CBC(密码块链)DES 加密协议来加密所有通信。

请注意,您必须已经有一个 Kerberos 环境建立了使用这种方法的验证。

Nessus 实现的基于 unix 的 Kerberos 身份验证 SSH 支持“aes-cbc”和“aes-ctr”加密算法。Nessus 与 Kerberos 如何概述如下:

最终用户为 KDC 的 IP

nessusd 问 sshd 如果它支持 Kerberos 身份验证

sshd 确定可行

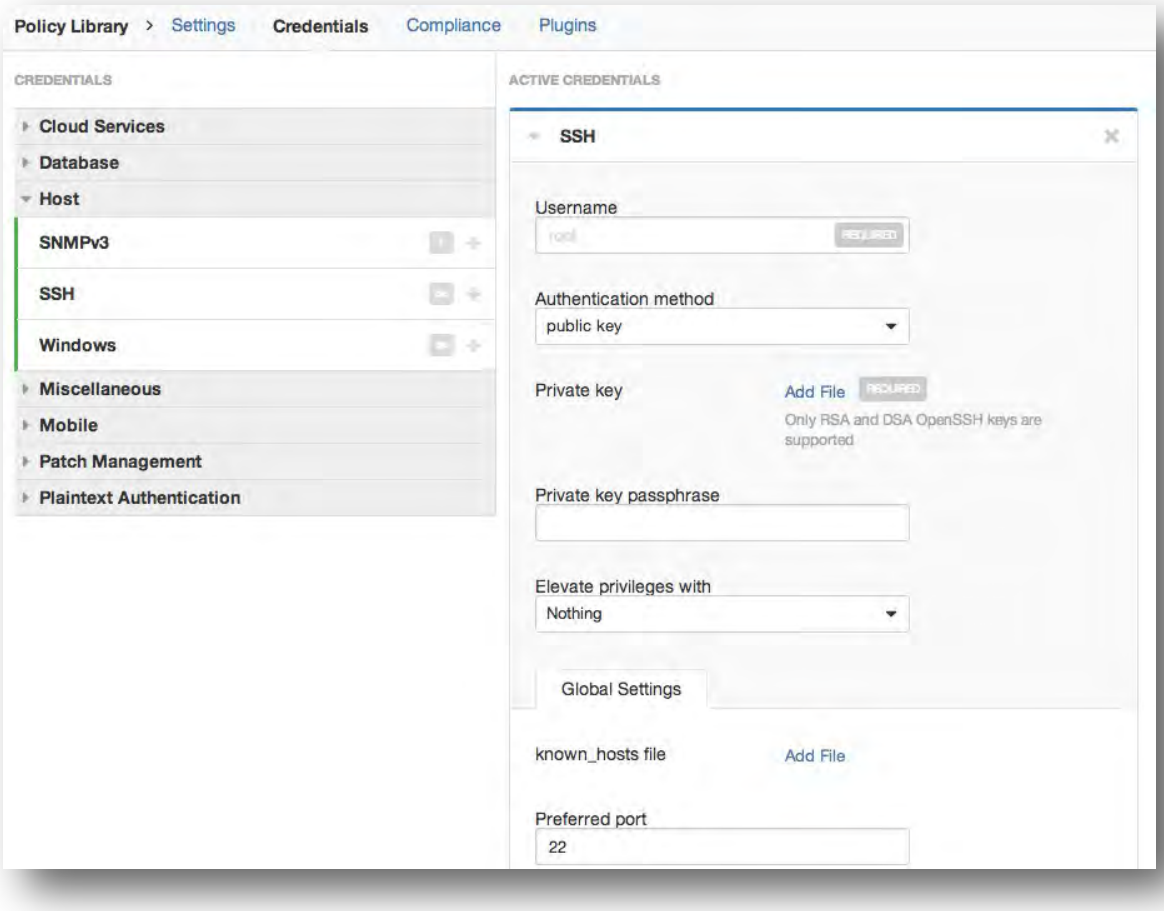
nessusd 请求一个 Kerberos TGT,登录名和密码

Kerbero 返回到 nessusd 的报告

nessusd gives the ticket to sshd

nessusd is logged in

在 Windows 和 SSH 凭证的设置中,您可以指定证书使用 Kerberos 密钥从远程系统进行登录。请注意,这样做的话和 SSH 配置窗口部分会有一定差异.



Kerberos 认证的 SSH 设置:

选项	描述
Password	像其他的凭证方法，这是关于目标系统的用户密码
Key Distribution Center(KDC)	该主机给用户提供会话许可证
KDC Port	这个选项可以直接设置为 Nessus 如果是在非 88 端口运行连接 KDC
KDC Transport	KDC 安装使用 TCP 默认的 Unix。对于 UDP，改变此选项。请注意如果您需要改变这个 KDC 传输，您可能还需要更改端口为 KDC UDP 使用默认端口 88 或 750，根据情况。
Realm	Realm 是认证域，通常称为目标的域名(例如，example.com)

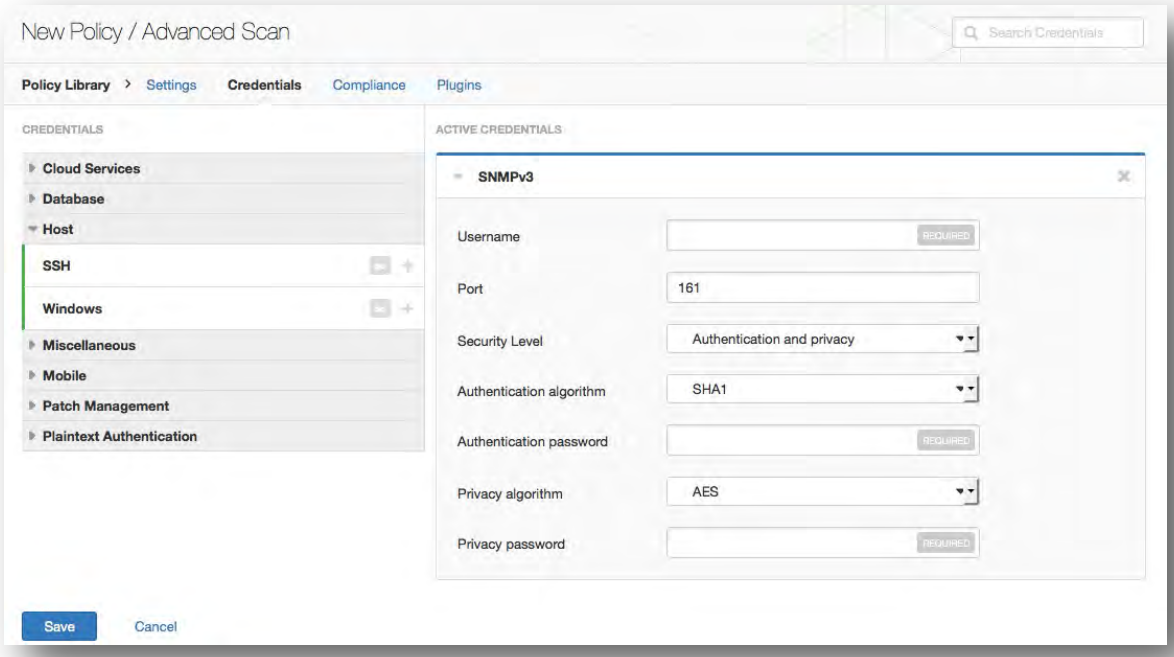
如果使用 Kerberos，sshd 必须配置 Kerberos 支持验证与 KDC。反向 DNS 查找必须正确配置这个工作。Kerberos 的交互方法必须 GSSAPI　MIC。

SNMPv3

用户可以在 Credentials 菜单选择“SNMPv3 settings”并且选中凭据扫描系统使用加密的网络管理协议的凭据。这些凭据用于从远程系统获取本地信息，包括网络设备，补丁审计或合规检查。有一个区域可以显示进入 SNMPv3 账户的用户名以及 SNMPv3 的详情，安全级别，认证算法和密码，隐私算法和密码。

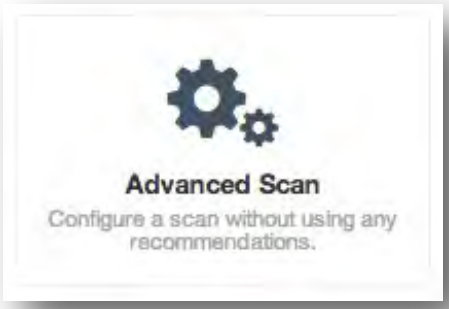
如果是无法猜测的社区字符串/密码，它不可能执行一个完整的审计与服务

选项	描述
User name	一个基于 SNMPv3 的账户的用户名
Port	直接搜索扫描一个不同的端口如果 SNMP 在非 161 端口上运行。
Security level	选择 SNMP 安全级别：认证，隐私，或两者
Authentication algorithm	选择 MD5 或 SHA1 算法的基础上，支持远程服务。
Authentication password	指定的用户名密码
Privacy algorithm	加密算法使用的 SNMP 流量。
Privacy password	密码用来保护加密的 SNMP 通信



创建高级策略

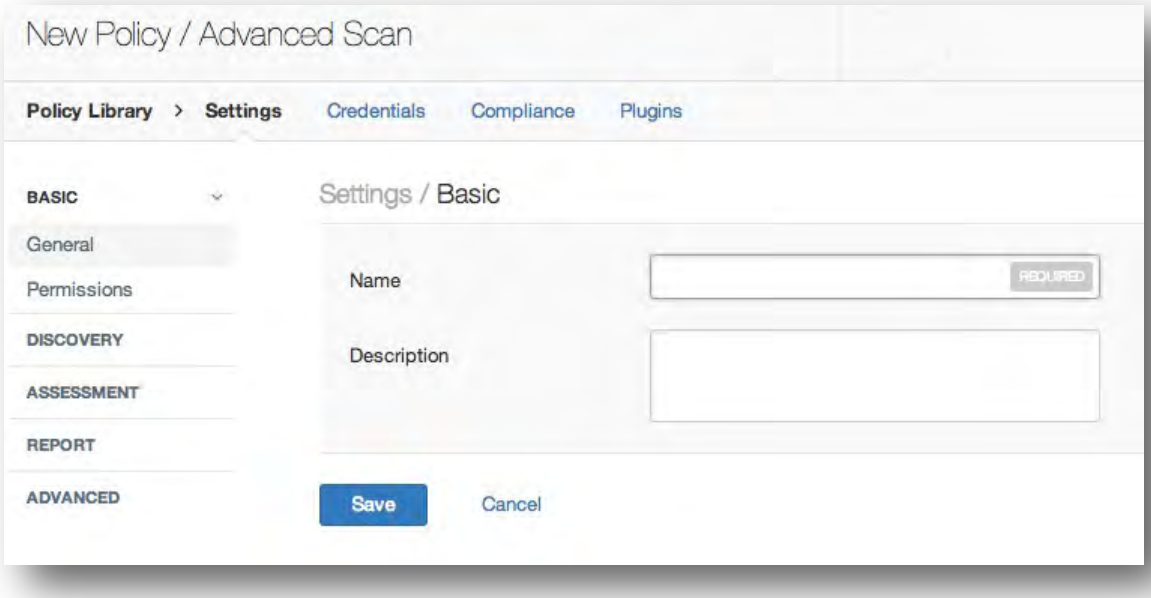
如果没有理想的策略模板可用，先进的扫描选项允许您在所有选项完全控制创建策略。



注意 四个设置标签：Settings，Credentials，Plugins 和 Compliance，这些标签的说明如下。

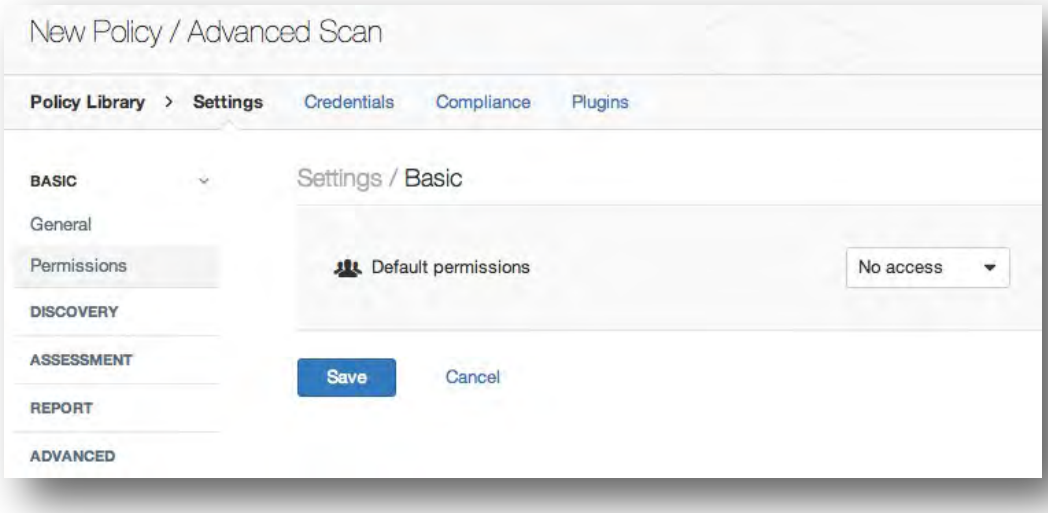
设定

“Settings”标签是你命名策略和配置扫描相关业务



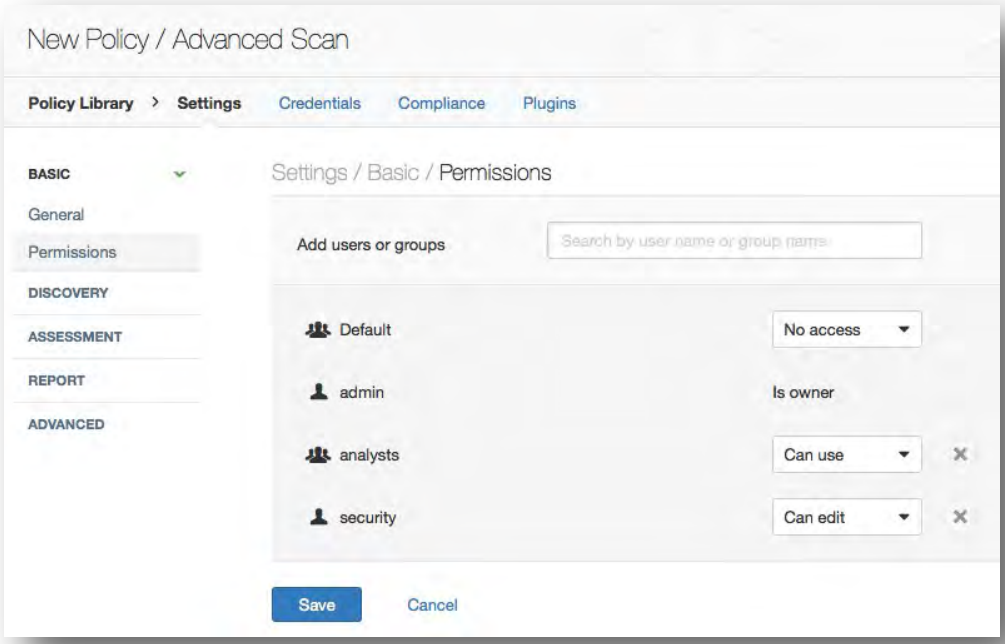
“Basic”屏幕用来定义策略本身的方面。标题下的选项“General”和“Permissions：”

一般选项	描述
Name	设置名字，名字将在 Nessus 界面上显示确定的策略
Description	用来简要说明该扫描策略，通常很好的总结总的目的（例如，“Web 服务器扫描无局部检测或非 HTTP 服务”）。

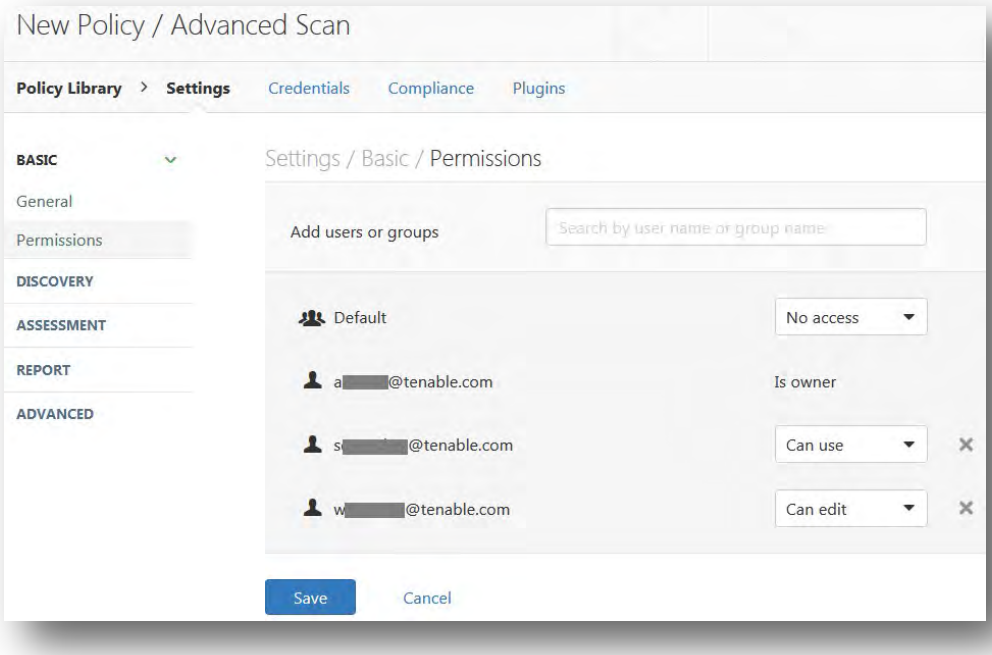


Nessus 的专业设置权限使您能够确定谁有访问权限：

权限	描述
Can Use	其他用户可以查看和使用它们的扫描策略。他们不能编辑策略
No Access	只有用户创建的策略可以查看，使用，或者编辑



Nessus Manager 策略 权限



Nessus Enterprise Cloud 策略 权限

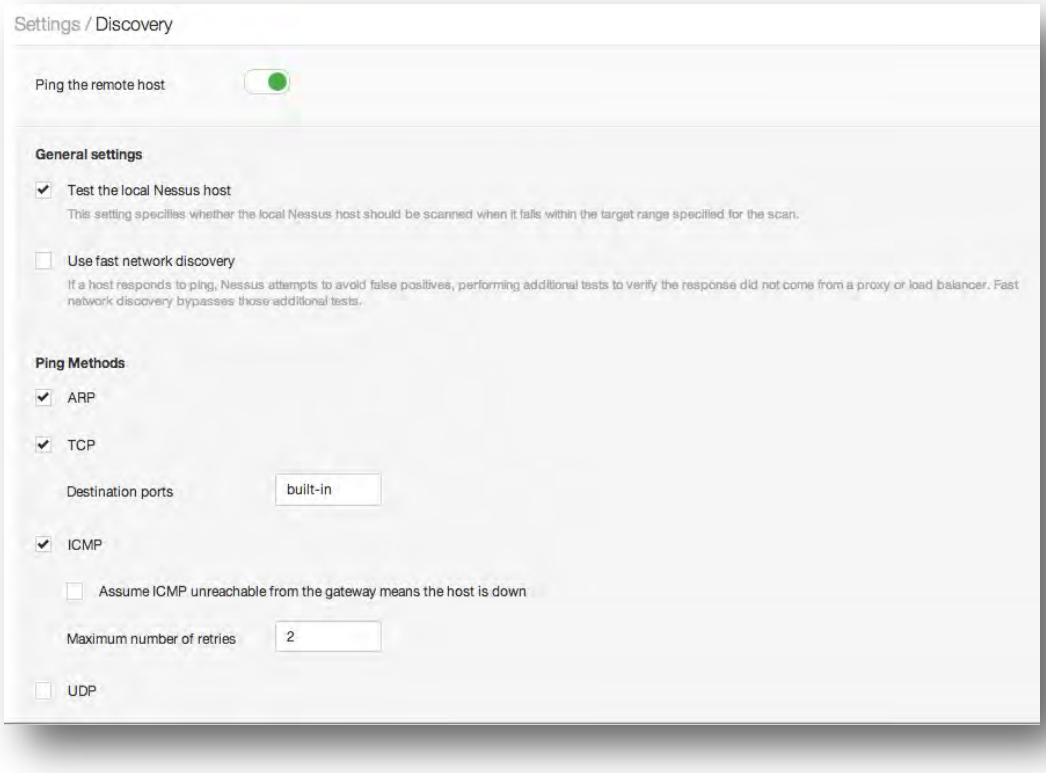
Nessus Manager 和 Nessus Enterprise Cloud 提供更精细的控制。权限可以设置组合用户。默认的是每个人都没有访问用户或组的权限。

权限	描述
Can Use	用户或用户组指定在这里可以查看并在扫描使用策略。他们不能编辑策略。
Can Edit	指定的用户或组可以改变策略，可以使用策略。
No Access	被指定的用户或用户组在这里无法查看，使用，或编辑策略

发现设定

“Discovery”屏幕控制相关的选项可以用来发现并进行端口范围和方法的扫描。标题下的选项“Host Discovery”，“Port Scanning”和“Service Discovery”。

“Ping the remote host”选项允许 Nessus 对 Ping 到的主机进行精细扫描发现功能。

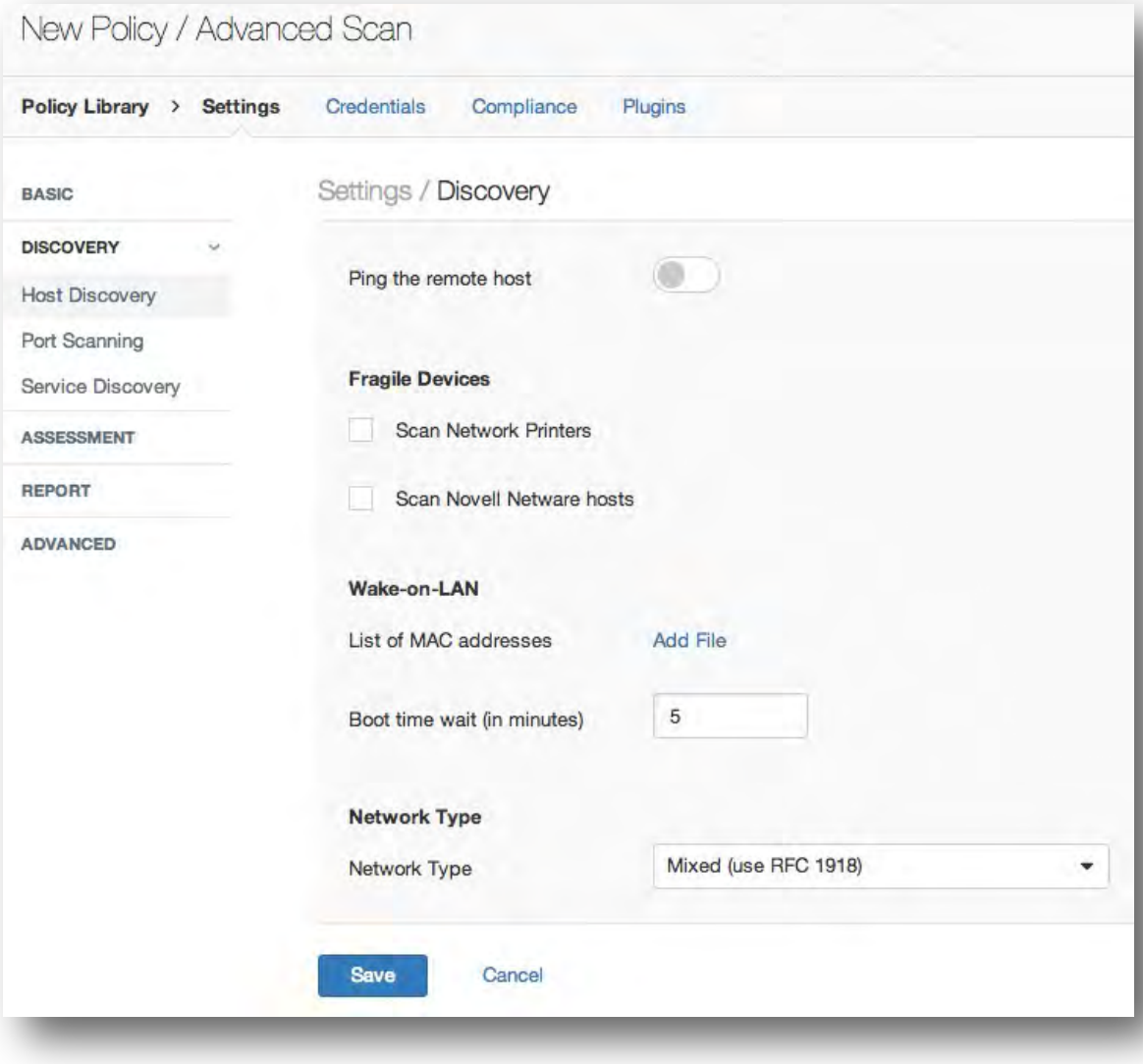


切换 Ping 远程主机开关将使萍选项下面列出。否则,选择不会启用或可见的 UI。

“Host Discovery”下面是 Ping 选项“Host Discovery”：

选项	默认	描述
Ping the remote host	**Enabled**	这个选项允许 Nessus ping 远程主机上多个端口以确定他们是否还活着。当选择时，会启用其他 ping 选项。
Test the local Nessus host	**Enabled**	如果启用了 Ping 远程主机,这对这一政策选项是默认启用。这个选项允许您包含或排除的本地 Nessus 主机扫描。这是 Nessus 主机时使用的目标网络范围内扫描。
Fast network discovery	**Disabled**	如果启用了 Ping 远程主机,您将能够看到这个选项。默认情况下,不启用这个选项。当 Nessus“ping”远程 IP 和接收应答,它执行额外的检查,以确保它不是透明代理或一个负载平衡器,返回噪音但没有结果(一些设备的回答每一个端口 1 - 65535 即使没有服务背后的设备)。这样的检查可以花一些时间,尤其是远程主机防火墙。如果启用了“高速网络发现”选项,Nessus 不会执行这些检查。
ARP	**Enabled**	Ping 主机使用的硬件地址通过地址解析协议(ARP)。这只能在本地网络。
TCP	**Enabled**	Ping 主机使用 TCP。
Destination ports (TCP)	**Built-in**	可以配置为使用特定的端口目的地港口 TCP 平。这个指定的端口列表将检查通过 TCP 平。如果你不确定的港口,离开这个设置默认的“Build-in”。
ICMP	**Enabled**	Ping 主机使用网际控制报文协议(ICMP)。
Assume ICMP unreachable from the gateway means the host is down	**Disabled**	当 ping 发送到主机,其网关可能返回一个 ICMP 不可到达的消息。当启用该选项时,当 Nessus 收到 ICMP 不可到达的消息,它将考虑目标主机死了。这是帮助加快发现在一些网络。 注意,有些防火墙和数据包过滤器的主机使用相同的行为,但被连接到一个端口或协议过滤。启用了这个选项,这将导致扫描考虑主机时,它确实是。
Number of Retries	**2**	允许您指定的数量尝试尝试 ping 远程主机。缺省值是两次。
UDP	**Disabled**	Ping 主机使用用户数据报协议(UDP)。 UDP 是一种“无状态”协议,这意味着沟通不是执行握手对话。UDP 通信并不总是可靠的,因为自然的 UDP 服务和筛选设备,他们并不总是远程检测。

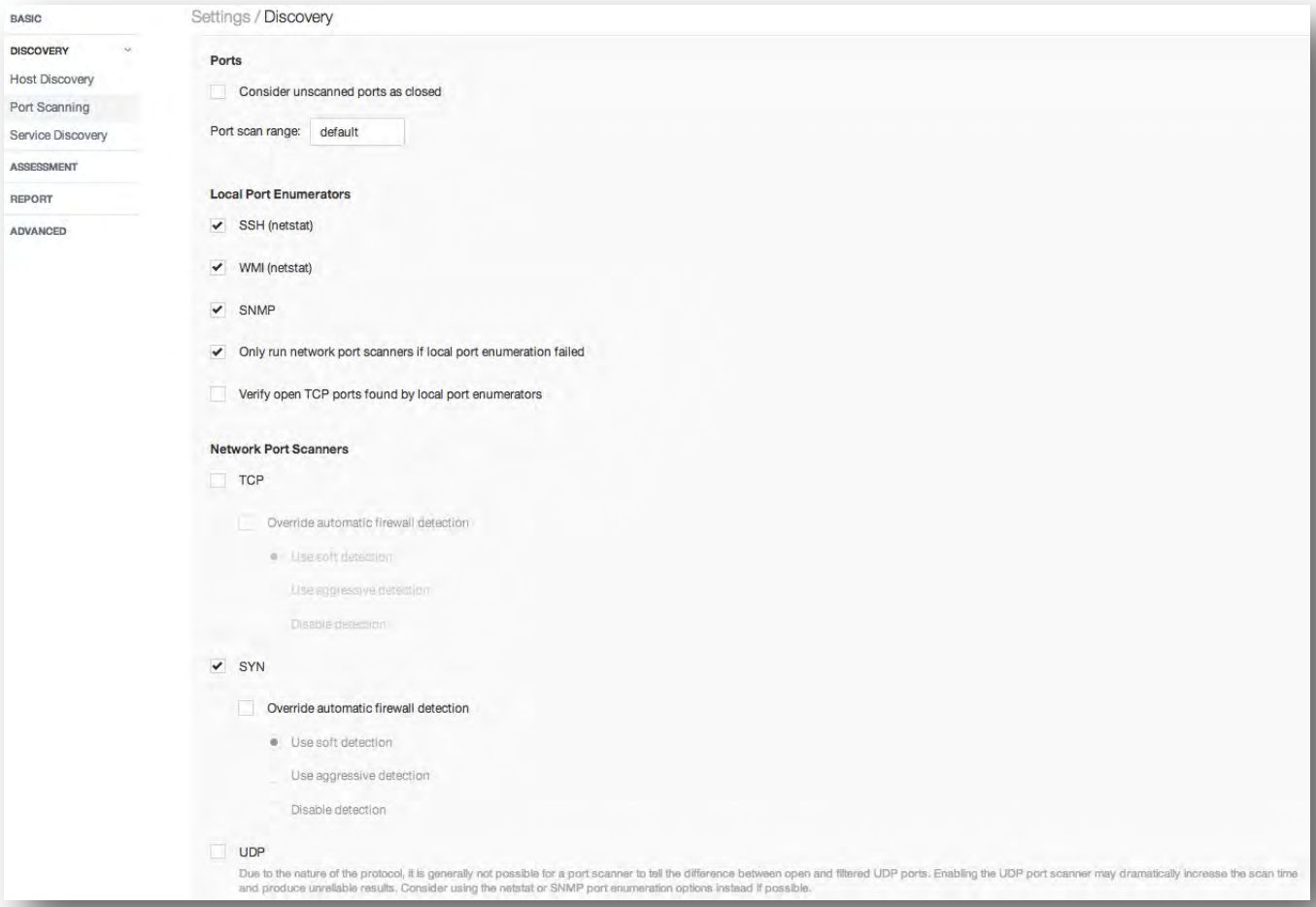
扫描 VMware 客户系统,必须禁用“Ping the remote host”。



其他主机勘探选项包括扫描发现 ragile devices, Wake-on-LAN 和 network type。这些选项如下所述:

选项	默认	描述
Fragile devices	**Disabled**	“**Fragile Devices**” 菜单中提供了两个选项,指导 Nessus 扫描器扫描主机没有被“脆弱”的历史,或容易崩溃当收到意想不到的输入。用户可以选择“扫描网络打印机”或“扫描网络操作系统主机”指示 Nessus 扫描这些特定的设备。Nessus 只会扫描这些设备如果这些选项是检查。建议扫描这些设备执行的方式,让 IT 人员监控系统问题。
Wake-on-LAN	**Disabled**	“**Wake-on-LAN**” 菜单控制哪些主机发送 WOL 魔法包之前执行扫描和等待多长时间(分钟)的系统。输入的 MAC 地址列表 WOL 使用上传文本文件每行一个主机的 MAC 地址。例如:

		00:11:22:33:44:55 aa:bb:cc:dd:ee:ff
Network Type	**Mixed**	允许您指定如果您使用的是公开可路由的 ip,私人非互联网可路由的 ip 或混合。选择“混合”如果您使用 RFC 1918 地址和有多个路由器在你的网络。



端口扫描选项定义端口扫描器将如何表现,端口扫描。

选项	默认	描述
Consider Unscanned Ports as Closed	**Disabled**	如果没有一个端口扫描选定的端口扫描器(如。指定的范围),Nessus 将考虑它关闭。
Port Scan Range	**Default**	指导扫描器针对一个特定的端口范围。接受“默认”(约 4790 常见的端口列表中发现 nessus-services 文件), “所有”(从 0-65535 扫描所有端口),或由用户指定一个自定义的端口列表。自定义列表可能包含个人港口和范围;例如, “21,23,25,80,110”

		和“1-1024,8080,9000-9200”是有效值。指定“1-65535”将扫描所有端口。 请参阅下面的端口扫描范围部分为更多的细节。.

端口扫描范围选择指导扫描器针对一个特定的端口范围。允许以下值:

值	描述
“default”	使用关键字“default”,Nessus 将大约 4790 常见的端口扫描。端口的列表中可以找到 nessus-services 文件。
“all”	使用关键字“all”,通过插件 Nessus 将扫描所有的 65536 端口,包括端口 0。
Custom List	自定义范围的端口可以通过使用一个用逗号分隔的列表选择端口或端口范围。例如,“80110 年 21 日 23 日 25 日”或“1 - 1024,1024,8080 - 1024”是允许的。指定“1 - 65535”将扫描所有端口。 你也可以指定一个分裂范围特定于每个协议。例如,如果你想扫描不同的 TCP 和 UDP 的端口范围相同的政策,您将指定“T:1-1024,U:300-500”。您还可以指定一组端口扫描协议,以及个人范围为每个单独的协议("1-1024,T:1024-65535,U:1025")。如果你扫描一个协议,只选择该端口扫描器和指定端口正常。

指定一个端口扫描范围既适用于 TCP 和 UDP 扫描。

本地端口扫描使用的事 netstat 和 SNMP 来检测服务. 以下为设置选项:

选项	默认	描述
SSH (netstat)	Enabled	这个选项使用 netstat 从本地机器检查开放端口。它依赖于 netstat 命令可以通过 SSH 连接到目标。这个扫描的目的是基于 unix 的系统,需要身份验证凭证。
WMI (netstat)	Enabled	基于 WMI 扫描使用 netstat 来确定开放端口,因此忽略任何端口和指定。如果任何港口枚举器(netstat 或 SNMP)成功,成为“所有”的端口范围。然而,Nessus 仍将荣誉“认为未测量的端口关闭”选项,如果选择。 这个选项使用 netstat 从本地机器检查开放端口。它依赖于 netstat 命令可以通过 WMI 连接到目标。本扫描适用于 windows 系统和需要身份验证凭证。

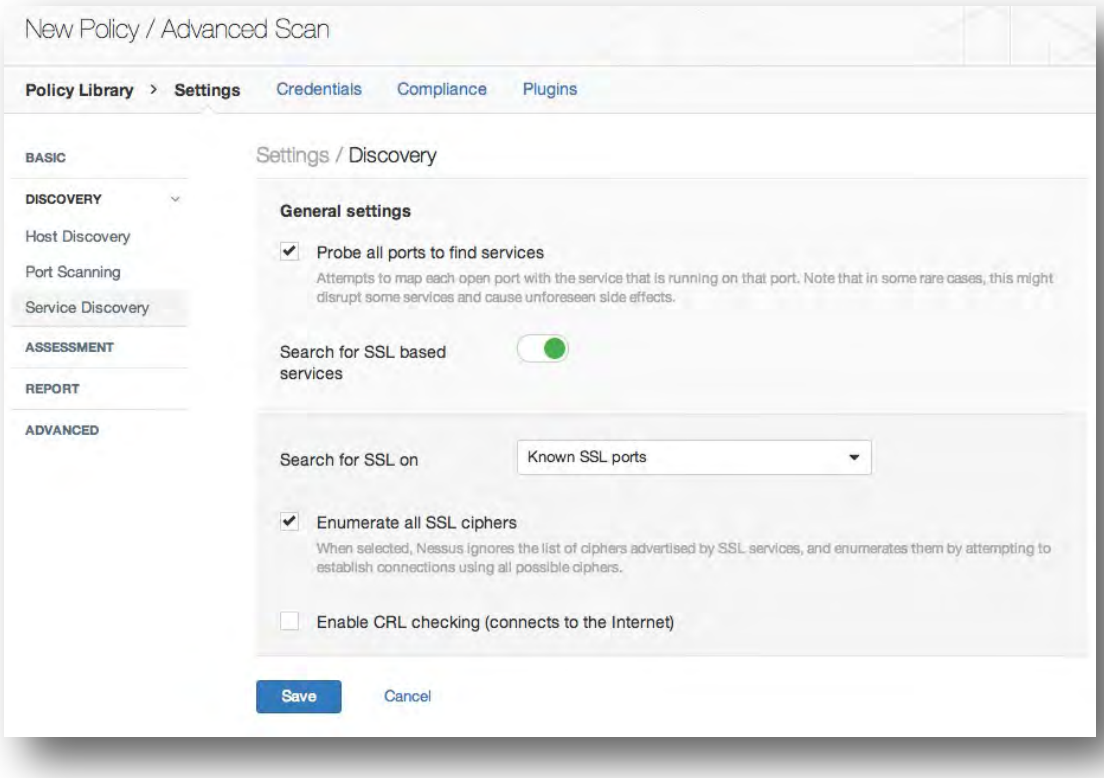
SNMP	Enabled	直接 Nessus 扫描目标简单网络管理协议(SNMP)的服务。Nessus 将试图想在扫描期间相关 SNMP 设置。如果用户提供的设置(在“凭证”),这将允许 Nessus 更好地测试远程主机和产生更详细的审计结果。例如,有许多 Cisco 路由器检查确定漏。洞目前通过检查返回的 SNMP 版本字符串。这对这些审计信息是必要的
Only run network port scanners if local port enumeration failed	Enabled	依靠本地端口枚举先依靠网络端口扫描。
Verify open TCP ports found by local port enumerators	Disabled	如果一个当地的港口枚举器(如.WMI 或 netstat)发现一个港口,Nessus 还将远程验证它是开放的。这有助于确定是否使用某种形式的访问控制(如.TCP 包装器、防火墙)

SYN,远程端口扫描器使用 TCP 和 UDP 数据包为开放端口扫描目标。下面列出的选项:

选项	默认	描述
TCP	Disabled	使用“内置 Nessus 传输控制协议(TCP)扫描器识别目标开放的 TCP 端口。这个扫描器是优化和有一些自调优的特性。 在某些平台上(如 Windows 和 Mac OS X),选择这个扫描器将导致 Nessus 使用 SYN 扫描来避免严重的性能问题本地操作系统。
SYN	Enabled	使用“内置 Nessus SYN 扫描目标识别开放的 TCP 端口。SYN 扫描是一个流行的方法进行端口扫描和一般被认为是有点不扰民的 TCP 扫描,根据安全监控设备,如防火墙、入侵检测系统(IDS)。扫描器将 SYN 数据包发送到港口,等待 SYN-ACK 回答,并确定港口国基于一个回复,或缺乏的回复。
UDP	Disabled	这个选项进行 Nessus 的内置 UDP 扫描器识别打开 UDP 端口上的目标。 由于协议的性质,一般是不可能的一个端口扫描器区分开放和过滤 UDP 端口。使 UDP 端口扫描器会大大提高扫描时间和产生不可靠的结果。考虑使用 netstat 或者 SNMP 接口枚举选项相反,如果可能的话。

Nessus 和 TCP SYN 扫描选项允许您更好地优化本机 SYN 和 TCP 扫描器检测防火墙的存在。TCP SYN 扫描可以帮助识别防火墙是否位于扫描器和默认目标间。

选项	描述
Use aggressive detection	将尝试运行插件即使港口似乎被关闭。建议此选项没有被用于生产网络。
Use soft detection	禁用监控频率的能力重置设置并确定是否有限制下游网络设备配置。
Disable detection	禁用防火墙检测功能。



切换搜索基于 SSL 服务开关将使服务发现下面列出的选项。否则,他们将不可见.

服务发现部分设置选项,尝试每个打开的端口映射的服务在这个端口上运行。

有可能探索破坏服务器或可能导致不可预见的副作用。

在一般设置,您可以设置调查所有端口找到任何正在运行的服务。

选项	默认	描述
Probe all ports to find services	**Enabled**	尝试每个打开的端口映射的服务在这个端口上运行。注意,在一些罕见的情况下,这可能会影响一些服务,导致不可预见的副作用。
Search for SSL based services	**Enabled**	寻找基于 SSL 服务控制 Nessus 如何测试 SSL 服务。 如果选中,选择已知 SSL 端口（如,443)和所有端口。测试 SSL 功能在所有测试主机端口可能是破坏性的。

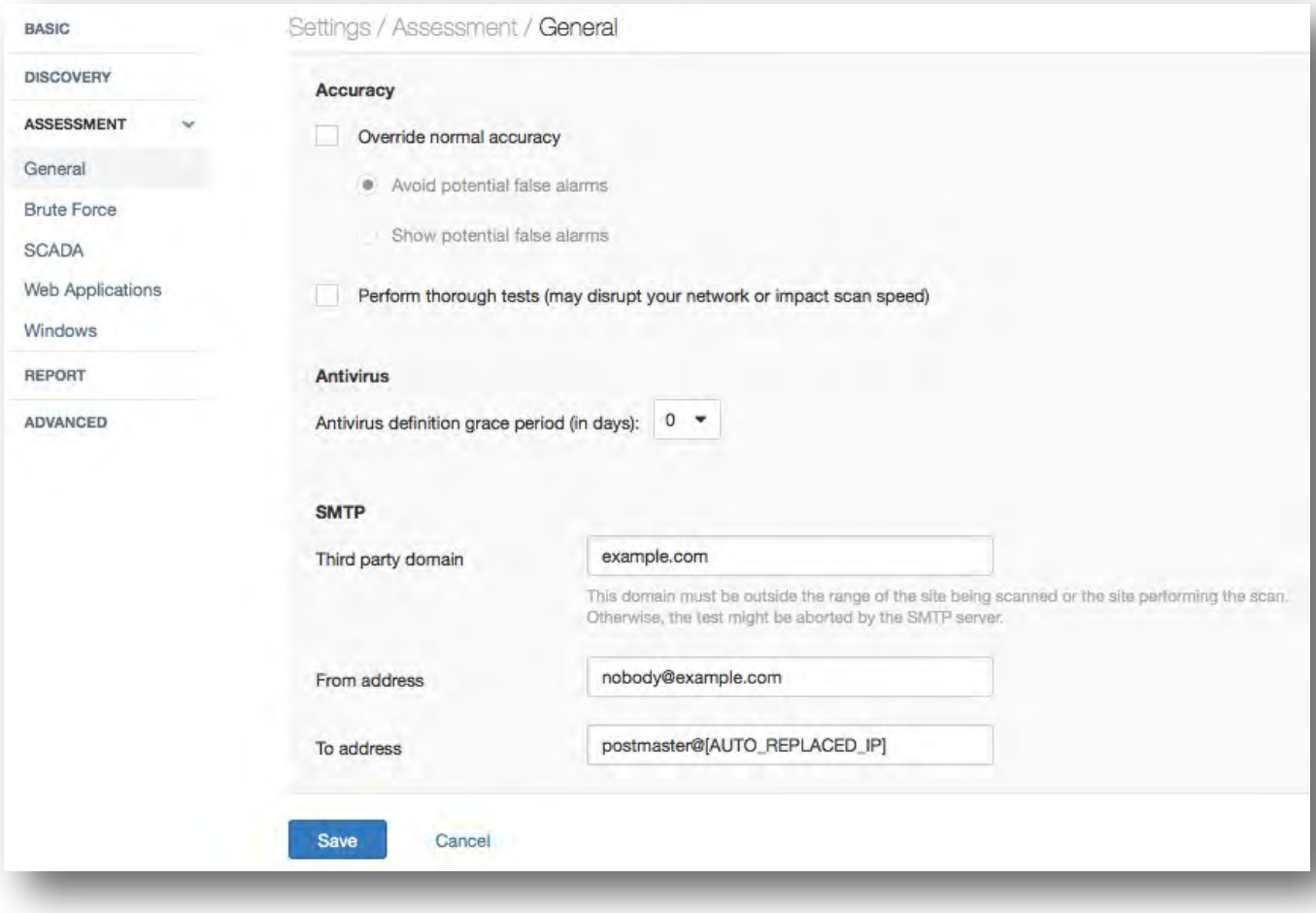
如果启用了搜索基于 SSL 服务,以下选项可用:

选项	默认	描述
Enumerate all SSL ciphers	**Enabled**	Nessus 执行 SSL 扫描时,它试图确定使用的 SSL 密码尝试建立连接远程服务器的每个不同记录 SSL 密码,不管服务器说什么是可用
Enable CRL checking (connects to Internet)	**Disabled**	直接 Nessus 对已知的证书撤销列表检查 SSL 证书 (CRL).

评估设定

“Assessment”屏幕控制评价安全评估的流行性。标题下的选项：

“**General**”, “**Brute Force**”, “**SCADA**”, “**Web Applications**”, 和 “**Windows**”.



以下设置下的通用部分。“Accuracy”选项允许细粒度控制假警报的报告和在扫描进行彻底的测试。

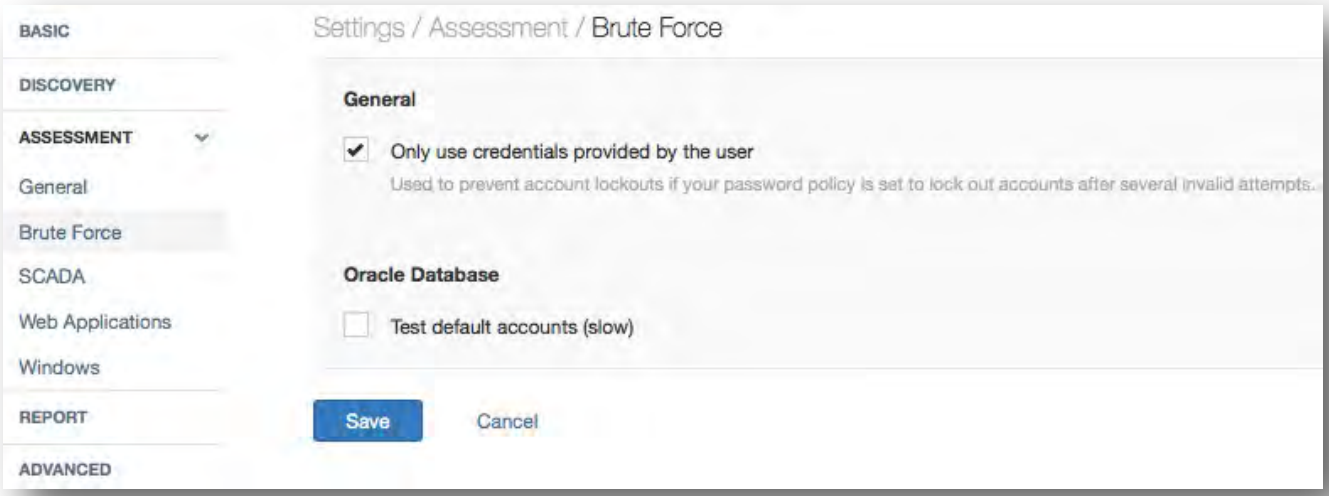
选项	默认	描述
Override normal accuracy	Disabled	在某些情况下,远程 Nessus 不能确定是否存在一个缺陷。如果报告偏执设置“显示潜在的假警报”然后一个缺陷将每次报道,即使有疑问的远程主机的影响。 相反,一个偏执的“避免潜在的假警报”将导致 Nessus 不报告任何缺陷只要有一丝的不确定性远程主机。不启用“覆盖正常的准确性”这两个设置之间的中间地带。
Perform thorough tests (may disrupt your network or impact scan speed)	Disabled	导致各种插件“努力工作”。例如,当通过 SMB 文件共享,一个插件可以分析 3 目录层次深,而不是 1。这可能会导致在某些情况下更多的网络流量和分析。注意,更彻底,扫描将更多的侵入性和更有可能扰乱网络,同时可能提供更好的审计结果。

“Antivirus”选项允许控制扫描杀毒软件设置。

选项	描述
Antivirus definition grace period (in days)	配置杀毒软件检查一组的延迟天数(0-7)。“Antivirus Software Check”菜单允许您直接 Nessus 允许特定的恩典时间在报道时防病毒签名被认为是过时了。默认情况下,Nessus 将考虑签名过时不管多久以前的更新是可用的(如“几小时前”)。这可以配置为允许长达 7 天前报告的日期。

“SMTP 设置”菜单指定选项简单邮件传输协议(SMTP)测试,运行在所有设备中扫描运行 SMTP 服务领域。Nessus 将试图通过设备传递信息到指定的“第三方域名”。如果消息发送到“第三方域”是被指定的地址在“地址”字段中,垃圾邮件的尝试失败了。如果消息被接受,那么 SMTP 服务器已成功用于继电器垃圾邮件。

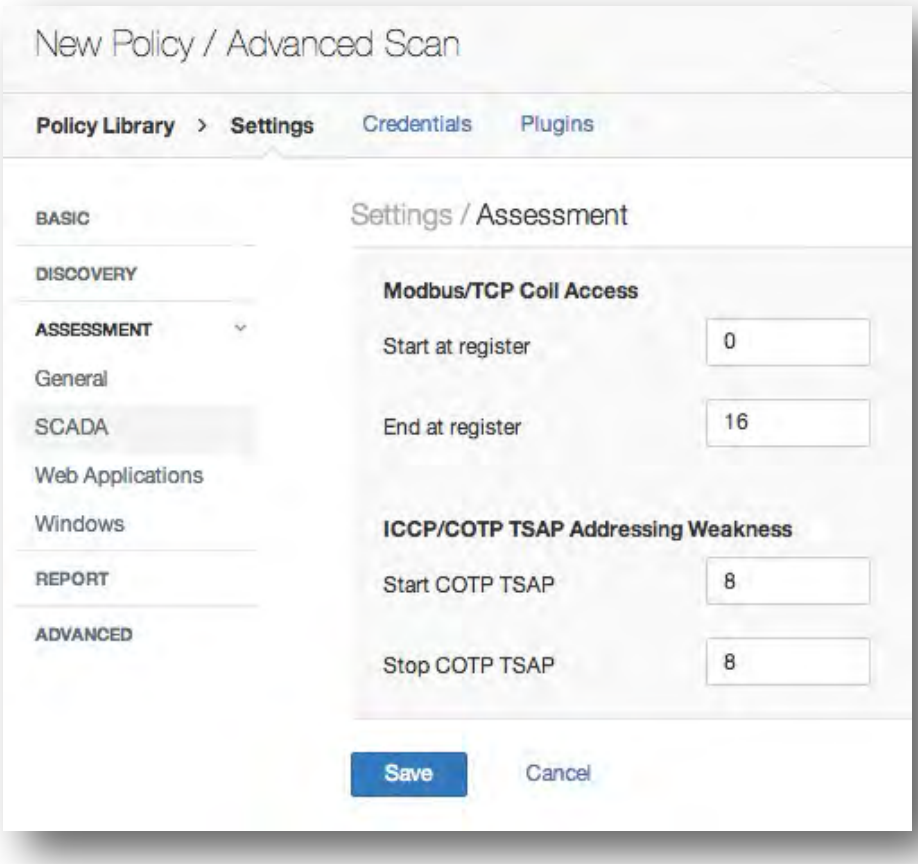
选项	描述
Third party domain	Nessus 将试图通过每一个 SMTP 设备发送垃圾邮件中列出的地址。这个第三方域名地址必须被扫描范围以外的网站或网站执行扫描。否则,测试可能是流产的 SMTP 服务器。
From address	测试消息发送到 SMTP 服务器将会出现,如果他们起源于这个字段中指定的地址。
To address	Nessus 将试图发送消息写给这个字段中列出的邮件收件人。邮政地址默认值,因为它是一个有效的地址邮件服务器。



“Brute Force”选项允许细粒度的控制占强力扫描。“Default Accounts”选项与扫描器测试可能默认账户。

选项	默认	描述
Only use credentials provided by the user	**Enabled**	在某些情况下,Nessus 可以测试默认账户和已知的默认密码。默认情况下,这是启用。这可能会导致帐户被锁定，如果连续太多的无效的尝试引发安全协议的操作系统或应用程序。
Test default Oracle accounts (slow)	**Disabled**	在 Oracle 软件测试已知的默认账户。

“SCADA”设置菜单选项指定监控和数据采集(SCADA)在扫描测试,在所有设备上运行运行 SCADA 服务领域。Nessus 漏洞扫描器执行 uncredentialed 和有资格的 SCADA 系统的扫描范围广泛的漏洞为商业客户。设置 SCADA 插件下面列出:



选项	描述
Modbus/TCP Coil Access	“Modbus/TCP Coil Access” 为商业用户选项可用。这个下拉菜单项是动态生成的 SCADA 的商业版本 Nessus 插件可用。网络通讯协议使用一个函数代码的阅读 Modbus 奴隶的“coils”。线圈代表二进制输出设置,通常映射到执行机构。阅读能力线圈可能帮助攻击者形象系统和确定范围的寄存器来改变通过“写线圈”消息。“Start reg”默认值是“0”， “End reg”默认值是“16”。
ICCP/COTP TSAP Addressing Weakness	“ICCP/COTP TSAP Addressing” 菜单决定面向连接的传输协议(COTP)运输服务访问点(TSAP)值组成服务器尝试可能的值。启动和停止值设置为默认“8”。

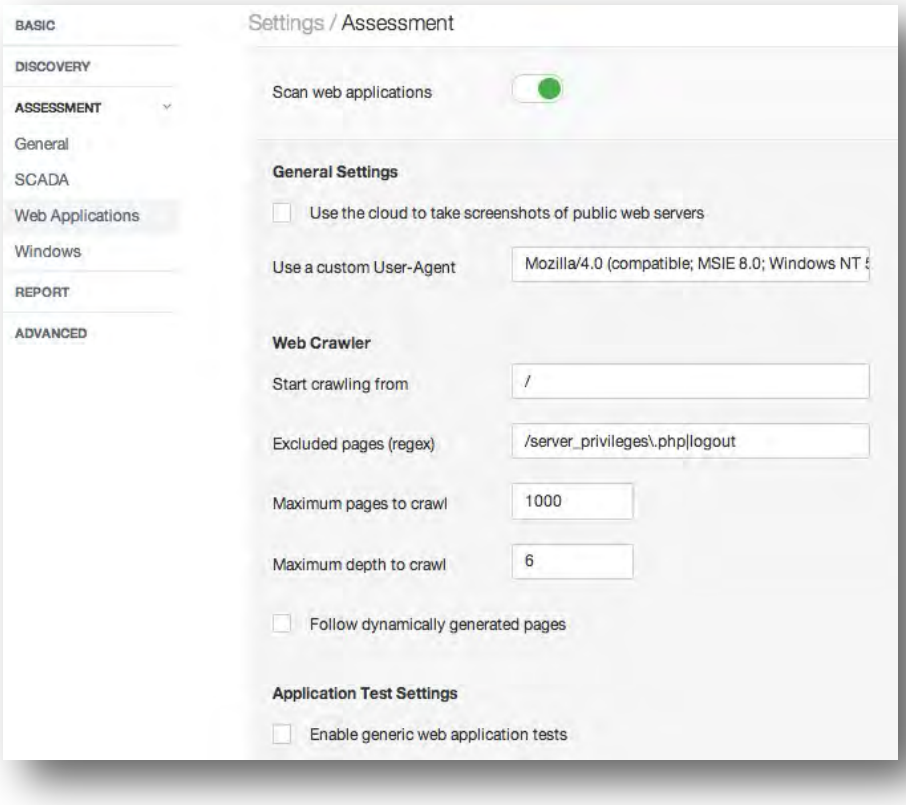
网页应用

“Web Applications”菜单测试参数的远程 CGI(公共网关接口)发现网络镜像过程试图通过跨站点脚本等常见 CGI 编程错误,远程文件包含命令执行,遍历攻击、SQL 注入。启用该选项选择“Scan web applications”复选框。这些测试依赖于以下极佳的插件:

- 11139, 42424, 42479, 42426, 42427, 43160, 51973 – SQL Injection (CGI abuses)
- 39465, 44967, 51528 – Command Execution (CGI abuses)

- 39466, 47831, 42425, 46193, 49067, 51972, 51529, 52483, 55904 – Cross-Site Scripting (CGI abuses: XSS)
- 39467, 46195, 46194, 50494 – Directory Traversal (CGI abuses)
- 39468 – HTTP Header Injection (CGI abuses: XSS)
- 39469, 42056, 42872 – File Inclusion (CGI abuses)
- 42055 – Format String (CGI abuses)
- 42423, 42054 – Server Side Includes a.k.a. SSI (CGI abuses)
- 44136 – Cookie Manipulation (CGI abuses)
- 46196 – XML Injection (CGI abuses)
- 40406, 48926, 48927 – Error Messages
- 56245 – XPath Injection
- 47830, 47832, 47834, 44134 – Additional attacks (CGI abuses)

这个列表相关的 web 应用程序插件更新频繁,可能不完整。额外的插件可能会依赖于这里的偏好设置。



点击 **Scan web applications** 按钮后，下方将列出所有的 Web 应用程序扫描选项。否则，他们将无法启用，或显示在 UI 中。

以下为通用模块下的设置，对所有 Web 应用扫描有效。

选项	默认设置	说明
Use the cloud to take screenshots of public webservers (使用云对公共服务器进行截屏)	不使用	此选项使 Nessus 运用截图来更好的展示其扫描结果。包括一些服务选项（例如，VNC，RDP），以及配置选项（例如，Web 服务器目录索引）。由于截图在托管服务器上生成并发送到 Nessus 扫描仪，该功能仅限于面向 Internet 的主机。 例如，如果 Nessus 发现虚拟网络计算（VNC）没有密码来限制访问，截图将显示会话并列入报告。 在下面的示例中，一个 VNC 被发现在登录屏幕显示管理员正登录到系统中：  请注意，截屏文件时请注意，截屏文件时不会随 Nessus 的扫描报告导出的。不会随 Nessus 的扫描报告导出的。
Use a custom User-Agent (使用订制的用户代理)	**Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)**	当进行扫描时，指定 Nessus 将模拟哪些类型的 Web 浏览器。

“Web Crawler”(网络爬虫) 选项为 Nessus 本地的 Web 服务器的内容镜像设置配置参数。Nessus 将镜像网站内容，以更好地分析漏洞的内容，并使得对 Web 服务器的影响最小化。

如果以 web 爬行参数设置的方式爬一个完整的网站,可能造成扫描过程中产生大量的交互流量。例如,如果有 1gb 的材料在一个 web 服务器上，Nessus 配置要求镜像所有内容，因此扫描时从服务器到 Nessus 扫描仪上至少将产生 1gb 的扫描流量。

选项	默认设置	说明
Start crawling from(开始爬取)	/	扫描目标站点 URL 的首页将被测试。若要求扫描多个页面，请使用冒号分隔符分开扫描目标 (例如： “/:/php4:/base”).
Excluded pages (regex) 不包含页面 (正则表达式)	/server_privileges\ .php|logout	使得部分指定网页不被扫描。例如，让“/manual”目录下和所有的 Perl CGI 不被扫描，请设置这样的字段: `(^/manual)|(\.pl(\?.*)?$)`. Nessus 支持 POSIX 正则表达式，以及兼容 perl 的正则表达式(PCRE)，以匹配和处理字符串。
Maximum pages to crawl(爬取最多页面)	1000	爬取最多页面数的设置
Maximum depth to crawl(爬取深度最大化)	6	限制 Nessus 从每个起始页面开始跟踪的最多链接页面数量。
Follow dynamic pages (跟踪动态页面)	不启用	若选择此项，Nessus 将跟踪动态链接，因此扫描的页面将可能超过之前设置的参数限制。

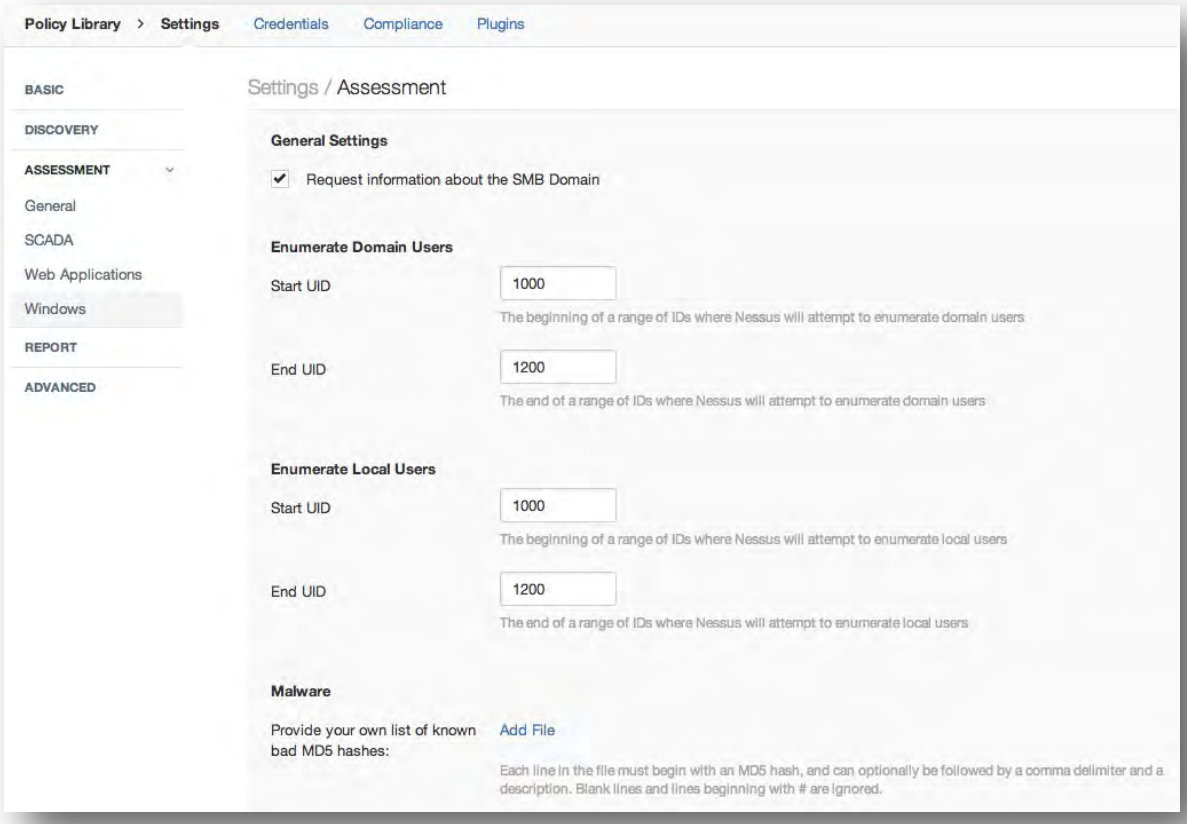
“**Application Test Settings**”(“应用程序测试设置”)选项可为 Nessus 本地 web 服务器的镜像内容进一步设置精准的配置参数。Nessus 将镜像网站内容，以更好地分析漏洞内容，并协助尽可能地减少对服务器的影响。

选项	默认设置	说明
Enable generic web application tests(启用通用的 web 应用测试)	不启用	使下列选项启用。
Abort web application tests if HTTP login fails(若 HTTP 登录失败，则放弃 web 应用测试)	不启用	若 Nessus 无法通过 HTTP 登录目标，则不启动任何 Web 应用测试。
Try all HTTP methods (尝试所有 HTTP 模式)	不启用	该选项将要求 Nessus 同时使用“POST 请求”以加强 web 表单测试。 默认情况下, 除非启用这个选项，web 应用测试将只使用 GET 请求。一般来说,当用户提交数据到应用程序时，较为复杂的应用程序将使用 POST 模式。而这个设置提供了更全面的测试，但可能因此大量增加所需时间。当此项被选择后，Nessus 将为每个脚本/变量以 GET 和 POST 请求进行测试。这个设置提供了更全面的测试,但可能因此大量增加所需的时间。
Attempt HTTP Parameter Pollution(尝试 HTTP 参数污染攻击)	不启用	当执行 web 应用测试时,试图通过在变量中注入内容来绕过过滤机制，虽然也是为同一变量提供有效内容。例如,一个正常的 SQL 注入测试可能看起来像“`/target.cgi?a='&b=2`”。启用了 HTTP 参数污染(HPP)选项，请求可能看起来像“`/target.cgi?a='&a=1&b=2`”.
Test embedded web servers (测试嵌入式 web 服务器)	不启用	嵌入式 web 服务器通常是静态的,不包含定制的 CGI 脚本。此外,扫描时可能容易造成嵌入式 web 服务器崩溃或造成服务无响应。Tenable 厂商

		建议将扫描嵌入式 web 服务器与其他 web 服务器时使用这个选项分开进行。
Test more than one parameter at a time per form **(同时对每个表格进行多个参数测试)**	不启用	该选项管理 HTTP 请求中使用的参数值的组合。未选中该选项时,默认为同时用一个攻击字符串测试一个参数,不尝试“非攻击”其他参数的变量。例如, 当“b”和“c”允许其他值时, Nessus 将尝试“/test.php?arg1=XSS&b=1&c=1”，而无需测试每个组合。这是能生成最小结果集的最快测试方法。 该下拉框有四个选项： Test random pairs of parameters(测试参数的随机对) –该测试形式将随机检查随机参数对的组合。这是用来测试多个参数的最快方法。 Test all pairs of parameters (slow)(测试所有参数对-较慢) – 该测试形式会稍慢，但比“单一值”测试更有效率。当测试多参数时，它将测试一个攻击字符串，成为一个单一变量，然后为所有其他变量使用第一个值。比如，Nessus 将尝试“/test.php?a=XSS&b=1&c=1&d=1”，然后循环变量，使得一方面提供攻击字符串，一方面循环通过所有可能的值 (就像在镜像过程中发现的), 以及其他变量的第一个值。在这种情况下，当每个变量返回的第一个值是“1”时，Nessus 将不再测试“/test.php?a=XSS&b=3&c=3&d=3”。 Test random combinations of three or more parameters (slower) (测试三个以上的随机参数组, 较慢) –该测试形式将随机检查三个或更多的参数组合。这比仅测试参数对更彻底。但需要注意的是增加三个或更多的组合数量将增加 web 应用测试的时间。 Test all combinations of parameters (slowest)(测试所有参数组合，最慢) –这种测试方法将在输入有效变量后，充分详尽地测试所有可能的攻击字符串组合。当“所有成对”的测试试图创建一个较小的数据集作为权衡速度时,“所有组合”会不计时间地使用一个完整的数据集来进行测试。这种测试方法可能需要很长时间才能完成。
Do not stop after first flaw is found per web page **(每个网页发现第一个问题后，不要停止，继续扫描)**	不启用	该选项决定是当一个新的问题被锁定时。它适用于多 脚本级别，发现 XSS 漏洞后不会禁用寻找 SQL 注入或报头注入，但除非设置了“thorough tests(彻底测试)”, 对于在给定端口的每种漏洞类型您将最多获取一个报告。请注意,几个相同类型的问题(如。XSS,SQL 等等)，当他们被相同的攻击发现时，有时也可能被报告。下拉框中有四个选项： **Stop after one flaw is found per web server (fastest) (当 web 服务器被发现一个问题时就停止扫描-最快)** –一旦在 web 服务器中发现一个问题时，Nessus 将停止扫描，并转而对其他端口的另一个 web 服务器进行扫描。

		Stop after one flaw is found per parameter (slow)(当参数发现问题后停止扫描-较慢) – 一旦 CGI 参数被发现一种问题后(比如：XSS), Nessus 将转而扫描同一个 CGI 下的另一个参数，或者下一个已知的 CGI，或者下一个端口/服务器。 **Look for all flaws (slowest)(寻找所有问题-最慢)**– 不管发现了哪些问题都进行广泛的测试。这个选项可以产生一个非常详细的报告。一般情况下不推荐。
URL for Remote File Inclusion (远程文件包的 URL 地址)	**http://rfi.nessus.org/rfi.txt**	在远程文件包(RFI)测试期间,该选项指定远程主机上的文件用于测试。默认情况下,Nessus 将使用一个安全的文件由 Tenable 的 RFI 测试。如果扫描仪无法达到互联网, 建议使用一个内部托管文件以更准确的进行 RFI 测试。
Maximum run time (min) (运行时间最大化-分钟)	**5**	该选项管理执行 web 应用测试花费的时间。默认为 60 分钟,适用于所有端口和给定的网站的 CGI。扫描本地网络的网站与小应用程序通常会在一个小时内完成,然而带有大型应用程序的网站可能需要更多时间值。

该 “Windows”(窗口)选项允许你调整窗口扫描的范围。



下列选项将影响窗口目标的 SMB 范围。

选项	默认设置	说明
Request information about the SMB Domain	**Enabled (启用)**	若设置了“**Request information about the domain**”(查询 SMB 域信息)选项, 将查询域用户信息而非本地用户。

以下设置将控制 Nessus 来枚举用户在域或本地系统:

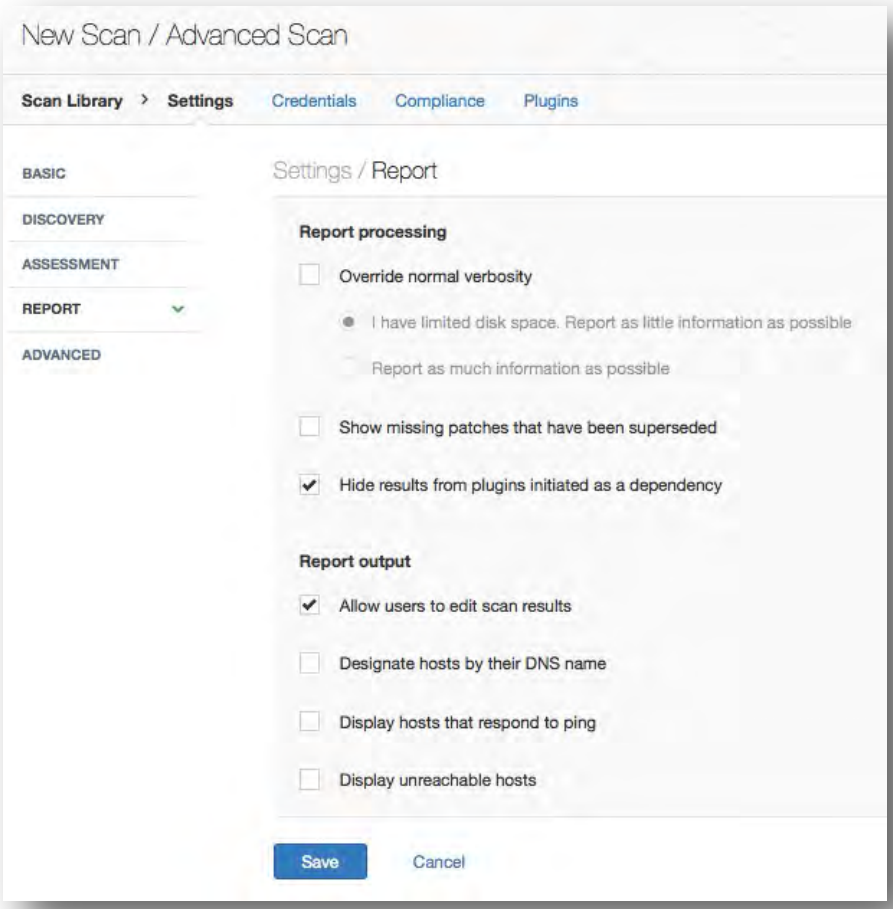
选项	说明
Enumerate Domain Users (枚举域用户)	“Enumerate Domain Users”(枚举域用户)菜单指定 SID 范围用于执行反向查找域中的用户名。该默认设置是适合大多数扫描。 该默认值为开始的 UID 到 1000 个为止；结束的 UID 到 1200 个为止.
Enumerate Local Users (枚举本地用户)	“Enumerate Local Users” (枚举本地用户)菜单指定 SID 范围用于执行反向查找本地用户的用户名。该默认设置为推荐设置。 该默认值为开始的 UID 到 1000 个为止；结束的 UID 到 1200 个为止.

“**Malware**”(恶意软件)选项允许您指定一个额外的 MD5 散列列表, Nessus 将使用为已知恶意软件扫描系统, 并用一组已知的好的散列以减少误报。这个列表使用的是插件 “恶意程序检测:用户定义的恶意软件运行”(Plugin ID 65548), 其功能如 Tenable 的“恶意程序检测” 插件(Plugin ID 59275).

选项	说明
Provide your own list of known bad MD5 hashes (提供您自己已知的坏 MD5 散列的列表)	额外的已知坏 MD5 散列可以通过一个文本文件上传, 其中包含每行一个 MD5 散列。 可以为每个上传文件中的散列添加描述(可选)。这是通过在散列后添加一个逗号,然后加上描述语句来实现。如果对目标进行扫描时找到任何匹配，或者提供了一个描述在散列中，描述将显示在扫描结果中。标准的散列分隔标点(如,#)除了逗号外也可以选择性地使用其他标点。
Provide your own list of known good MD5 hashes (提供您自己已知的好的 MD5 散列的列表)	额外的已知好的 MD5 散列可以通过一个文本文件上传, 其中包含每行一个 MD5 散列。 可以为每个上传文件中的散列添加描述(可选)。这是通过在散列后添加一个逗号,然后加上描述语句来实现。如果对目标进行扫描时找到任何匹配，或者提供了一个描述在散列中，描述将显示在扫描结果中。标准的散列分隔标点(如,#)除了逗号外也可以选择性地使用其他标点。
Hosts file whitelist (主机文件白名单)	Nessus 检查系统主机文件受损的迹象（例如，插件 ID#23910 题为“受损的 Windows 系统（主机文件检查”）。这个选项允许你上传一个包含主机名列表的文件，该列表内的主机将在 Nessus 扫描时被忽略，不再扫描。该文件是一个每行列一个主机名的普通的文本文件。

报告

“ **Report**”(报告) 选项将影响报告的生成和导出。



“**Report processing**”(报表处理)选项会影响报告中的所有插件信息。

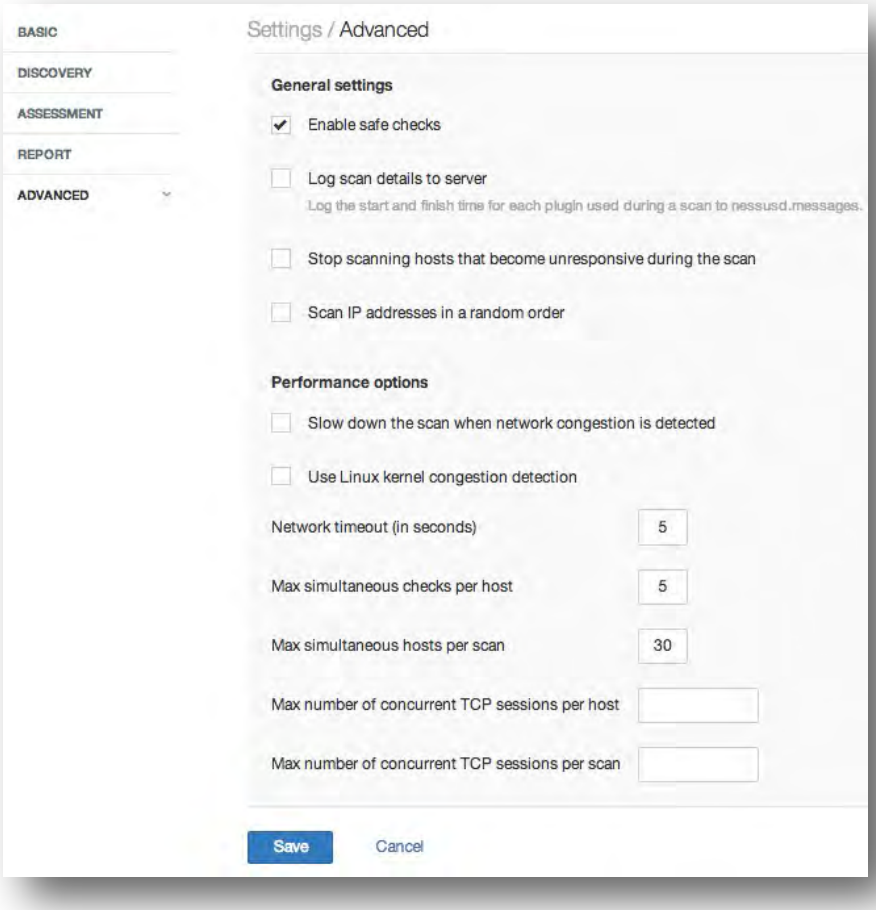
选项	默认设置	说明
Override normal verbosity (覆盖正常的冗长)	不启用	“**I have limited disk space. Report as little information as possible**”(我的磁盘空间有限，报告尽可能少的信息)将在报告中提供较少的插件更新信息，以减少对磁盘空间的影响。 “**Report as much information as possible**”(报告尽可能多的信息)将在报告中提供更多的插件更新情况信息。
Show missing patches that have been superseded (显示已被替代的丢失补丁)	不启用	该选项允许您配置 Nessus,使其在扫描报告中包含或删除被取代的补丁信息。除非策略库中创建了使用内部 PCI 网络扫描模板的策略，否则该选项默认是关闭的。
Hide results from plugins initiated as a dependency(隐藏依赖插件启动的结果)	启用	如果选中这个选项,依赖关系列表将不包括在报告中。若您想在报告中包括依赖关系列表，请取消选中对应的复选框。

“**Report output**”(报告导出)选项会影响报告结果

选项	默认配置	说明
Allow users to edit scan results(允许用户修	启用	改选项允许用户在检查报告时从中删除条目。当执行合规扫描或其他审计时,取消这个选项会显示不被篡改的扫描结果。
Designate hosts by their DNS name(指定主机的 DNS 名称)	不启用	报告输出时使用主机名而不是 IP 地址。
Display hosts that respond to ping (显示应答 ping 的	不启用	选择这个选项将详细报告可被成功 ping 到的远程主机性能
Display unreachable hosts(显示不可达	不启用	如果选中此选项，主机没有回复 ping 请求时，该主机将被作为无效主机包括在安全报告中。

高级选项

“**Advanced**”(高级选项)广泛包含了各种配置选项，以提供更细粒度的控制项来操作扫描仪。



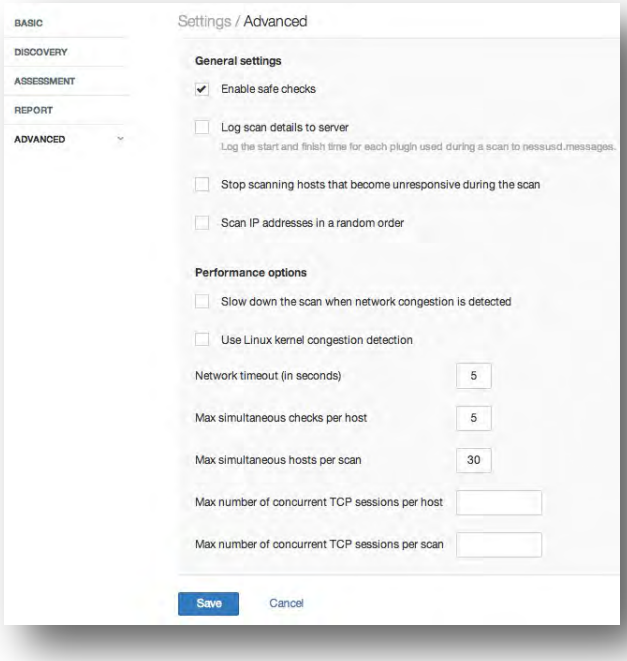
“**General**”(概要) 菜单进一步明确了相关的扫描行为选项:

选项	默认设置	说明
Enable Safe Checks (允许安全检查)	启用	该选项将禁用所有可能对远程主机产生不利影响的插件。
Log Scan Details to Server(服务器的日志扫描细节)	不启用	在 Nessus 服务器日志（nessusd.messages）上保存额外的扫描细节，包括插件启动，插件完成，或者如果一个插件被删除。由此产生的日志可用于确认特定的被使用的插件，以及被扫描的主机。
Stop scanning hosts that become unresponsive during the scan(停止扫描会在扫描过程中变得反应迟钝的主机)	不启用	若选中该项，一旦 Nessus 检测到主机已变得反应迟钝，将停止扫描。这可能导致若在扫描过程中用户关闭他们的电脑，在拒绝服务插件发起时主机已停止响应，或安全机制（例如，IDS）已开始阻塞服务器。继续扫描这些机器会发出不必要的在网络上的流量并延迟扫描。
Scan IP addresses in a random order (扫描随机指令中的 IP 地址)	不启用	默认情况下，Nessus 按 IP 地址列表顺序扫描。如果选中此项，Nessus 将以随机的顺序扫描的主机列表。这在大量扫描时，通常对帮助分发针对特定子网在网络流量是很有用的。 2013 年 7 月前，该选项在每个子网的基础上工作。这个功能已随机在整个目标 IP 空间被加强。

“**Performance**”(性能) 选项帮助控制扫描发起的数量。当配置一项扫描，对扫描时间和网络活动引起最严重影响时，这些选项可能
是最重要的。

选项	默认设置	说明
Slow down the scan when network congestion is detected(当检测到网络拥塞时减慢扫描)	不启用	当发送过多的数据包和网络带宽快要不能负荷时，这将使 Nessus 检测到此现象。如果检测到，Nessus 扫描将调节扫描速率以适应和缓解拥堵。一旦拥塞已经消退，Nessus 会自动再次使用可用空间的网络带宽。
Use Linux kernel congestion detection (使用 Linux 内核拥塞检测)	不启用	使 Nessus 可以监控 CPU 和其他内部运作的拥塞，并相应缩减扫描速率。Nessus 将始终尝试使用尽可能多的每个可用资源。此功能仅可用于部署在 Linux 上的 Nessus 扫描仪。
Network timeout (in seconds)(网络超时-秒)	**5**	默认设置为五秒。这是 Nessus 将等待来自主机的响应的时限，除非在插件中另有规定。如果您在扫描慢速连接，您可能希望设置到一个更长的秒数时
Max simultaneous checks per host (单个主机最大并发检查数)	**5**	该设置限制了同时针对单个主机情况下，Nessus 扫描仪将执行的最大检查数量。
Max simultaneous hosts per scan(扫描最多主机并发数)	**30**	该设置限制了 Nessus 扫描仪同时可以扫描的主机最大并发数量。
Max number of concurrent TCP sessions per host(主机最大并发 TCP 会话数)	无	该设置限制了单个主机建立 TCP 会话的最大数量。

		这个 TCP 节流选项也控制了每秒的 SYN 扫描器最终将发送的包的数量（例如，如果将此选项设置为 15，SYN 扫描器每秒最多会发送 1500 个数据包）
Max number of concurrent TCP sessions per scan (每个扫描 TCP 会话的最大并发数量)	无	该设置限制了在整个扫描过程中建立的 TCP 会话最大数量，不论扫描了多少主机。 对于装载在 Windows XP, Vista, 7, and 8 主机上的 Nessus 扫描仪，设定的数量必须在 19 或以下，以取得准确结果。



下列选项针对 **General settings(常规设置)**:

选项	默认设置	说明
Enable Safe Checks(启用安全检查)	启用	安全检查将禁用所有可能对远程主机产生不利影响的插件。
Log Scan Details to Server(服务器的日志扫描细节)	不启用	保存额外扫描细节到 Nessus 服务器日志上（nessusd. messages），包括插件的发起，插件的完成，或者如果一个插件被去除。由此产生的日志可用于确认特定的被使用的插件和被扫描的主机。
Stop scanning hosts that become unresponsive during the scan(对扫描期间无响应的主	不启用	如果勾选此项，一旦 Nessus 检测到主机变得反应迟钝将停止扫描。这可能导致若在扫描过程中用户关闭个人电脑，在拒绝服务插件发起时主机已停止响应，或安全机制（例如，IDS）已开始阻塞服务器。继续扫描这些机器会发出不必要的在网络上的流量并延迟扫描。

Scan IP addresses in a random order(随机扫描 IP 地址)	不启用 子网	默认情况下,Nessus 将按 IP 地址的列表顺序进行扫描。如果勾选此项,Nessus 将随机扫描的主机列表。这在大量扫描时，通常对帮助分发针对特定在网络流量是很有用的。

下列选项定义了 **Performance options(性能选项)**:

选项	默认设置	说明
Slow down the scan when network congestion is detected (当检测到网络拥塞时减缓扫描速度)	无	当发送过多的数据包和网络带宽快要不能负荷时，这将使 Nessus 检测到此现象。如果检测到，Nessus 扫描将调节扫描速率以适应和缓解拥堵。一旦拥塞已经消退，Nessus 会自动再次使用可用空间的网络带宽。
Use Linux kernel congestion detection (使用 Linux 内核拥塞检测)	无	使 Nessus 可以监控 CPU 和其他内部运作的拥塞，并相应缩减扫描速率。Nessus 将始终尝试使用尽可能多的每个可用资源。此功能仅可用于部署在 Linux 上的 Nessus 扫描仪。
Network timeout (in seconds) (网络超时-秒)	**5**	默认设置为五秒。这是 Nessus 将等待来自主机的响应的时限，除非在插件中另有规定。如果您在扫描慢速连接，您可能希望设置到一个更长的秒数时间。
Max simultaneous checks per host(单个主机最大并发检查数)	**5**	该设置限制了同时针对单个主机情况下，Nessus 扫描仪将执行的最大检查数量。
Max simultaneous hosts per scan(单个主机最大并发检查数)	**30**	该设置限制了 Nessus 扫描仪同时可以扫描的主机最大并发数量。
Max number of concurrent TCP sessions per host (主机最大并发 TCP 会话数)	无	这个 TCP 节流选项也控制了每秒的 SYN 扫描器最终将发送的包的数量（例如，如果将此选项设置为 15，SYN 扫描器每秒最多会发送 1500 个数据包） 该设置限制了单个主机建立 TCP 会话的最大数量。
Max number of concurrent TCP sessions per scan (每个扫描 TCP 会话的最大并发数量)	无	该设置限制了在整个扫描过程中建立的 TCP 会话最大数量，不论扫描了多少主机。 对于装载在 Windows XP, Vista, 7, and 8 主机上的 Nessus 扫描仪，设定的数量必须在 19 或以下，以取得准确结果。

移动设备管理

随着个人和企业越来越依赖移动设备来处理平时的事务，其渗透率已达到历史新高。围绕“自备设备”(BYOD)安全性和集成的市场业已得到迅速发展。不论喜欢还是不喜欢,也不管知道与否,移动设备越来越普遍地被连接到公司网络。在某些情况下,这样的连接似乎是无害的，例如电池充电等活动。但事实上，简单的设备充电通常是通过 USB 连接执行的，而这一样可能桥接到设备和电脑。

由于这些移动设备并不一直连接在网络上，所以有时主动扫描无法直接从网络中的侦测到它们。有几种方法可以甄别移动设备连接到网络的途径。一是利用移动设备管理（MDM）控制台，其中就包含网络中移动设备的很多有用信息。

这种方法的缺点正是该问题被称为“自带设备”的原因，这类设备通常是一个不参加 MDM 系统的个人设备。

一个更好的方法是利用从连接到微软 Exchange 服务器获得的设备信息。基本上，所有自行加入网络的员工都将自己移动设备的操作系统版本和其他信息同步返回到了 Exchange 服务器。这提供了一个非侵入性的方法，以获得的设备类型和操作系统版本。由于 Exchange 服务器是广泛部署的，这些信息在许多基础设施上都是可用的。但这种方法的缺点是，这样所获得的信息比从 MDM 上获得的要少很多。

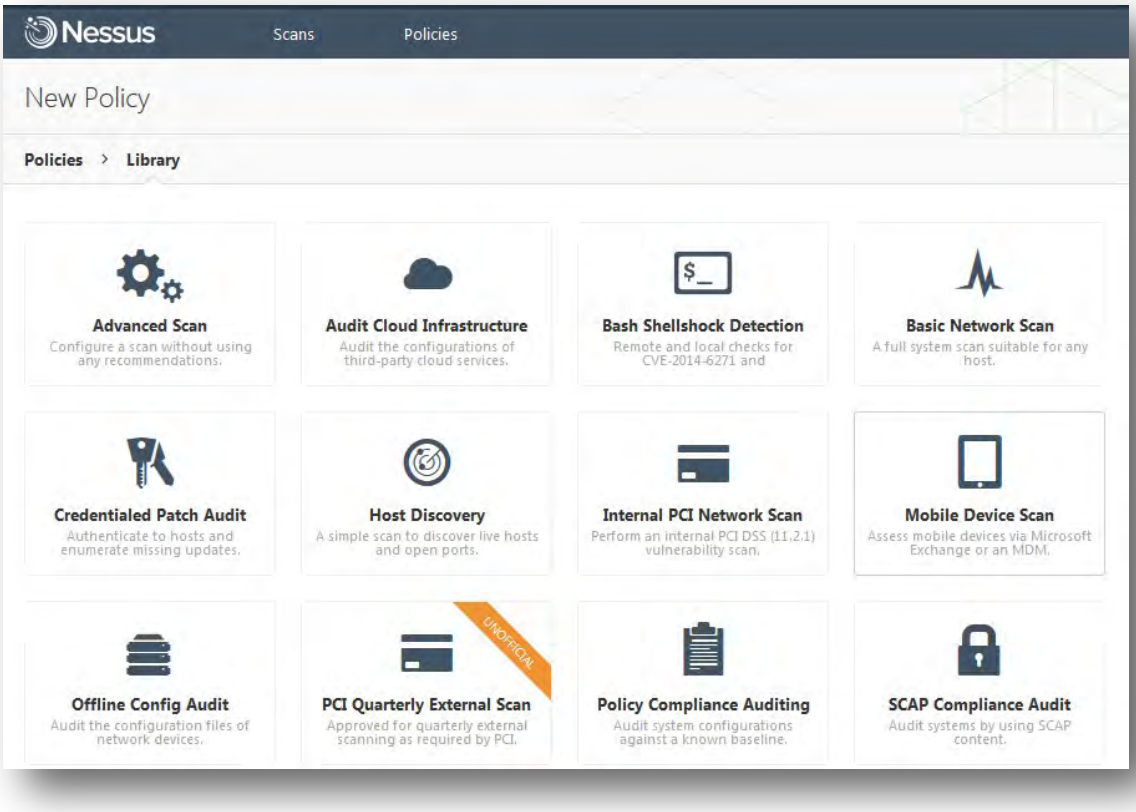
使用 Nessus Manager(Nessus 管理版), Nessus 的“移动设备”插件组提供了获取信息的能力，这些信息有来自 MDM 的设备注册信息，也有 Active Directory 服务器中提供的来自 MS Exchange 服务器上的信息。目前，这些信息包括苹果 iPhone, 苹果 iPad,Windows Phone,和 Android 设备提供的版本信息, 也有在过去的一年(365 天)中“checked in（检入）”的服务器。

Nessus 扫描仪必须能够达到移动设备管理服务器(MDM)以查询信息。您必须确保没有筛选设备阻止这些系统流量通过 Nessus 扫描仪。此外, Nessus 必须被赋予对 Active Directory 服务器的管理凭证(如:域管理员)。

要扫描移动设备，Nessus 必须配置管理服务器和相关手机插件的身份验证信息。由于 Nessus 直接向管理服务器认证，扫描指定主机时不需要配置扫描策略。

创建扫描任务

为了扫描移动设备系统，需要创建一个新的策略，并选择“**Mobile Device Scan(移动设备扫描)**”策略向导。它将要求执行扫描所需的基本信息并自动创建其他策略。向导还允许您控制报告长度,共享扫描结果,并导入凭证以访问移动设备管理器。

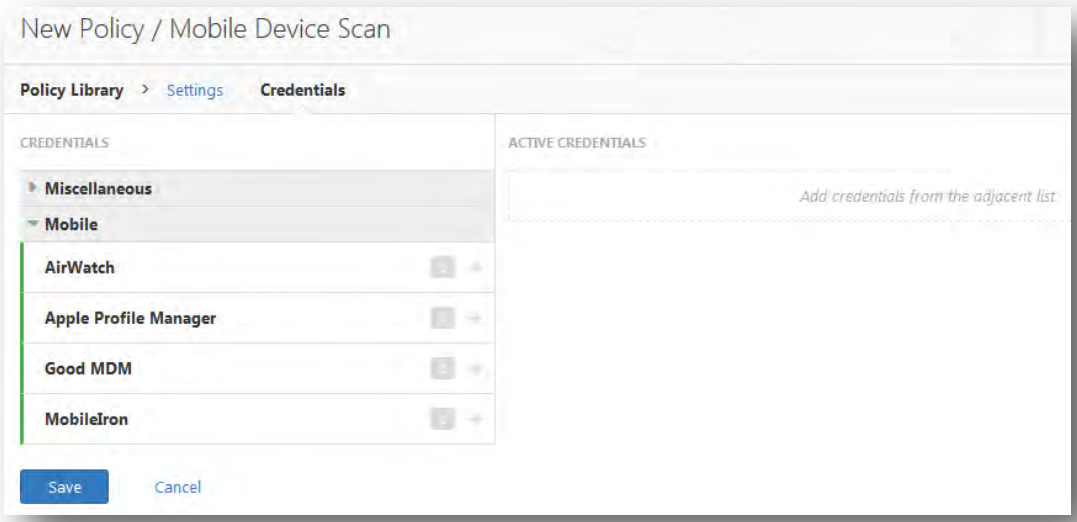


从 Microsoft Exchange 服务器访问数据的 ActiveSync 同步扫描, Nessus 将从手机检索在过去的 365 天已经更新的信息。

Plugins(插件)和策略优选

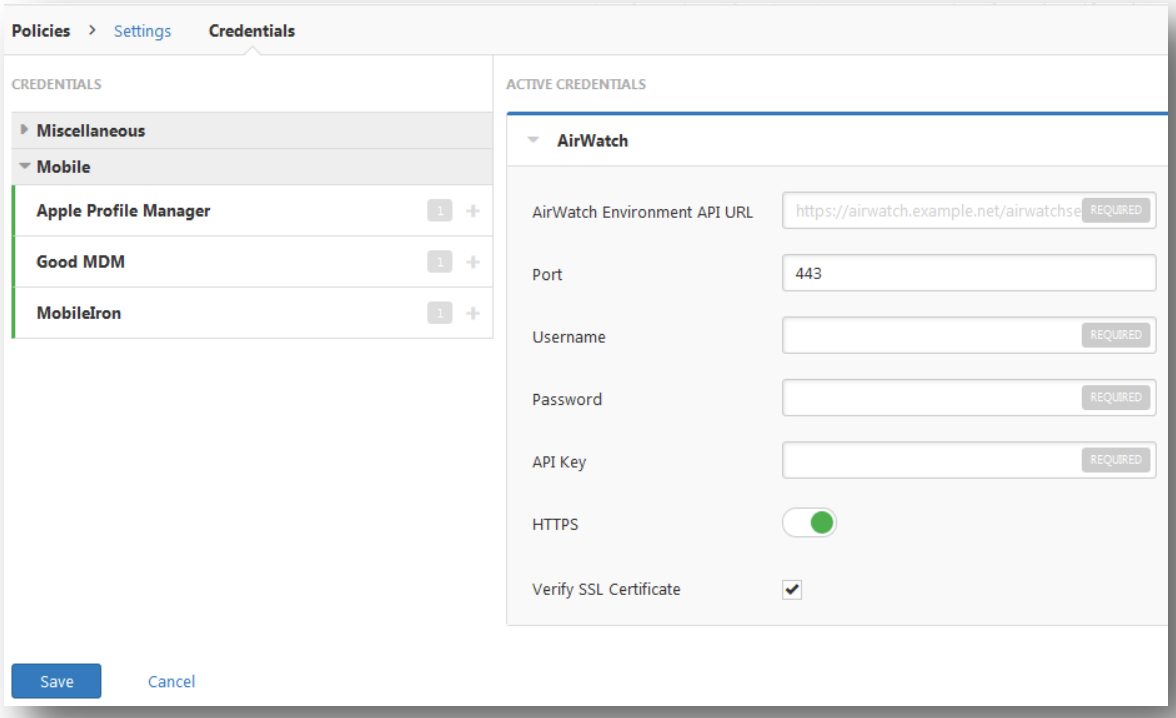
移动设备的策略也可以用“**Advanced Scan**(高级扫描)”模板创建。

扫描移动设备管理服务器,身份验证凭证建立在“**Credentials**(凭证)”标签和“**Advanced Scan**(高级扫描)”的子标题“**Mobile**(移动设备)”下,或在移动扫描策略向导的步骤 2 中。您的扫描策略不需要配置为扫描任意端口或使用任意端口扫描器。



移动设备管理证书

“**Apple Profile Manager API Settings**”(苹果配置文件管理器 API 设置), “**AirWatch API Settings**”(AirWatch API 设置), “**Good MDM Settings**”(Good MDM 设置), 以及 “**MobileIron**” 主机设备不需要就直接可以获取信息。其他系统，Nessus 扫描仪必须能扫到移动设备管理器(MDM) 来获取设备信息。当这些选项被配置后，扫描策略不要求目标主机来扫描；您可以针对目标“localhost” (本地主机)，该策略仍然会接触到 MDM 服务器获取信息。



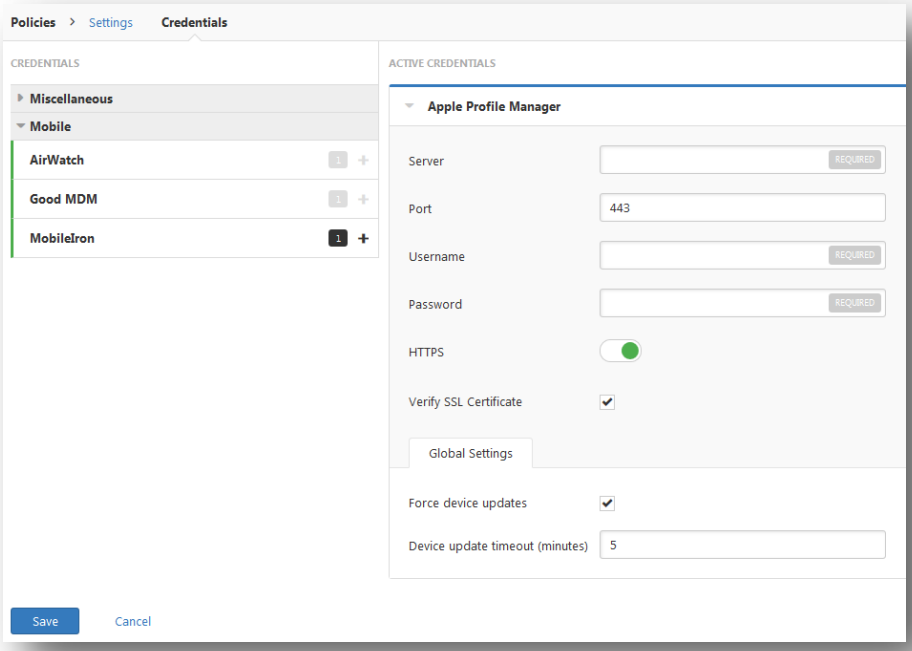
AirWatch

“**AirWatch**”允许 Nessus 通过使用指定的凭证和 API key 来索取 AirWatch 的 API, 集成所管理的移动设备信息。这些特征不要求在扫描策略中指定任何端口。您可以选择通过可被指定的 SSL，以及验证 SSL 证书来通信。

选项	默认设置	说明
AirWatch Environment API URL(AirWatch 环境 API URL)	无	这是用以访问服务器 API 的 URL。这是一个必需的字段。
Port(端口)	**443**	Nessus 与 Airwatch 通信的默认端口。
Username(用户名)	无	访问 AirWatch 的用户名。这是一个必需的字段。
API Key	无	访问 AirWatch 的 API key。这是一个必需的字段。
HTTPS	启用	通过 HTTPS，而不是 HTTP 访问 AirWatch。这将加密连接。
Verify SSL Certificate (验证 SSL 证书)	启用	验证 SSL 证书有效性

苹果的配置文件管理器

“**Apple Profile Manager**”(苹果的配置文件管理器)允许 Nessus 查询苹果文件管理器服务器，以枚举在网络上的苹果 iOS 设备（例如，iPhone, iPad）。使用证书和服务器信息，Nessus 直接从文件管理器验证配置，查询设备信息。另外，通过 SSL 的通信也可以被指定，并指导服务器强迫设备信息更新（即，每个设备将对配置管理服务器更新信息）。



配置 Apple Profile Manger 的选项如下:

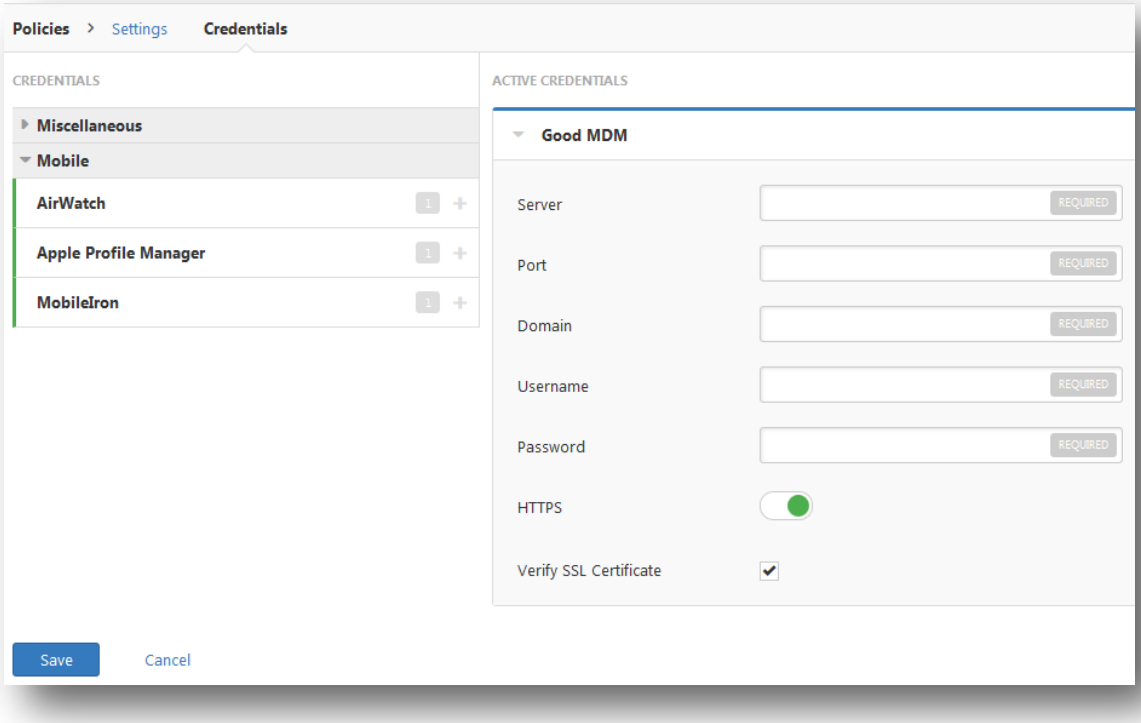
选项	默认设置	说明
Server(服务器)	无	苹果的配置文件管理器的服务器名称。这是一个必需的字段。
Port(端口)	**443**	Nessus 为 Apple Profile Manager 做检查的端口.
Username(用户名)	无	访问 Apple Profile Manager 的用户名。这是一个必需的字段。
API Key	无	访问 Apple Profile Manager 的 API key。这是一个必需的字段。
HTTPS	启用	通过 HTTPS，而不是 HTTP 访问 Apple Profile Manager。这将加密连接。
Verify SSL Certificate (验证 SSL 证书)	启用	验证 SSL 证书有效性

对于 Apple Profile Manager(苹果的配置文件管理器)的全局设置：

选项	默认	说明
Force Device Updates(强制设备更新)	启用	此选项强制要求 Apple Profile Manager 启动更新。.
Device update timeout (minutes)(设备更新超时-分钟)	**5**	此项是 Apple Profile Manager 更新超时的限定值。

Good MDM

“**Good MDM**” 允许 Nessus 在 Good 服务器上查询网络上列举的移动设备。使用证书和服务器信息，Nessus 验证 Good 服务器，以直接查询设备信息。同样的，通信可以通过指定的 SSL 以及严格的 SSL 证书验证来实现。

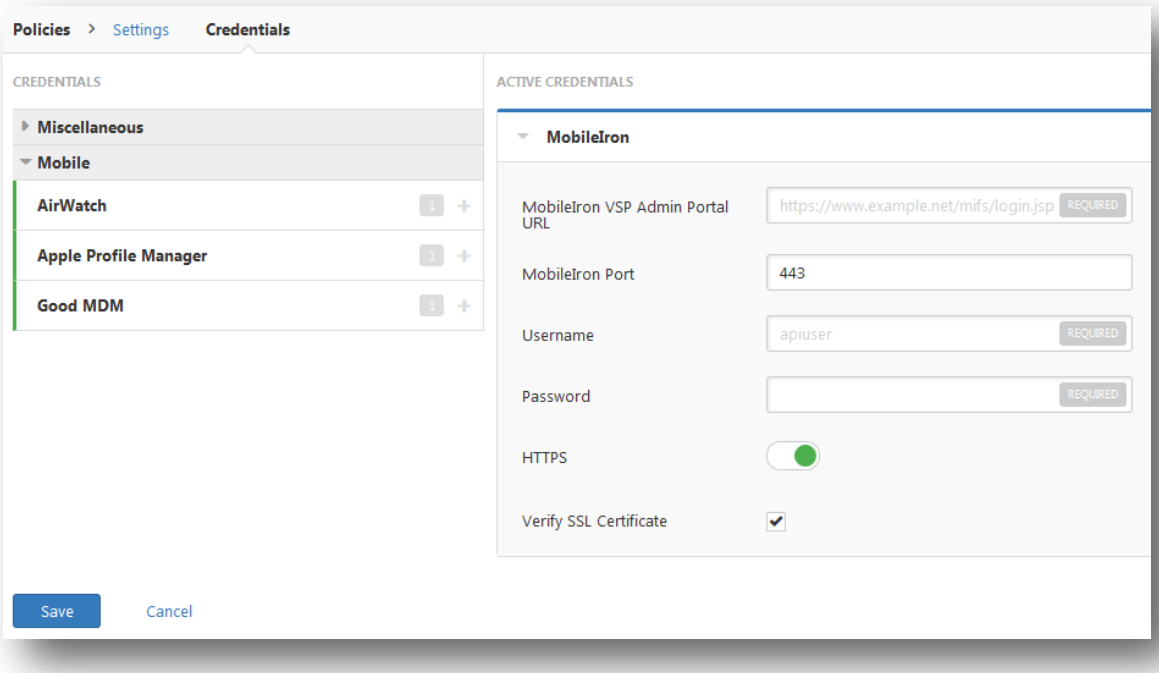


Good MDM 的配置选项如下：

选项	默认设置	说明
Server(服务器)	无	Good MDM 服务器的名字。这是一个必需的字段。
Port(端口)	无	Nessus 检测 Good MDM 的默认端口
Domain(域)	无	Good MDM 的域
Username(用户名)	无	访问 Good MDM 的用户名。这是一个必需的字段。
Password(密码)	无	之前提交的用户名所对应的密码
HTTPS	启用	通过 HTTPS，而不是 HTTP 访问 Good MDM。这将加密连接。
Verify SSL Certificate (验证 SSL 证书)	启用	验证 SSL 证书有效性

MobileIron

“**MobileIron**”允许 Nessus 在 MobileIron 服务器上查询列举的移动设备 (如, iPhone, iPad, HTC, BlackBerry, Android)。使用证书和服务器信息，Nessus 使用身份验证 API 调用来查询设备信息的服务器。同样的，通信可以通过指定的 SSL，或引导服务器验证 SSL 证书增强安全性。

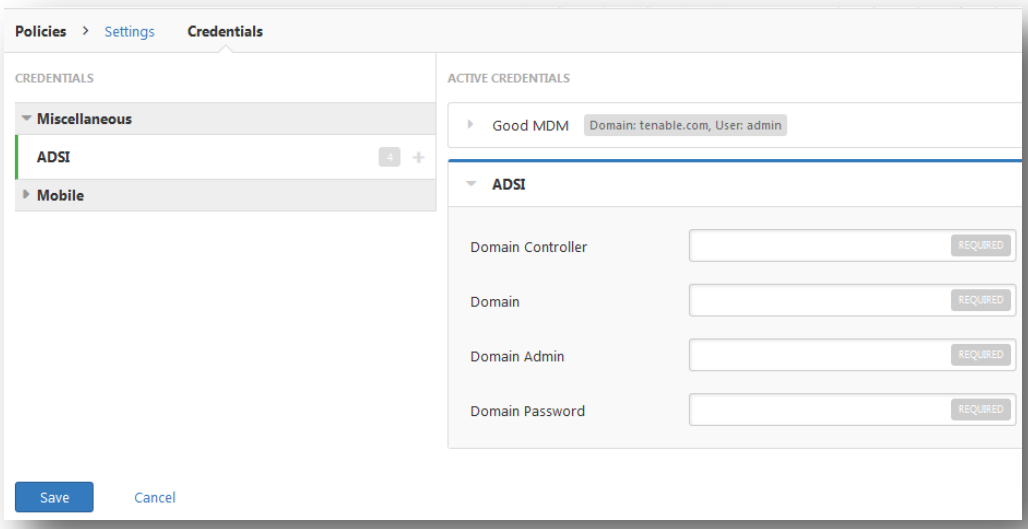


MobileIron 的配置选项如下：

选项	默认设置	说明
MobileIron VSP Admin Portal URL	无	访问 MobileIron VSP Admin 端口的 URL。这是一个必需的字段。
Port(端口)	**443**	Nessus 检测 MobileIron 的默认端口。
Username(用户名)	无	访问 MobileIron 的用户名。这是一个必需的字段。
Password(密码)	无	之前提交的用户名所对应的密码
HTTPS	启用	通过 HTTPS，而不是 HTTP 访问 MobileIron。这将加密连接。
Verify SSL Certificate	启用	验证 SSL 证书有效性

ADSI

Nessus 还可以利用动态同步到移动设备管理器:



“**ADSI**” 允许 Nessus 查询动态同步服务器，以确定是否有任何 Android 或 iOS 设备连接。使用证书和服务器信息，Nessus 授权给域控制器（不是 Exchange 服务器）直接查询它的设备信息。这个功能不需要到任何端口上的指定扫描策略。移动设备扫描需要这些设置。

ADSI 配置选项见下表:

选项	描述
域控制器	动态同步的域控制器的名称
域	动态同步的域 Windows 的名称
域管理员	与管理员的用户名
域密码	域管理员的密码

Nessus 仅支持从 Exchange Server 2010 和 2013 获得移动信息。 Nessus 不能从 Exchange Server2007 检索信息。

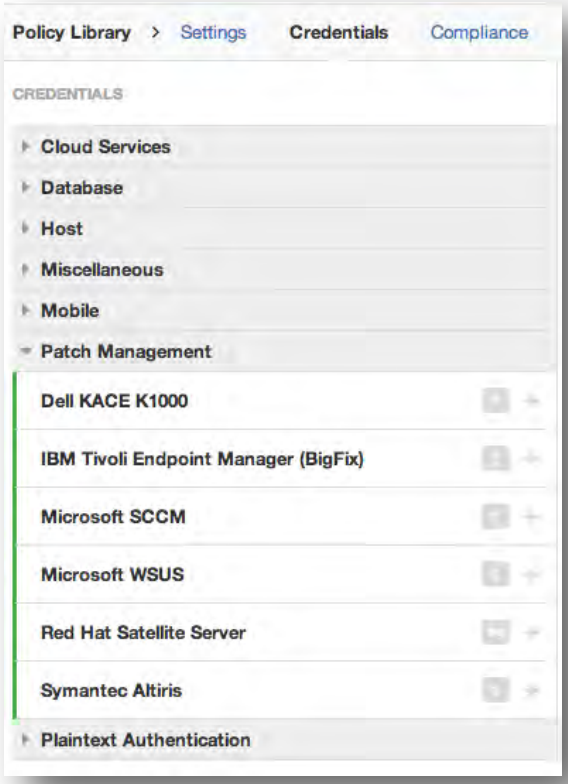
补丁管理

Nessus Manager 可以利用红帽网络卫星、IBM TEM、Dell KACE 1000、WSUS and SCCM 补丁管理系统对于可能无法使用 Nessus 扫描仪的证书进行补丁审计。 这些补丁管理系统选项可以在各自的下拉“证书”中被发现，在各自的下拉被发现

菜单: “**Symantec Altiris**”, “**IBM Tivoli Endpoint Manager (BigFix)**”, “**Red Hat Satellite Server**”, “**Microsoft SCCM**”, “**Dell**

KACE K1000”, 和 “**Microsoft WSUS**”.

IT 管理员需要管理补丁监控软件并在他们的系统安装所有需要的补丁管理系统的 agents 。



IBM Tivoli Endpoint Manager (BigFix)

Tivoli Endpoint Manager (TEM) 可以从 IBM 为桌面系统管理更新和修补程序的分布。 Nessus 和 SCCV 具有查询 TEM 的能力，以验证由 TEM 管理的系统是否安装补丁，并通过 Nessus Manager 显示补丁信息。

- 如果证书检查看到一个系统，但它无法验证该系统，将使用从补丁管理系统获得的数据进行检查。如果 Nessus 是能够连接到目标系统，它将在该系统上执行检查，并忽略 TEM 输出。
- TEM 服务器已经从托管主机获得的数据，通过 TEM 回传到 Nessus 仅作为当前的最新数据。

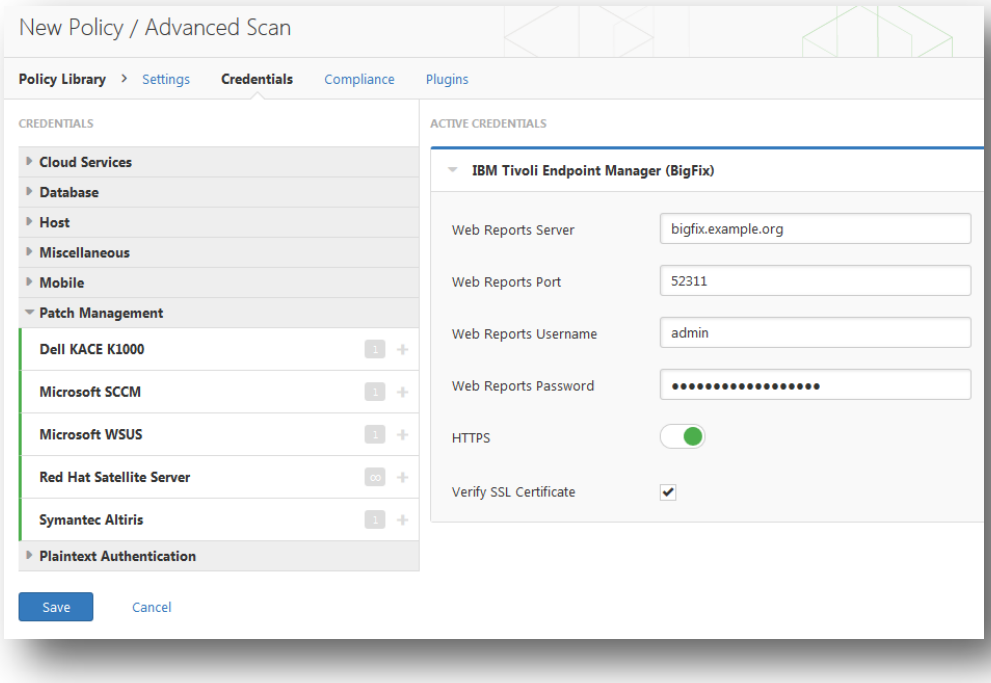
TEM 通过使用 5 个 Nessus 插件来扫描:

- 补丁管理: Tivoli Endpoint Manager Computer Info Initialization (Plugin ID 62559)
- 补丁管理: Missing updates from Tivoli Endpoint Manager (Plugin ID 62560)

- 补丁管理: IBM Tivoli Endpoint Manager Server Settings (Plugin ID 62558)
- 补丁管理: Tivoli Endpoint Manager Report (Plugin ID 62561)
- 补丁管理: Tivoli Endpoint Manager Get Installed Packages (Plugin ID 65703)

IBM Tivoli Endpoint Manager 服务器的证书必须提供用于 TEM 扫描的正常工作。

“Credentials” 菜单中, 选择 “Patch Management: IBM Tivoli Endpoint Manager Server (BigFix)” 从插件下拉菜单:



补丁管理: TEM 服务器设置

证书	默认	描述
Web 报告服务器	无	IBM TEM Web 报告服务器名称
Web 报告端口	无	IBM TEM Web 报告服务器监听端口
Web 报告用户名	无	Web 报告管理员用户名
Web 报告密码	无	Web 报告管理员用户名密码
HTTPS	启用	如果 Web 报告服务器正在使用 SSL
确认 SSL 证书	启用	确认 SSL 证书有效

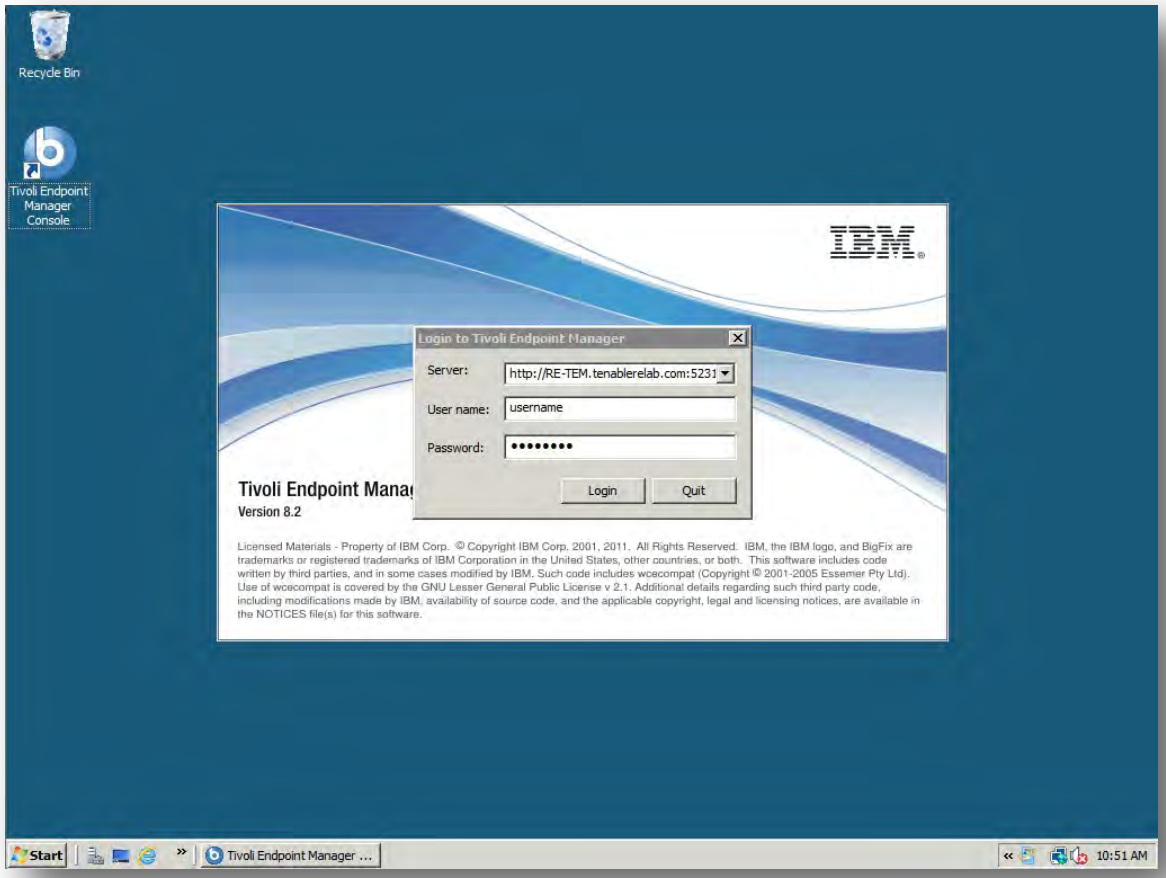
套餐报告是由 IBM TEM 正式支持的基于 RPM 和基于 Debian 的版本来支持。这包括红帽衍生物例如 RHEL、CentOS、Scientific Linux 和 Oracle Linux，以及 Debian 和 Ubuntu。其他的版本也可能工作，但除非 TEM 官方支持，否则将不提供支持。

对于触发本地插件，只有 RHEL、CentOS、Scientific Linux、Oracle Linux、Debian 和 Ubuntu 是支持的。必须启用插件“Patch Management: Tivoli Endpoint Manager Get Installed Packages”。

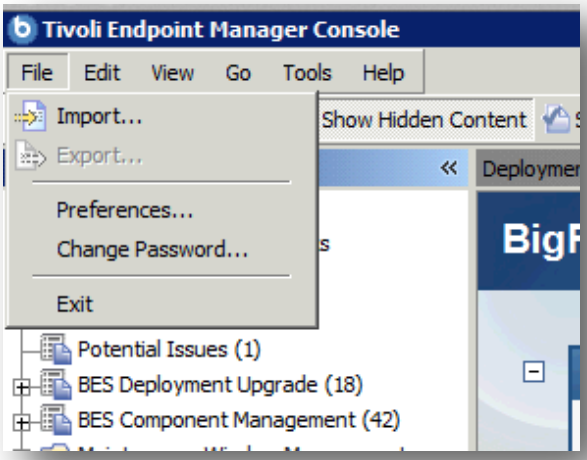
为了使用这些审计功能，必须对 IBM TEM 服务器做改变. 自定义分析必须导入 TEM，这样详细的的软件包信息将被检索，并提供给 Nessus。此过程概述如下。在开始前，下面的文本必须保存到 TEM 系统上的文件中，并用一个**.bes** 扩展命名:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:noNamespaceSchemaLocation="BES.xsd">
         <Analysis>
             <Title>Tenable</Title>
             <Description>This analysis provides Nessus with the data it needs for
           vulnerability reporting. </Description>
             <Relevance>true</Relevance>
              <Source>Internal</Source>
              <SourceReleaseDate>2013-01-31</SourceReleaseDate>
              <MIMEField>
                       <Name>x-fixlet-modification-time</Name>
                       <Value>Fri, 01 Feb 2013 15:54:09 +0000</Value>
             </MIMEField>
             <Domain>BESC</Domain>
             <Property Name="Packages - With Versions (Tenable)" ID="1"><![CDATA[if
           (exists true whose (if true then (exists debianpackage) else false)) then
           unique values of (name of it & "|" & version of it as string & "|" & "deb" &
           "|" & architecture of it & "|" & architecture of operating system) of
           packages whose (exists version of it) of debianpackages else if (exists true
           whose (if true then (exists rpm) else false)) then unique values of (name of
           it & "|" & version of it as string & "|" & "rpm" & "|" & architecture of it
           & "|" & architecture of operating system) of packages of rpm else
           "<unsupported>"
           ]]></Property>
           </Analysis>
</BES>
```

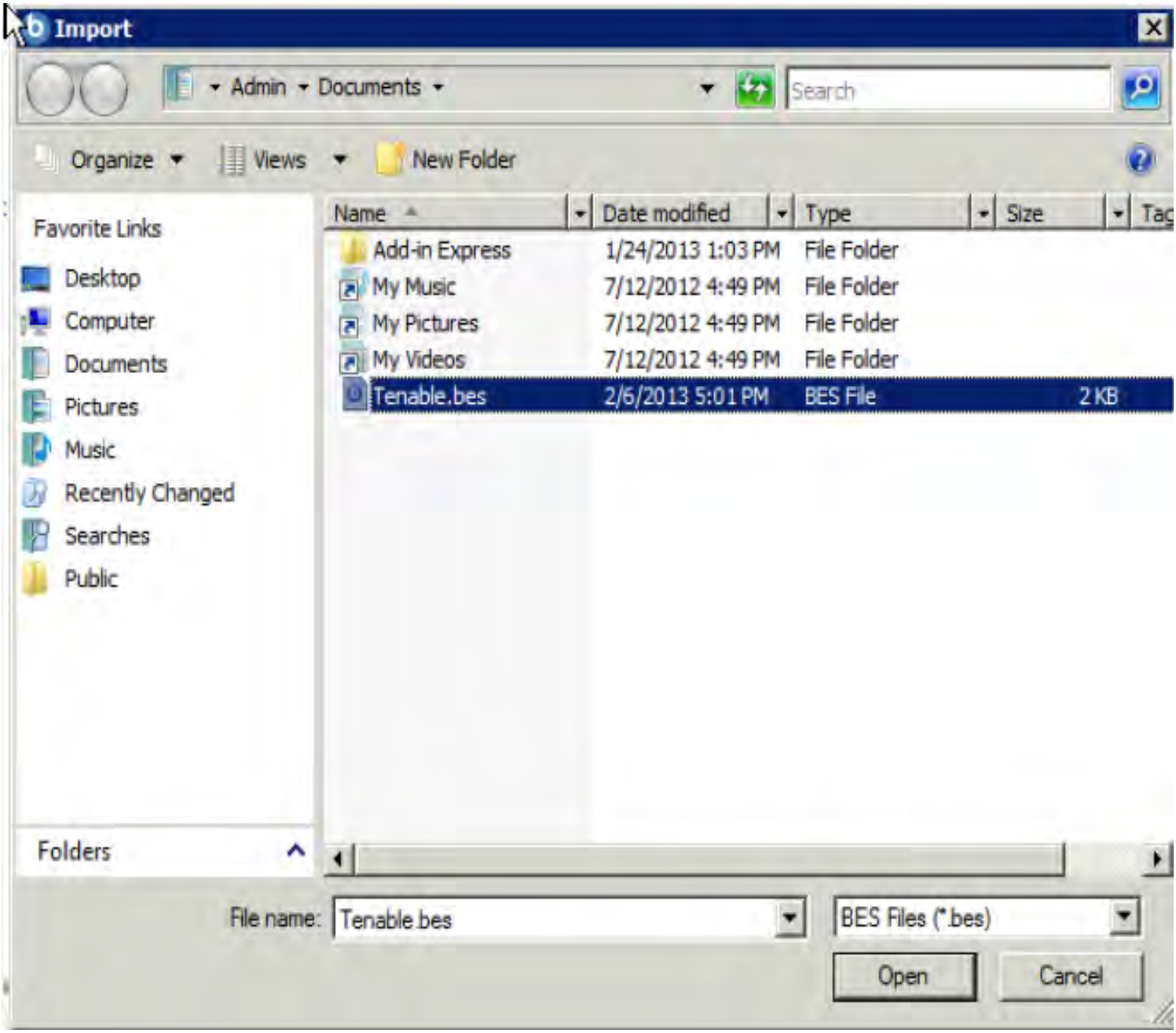
打开 TEM 控制台并登录:



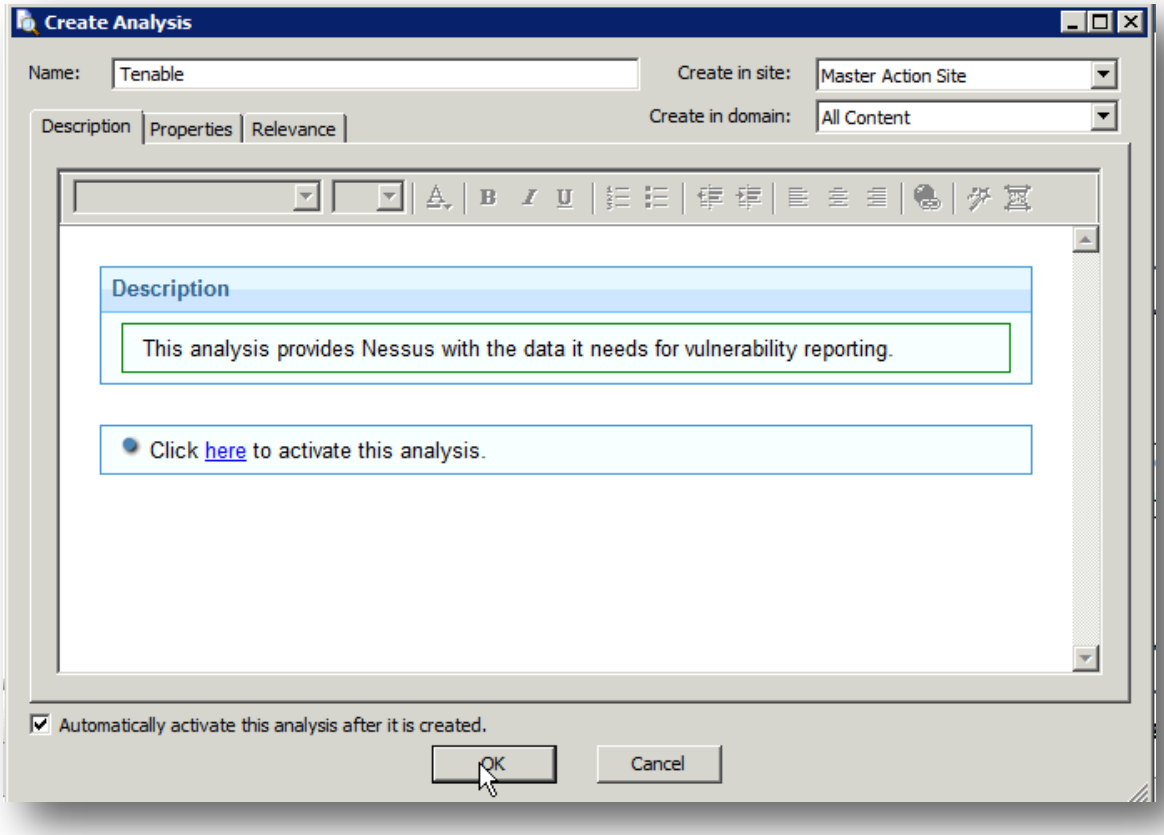
一旦被授权, 点击 “**File**” 菜单项目, 然后 “**Import…**”:



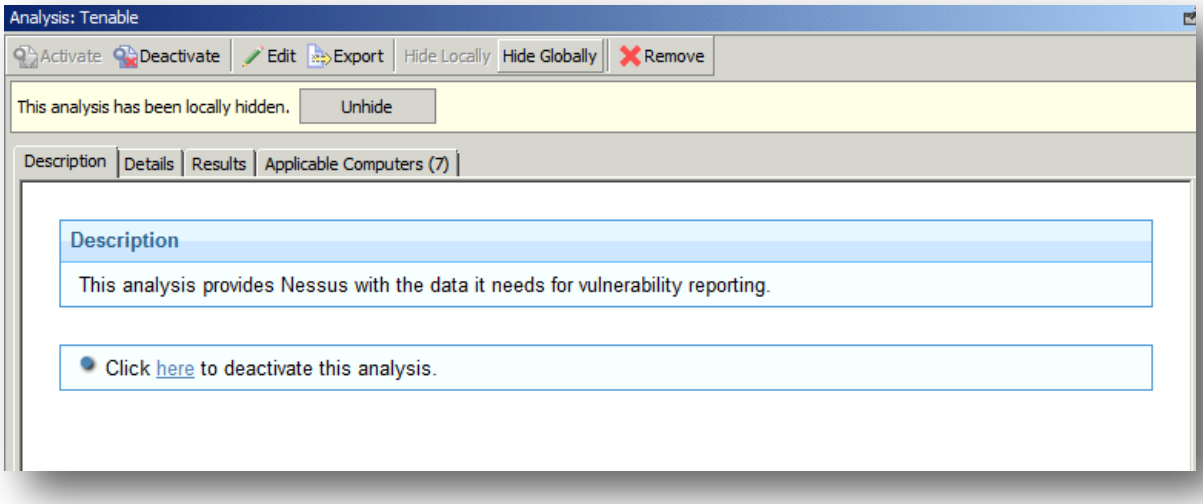
找到配置细节中包含 bes 的文件，然后单击“Open”



当“Create Analysis”对话框打开，点击“**OK**”:



可选的，你可以点击“Hide Locally”，然后 “Hide Globally”从视图中移除，以避免混乱:



这些步骤完成后，它会花费一段时间（根据你的网络和报告进度）来分析至完全填写。你可以通过在标签上的“Applicable Computers”计算目前还有多少台计算机在扫描中。

WSUS

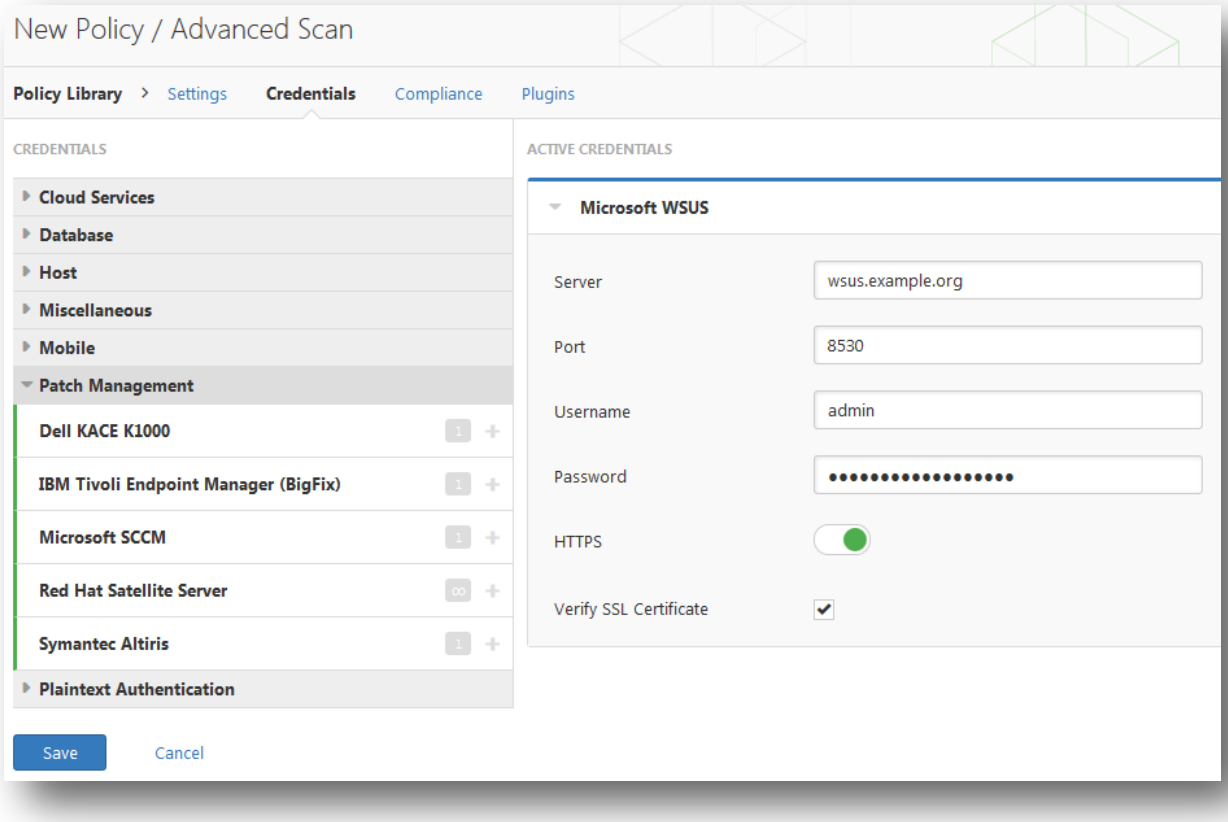
Windows Server Update Services (WSUS) 可通过 Microsoft 管理更新版本和修补程序。 Nessus 和 SCCV 具有查询 WSUS 的能力，以验证由 WSUS 管理的系统是否安装补丁，并通过 Nessus 或 SecurityCenter GUI 显示补丁信息。

- 如果证书检查看到一个系统，但又无法验证该系统，将使用从补丁管理系统获得的数据进行检查。如果 Nessus 能够连接到目标系统，它将在该系统上执行检查，并忽略 WSUS 输出。
- 由 WSUS 服务器从它的托管主机获得的数据，回传到 Nessus 只能作为当前的最新数据。

WSUS 使用三个 Nessus 插件进行扫描:

- 补丁管理: WSUS Server Settings (Plugin ID 57031)
- 补丁管理: Missing updates from WSUS (Plugin ID 57032)
- 补丁管理: WSUS Report (Plugin ID 58133)

WSUS 扫描正常工作必须提供 WSUS 证书。在 “Credentials” 选项中选择 “Patch Management” ，然后 “Microsoft WSUS”。



证书	默认	描述
服务器	无	WSUS IP 地址或服务器名称
端口	8530	WSUS 端口正在运行(通常 TCP 80 或 443)
用户名	无	WSUS 管理员用户名
密码	无	WSUS 管理员密码
HTTPS	启用	如果 WSUS 服务正在运行 SSL
确认 SSL 证书	启用	确认 SSL 证书有效

SCCM

System Center Configuration Manager (SCCM)可从 Microsoft 管理基于 Windows 系统的大型组。 Nessus 有查询 SCCM 服务的能力，以验证由 SCCM 管理的系统是否安装补丁，并通过 Nessus 或 SecurityCenter GUI 显示补丁信息。

- 如果凭证检查看到一个系统，但它无法验证该系统，将使用从补丁管理系统获得的数据进行检查。如果 Nessus 是能够连接到目标系统，它将在该系统上执行检查，并忽略 SCCM 输出。
- SCCM 服务器从它的托管主机获得的数据，返回的数据只能作为当前的最新数据。
- Nessus 连接到运行在 SCCM 站点的服务器（例如，证书必须是对 SCCM 服务有效的，这意味着与在 SCCM 的管理员帐户有权可以查询所有在 SCCM MMC 的数据）。该服务器还可以运行 SQL 数据库或 SCCM 单独的服务器数据库。当借助这次审计，如果他们是在一个单独的盒子，Nessus 必须连接到 SCCM 服务器，而不是 SQL 或 SCCM 服务器。

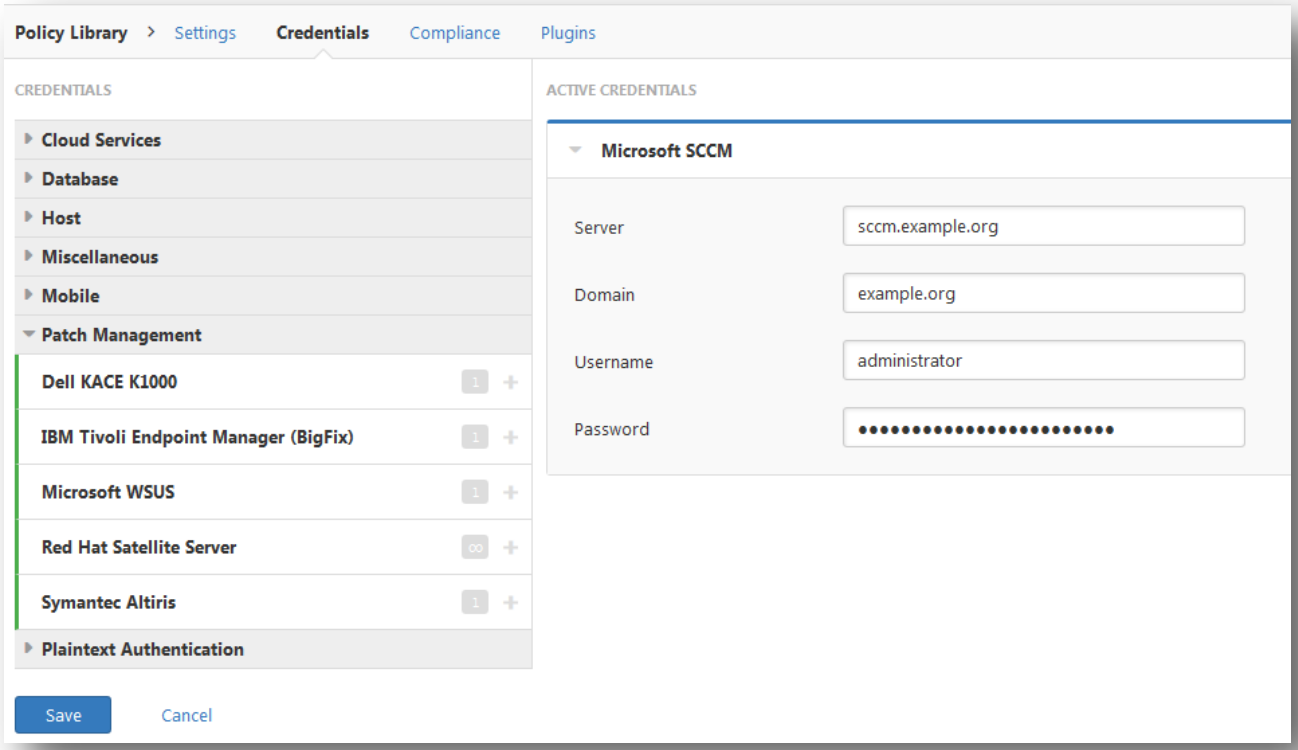
:

Nessus SCCM 补丁管理插件支持 SCCM 2007 和 SCCM 2012。

SCCM 执行扫描使用四个 Nessus plugins:

- 补丁管理: SCCM Server Settings (Plugin ID 57029)
- 补丁管理: Missing updates from SCCM(Plugin ID 57030)
- 补丁管理: SCCM Computer Info Initialization(Plugin ID 73636)
- 补丁管理: SCCM Report(Plugin ID 58186)

SCCM 系统必须提供凭据以便 SCCM 扫描正常工作。在“**Credentials**” 选项下面选择“**Patch Management**” 然后“**Microsoft SCCM**”。



凭据	描述
Server	SCCM IP 地址或系统用户名
Domain	域是 SCCM 服务器的一部分
Username	SCCM 管理员用户名
Password	SCCM 管理员密码

Red Hat Network Satellite

Red Hat Satellite 是基于 Linux 的系统上的系统管理平台。 Nessus 和 SCCV 具有查询卫星的能力，以验证卫星管理的系统是否补丁安装上了没有，并通过 Nessus 或 SecurityCenter GUI 显示补丁信息。

虽然 Tenable 不支持，RHN 卫星插件也可与 Spacewalk 服务器和 Red Hat 开源版本工作。Spacewalk 有能力管理在 Red Hat (RHEL, CentOS, Fedora) 和 SUSE 基础上的版本。Tenable 支持 Red Hat Enterprise Linux 的服务器。

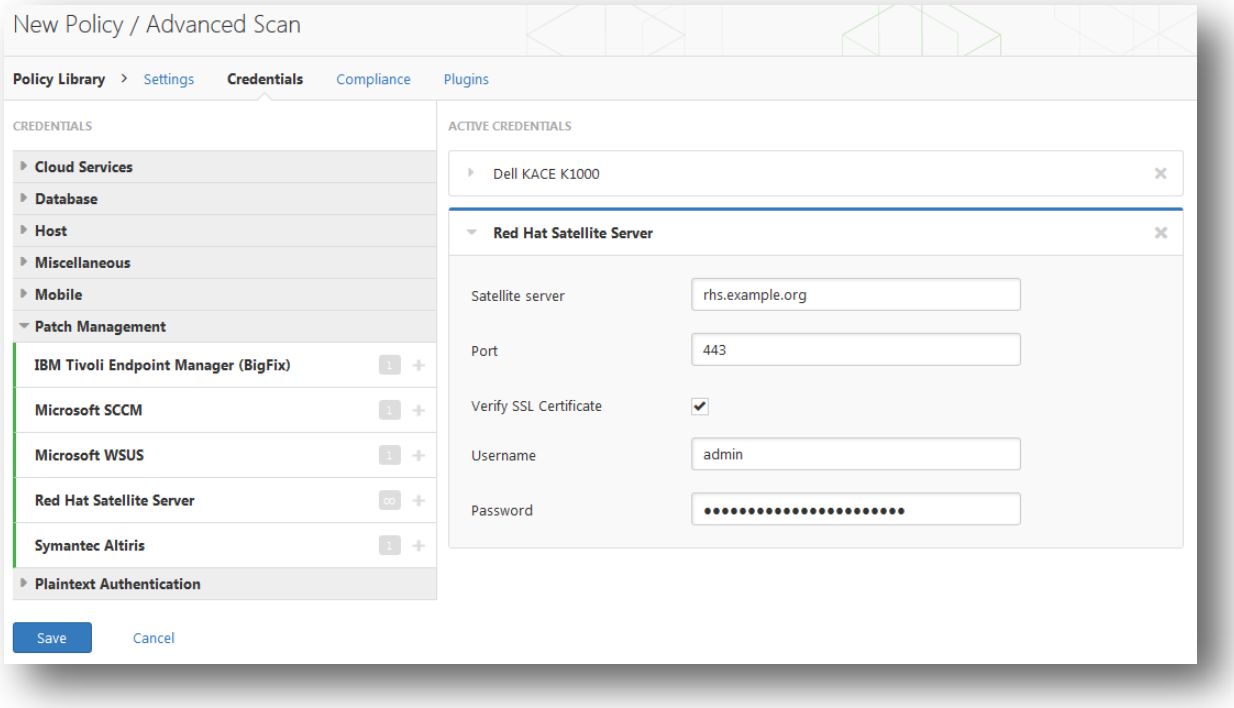
如果凭证检查看到一个系统，但它无法验证该系统，将使用从补丁管理系统获得的数据进行检查。如果 Nessus 是能够连接到目标系统，它将在该系统上执行检查，并忽略 RHN Satellite 输出。

- 卫星服务器从它的托管主机获得的数据，返回的数据只能作为当前的最新数据。

卫星扫描用 5 个 Nessus 插件运行:

- 补丁管理: Patch Schedule From Red Hat Satellite Server (Plugin ID 57066)
- 补丁管理: Red Hat Satellite Server Get Installed Packages (Plugin ID 57065)
- 补丁管理: Red Hat Satellite Server Get Managed Servers (57064)
- 补丁管理: Red Hat Satellite Server Get System Information (Plugin ID 57067)
- 补丁管理: Red Hat Satellite Server Settings (Plugin ID 57063)

Red Hat Satellite 系统的凭证必须提供给 Satellite 系统来使之正常工作。在“Credentials”菜单上选择“Patch Management” 然后 “Red Hat Satellite Server”:



凭证	默认	描述
Satellite server	无	RHN Satellite IP 地址或系统名称
Port	**443**	Satellite 端口正在运行 (通常 TCP 80 or 443)
Verify SSL Certificate	启用	确认 SSL 证书有效
Username	无	Red Hat Satellite 用户名

Password	无	Red Hat Satellite 密码

Dell KACE K1000

KACE K1000 可通过 Dell 管理更新和修补在 Linux、Windows 和 Mac OS X 系统的版本程序。 Nessus 和 SCCV 具有查询 KACE K1000 的能力，以验证 KACE K1000 管理系统是否安装补丁，并通过 Nessus 或 SecurityCenterGUI 显示补丁信息。

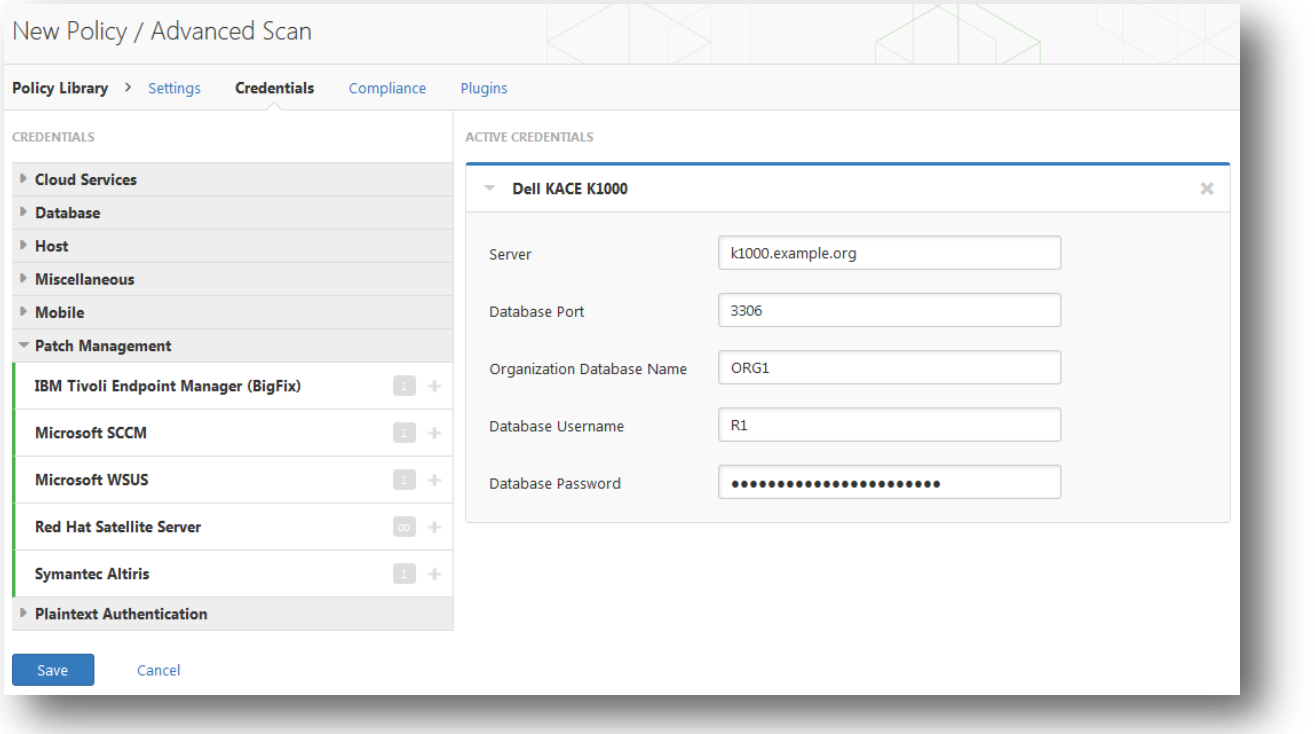
如果凭证检查看到一个系统，但它无法验证该系统，将使用从补丁管理系统获得的数据进行检查。如果 Nessus 是能够连接到目标系统，它将在该系统上执行检查，并忽略 KACE K1000 输出。

- KACE K1000 从它的托管主机获得的数据，返回的数据只能作为当前的最新数据。

KACE K1000 使用 4 个 Nessus 插件进行扫描:

- kace_k1000_get_computer_info.nbin (Plugin ID 76867)
- kace_k1000_get_missing_updates.nbin (Plugin ID 76868)
- kace_k1000_init_info.nbin (Plugin ID 76866)
- kace_k1000_report.nbin (Plugin ID 76869)

Dell KACE K1000 系统的凭证必须提供给 K1000 扫描来使之正常工作。 在“**Credentials**” 菜单下选择 “**Patch Management**” 然后“**Dell KACE K1000**”:



凭据	默认	描述
Server	无	KACE K1000 IP 地址或系统名。这是一个必填字段。
Database Port	**3306**	K1000 数据库端口正在运行 (通常 TCP 3306).
Organization Database Name	**ORG1**	KACE K1000 数据库的组件名称。该组件将开始以字母“ORG”，并在结尾加上一个数字，与 K1000 数据库用户名对应。
Database Username	无	所需登录到 K1000 数据库的用户名。 R 1 是默认的，如果没有用户定义的。用户名开始以字母“R”。代表该组织进行扫描的数目相同，这个用户名会结束。这是一个必填字段。
K1000 Database Password	无	K1000 数据库用户名需要密码验证。这是一个必填字段。

Symantec Altiris

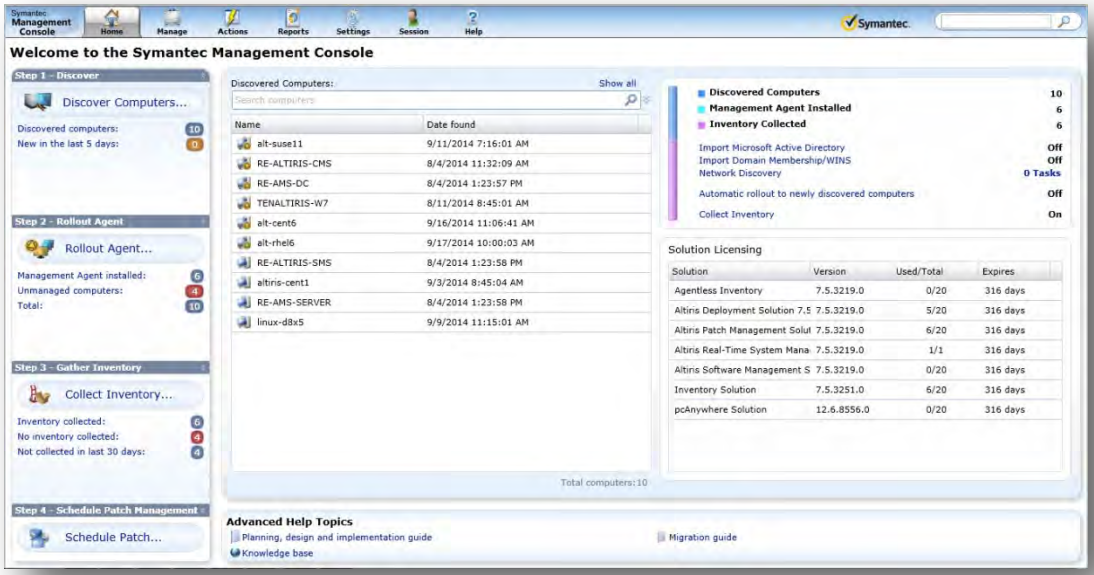
Altiris 可通过 Symantec 管理更新和修补在 Linux、Windows 和 Mac OS X 系统分布的程序。 Nessus 和 SCCV 有能力使用 Altiris API 去以验证是否在 Altiris 公司管理的系统安装补丁，并通过 Nessus 或 SecurityCenterGUI 显示补丁信息。

- 如果凭证检查看到一个系统，但它无法验证该系统，将使用从补丁管理系统获得的数据进行检查。如果 Nessus 是能够连接到目标系统，它将在该系统上执行检查，并忽略 Altiris 输出。
- Altiris 从它的托管主机获得的数据，返回的数据只能作为当前的最新数据。
- Nessus 连接到 Altiris 主机上运行的 Microsoft SQL 服务器（例如， MSSQL 数据库的证书必须是有效的，这意味着数据库帐户有权限查询在 Altiris MSSQL 数据库所有的数据）。数据库服务器可以从 Altiris 部署在单独的主机上运行。当利用这次审计，Nessus 必须连接到 MSSQL 数据库，而不是 Altiris 服务器，如果他们是在一个单独的盒子。

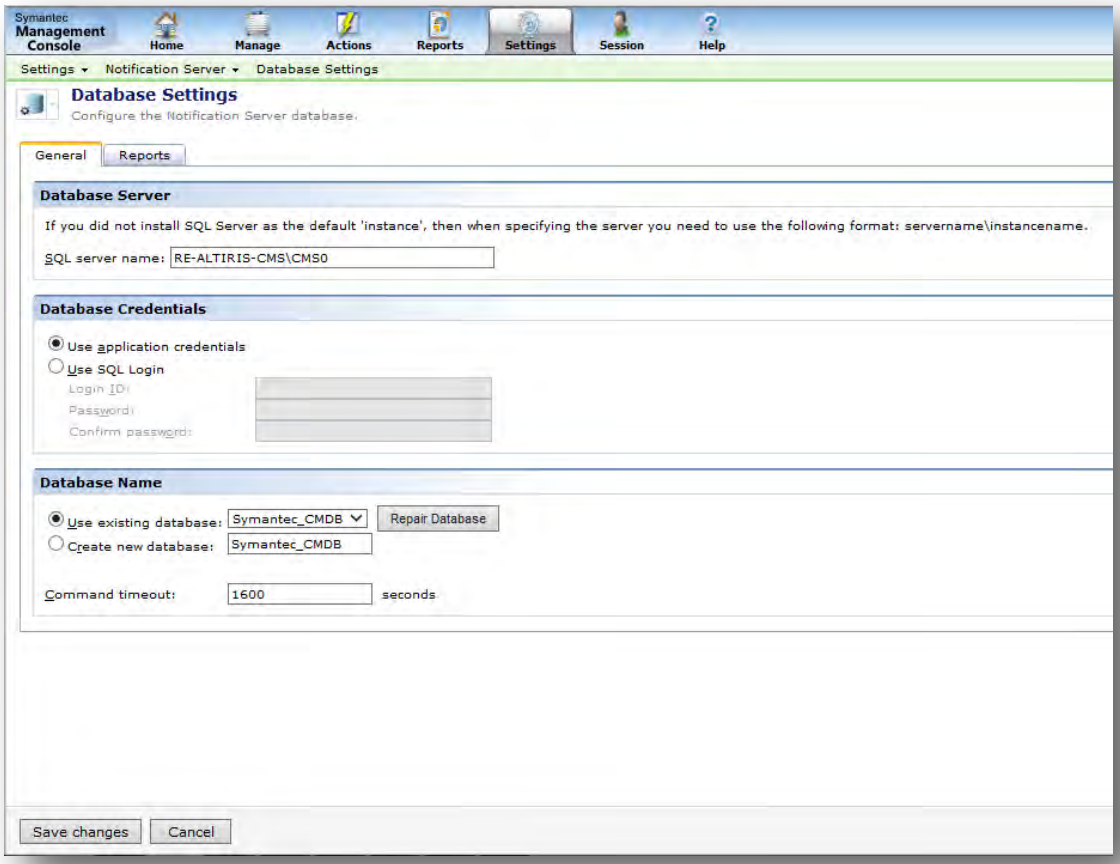
Altiris 使用 4 个 Nessus 插件扫描:

- symantec_altiris_get_computer_info.nbin (Plugin ID 78013)
- symantec_altiris_get_missing_updates.nbin (Plugin ID 78012)
- symantec_altiris_init_info.nbin (Plugin ID 78011)
- symantec_altiris_report.nbin (Plugin ID 78014)

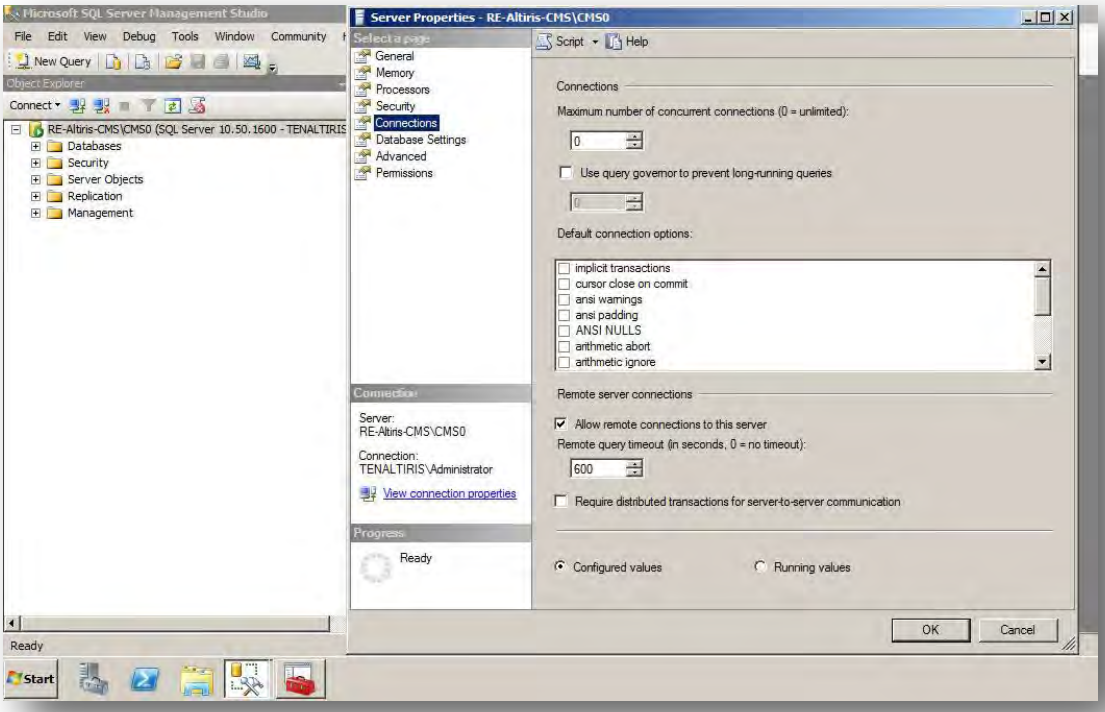
为了确保 Nessus 可以正常使用 Altiris 拉取补丁管理信息，则必须这样配置。



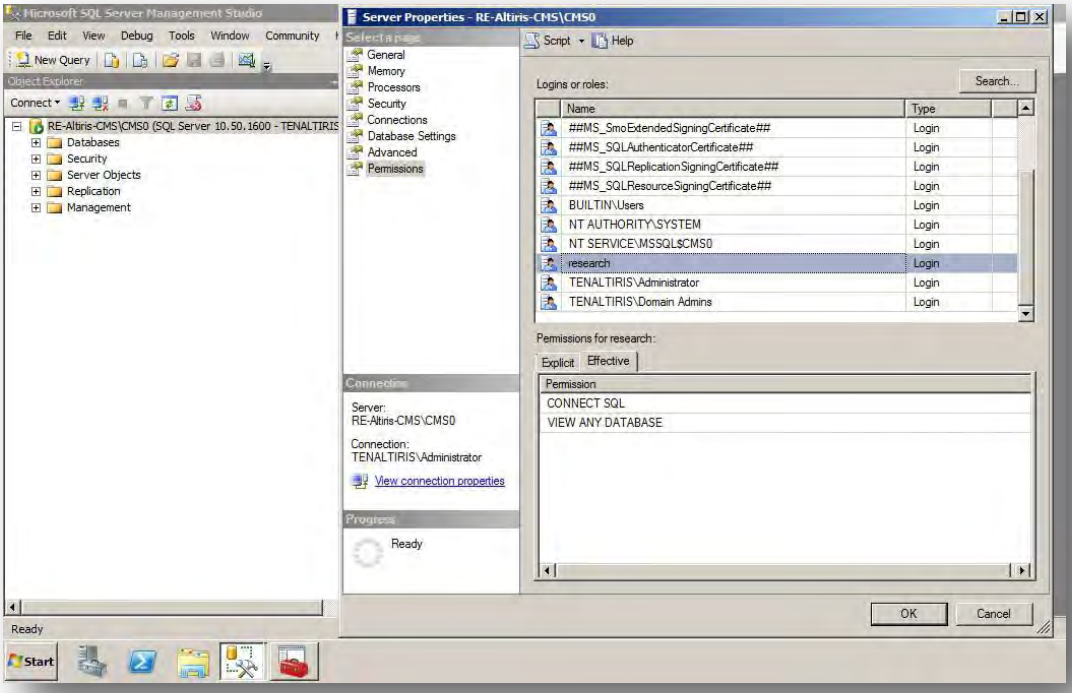
从仪表板（如上所示），点击 “Settings” 然后 “Database Settings”:



确保 SQL 服务器名被设置，并且选择数据库。接下来，配置 Microsoft SQL 服务器:

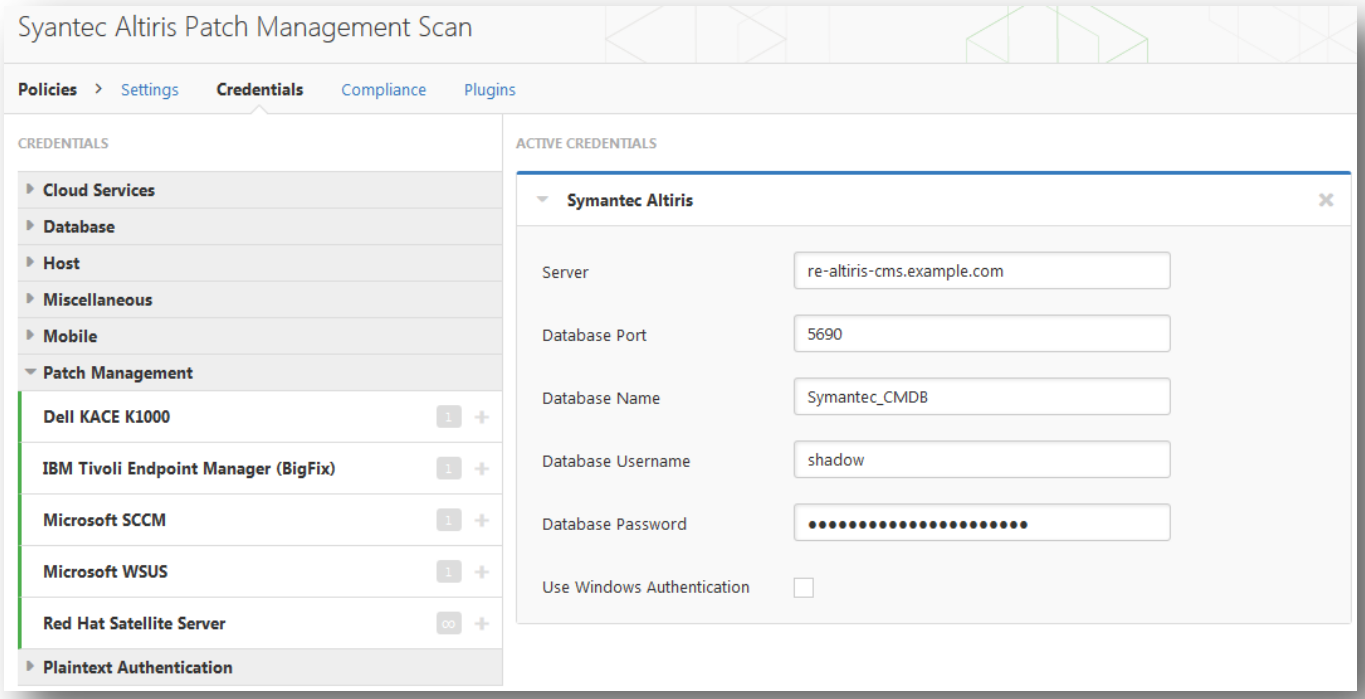


在 “**Connections**”菜单下, 必须选择“Allow remote connections to this server”，下一步导航到“**Permissions**” 菜单:



Nessus 用“CONNECT SQL” 和 “VIEW ANY DATABASE” 凭证配置账户。

Altiris Microsoft SQL (MSSQL) 数据库凭证必须提供以便 Altiris 扫描正常工作。在“**Credentials**”菜单下选择“**Patch Management**” 然后“**Symantec Altiris**”:



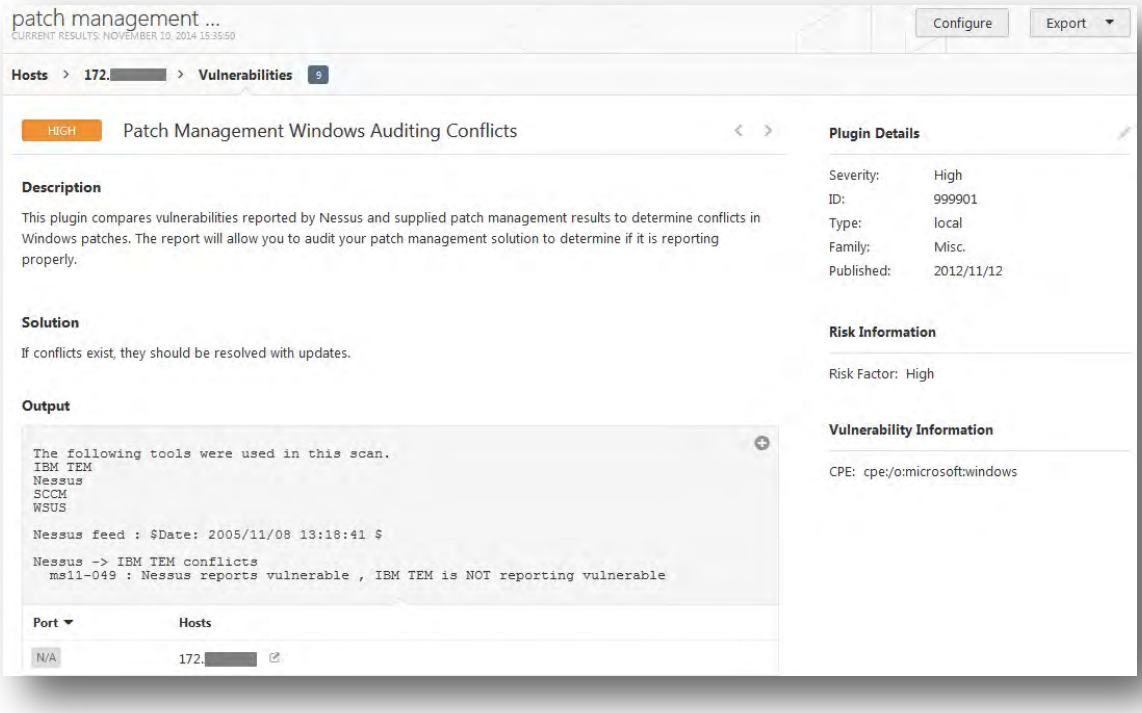
凭证	默认	描述
Server	无	Altiris IP 地址或系统名。这是一段必填字段。
Database Port	**5690**	Altiris 数据库端口正在运行(通常 TCP 5690)
Database Name	**Symantec_CMDB**	MSSQL 数据库管理 Altiris 补丁信息的名称。
Database Username	无	Altiris MSSQL 数据库登录的用户名。这是一段必填字段。
Database Password	无	需要验证的 Altiris MSSQL 数据库密码。这是一段必填字段。
Use Windows Authentication	禁用	表示是否使用 NTLMSSP 兼容旧 Windows 服务器，否则将使用 Kerberos

用多个修补程序管理员扫描

如果多组凭证提供给 Nessus 作为补丁管理工具，Nessus 将会使用他们。有效的凭证如下:

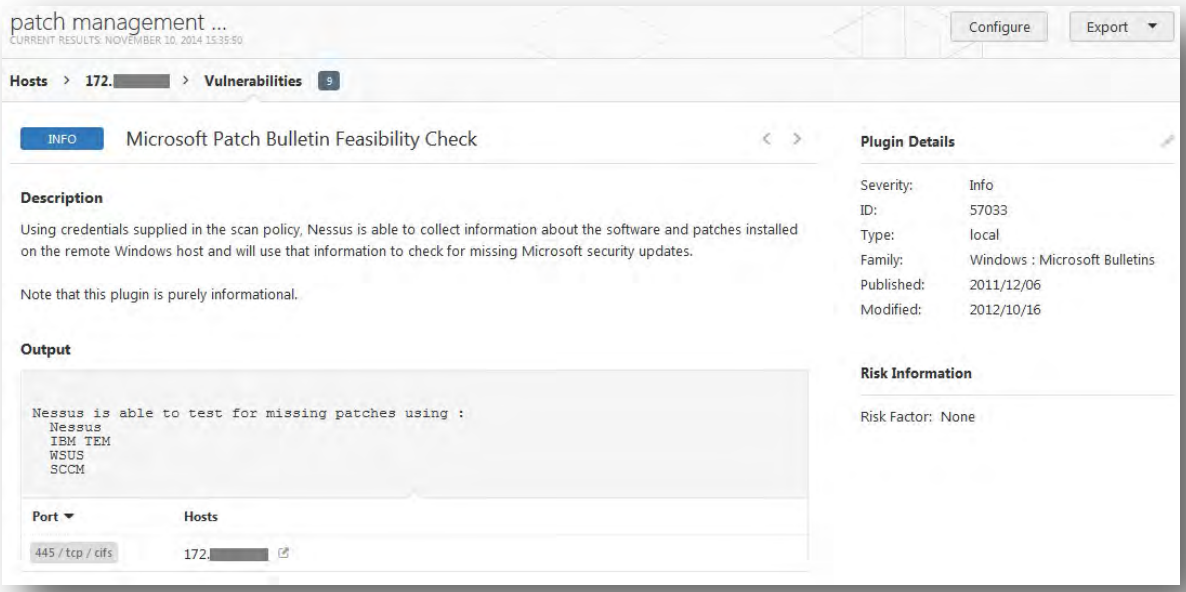
- 直接验证到目标的凭据
- IBM TEM
- Microsoft WSUS
- Microsoft SCCM
- Red Hat Network Satellite
- Dell KACE 1000
- Altiris

如果提供的主机、以及一个补丁管理系统或者多个补丁管理系统证书，Nessus 将会比较所有方法之间的结果，并在冲突报告或提供“满意”的发现。使用“Patch Management Windows Auditing Conflicts”插件，主机和补丁管理系统的补丁数据的差异（冲突）将被突出。例如，如果你提供目标主机和 SCCM、IBM TEM、KACE1000 和 WSUS 补丁管理系统凭据，如果有发现冲突，Nessus 将会产生以下报告以“高”严重等级:



这强调交叉引用补丁管理系统和认为是在系统上的补丁管理系统的补丁的重要性。在上面的输出，你可以看到，Nessus 登录到目标系统本身的凭证（通过“Nessus ->”表示）。 Nessus 也能够从 SCCM 拉补丁级别（用“-> SCCM conflicts”表示）。该报告对每个补丁和差异显示在插件输出。作为第一项表示主机，Nessus 发现 MS11-049 缺失，但 IBM TEM 报道称，作为补丁被应用。

该功能不仅提供主机审计，还能确保补丁管理软件提供准确的信息。 如果没有遇到冲突，Nessus 会将严重等级评估为“Info”级别



虚拟化

Tenable 还支持 VMware 虚拟化平台和 Red Hat 企业版的虚拟化身份验证. 利用多种远程身份检查方法，Nessus 能够对虚拟平台实施一系列的审计，就如软件运行在该平台上一样。 当虚拟主机的某些硬件因不需要而被移除时，会有新的硬件加入从而导致被攻击。因此不仅要确保运行在虚拟平台上的操作系统和程序要被测试，而且还要保证虚拟软件平台本身也被测试。

VMware

Nessus 包含了对 VMware 的产品各种支持。 插件的编写是基于相关漏洞的严重程度而不是优先考虑个别产品本身。通常情况下，VMware 产品的漏洞扫描插件会在漏洞出现后的一至二天后发布，包括前期的漏洞评估和制定对应措施。

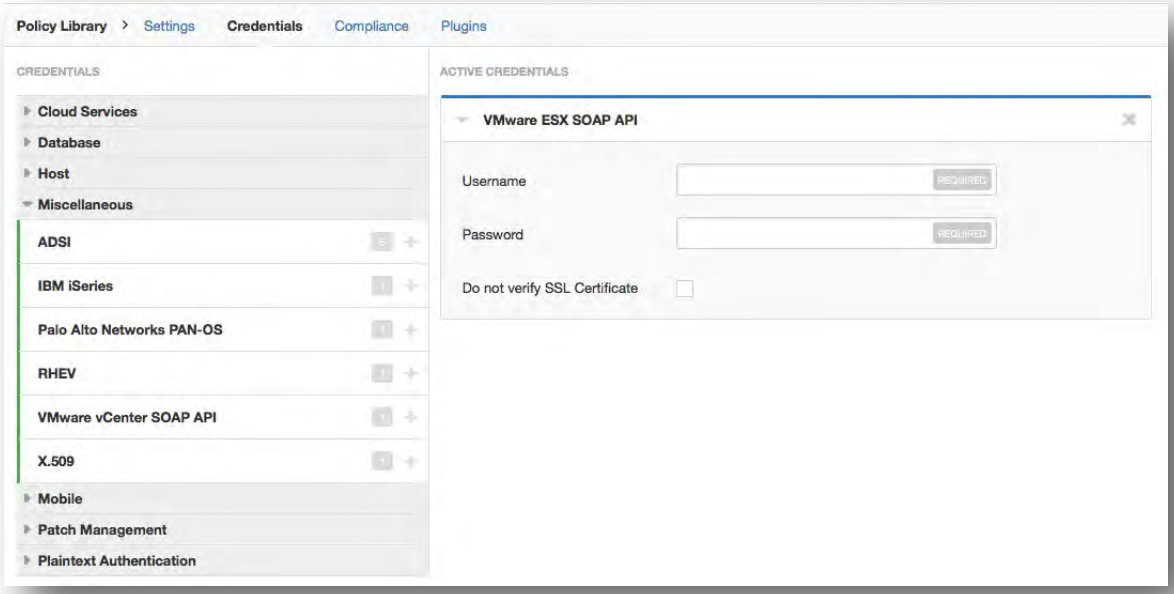
Nessus 能够探测活动的 ESX, ESXi,VSphere 和 vCenter 虚拟机器.

Nessus 在多方面支持 vCenter。Tenable 尽可能的核查已发布的漏洞以用于远程审计虚拟主机。此外，在 vCenter4.5 及更高版本中，Nessus 还能够通过 SOAP API 的方式查询受 Nessus 管理的 ESX 主机补丁信息

对于 ESX/ESXi, Tenable 通过本地检查的方式检查补丁应用情况(ESX/ESXi3.5 及更高版本)。 如果一个补丁已被应用，但是服务器并没有重启，该补丁有可能无法被探测到，那么 Nessus 会报告这台主机为易受攻击。 这些检查是在 ESXi 主机或着 vCenter 上，以 SSH 登陆凭证或着 SOAP 接口的方式来实施的。

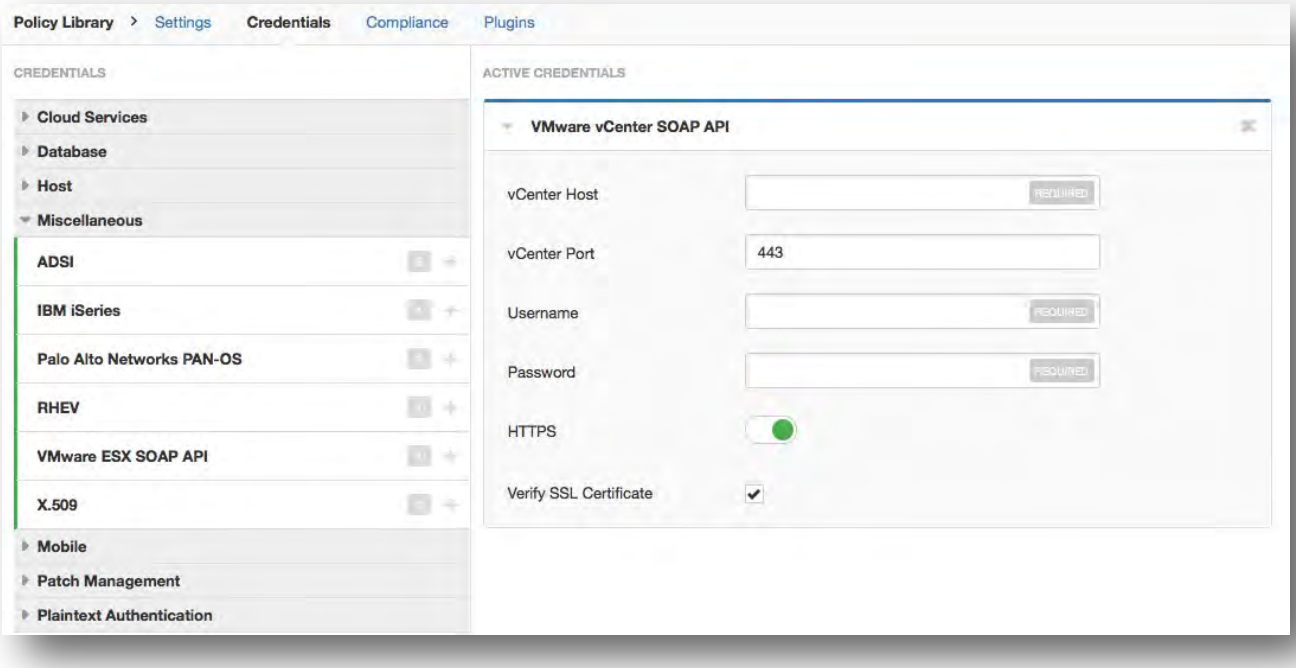
此外， Nessus 还提供多种本地凭证检查的方式来检查其它的 VMware 产品，包括 Fusion, Workstation, vMA,和 OVF Tool.

通过本地 SOAP API，可访问 VMware 的服务器 。 以 VMware ESX SOAPI API 的方式，允许你通过用户名和密码访问 ESX 和 ESXi 服务器。此外，你也可以禁用 SSL 证书验证。



凭证	默认	描述
Username	none	登陆到 ESXi server 的用户名. 必填项
Password	none	登陆到 ESXi server 的密码. 必填项.
Do not verify SSL Certificate	Disabled	不验证证书是否有效合法

通过 VMware vCenter SOAP API 的方式可访问 vCenter. 需要用户名，密码，vCenter 主机名以及 vCenter 端口号。此外，你也可以启用 HTTPS 以及启用 SSL 证书校验



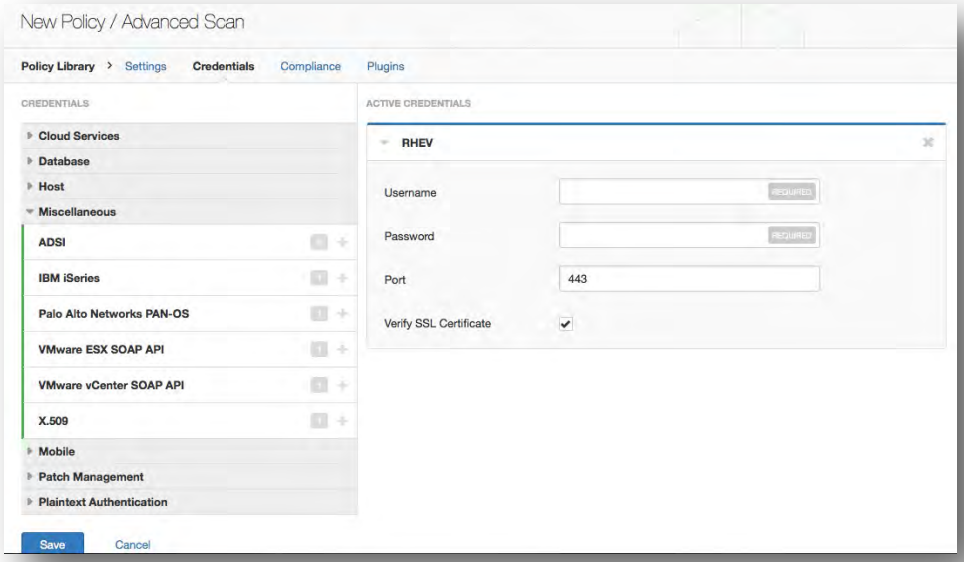
凭证	默认	描述
vCenter Host	**none**	vCenter 的主机名。 必填项.
vCenter Port	**443**	端口号
Username	**none**	登陆到 vCenter 服务器的用户名。. 必填项
Password	**none**	登陆到 vCenter 服务器的密码。必填 项
HTTPS	**Enabled**	通过 SSL 方式连接.
Verify SSL Certificate	**Enabled**	校验证书是否合法有效

Tenable 目前提供 ESXi 的一致性检查. 更多信息请参考 “Nessus VMware vCenter Patch Auditing Now Available” blog.

注意，默认本地 ESXi 用户限制于 “只读”角色，使用这样的账户将会产生 21745 错误。任何一个管理员账户或拥
有“Global” -> “Setting”权限的用户必须用于审计。当创建一个新策略时，ESX SOAP API 的凭证会被应用。

Red Hat Enterprise 虚拟化 (RHEV)

RHEV 需要用户名，密码以及网络端口。 此外，你还可启用 SSL

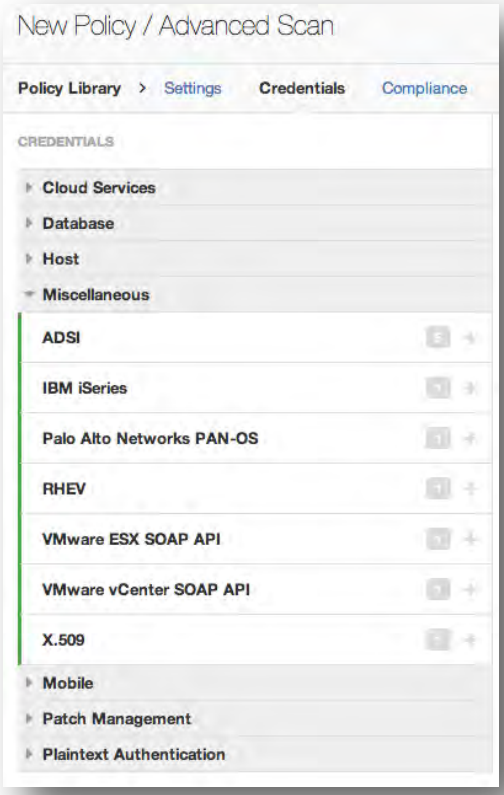


凭证	默认	描述
Username	none	登陆到 RHEV 服务器的用户名。必填项
Password	none	登陆到 RHEV 服务器的密码。必填项
Port	**443**	RHEV 服务器监听商品端口
Verify SSL Certificate	**Enabled**	验证证书是否合法有效。

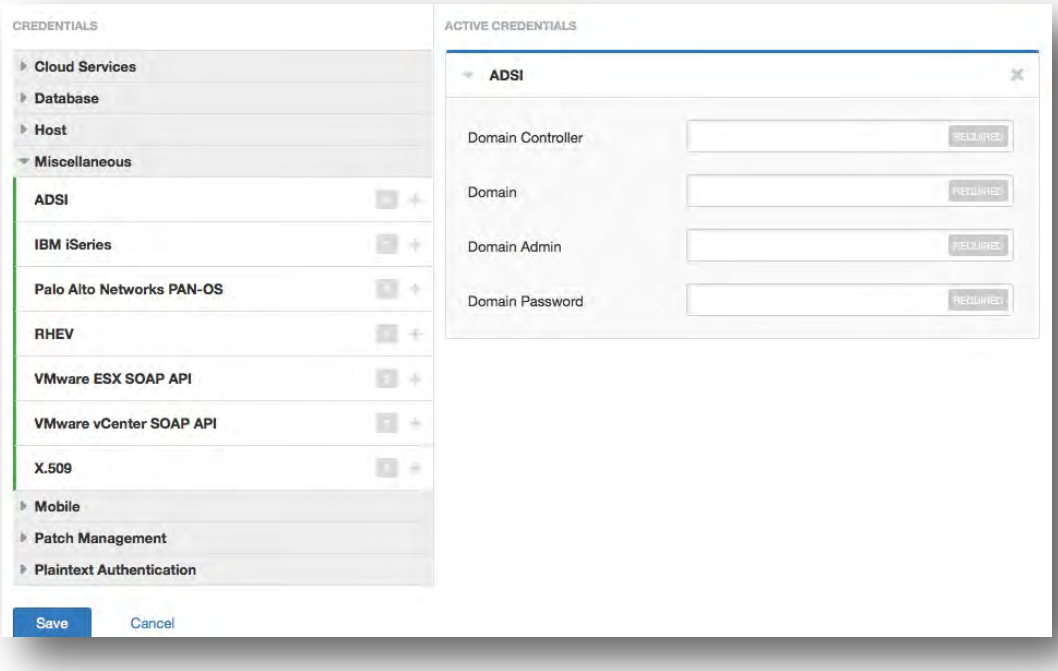
其它身份验证

Nessus 有能力扫描各种各样的不同功能的服务和设备，包括 IBM iSeries, Palo Alto 网络防火墙， X.509 服务，和活动目录服务接口（ADSI）.Nessus 能被配置以用于验证这些服务器并能报告任何问题。

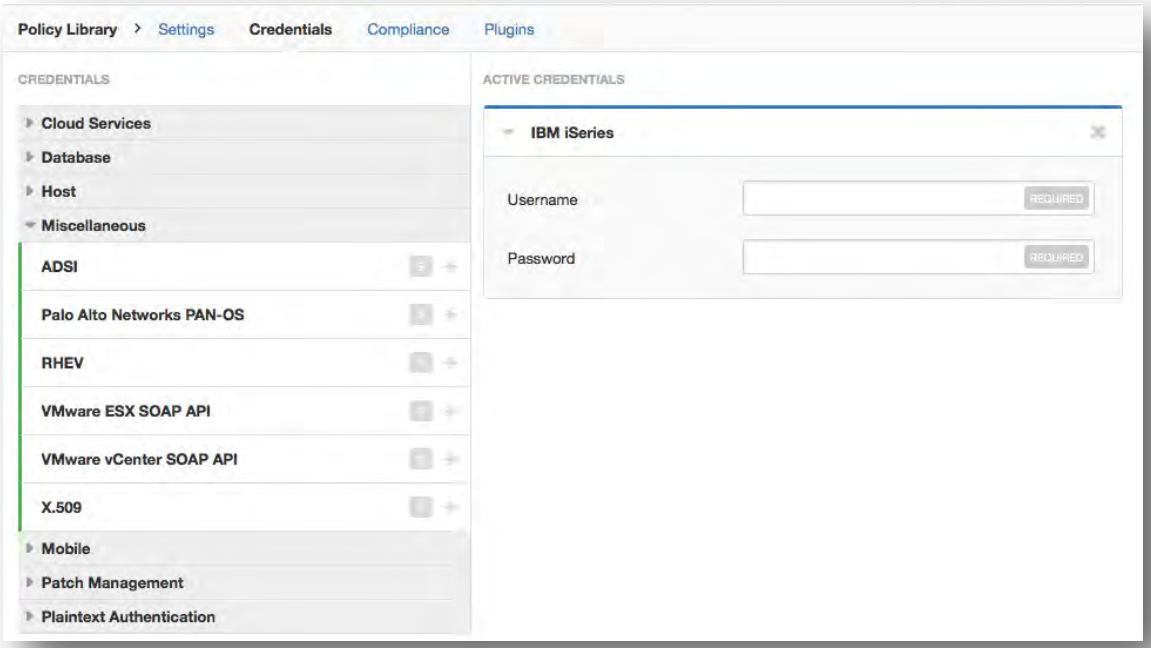
VMware ESXi, VMware vCenter 和 RHEV are 在本文档的虚拟化章节讨论



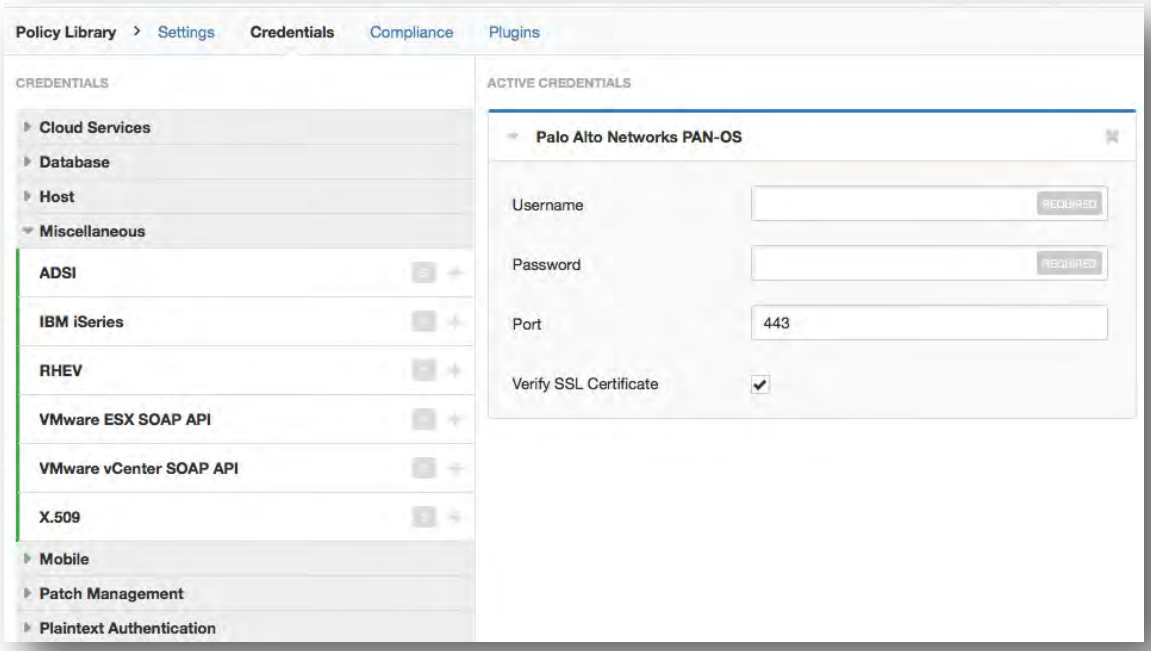
ADSI 需要域控信息, 域名, 以及域管理的用户名和密码:



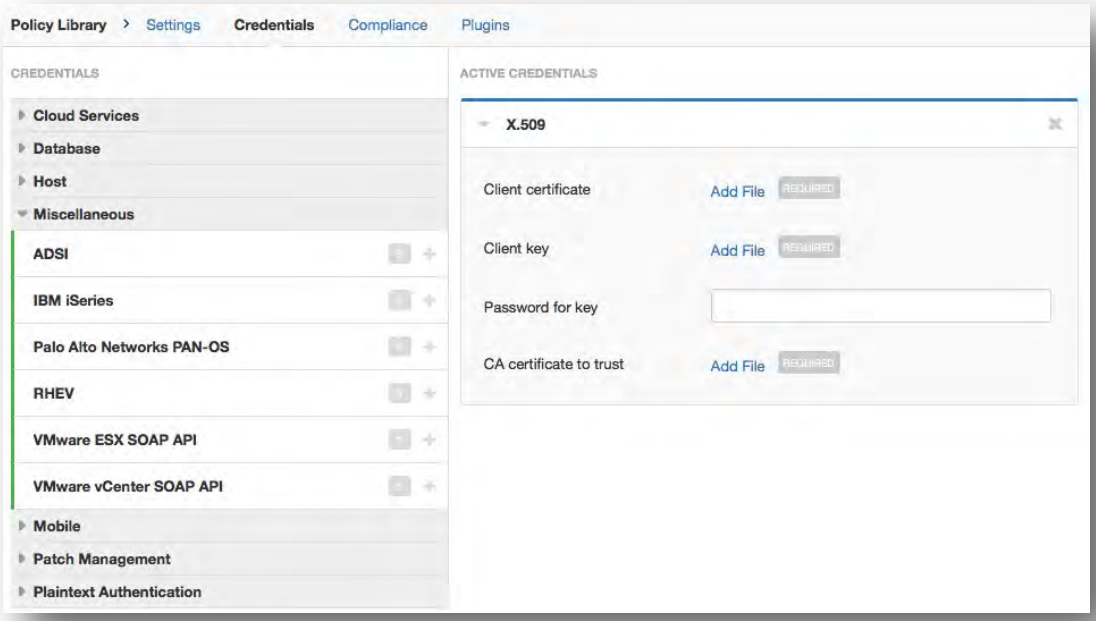
IBM iSeries 只需要一个 iSeries 用户名和密码:



Palo Alto Networks PAN-OS 需要 PAN-OS 用户名、密码以及管理端口. 此外, 你可以验证 SSL 证书:



使用 X.509，您需要提供客户端认证证书, 客户端私钥和其相应的密码, 以及可信任的 CA 数字证书:

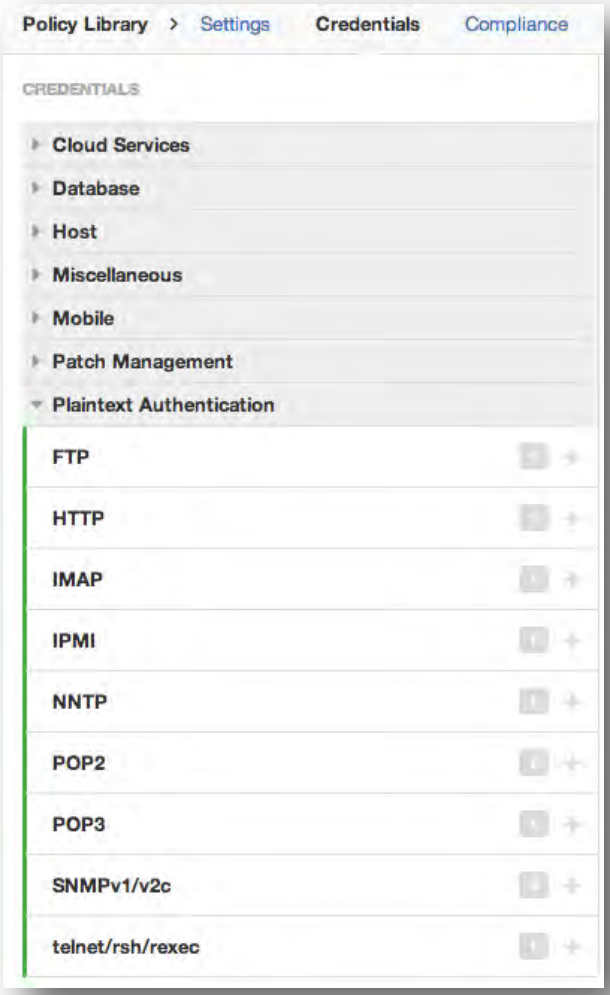


纯文本身份验证

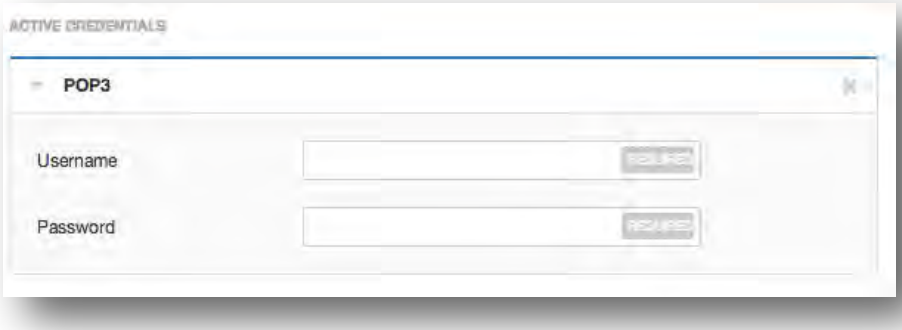
最后, 如果一个安全可信的认证方式不可用的情况下, 用户可以在 Nessus 通过 “**Plaintext Authentication**” 的下拉菜单进行不验证安全方法的认证方式。

这个菜单可以允许 Nessus 扫描器使用提交的凭证对 HTTP, NNTP, FTP, POP2, POP3, IMAP, IPMI, SNMPv1/v2c, and telnet/rsh/rexec.进行扫描, Nessus 有能力使用更广泛的检查来确定漏洞. HTTP 认证值提供了基本的和摘要式的认证。.

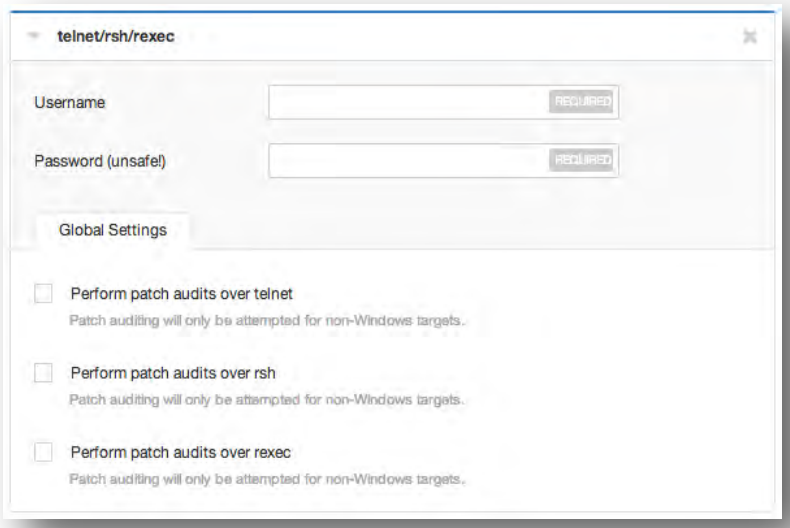
明文协议



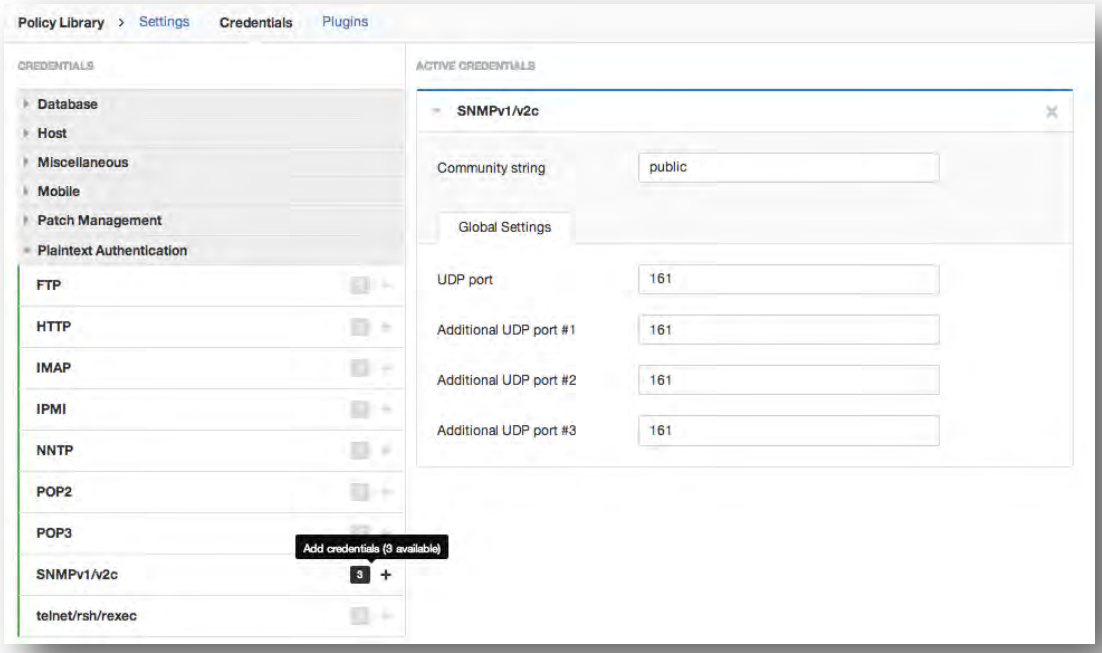
对于 FTP, IPMI, NNTP, POP2, 以及 POP3 的认证只需要用户名和密码.



telnet/rsh/rexec 认证的配置也只需要用户名和密码, 但是可以进行全局的配置，允许你在补丁审计时使用任意其中一个协议来进行 。

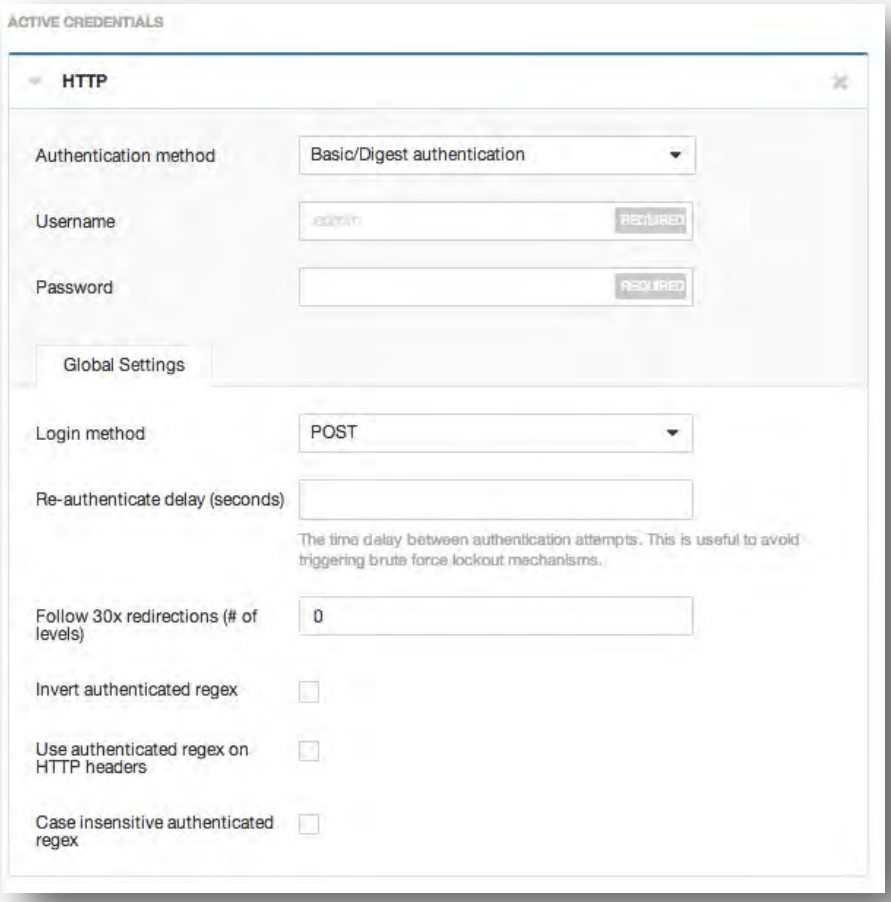


SNMPv1/v2c 的配置允许你使用 community 字符串来验证你的网络设备. 最多可以配置 4 个 SNMP community.



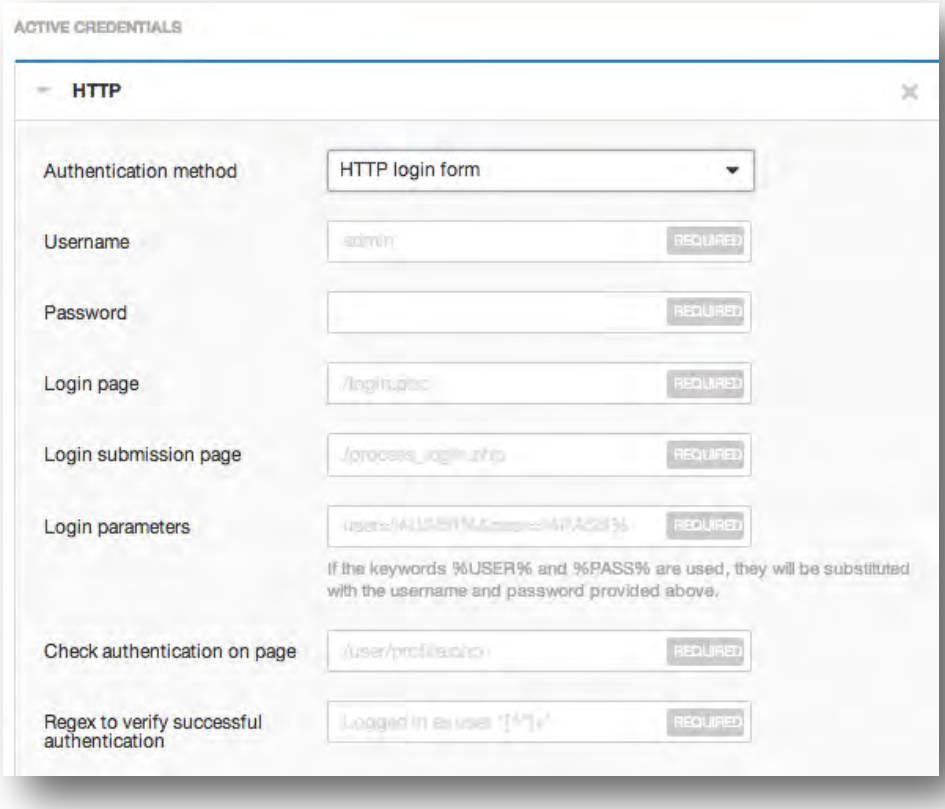
Web 应用扫描

这里有 4 种不同的基于 HTTP 认证的方式: **自动认证**, **基本的/摘要式认证**， **通过 WEB 应用登陆**, 以及 **HTTP cookies 的导入**. 所有 HTTP logins 的方式都包含全局配置:



选项	默认	描述
Login method	POST	指定是否通过 GET 或 POST 请求执行登录操作.
Re-authenticate delay (seconds)	none	身份验证尝试之间的时间延迟。这是有用的,以避免引发蛮力锁定机制.
Follow 30x redirections (# of levels)	**0**	如果从 WEB 服务器返回 30X 的错误，设置是否需要 Nessus 提供链接.
Invert authenticated regex	**Disabled**	通过正则表达式寻找登陆页面, 如果找到则会告诉 Nessus 认证不成功, (例如., “Authentication failed!”).
Use authenticated regex on HTTP	**Disabled**	Nessus 可以搜索 HTTP 响应头通过一个给定的正则表达式,以更好地确定身份验证状态.
Use authenticated regex on HTTP headers	**Disabled**	正则表达式默认是区分大小写的，这选项设置 Nessus 忽略大小写.

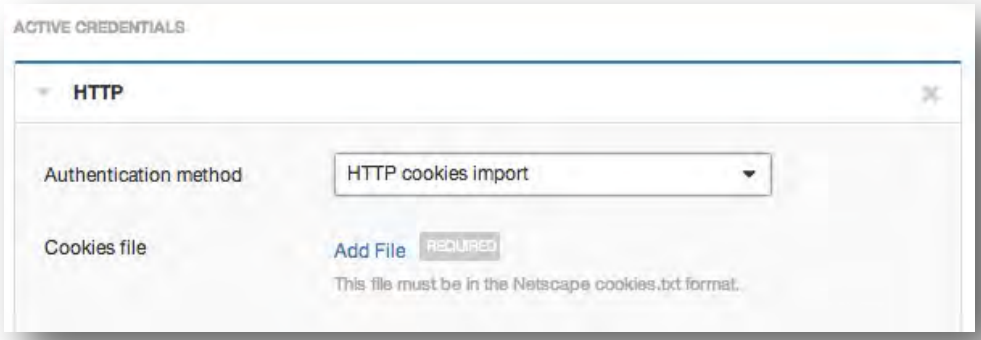
“**HTTP login page**” 设置，提供用户基于 WEB 登陆的认证测试信息.



除了用户名密码，一下选项也是必须的:

选项	描述
Login page	WEB 应用登陆的绝对路径, 例如., “/login.html”.
Login submission page	“action”参数。例如, 登陆 `<form method="POST" name="auth_form" action="/login.php">` 将会出现 “`/login.php`”。
Login parameters	指定的认证参数 (例如., login=%USER%&password=%PASS%)。如果已经在“Login configurations”中配置了认证信息，%USER%和%PASS%将取代之前输入的用户名和密码。如果需要，这个选项可以提供超过两个以上的参数(例如., 一个“group” 名称或者其他关于登陆时需要提供的验证信息).
Check authentication on page	验证登陆后的 WEB 页面的绝对路径, 更好的帮助 Nessus 确认登陆状态, 例如., “/admin.html”.
Authenticated regex	在登录页面中使用正则表达式来寻找认证信息. 简单的 200 状态不能证明其认证的状态. Nessus 需要匹配制定的字符串。例如 “Authentication successful!”

为了方便 Web 应用的扫描, Nessus 可以导入 HTTP cookies。 (例如., web 浏览器, web 代理, etc 文件.) 使用 “**HTTP cookies import**” 配置项. 可以上传一个 cookie 文件用于 Nessus 登陆一个 Web 应用. 这个 cookie 文件 必须是 Netscape 的格式.



默认, 所以的密码 (以及策略本身) 在 Nessus 中都是加密的. 如果策略文件以 **.nessus** 文件导出,密码在导出时被删除. 一旦你导入你的策略到目标 Nessus Scanner, 在使用前你需要重新配置密码和认证信息. 这样做的原因是,所有的密码策略在导入的设备是不可用的,因为它们无法被解密.

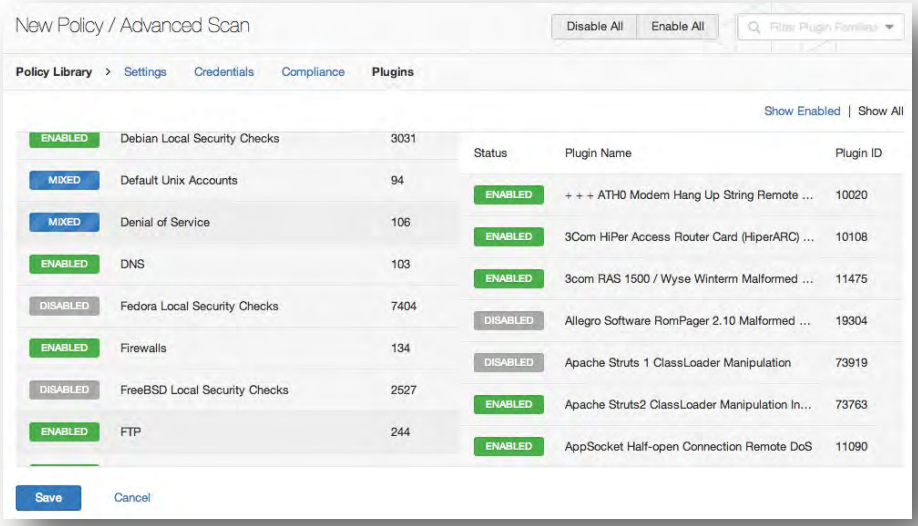
不推荐使用明文的认证方式! 如果认证信息远程发送 (例如., via a Nessus scan), 可能会在网络中被被截取. 尽量使用加密的身份验证机制.

合规性

在合规的详细信息,请参见下面的审计政策部分.

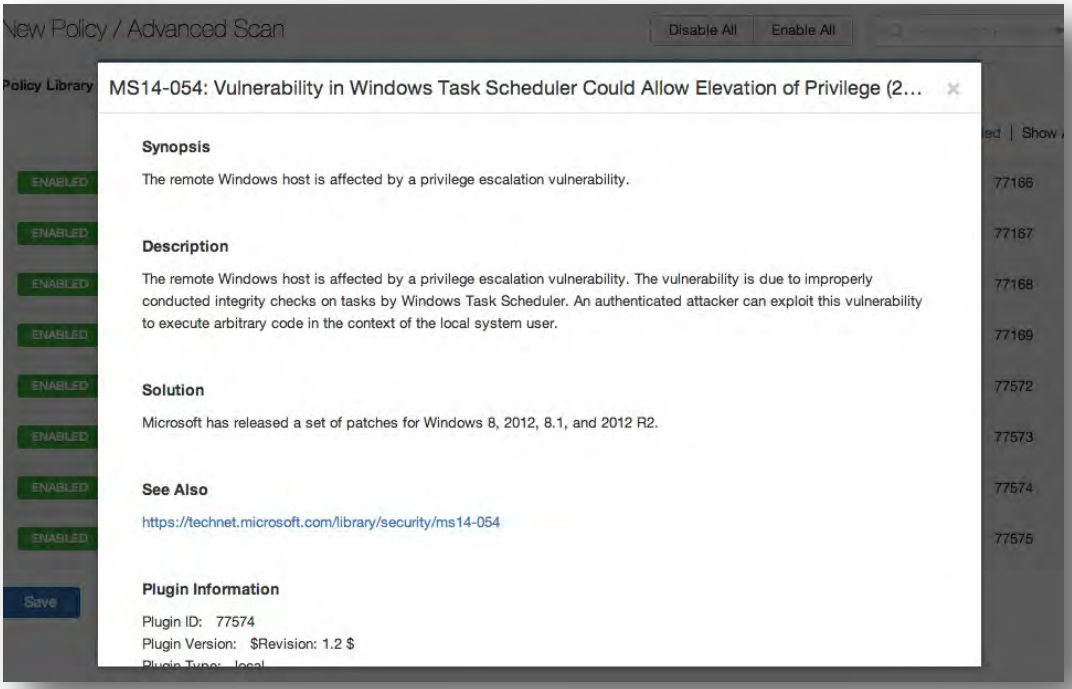
Plugins

“**Plugins**” 菜单允许用户选择一类的 plugin 或者 单个检查项进行特定的安全检查。

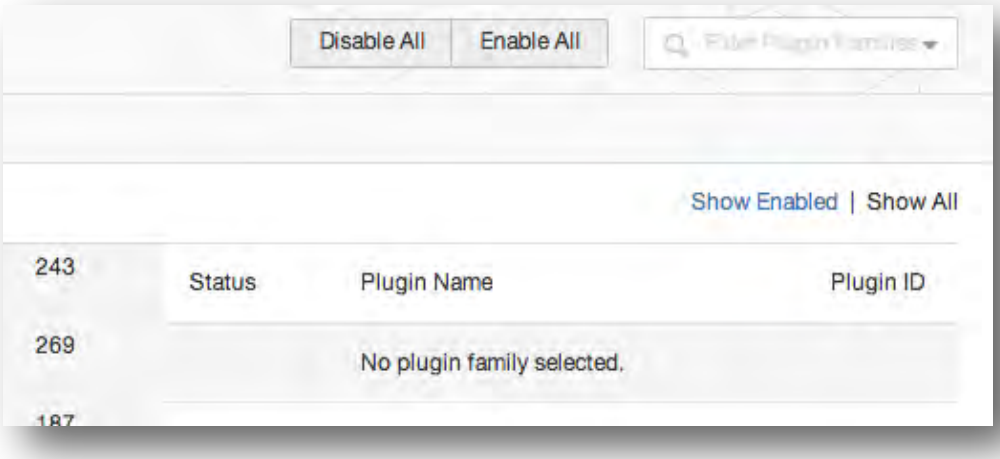


点击“plugin family” 允许 (绿色) 或者禁用 (灰色) 全部审计类. 选定一个类型后将显示 plugins 列表. 单个 plugins 可以通过启用或者禁用用于创建特殊的扫描策略. family 中有一些 plugins 被禁用将变为蓝色同时显示为 “mixed” 说明是由某些 plugins 被应用. 点击“plugin family” 将加载 plugins 发的完整列表, 同时根据您的扫描偏好进行选择。.

选择一个特殊的 plugin，该plugin 的输出信息将在报表中显示. 简介和描述将提供更多细节漏洞检查. 向下滚动在浏览器中也会显示解决方案信息,额外的引用,风险信息,利用信息和漏洞数据库或交叉引用的信息.

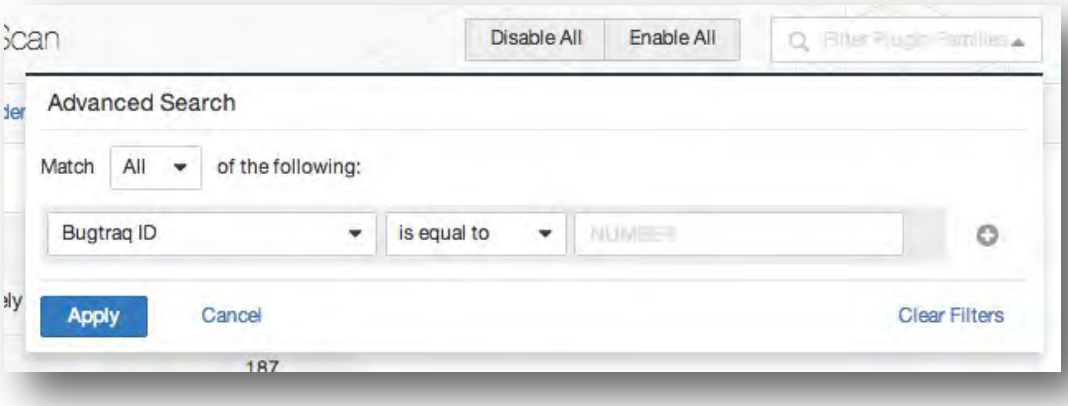


在 plugin family 页面的顶部, 您可以创建过滤器来构建 plugin 的列表中包含的策略, 更好的禁用或启用所有的 plugins. 过滤器允许细粒度控制插件的选择. 多个过滤器可以设置在一个单的策略.

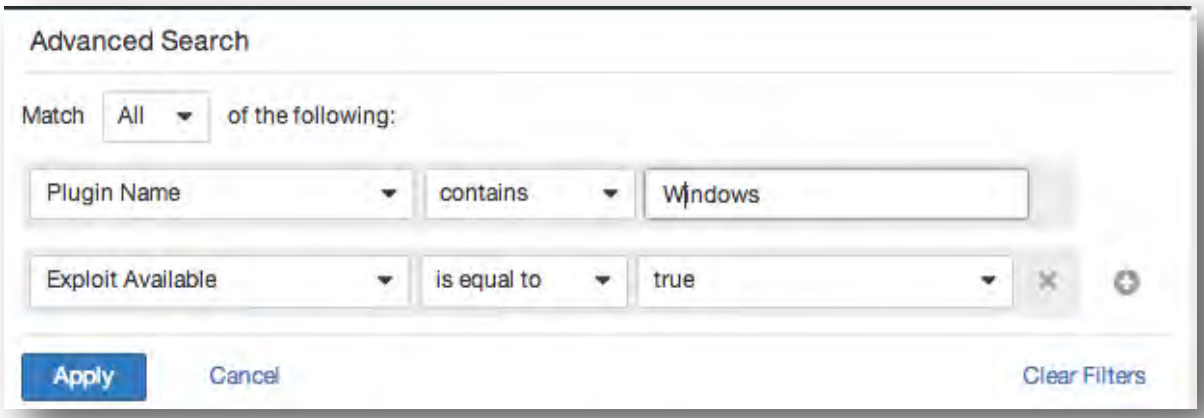


点击 “**Filter Options**” 按钮创建一个过滤器,

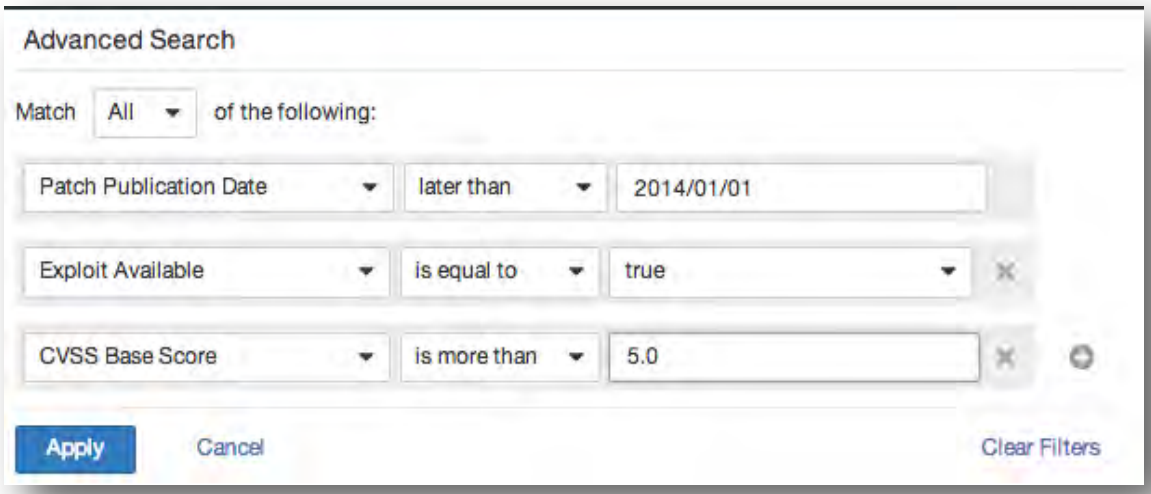
快速过滤器，您可以输入搜索基于 plugin families,. 会动态过滤出 plugin families.



每个过滤器提供几个选项,创建为精炼搜索. 过滤条件可以基于“any”,在任何一个标准返回进行匹配, 或者 “ALL” 每个过滤标准必须出现. 例如, 如果我们想要一个策略,只有包含可利用的 plugin,, 我们创建两个过滤器和选择“任何”为标准:



如果我们想要创建一个策略,其中包含插件符合几个标准, 我们选择“ALL”,并添加所需的过滤项. 例如, 策略包括任何 2014 年 1 月 1 日后发布的,漏洞补丁和 CVSS 5.0 以上的:



过滤条件的完整列表和细节, 点击 Report Filters 的文章.

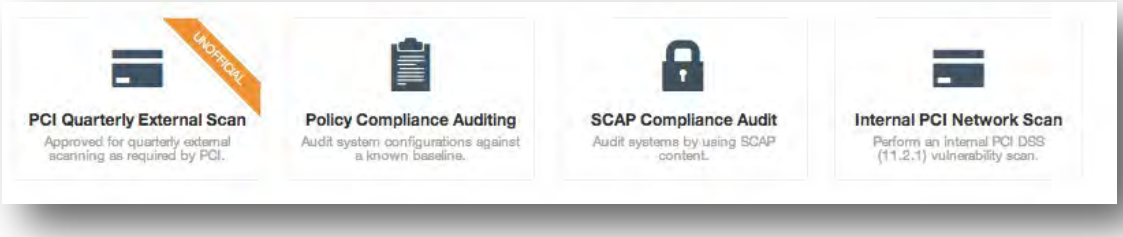
使用过滤器来创建一个策略,建议你先禁用所有 plugins. 使用 plugin 过滤器, 在你的策略中缩小 plugin 的范围. 一旦完成, 选择每一个 plugin family 同时点击 “Enable Plugins”.

当一个政策是创建并保存，它记录了所有的最初选择的 plugin。当 plugin，通过 plugin 更新了，他们会自动被启用如果他们与 family 是启用的。如果 family 已被禁用或启用新的插件部分，其在 family 里也将自动禁用.

如果 “Safe Checks” 选项没有开启, “Denial of Service” family 包含的一些 plugins 可能会导致网络中断， 但是 也包含了一些有用的没有危害的检查项. “Denial of Service” family 可以与 “Safe Checks” 一起使用确保有潜在危险的 plugin 不在运行. 然而, 建议 “Denial of Service” family 不要应用与生产环境网络 除非是在例行维护期间，或者有足够充分的准备应对发生的问题.

审计策略

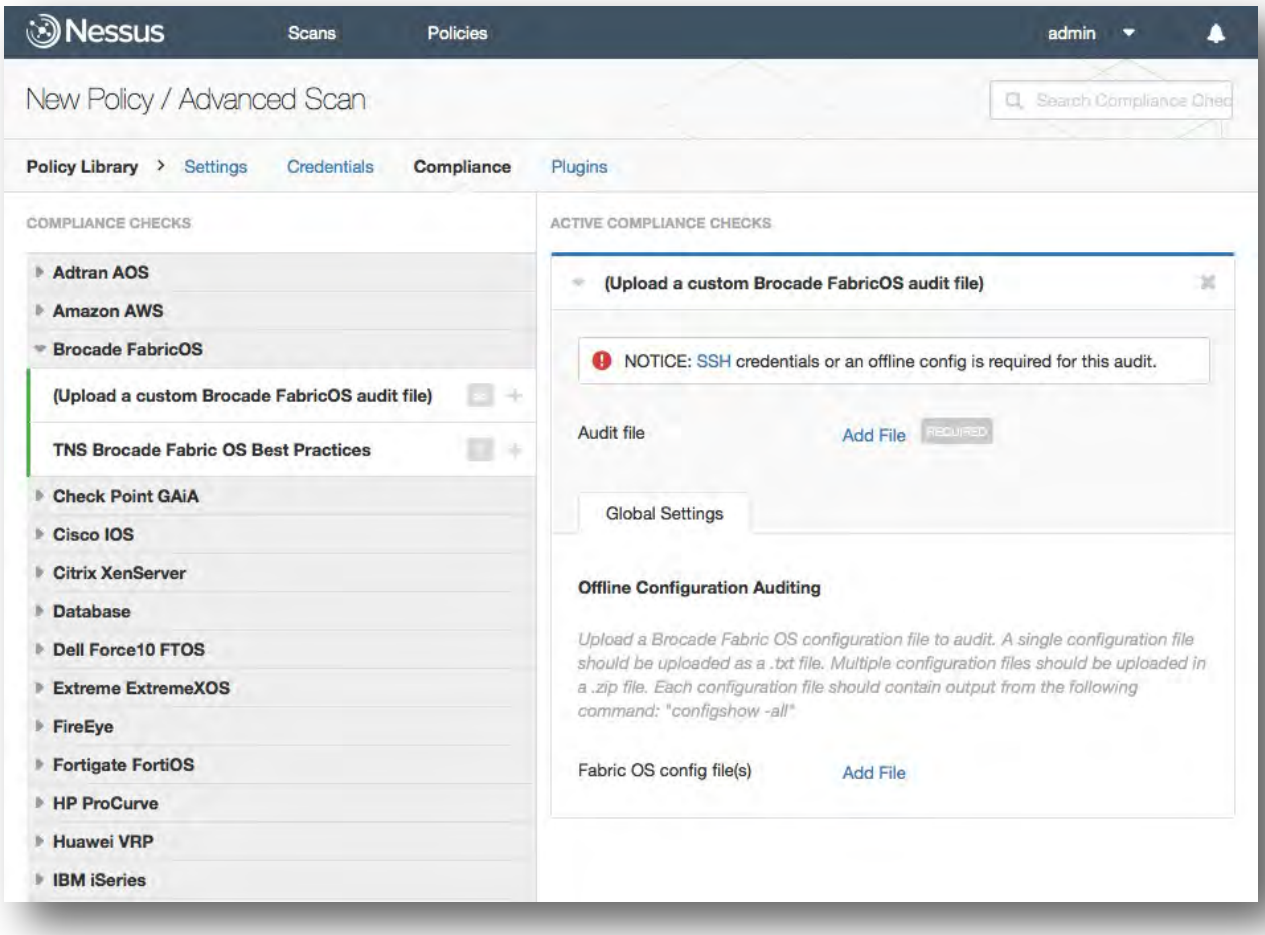
Nessus 合规审计可以使用 4 种配置其中一个, PCI 季度外部扫描, 内部 PCI 网络扫描, 策略合规审计, 以及 SCAP 合规审计:



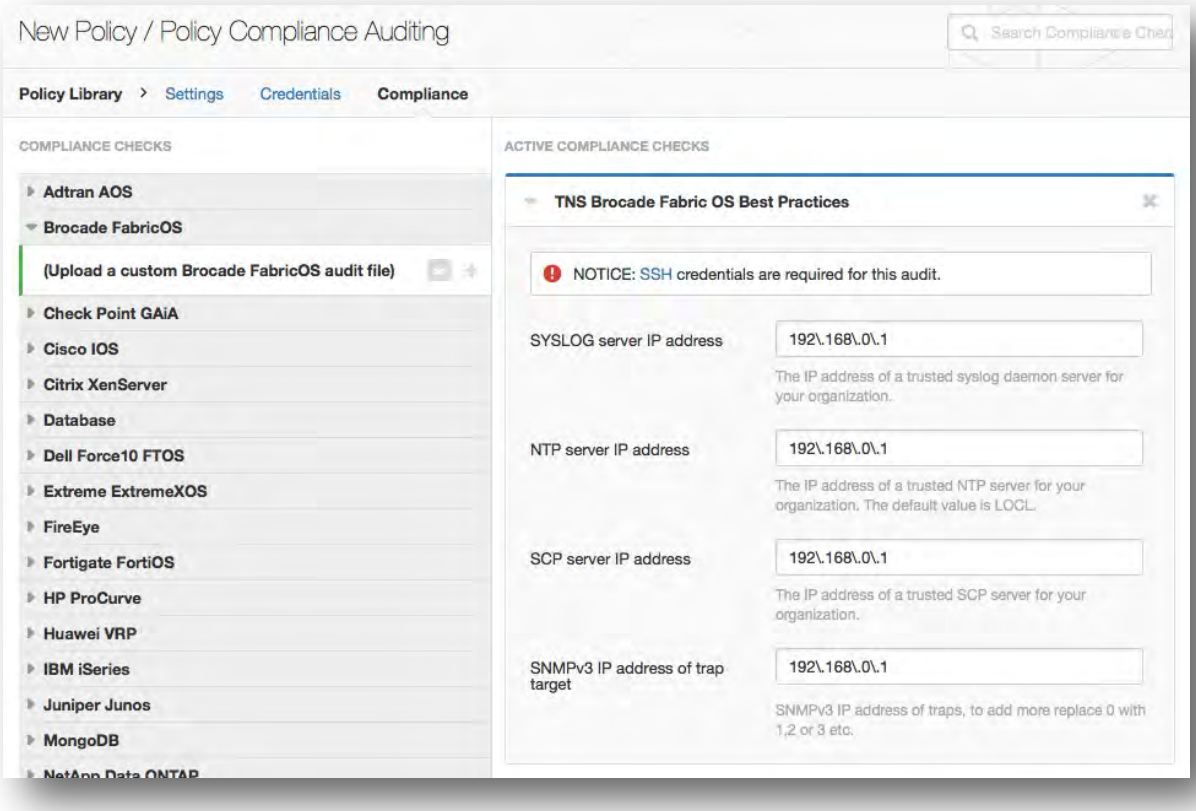
合规性审计策略

Nessus 提供了一个策略库用于策略合规审计. 你可以自定义创建审计文件用来审计 操作系统, 数据库, 网络设备, 程序, 以及其他企业级的应用.

与 “**Credentials**” 章节一样,合规在右上角有一个搜索框.如果与输入没有可匹配的内容，则左侧将没有内容显示

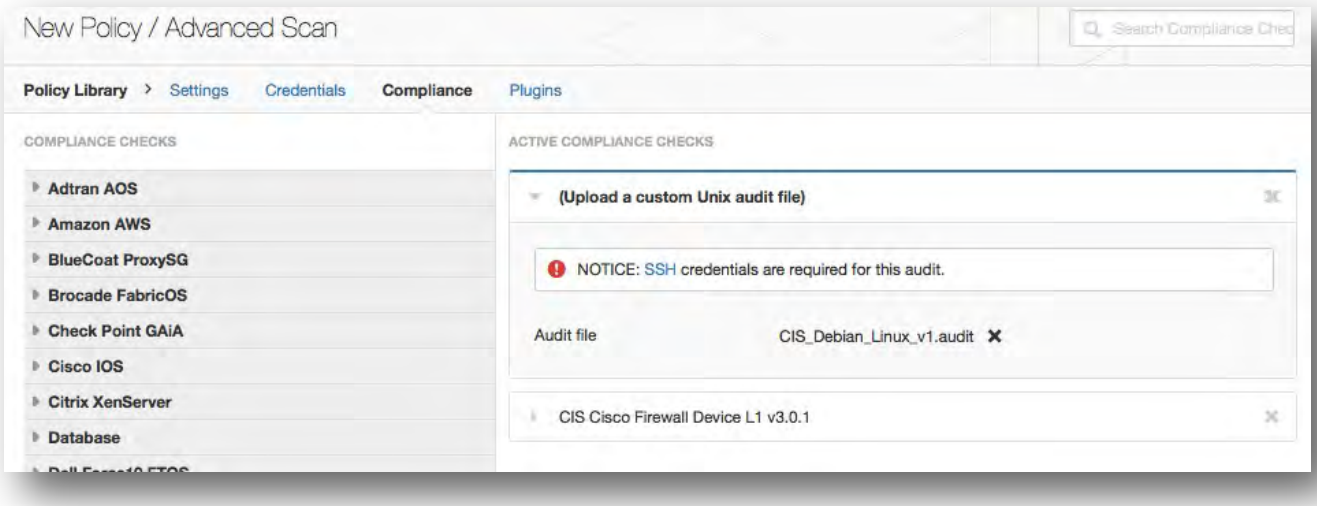


这个菜单允许商业客户上传的策略文件,将被用来确定受支持的设备,应用程序,或操作系统符合指定的合规标准。最多一次选择 5 个文件。



一旦保存了合规策略，用户可以打开合规策略和下载所有自定义审计文件。这使得用户可以不仅能使用 Nessus 默认的合规策略和审计文件，也可以使用自定义模板。

:



某些策略也有最佳实践可以提供，这是用户提供的值，以他们的环境中的预先定义的审计文件。在某些情况下，也有预先定义的 DISA STIG，CIS 和 PCI 审核策略可供使用。

当需要创建一个新的策略时，请单击 Policy Compliance Auditing(策略合规性审计)，在凭据后会有第三选项，显示可用的合规性选项。

下表提供了所有合规性检查的概要。若需要每个项目的详细信息，请查看 Tenable Network Security 的文件, "Nessus Compliance Checks".

合规性策略	要求的证书	描述
Adtran AOS Compliance Checks	SSH	该选项允许一个系统或策略文件来对 ADTRAN AOS 基础设备进行标准符合性测试
Amazon AWS Compliance Checks	SSH	该选项允许系统对 AWS 帐户配置进行标准符合性测试.
Blue Coat ProxySG Compliance Checks	SSH	该选项允许系统对 Blue Coat ProxySG 设备进行标准符合性测试
Brocade FabricOS Compliance Checks		该选项允许一个系统或策略文件来对 **Brocade** Fabric OS 基础设备进行标准符合性测试。
Check Point GAiA Compliance Checks	SSH	该选项允许系统对 Check Point GAiA 设备进行标准符合性测试。
Cisco IOS Compliance Checks	SSH	该选项允许设备或策略文件来对 **Cisco** IOS 设备进行标准符合性测试。除了能够上传自己的.audit 文件，也有 DISA STIG 等最佳实践文件可提供。
Citrix XenServer Compliance Checks	SSH	该商业选项允许系统测试 Citrix XenServer 的合规性
Database Compliance Checks	Database credentials	该选项允许策略文件来测试数据库如 DB2，SQL 服务器，MySQL 和 Oracle 的合规性
Dell Force10 FTOS Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 Dell Force10 FTOS 设备是否符合标准
Extreme ExtremeXOS Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 Extreme 的 ExtremeXOS 基础设备的合规性.
FireEye Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 FireEye 设备的合规性.
Fortigate FortiOS Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 FortiGate 的 FortiOS 基础设备的合规性
Huawei Compliance Checks	SSH	该选项允许设备或策略文件来测试华为 VRP 设备的合规性。
HP ProCurve Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 HP ProCurve 设备的合规性
IBM iSeries Compliance Checks	IBM iSeries	该选项允许策略文件来测试 IBM iSeries 系统的合规性

Juniper Junos Compliance Checks	SSH	该选项允许设备或策略文件来测试 Juniper 的 Junos 设备的合规性.
MongoDB Compliance Checks	MongoDB	该选项允许一个系统或策略文件来测试 MongoDB 的系统的合规性
NetApp Data ONTAP Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 NetApp 数据 ONTAP 设备的合规性
Palo Alto Networks PAN-OS Compliance Checks	PAN-OS	该选项允许系统测试 Palo Alto 的网络 PAN-OS 设备的合规性
Red Hat Enterprise Virtualization Best Practices	RHEV	该选项允许系统测试 Red Hat 的 Enterprise Virtualization 设备的合规性
Salesforce	Salesforce SOAP API	该选项允许系统测试的 Salesforce 应用的合规性
SonicWALL SonicOS Compliance Checks	SSH	该选项允许一个系统或策略文件来测试 SonicWALL 的 SonicOS 设备的合规性
Unix Compliance Checks	SSH	该选项允许策略文件测试 Unix 系统的合规性。
Unix File Contents Compliance Checks	SSH	“**Unix File Contents Compliance Checks**”(Unix 文件内容合规性检查)菜单允许用户为用特定的内容类型来搜索一个系统而上传基于 Windows 的审计文件（例如，源代码中的错误，信用卡，社会安全号码），以帮助确定是否符合公司规定或第三方标准.
VMware vCenter/vSphere Compliance Checks	VMware ESX SOAP API or VMware vCenter SOAP API	该选项允许系统测试 VMware 设备的合规性.
Windows Compliance Checks	Windows	该选项允许策略文件来测试 Windows 系统的合规性
Windows File Contents Compliance Checks	Windows	“**Windows File Contents Compliance Checks**”(Windows 文件内容合规性检查)菜单允许用户为用特定的内容类型来搜索一个系统而上传基于 Windows 的审计文件（例如，信用卡，社会安全号码），以帮助确定是否符合公司规定或第三方标准。

如需更多的具体合规策略信息，请参阅 Tenable Network Security 文件, “Nessus Compliance Checks”.

离线配置审计策略

Tenable 提供直接将配置策略上传给 Nessus 的功能，这使用户可以上传关键设备的配置来进行审计，而不需要任何设备访问接口。该功能要求被审计的设备在被进行配置审计时保持在线状态。

对于离线配置审计目前支持的设备:

- Adtran AOS
- Blue Coat ProxySG Compliance Checks
- Brocade Fabric OS
- Cisco IOS
- Check Point GAiA Compliance Checks
- Dell Force10 FTOS
- Extreme ExtremeXOS
- FireEye
- HP ProCurve
- Huawei VRP
- Juniper Junos
- Netapp Data ONTAP
- SonicWALL SonicOS

PCI 策略

Tenable 的 Nessus 中提供了两种支付卡行业数据安全标准（PCI DSS）的策略：一个用于测试的内部系统，一个用于外部扫描。外部扫描策略只能通过 Nessus 的企业云进行。Nessus 企业云将测试所有 PCI DSS 外部扫描需求，包括 Web 应用程序。每季度一次的 PCI 外部扫描旨在帮助您满足经批准的扫描服务提供商（ASV）的 PCI 扫描要求。

Nessus 的扫描结果可以在 PCI 合规评估中使用，以定期证明系统在评估期间始终保持与众多 PCI DSS 的要求相符。

为 PCI 认证提交一次 Nessus 扫描，扫描必须进行，并需要通过 Nessus 企业云进行提交。.

PCI 策略	说明
PCI Quarterly External Scan	Nessus 企业云是唯一可以指导 Nessus 将扫描结果与 PCI DSS 标准(PCI DSS standards)进行比对的选项。
Internal PCI Network Scan	该策略用于部署内网 PCI DSS 漏洞扫描。

SCAP 策略

NIST 的安全内容自动化协议(Security Content Automation Protocol，简称 SCAP)是一套政府机构用于管理漏洞和策略合规的策略。它基于众多公开的标准和策略，包括 OVAL, CVE, CVSS, CPE 以及 FDCC 策略。如需 SCAP 的更多信息，请访问网页 NIST Security Content Automation Protocol。

SCAP 合规审计要求发送一个可执行文件到远程主机。系统若运行安全软件(例如：McAfee Host Intrusion Prevention)可能阻止或隔离审计所需的执行文件。对于这些系统，可由主机或者可执行文件的发送来作出例外。

Nessus 有两个 SCAP 合规策略可供您的商业版账号使用：

SCAP 策略	说明
SCAP Windows Compliance Checks	该商用版选项允许所有商业版用户上传 SCAP 的 zip 文件，以用于说明一个经过测试的 Windows 系统是否可以符合 SP 800-126 特别规定的策略要求。
SCAP Linux Compliance Checks	该商用版选项允许所有商业版用户上传 SCAP 的 zip 文件，以用于说明一个经过测试的 Linux 系统是否可以符合 SP 800-126 特别规定的策略要求。

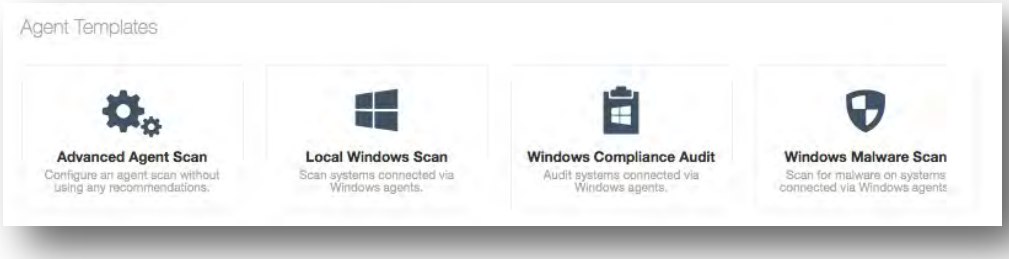
若需更多指定合规策略的信息，请查阅 Tenable Network Security 的相关文件：Nessus SCAP Assessments.

Nessus Agent 模板

使用 Nessus Manager(管理版)，您可以创建对于 Nessus Agents 的策略和扫描。

Nessus Manager(管理版)是目前 Nessus 家族产品中唯一可以运行 Nessus Agents 的软件。

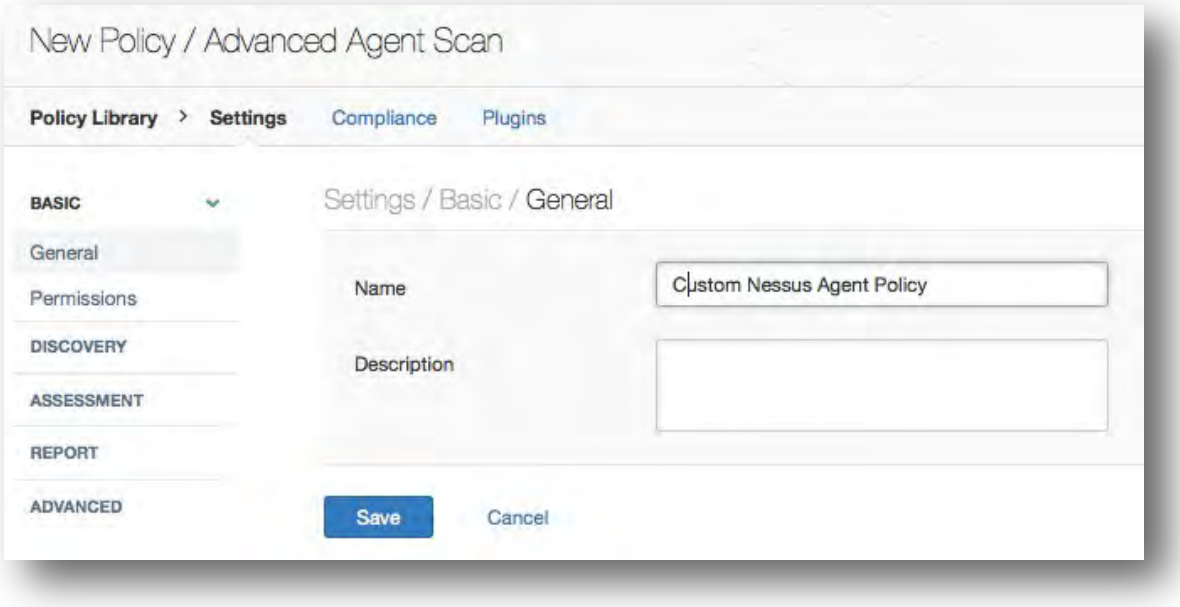
Nessus Agents 目前可对 Windows 运行本地扫描和合规检测。有三种 Nessus Agent 模板：



Windows Agent 策略	说明
Local Windows Scan	对 Windows 系统通过 Windows Nessus Agent 来运行本地扫描检测。该策略仅对 Windows 本地检测有效。
Windows Compliance Audit	对 Windows 系统通过 Windows Nessus Agent 来运行本地合规检查。该策略仅对 Windows 合规检查和 Windows File Contents(文件内容)合规检查有效。
Windows Malware Scan	通过 Windows Nessus Agent 在 Windows 系统上搜索恶意软件。该策略仅对 Windows 本地恶意软件检测有效。
Advanced Agent Scan	若没有可用的策略模板匹配所需要求，Advanced Agent 扫描选项允许您可以对所有控制项从头开始创建一个策略。该选项包含所有本地 Windows 扫描和合规审计的插件及策略项。

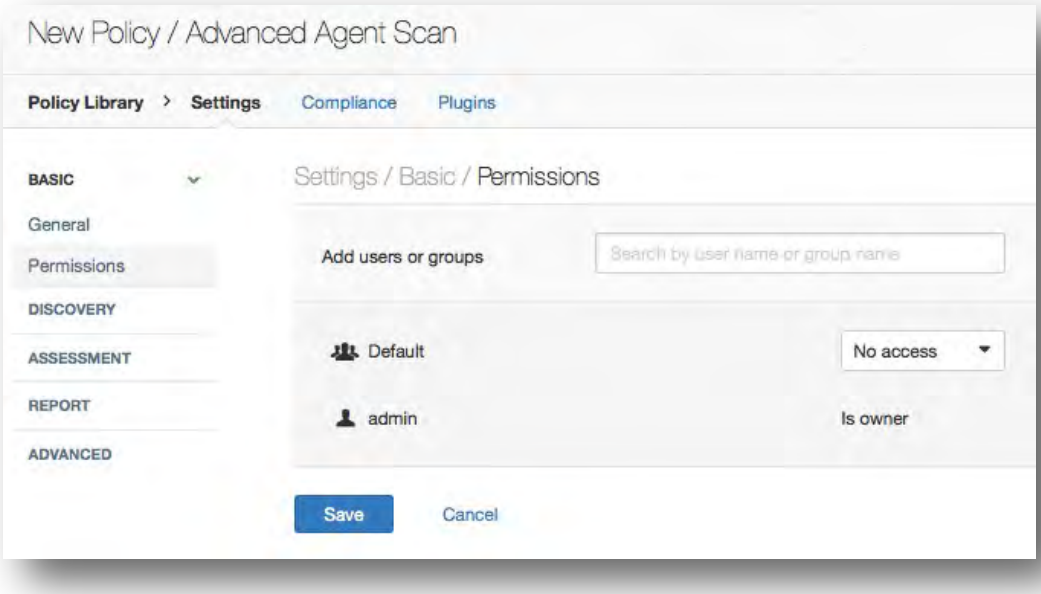
通用设置

“**General**”(通用)设置允许您命名策略，并配置扫描相关的操作。



“**Basic**”(基础)界面用于定义策略本身的问题。该选项在标题为“**General**”(通用)和“**Permissions**”（权限）项下：

General (通用)选项	说明
Name	设置在 Nessus UI 中显示的名称以定义策略。
Description	对扫描策略提供一个简要说明，提要总结策略目的。 (例如：“Web Server scans without local checks or non HTTP services”).

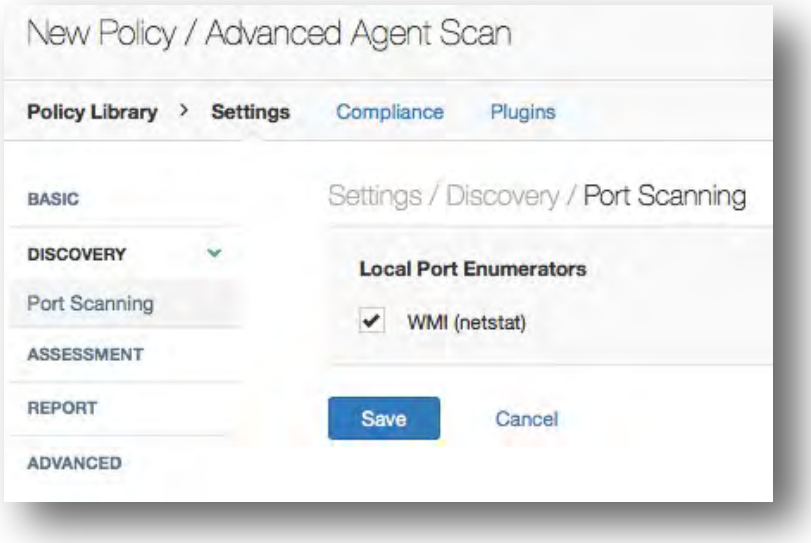


Nessus Manager(管理版)提供访问 Agent 策略的颗粒度控制。权限可以设置组或用户。默认设置是每个人都可以访问，而不需指定用户或组。

权限	说明
Can Use	其他用户可以在他们的扫描中查看并使用策略。但他们不能修改策略。
Can Edit	可以修改策略并使用。
No Access	仅创建策略者可以查看、使用或修改策略。

Discovery 设置

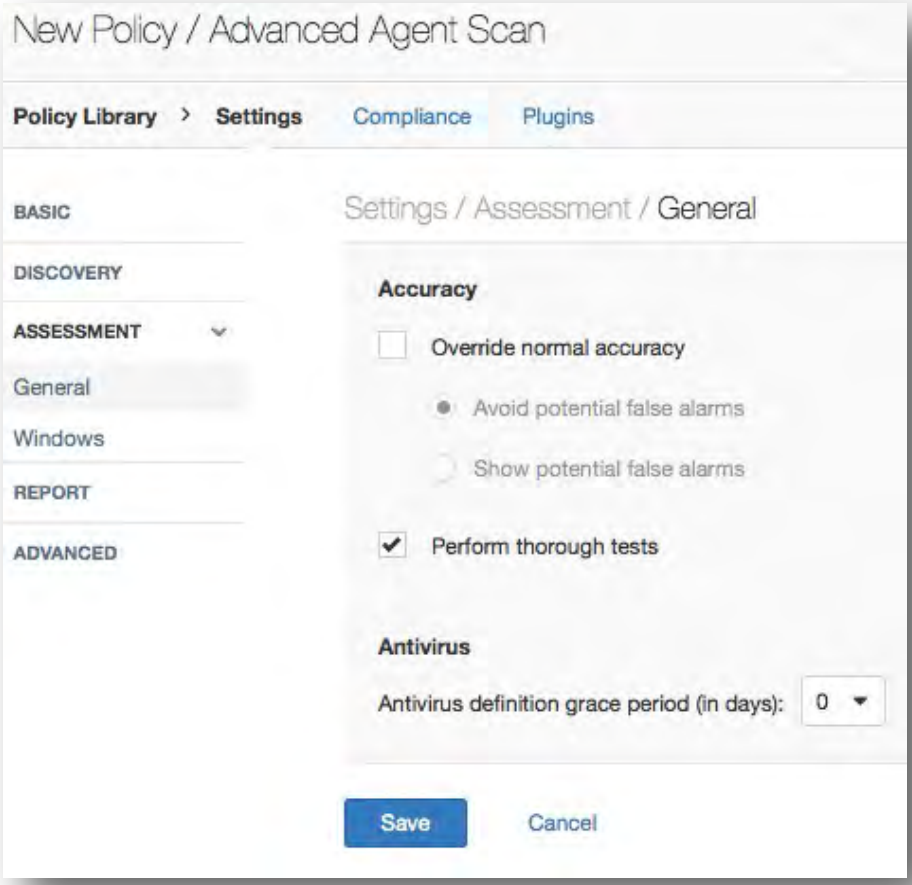
“Discovery”(发现)界面提供用于启用端口枚举的选项。



选项	默认设置	说明
WMI (netstat)	启用	该选项使用 **netstat** 来检查本地机器上开放的端口。它基于 **netstat** 命令使得通过 WMI 连接目标可以实现。该扫描用于基于 Windows 的系统，并要求身份认证。 基于 WMI 的扫描使用 **netstat** 来发现开放的端口，从而忽略任意指定的端口范围。若任意端口枚举(**netstat** or SNMP) 成功完成，端口范围将变成“all”。然而，若选择了“consider unscanned ports as closed”(将未扫描端口设为关闭)选项，Nessus 将仍将执行该选项。

Assessment(评估)设置

“Assessment”(评估)界面提供对 Nessus Agent 安全评估的控制选项。



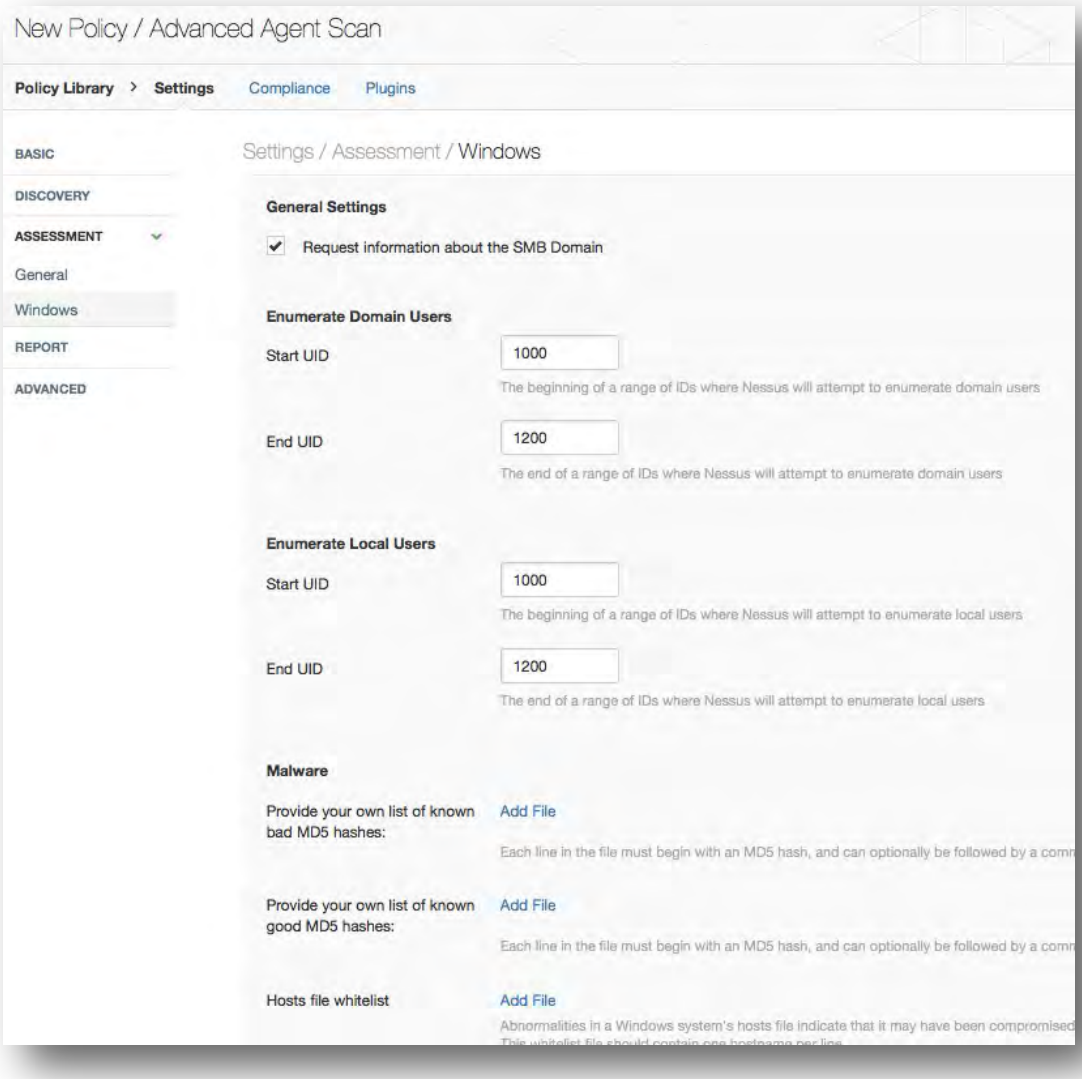
下列选项在 **General** 模块下。**“Accuracy”**(精准)选项允许对扫描中的错误告警报告和运行测试的彻底程度提供颗粒度控制。

选项	默认设置	说明
Override normal accuracy	不启用	在有些情况下，Nessus 不能远程定义是否存在缺陷。若报告被设置为“**Show potential false alarms**”(显示潜在的错误警报)，则每次错误都会被报告，甚至包括当远程主机有被侵入的怀疑时。相反，设置 “**Avoid potential false alarms**”(避免潜在错误报警) 会导致 Nessus 不报告任何错误，不论远程主机是否存在问题。 不启用 “**Override normal accuracy**”(覆盖普通精度)是介于这两种设置中间的一种选择。
Perform thorough tests	启用	使各种插件“工作更努力”。例如，当通过 SMB 文件共享，插件可以分析 3 层目录的深度，而不是 1 层。这可能导致在某些情况下产生更多的网络流量分析。值得注意的是，通过更彻底的扫描，扫描将更深入，且更可能破坏网络，而产生更有效的审计结果。

“**Antivirus**”(防病毒)选项允许在扫描中控制防病毒设置。

选项	说明
Antivirus definition grace period (in days)	配置防病毒软件检查的延迟天数(0-7)。“Antivirus Software Check”(防病毒软件检查)菜单允许您指示 Nessus 当防病毒的签名已经过期后在报告中允许一个特定的宽限时间。默认情况下，Nessus 会搜索签名过期的软件，不论它在多久以前更新过(例如，“几小时以前”)。这可以被设置为允许报告前最长过期 7 天。

“Windows”选项允许您微调 Windows 的扫描范围



如下选项影响了 Windows 目标 SMB 的范围：

选项	默认选项	说明
Request information about the SMB Domain	启用	若设置了“**Request information about the domain**”(要求域信息)选项，则将要求域用户信息，而不是本地用户。

下列设置项设置了对本地或域上用户数量枚举的值：

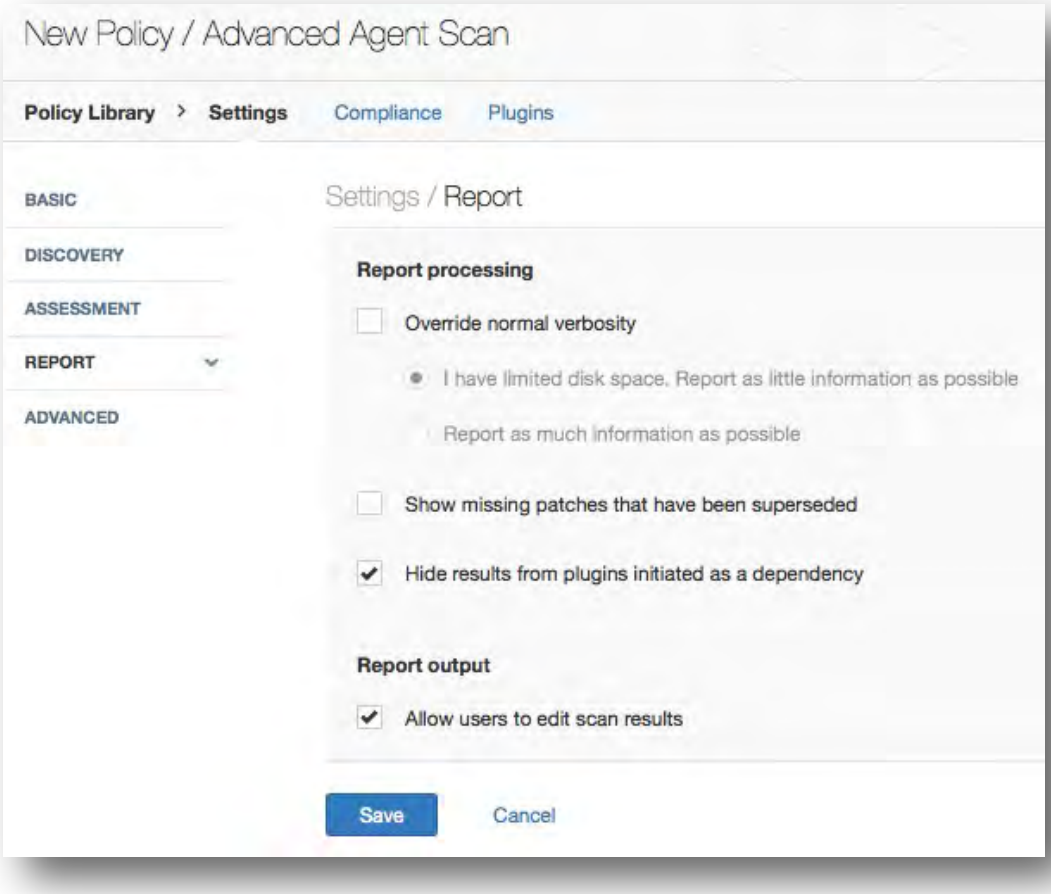
Option	Default	Description
Enumerate Domain Users	**Start UID: 1000 End UID: 1200**	“**Enumerate Domain Users**”(枚举域用户)菜单为使用定义了 SID 范围，以在域中执行反向查找用户名。默认设置对大多扫描可推荐使用。
Enumerate Local Users	**Start UID: 1000 End UID: 1200**	“**Enumerate Local Users**” (枚举域用户)菜单为使用定义了 SID 范围，以在本地执行反向查找用户名。默认设置推荐使用。

“Malware”(恶意软件)选项允许您指定一个额外的 MD5 哈希列表，以便 Nessus 用于从系统中扫描已知的恶意软件；并指定一个已知的好的哈希列表来减少误报。该列表由名为“Malicious Process Detection: User Defined Malware Running”(恶意程序检测: 用户定义恶意软件运行)的插件来使用(插件 ID 65548), 其功能类似 Tenable 的“Malicious Process Detection”(恶意程序检测)插件(插件 ID 59275).

选项	说明
Provide your own list of known bad MD5 hashes	额外的已知的坏的 MD5 哈希可以通过文本文件上传，该文本内容为每行一个哈希值。 可以在上传的文件中为每个哈希值添加描述(可选)。这可以通过在哈希值后添加一个逗号, 再添加描述来完成。如果扫描目标时找到任何匹配项，哈希值的描述说明会显示在扫描结果中。标准的哈希分隔符号(如, #)也可以使用除了以逗号以外的其他分隔符号。
Provide your own list of known good MD5 hashes	额外的已知的坏的 MD5 哈希可以通过文本文件上传，该文本内容为每行一个哈希值。 可以在上传的文件中为每个哈希值添加描述(可选)。这可以通过在哈希值后添加一个逗号, 再添加描述来完成。如果扫描目标时找到任何匹配项，哈希值的描述说明会显示在扫描结果中。标准的哈希分隔符号(如, #)也可以使用除了以逗号以外的其他分隔符号。
Hosts file whitelist	Nessus 检查系统主机文件被篡改的迹象(如：插件 ID 23910 名为“Compromised Windows System (hosts File Check”(Windows 系统问题(主机文件检查))。该选项允许您上传一个包含主机名的文件，其中包含 Nessus 扫描时被忽略的主机名列表。这是每行包括一个主机名的常规文本文件。

Report 报告

“**Report**”(报告)模块将影响报告的生成和导出



“**Report processing**”(报告生成)选项对报告中会包含的所有插件信息产生影响。

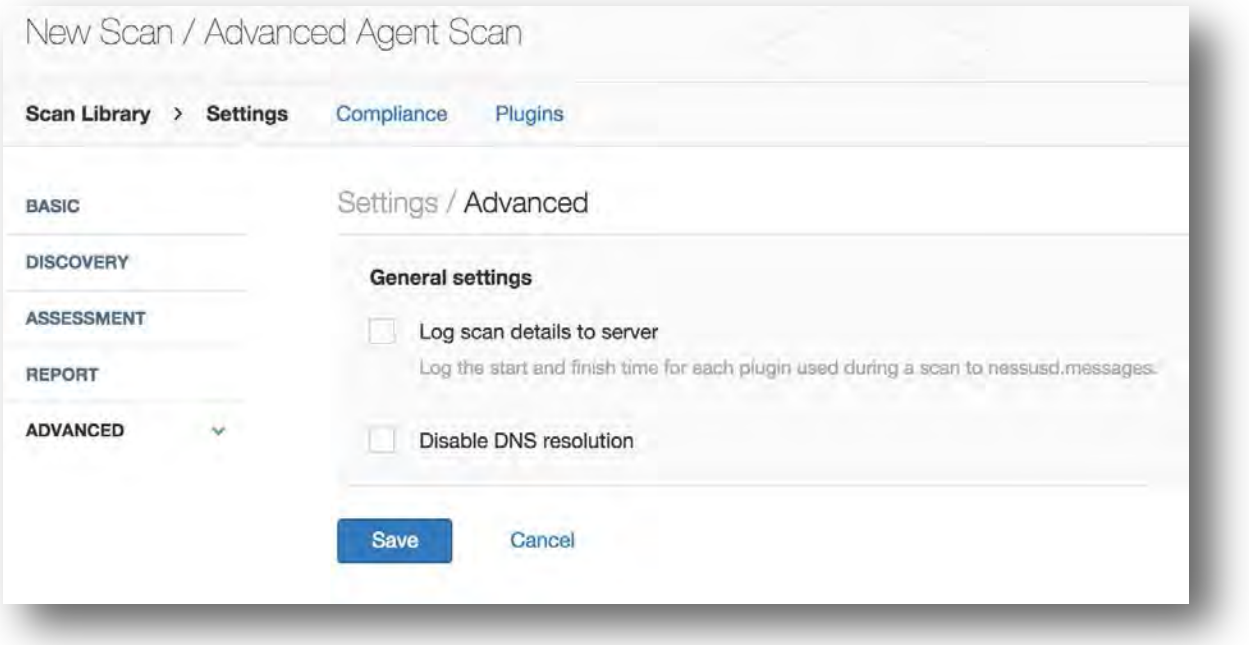
选项	默认设置	说明
Override normal verbosity	不启用	“**I have limited disk space. Report as little information as possible**”(我只有有限的磁盘空间，尽量减少报告中的信息) 将在报告中提供较少的关于插件活动的信息以减少对磁盘空间的影响。 “**Report as much information as possible**”(尽可能多的提供报告信息) 将在报告中提供较多的插件活动信息。
Show missing patches that have been superseded	不启用	此选项允许您配置 Nessus 来加入、移除或者取代扫描报告中的补丁信息。此选项默认是关闭的，除非该策略的创建使用了策略目录中的内网 PCI 网络扫描模板。
Hide results from plugins initiated as a dependency	启用	若勾选此项，依赖项的列表不包括在报告中。若您希望将依赖项的列表纳入报告，请取消勾选。

“**Report output**”(报告导出)选项会对报告结果产生影响。

选项	默认设置	说明
Allow users to edit scan results	启用	若勾选，此功能允许客户从报告中删除项目。当执行合规性扫描或其他类型的审计时, 取消这个选项可以让显示的扫描无法被篡改。

Advanced 高级选项

“**Advanced**”高级选项模块包含各种配置选项，提供对 Agent 更细颗粒度的操作控制。

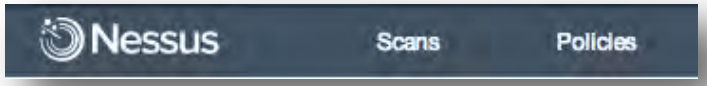


“**General Settings**”(通用设置)菜单进一步说明扫描如何被日志记录

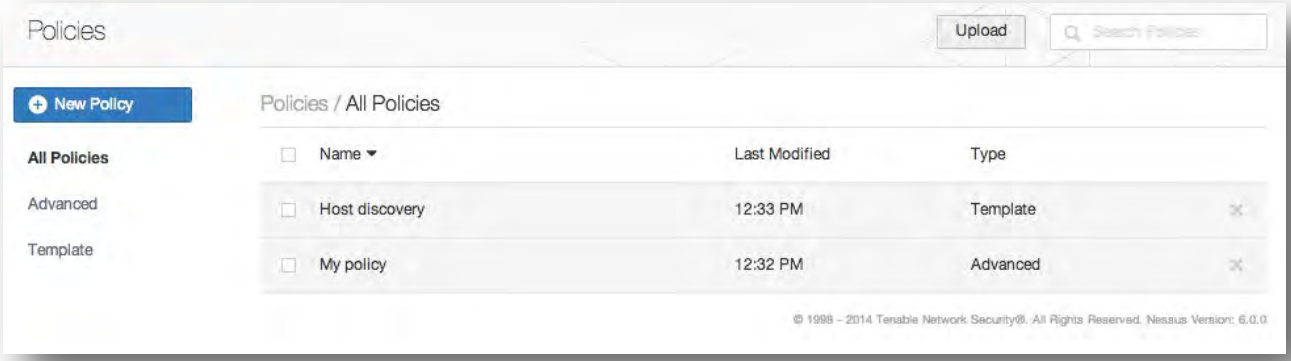
选项	默认设置	说明
Log Scan Details to Server	不启用	保存扫描的其他细节到 Nessus 服务器日志（**nessusd.messages**），包括插件的启用、完成，或者若插件被取消。此结果日志可用于确认被使用的特殊插件和被扫描的主机。
Disable DNS Resolution	不启用	不启用域名解析。此选项将保证代理服务器完成扫描时不依赖于网络。

Managing Policies 管理策略

查看所有您的定制策略，请点击您屏幕顶部的“**Policies**”(策略)菜单项：

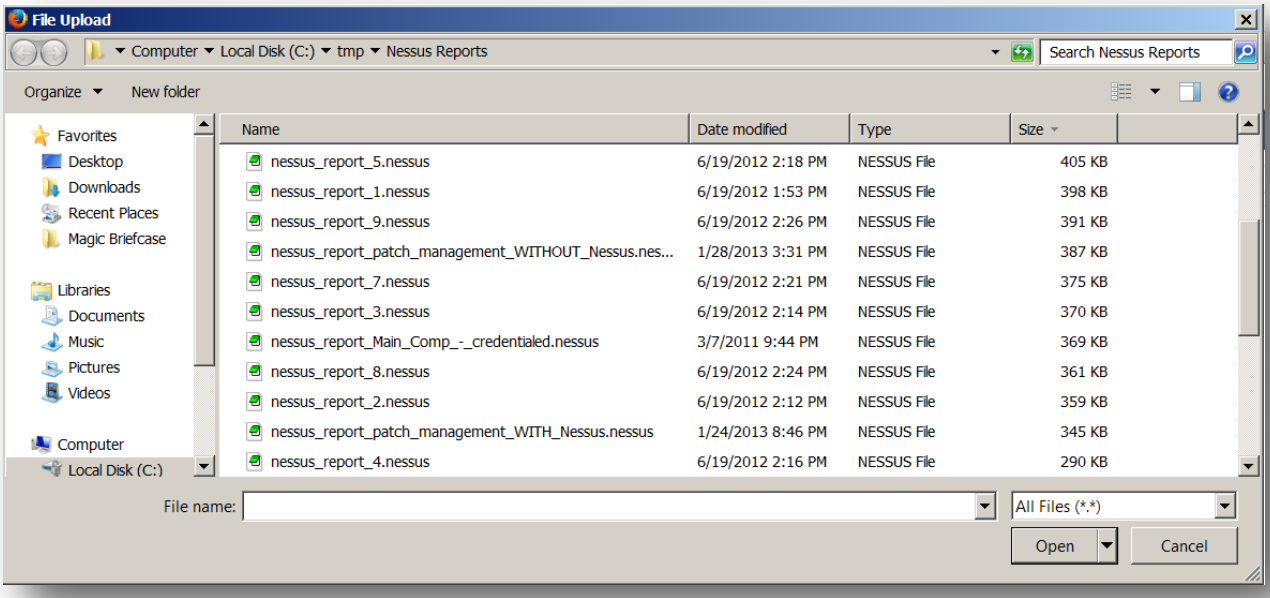


为方便企业，Nessus 在左侧有 2 个预置滤波器，“**Advanced**”(高级)和“**Template**”(模板)策略。需要注意的是，除非你在每个策略类型里至少一个出现项目，否则它将不会显示：

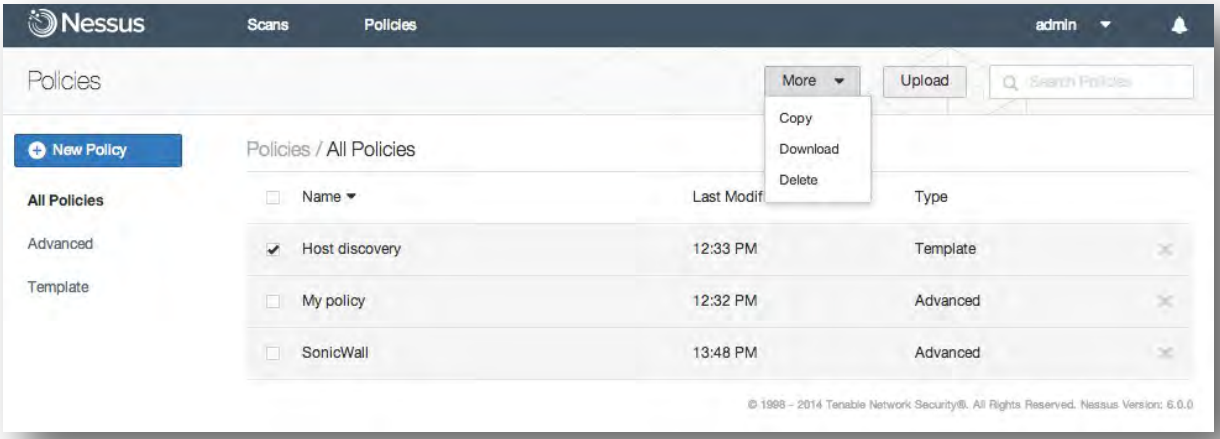


Importing, Exporting, and Copying Policies 导入、导出和复制策略

策略菜单栏中的“**Upload**”(上传)按钮，允许您上传先前创建的策略到扫描仪。使用本地文件浏览器，从您本地系统中选择策略，并点击 “**Open**”(开启)：



点击扫描仪的策略选择复选框，使“Upload”按钮旁的三个选项启用。这些选项是“Copy”(复制), “Download”(下载)和“Delete”(删除)。



点击“**Download**”(下载)可以打开下载对话窗口，以便您可以在一个外部程序(比如：文本编辑)中开启策略，或将策略保存到您选择的目录下。策略根据从浏览器中自动下载。

策略中包含的密码和`.audit` 文件无法被导出。

若您打算创建一条和现有策略类似，仅需作一些微小调整的策略，您可以选择列表中的基本策略，点击菜单中的“**Copy**”(复制)按钮。这可以创建一条复制于原始策略并根据修正要求进行编辑来完成的策略。这对于在一个已有环境中从一条在标准策略上按要求进行细微改变，然后创建出新的策略来说是很有用的。

Scans 扫描

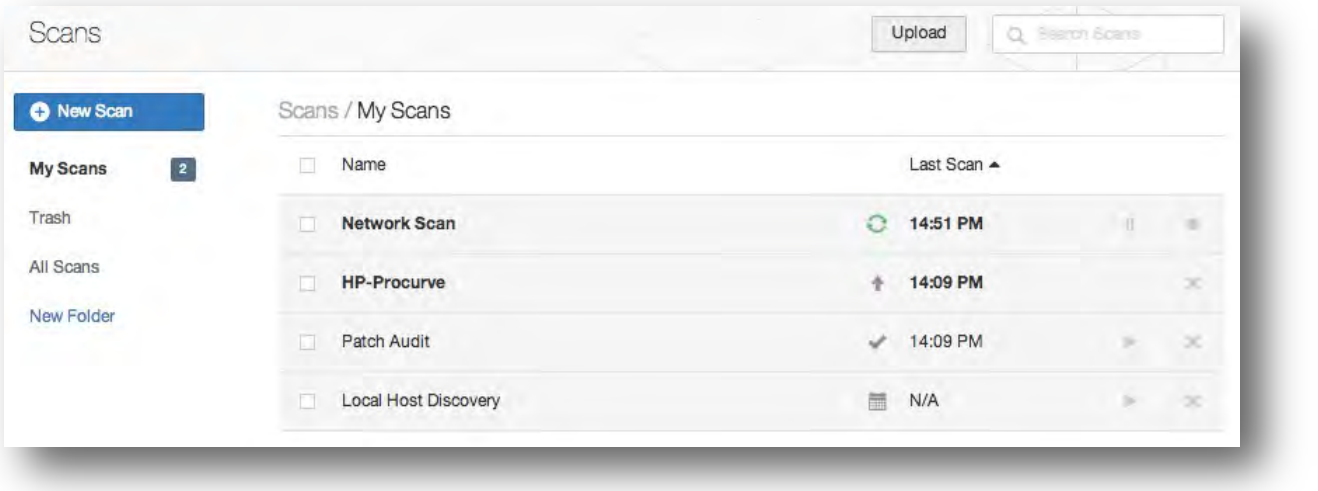
在创建一条策略或者使用了策略模板后，您需要创建一次扫描。扫描会提供扫描的名称，扫描的描述，扫描的储存文件夹，使用的扫描仪或代理服务器，扫描目标的信息。

Creating, Launching, and Scheduling a Scan 创建、发起并制定扫描计划

每次扫描默认的 Nessus UI 文件夹在 **My Scans** 文件夹下，这是无法被删除的。

任何尚未能查看但已经发起的扫描将在该文件夹下以粗体字形式显示。此外，新发起的扫描数量会显示在该文件夹旁。

Nessus DB 数据库格式是一种加密的专有格式。请注意，Nessus DB 数据库中记录了所有关于扫描可能的数据，包括但不限于扫描结果、审计记录和附件。



下列扫描状态将在扫描列表盘中可见：

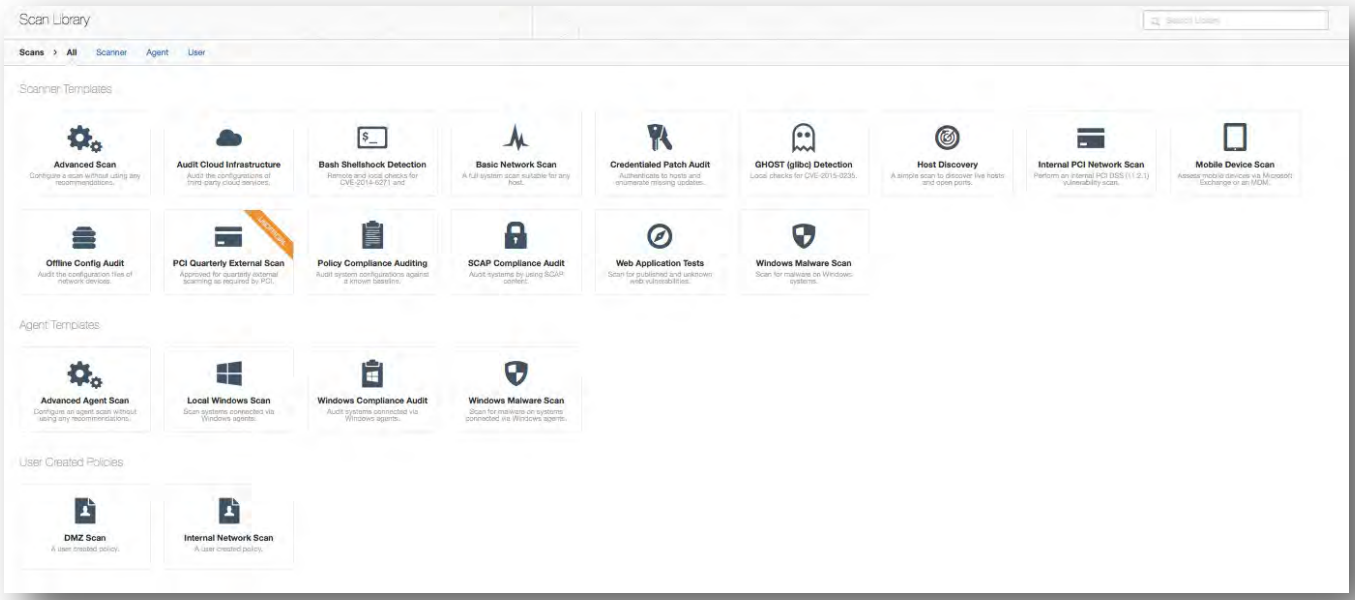
扫描状态	描述
Completed	扫描已全部完成
Running	扫描正在进行中
Canceled	用户在扫描完成前已经主动使它停止
Aborted	该扫描由于一个无效目标列表或一次服务器错误(比如：服务器重启或死机)而被放弃继续扫描进程
Imported	该扫描已通过上传功能被成功导入

这些状态仅适用于新发起的扫描。旧的扫描记录将均为“Completed”(已完成)，且无法再运行。同种状态下的扫描可以列出在左边导航面板上的虚拟文件夹中。

Configuring a Scan 配置扫描

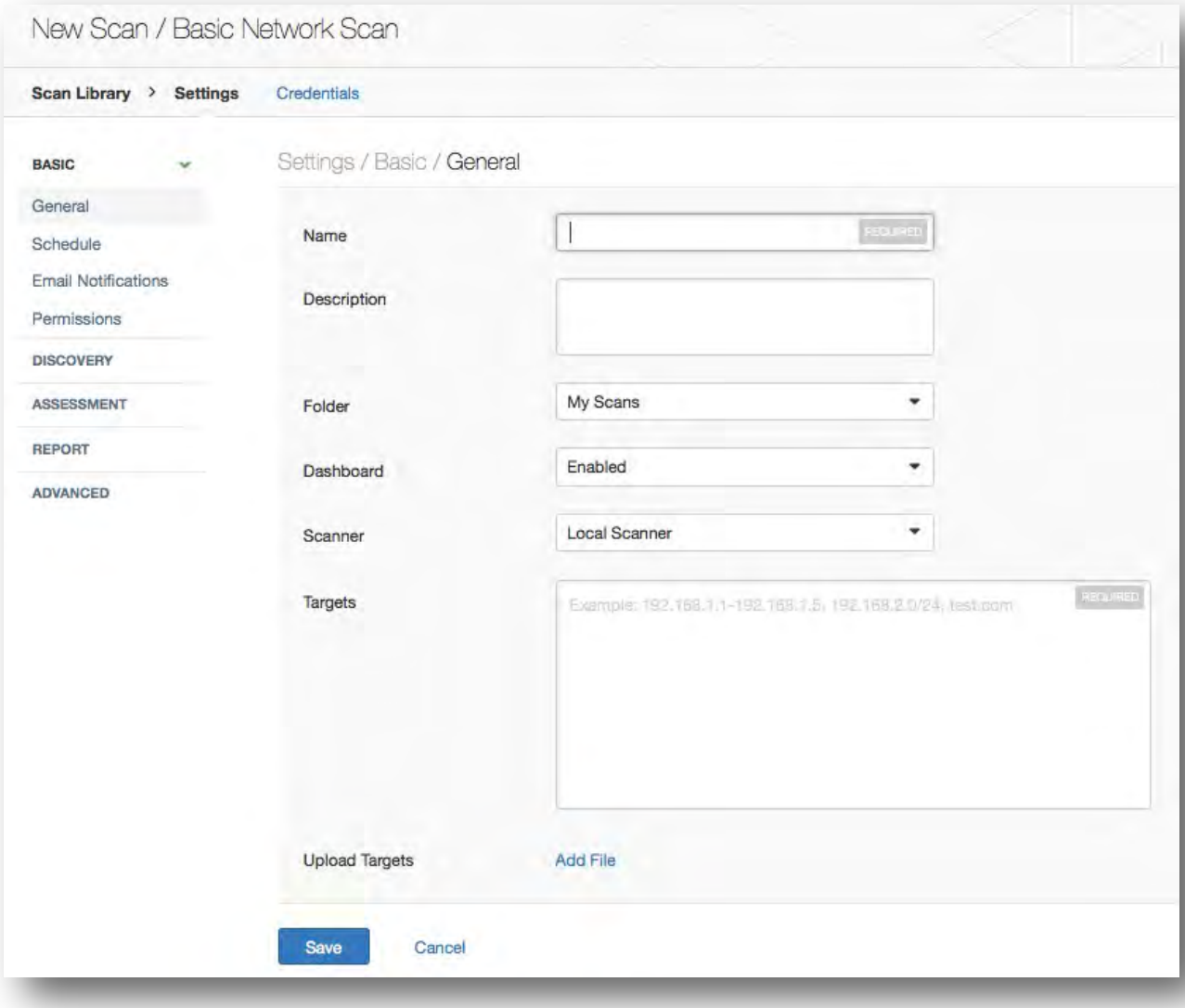
在创建或选择了一条策略后，要创建一次新的扫描可以通过点击菜单栏顶部的“**Scans**”(扫描)选项，然后点击左边的“**+New Scan**”(+新发起扫描)按钮。这将使您进入新的策略进程，定义策略创建模块。

一般情况下，并不需从创建策略开始。点击“**New Scan**”允许您用一个默认的模板来创建策略。请注意，屏幕将同时显示默认模板和用户创建的模板。



这可以使您或者通过从 Scanner Templates(扫描仪模板)或 Agent Templates(代理服务器模板)中选择一个模板创建一个新的策略，或者选择一个您已经在 User Created Policies（用户创建的策略）中创建的策略。

创建或配置一个新策略后，“New Scan”屏幕如下所示:



在”General”页面下，有如下区域输入扫描模板:

选项	默认	描述
Name	无	设置名字，用以在 Nessus UI 上分辨扫描。
Description	无	选项栏用于显示更多的扫描详细描述。
Folder	**My Scans**	Nessus UI 文件夹，存储扫描结果。
Dashboard	**Enabled**	启用或禁用扫描仪表盘。仪表板默认启用所有新扫描。然而, 除非你启用他们，他们在现有或导入扫描上是被禁用的。

Scanner	**Local Scanner**	Nessus 扫描仪进行扫描。这将提供多个选项如果你有配置额外 Nessus 扫描仪是次要的。
Targets	无	目标可以输入单独 IP 地址 (e.g., 192.168.0.1), IP 范围(e.g., 192.168.0.1-192.168.0.255), CIDR 标记的子网段 (e.g., 192.168.0.0/24), 可解析的主机 (e.g., www.nessus.org),或者单独的 IPv6 地址 (e.g., link6%eth0, fe80::2120d:17ff:fe57:333b, fe80:0000:0000:0000:0216:cbff:fe92:88d0%eth0).
Upload Targets	无	带有主机列表的文本文件，点击“Add File”和选择来自本地机器的文件

只有本地扫描器能在 Nessus Professional 使用。

主机文件必须为 ASCII 文本，每行一个主机，没有多余空格或行。不支持 Unicode/UTF-8 代码。

样板主机文件格式:

独立主机:

192.168.0.100
192.168.0.101
192.168.0.102

主机范围:

192.168.0.100-192.168.0.102

主机 CIDR 块:

192.168.0.1/24

虚拟主机:

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]

IPv6 地址:

link6
fe80::212:17ff:fe57:333b
fe80:0000:0000:0000:0216:cbff:fe92:88d0

IPv6 地址，有基于 Unix 操作系统的区索引 (e.g., Linux, FreeBSD):

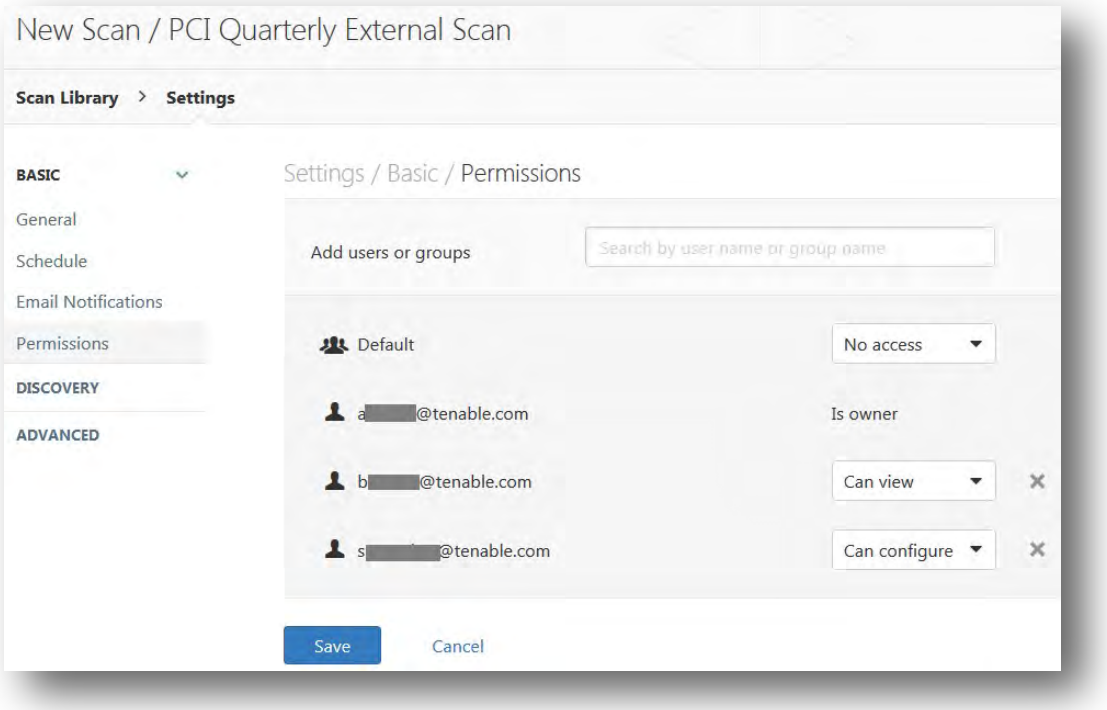
link6%eth0
fe80::212:17ff:fe57:333b%dc0
fe80:0000:0000:0000:0216:cbff:fe92:88d0%eth0

IPv6 地址，有 Windows 操作系统的区索引：

link6%23
fe80::212:17ff:fe57:333b%1
fe80:0000:0000:0000:0216:cbff:fe92:88d0%6

根据你的扫描设定， 比如 “**max hosts**” or “**max checks per host**”, 可能导致虚拟主机被限制和 Nessus 看到的一样 IP 地址。 在非 Windows 主机上，Nessus 管理员可以添加名为 multi_scan_same_host 的自定义高级设定并设置其为“是的”。 这将允许扫描仪对相同的 IP 地址执行多个扫描。注意,在 Windows 上,PCAP 驱动不允许这无视 Nessus 配置。在 Nessus 5.2.0 及以后版本有这个功能。

在 Nessus Manager 和 Nessus Enterprise Cloud 中，你可以配置扫描的粒度权限：

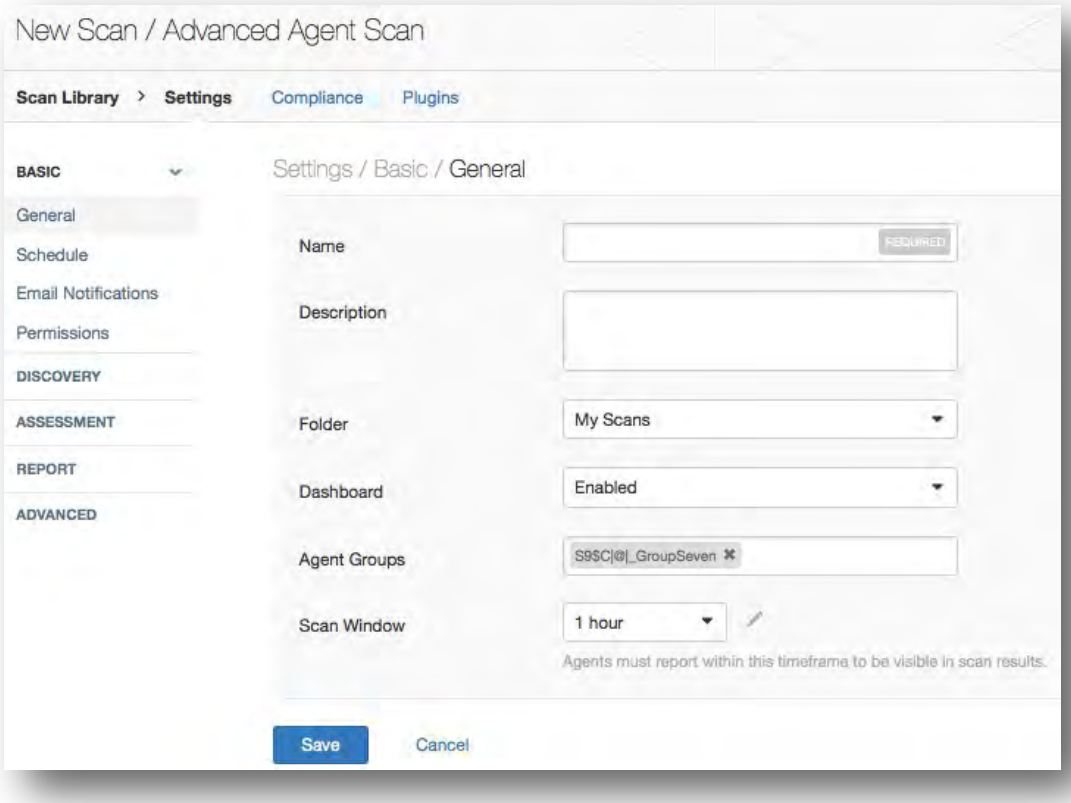


“**Permissions**”功能影响哪个用户有权限访问或配置扫描：

权限	描述
No Access	只有创建策略的用户可以查看、使用或编辑政策。
Can View	其他用户可以查看扫描结果。他们将无法控制或配置扫描。
Can Control	其他用户可以控制扫描(启动、暂停和停止),查看扫描结果。他们将无法配置扫描。
Can Configure	其他用户可以控制扫描(启动、暂停和停止),查看扫描结果。他们将无法配置扫描。

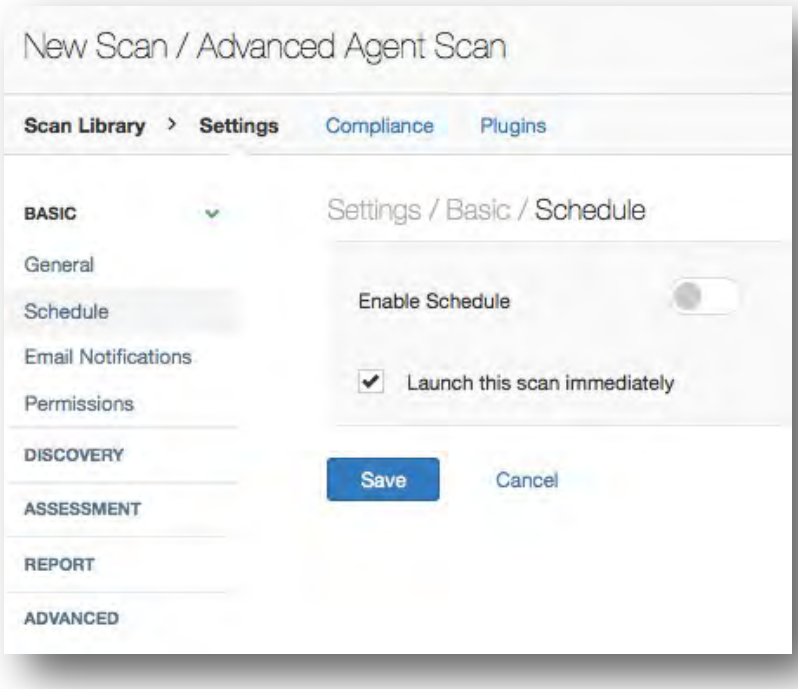
配置带有 Nessus Agents 的扫描

有 Nessus Manager,你也能执行带有 Nessus Agents 的扫描.

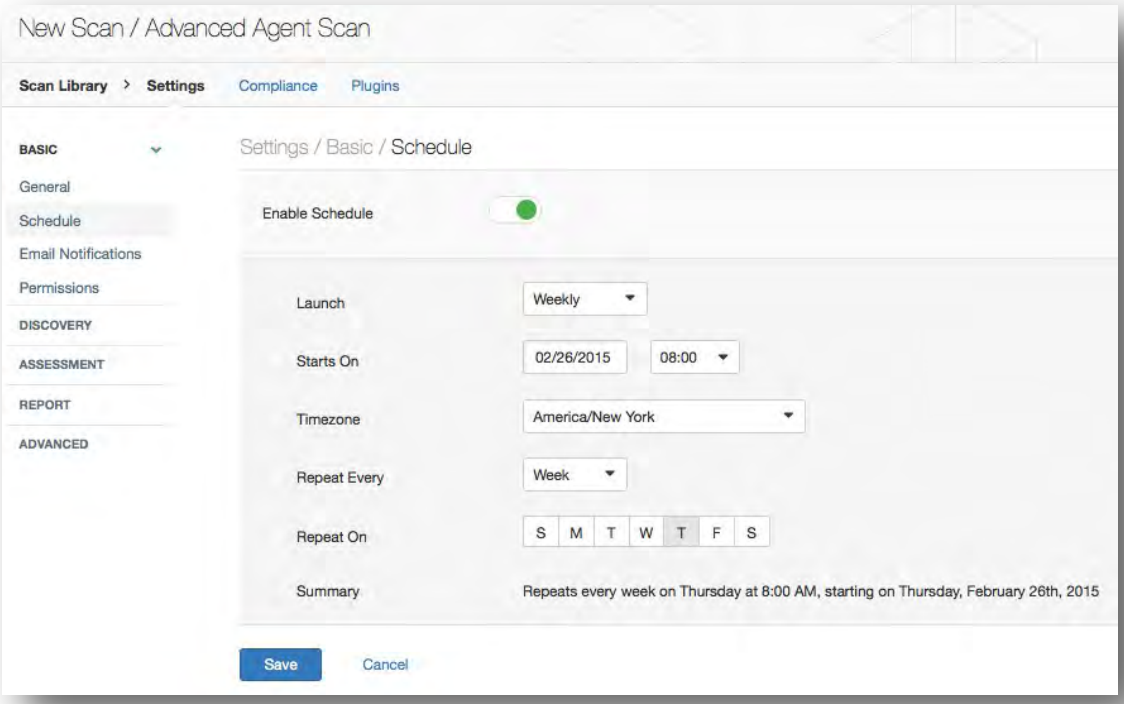


选项	默认	描述
Name	无	设定将显示在 Nessus UI 用来识别扫描的名称。
Description	无	可选字段进行更详细描述的扫描。
Folder	**My Scans**	Nessus UI 文件夹，存储扫描结果。
Dashboard	**Enabled**	启用或禁用扫描仪表盘。仪表板默认启用所有新扫描。然而, 除非你启用他们，他们在现有或导入扫描上是被禁用的。
Agent Groups	无	哪个 Nessus Agents 扫描器组去执行这次扫描. 这将提供多个选项如果你有配置额外 Nessus 代理组用于扫描。
Scan Window	**1 小时**	Nessus 代理的时间必须回到 NessusManager 汇报。然而,如果你点击自定义,您可以更改变量你想拥有 Nessus 代理返回它的扫描的分钟时长。

在“**Schedule**”页面下，有一个下拉菜单控制扫描时就会启动。注意 Launch this scan immediately 是默认启动的。



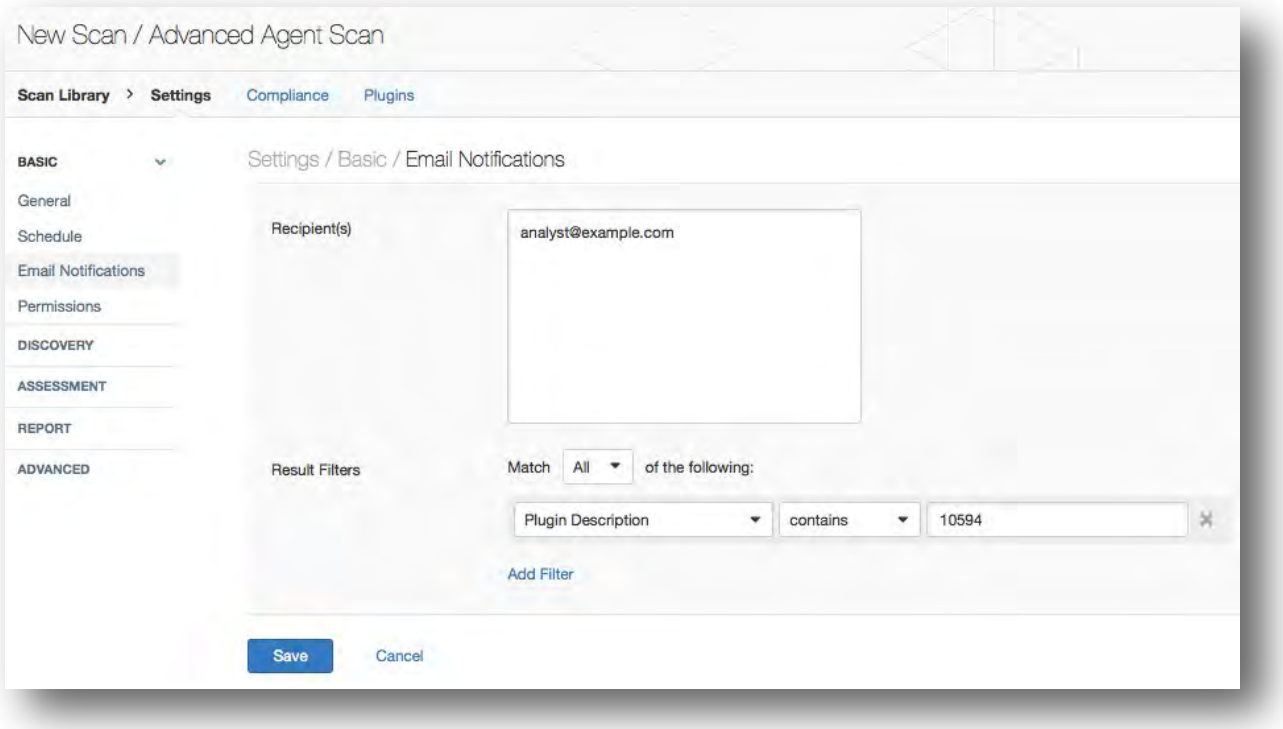
打开 Enable Schedule 开关来启动计划任务:



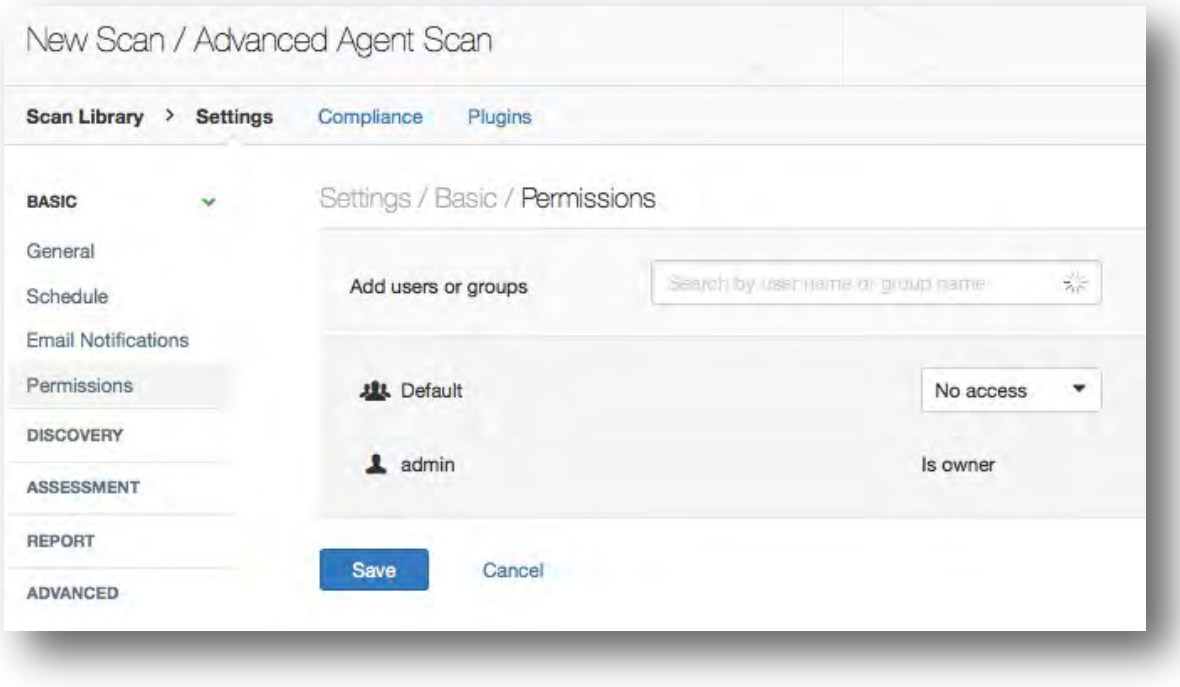
计划选项如下:

权限	描述
On Demand	创建扫描作为模板，以便可以在任何时间（此功能以前处理下"扫描模板"选项）手动启动。选中的复选框，“**Launch this scan immediately**”立即启动扫描。
Once	安排在特定的时间扫描。
Daily	安排扫描至 20 天发生在日常的基础上向上的在特定的时间或时间间隔。
Weekly	安排扫描在定期的基础上发生的时间和周、 20 周的时间为一天。
Monthly	安排扫描通过时间和每天或每周的月，长达 20 个月来每个月。
Yearly	安排扫描，每年，发生的时间和日期，达 20 年之久。

在“**Email Notifications**” 页面，您可以配置电子邮件地址用来通过电子邮件通知扫描完成。收件人单独列出,由换行符分隔。过滤器将影响什么是显示在电子邮件。例如,如果你只想看到关键邮件插件,他们就会显示。



对于 Nessus Agents，你可以在配置扫描的粒度权限：



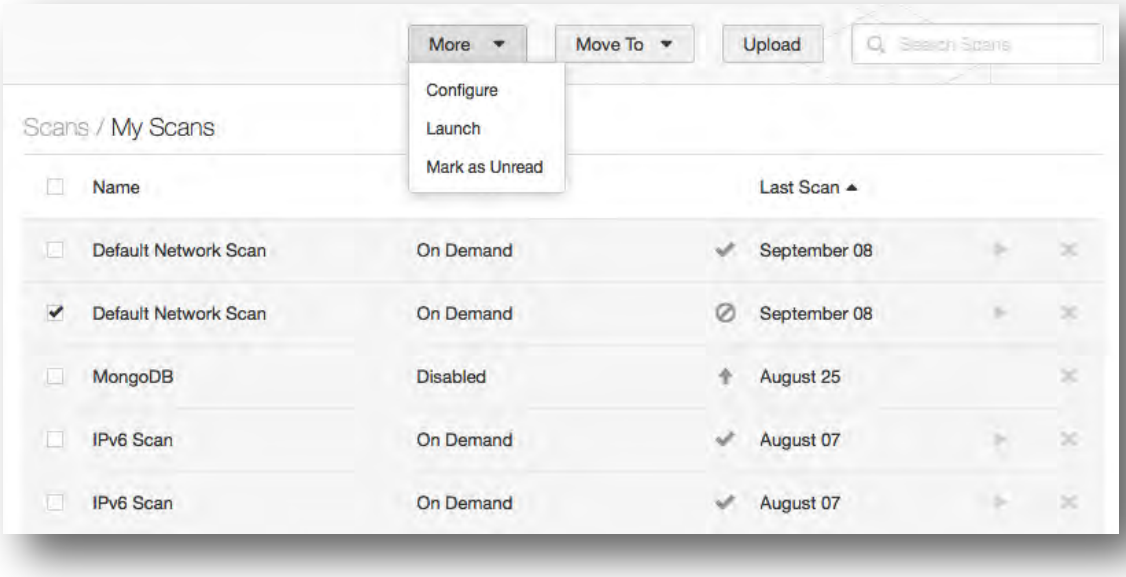
“**Permissions**”功能影响哪个用户有权限访问或配置扫描:

权限	描述
No Access	只有创建策略的用户可以查看、使用或编辑政策。
Can View	其他用户可以查看扫描结果。他们将无法控制或配置扫描。
Can Control	其他用户可以控制扫描(启动、暂停和停止),查看扫描结果。他们将无法配置扫描。
Can Configure	其他用户可以控制扫描(启动、暂停和停止),查看扫描结果。他们将无法配置扫描。

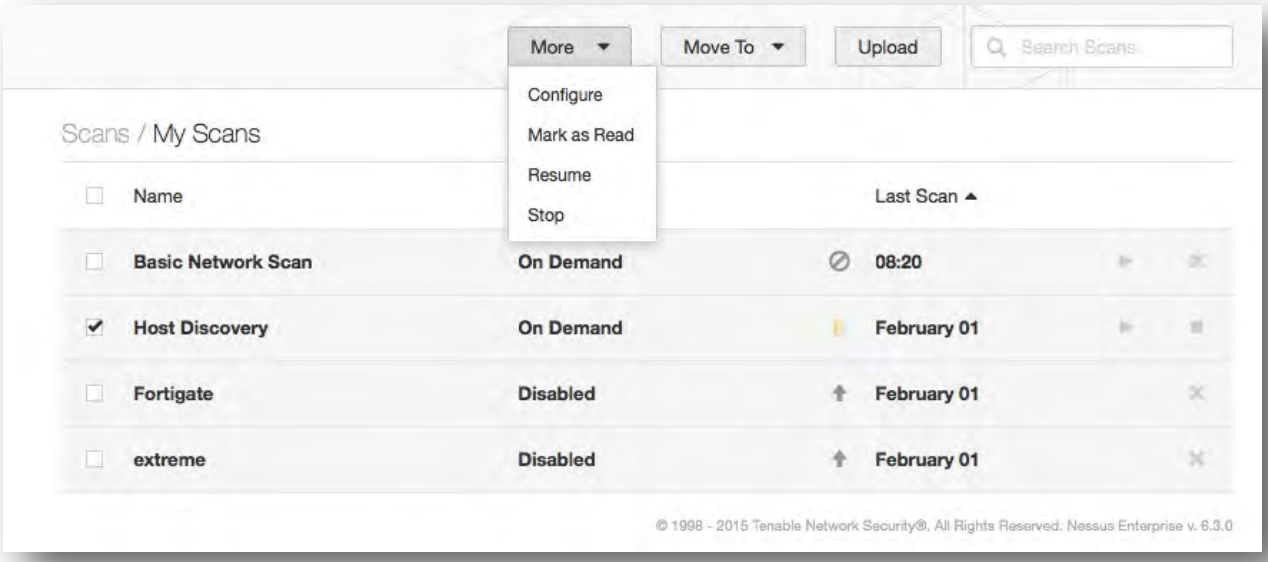
"电子邮件扫描结果"功能需要 Nessus 管理员配置了 SMTP 设置。有关配置 SMTP 设置的详细信息，请参阅 “Nessus 6.3 Installation and Configuration Guide” 。如果不配置这些设置后，Nessus 将警告您必须将其设置为工作的功能。

管理扫描

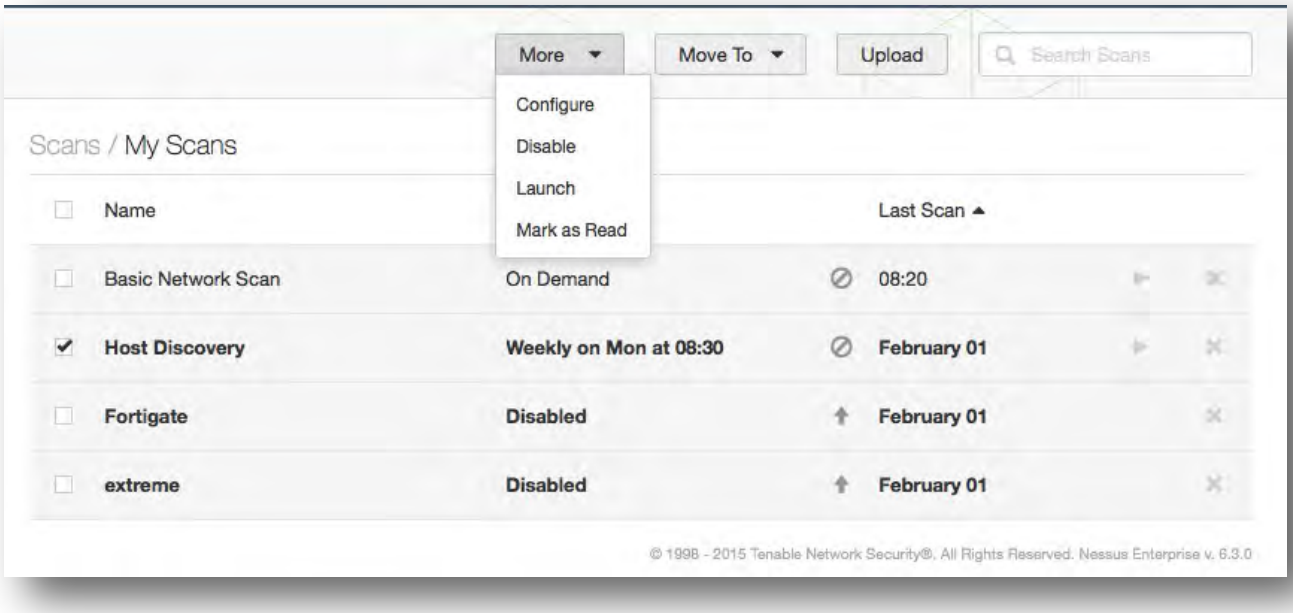
一旦创建了一个扫描,它可以访问通过顶部的“More”菜单。从这里,您可以切换扫描的阅读状态标记为未读或标记为已读。此外,选择“Configure”允许您管理扫描,包括他们的日程安排和设置,并根据需要更新它们。



注意如果你有扫描选定 Nessus 这个实例上创建的,您也可以从“更多”菜单中运行的控制命令。

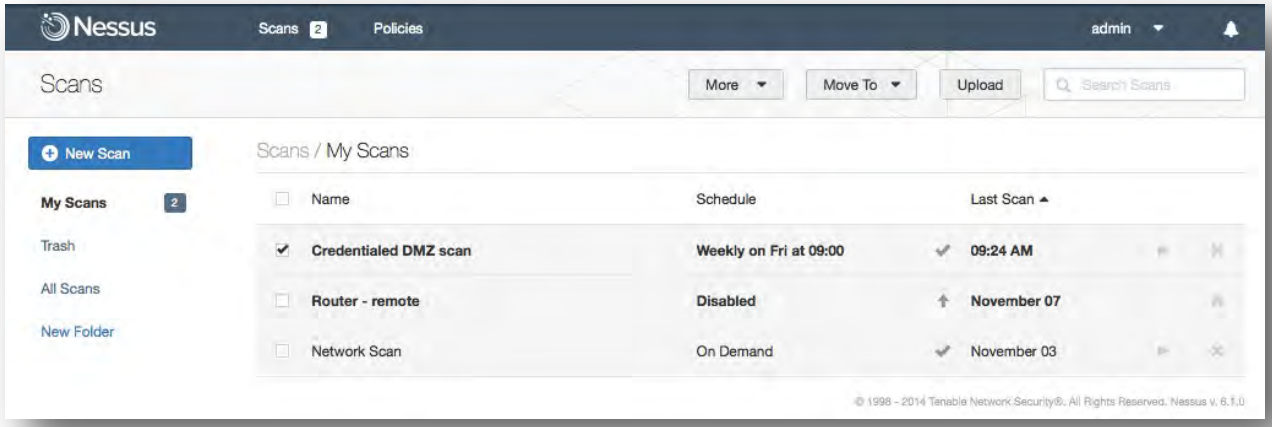


如果选择安排扫描,您可以禁用它的“More”菜单:

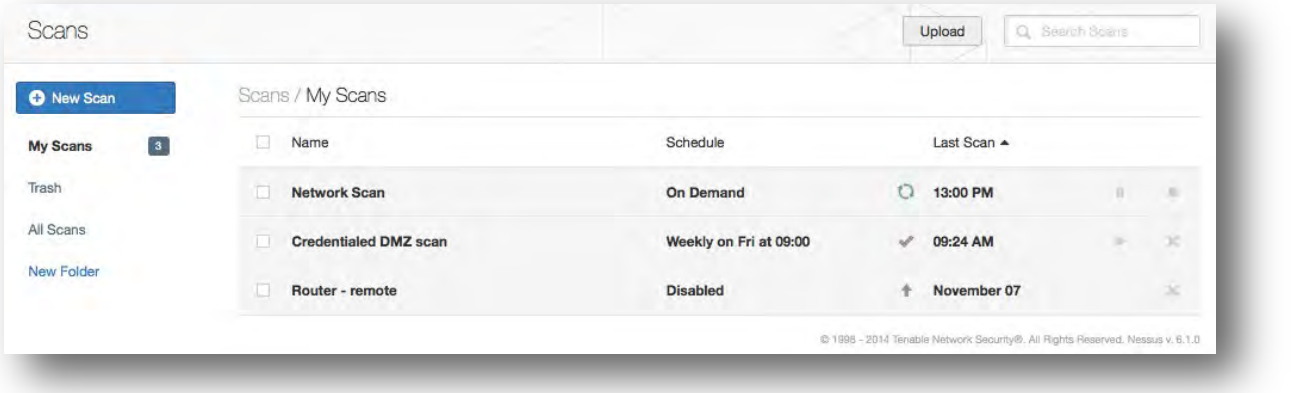


进入扫描信息后,点击“Save”。提交后,将立即开始扫描(如果选择“Launch this scan immediately”)在显示之前返回到“Scans”页面。顶部菜单栏

也将更新数量覆盖“扫描”按钮来显示有多少总扫描未读。.



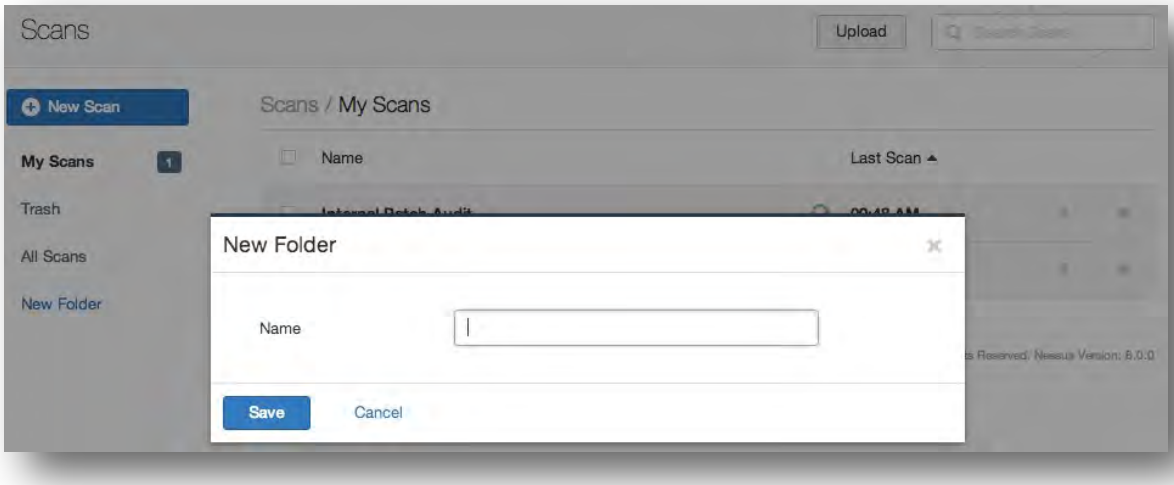
扫描发起了一次,“Scans”列表将显示所有正在运行扫描列表或停顿了一下,还有关于扫描的基本信息。在扫描时,暂停和停止按钮左边改变现状:



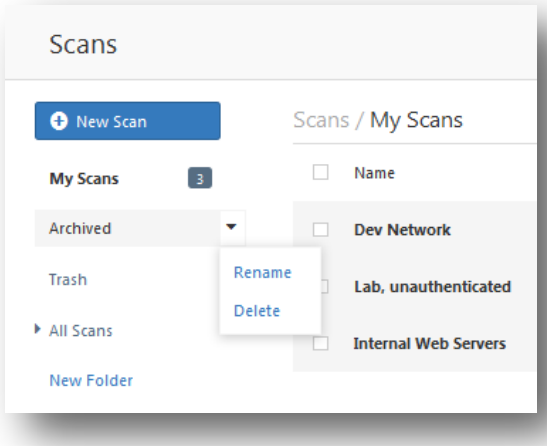
在选择一个特定的扫描通过左边的复选框列表,“More”和“Move To”按钮在右上角将允许您执行进一步的操作包括重命名的能力，操作扫描状态，标记为已读，或者将其移至一个不同的文件夹。

创建和管理扫描文件夹

扫描可以组织到文件夹。左边是两个默认文件夹,我的扫描和垃圾。默认情况下,所有新扫描将出现在我的扫描虚拟文件夹。可以创建额外的文件夹通过左边的“New Folder”选项和随后的弹出窗口,如下图所示:

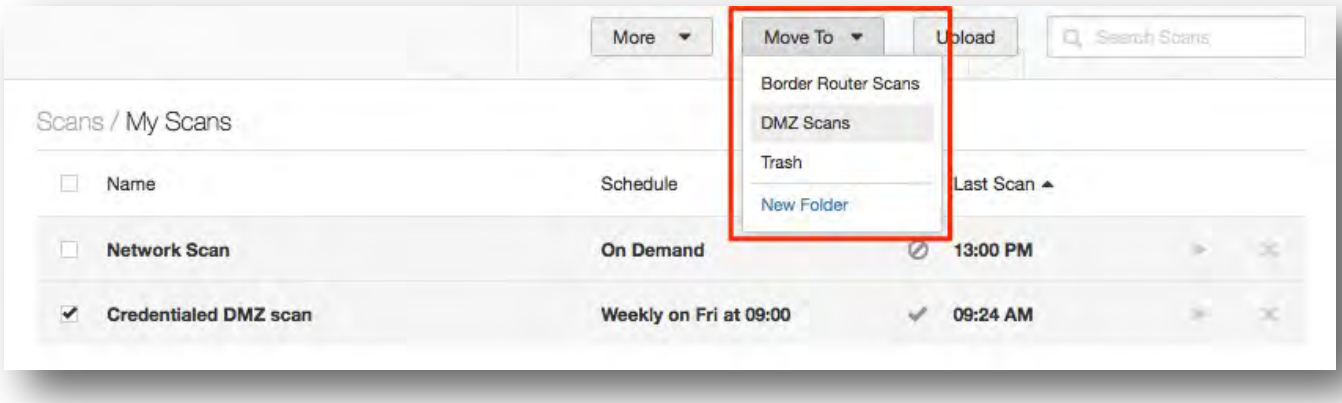


文件夹可以通过鼠标在一个文件夹重命名或删除,弹出一个下拉箭头,并点击它:



"Trash"文件夹中的扫描会自动删除后 30 天。他们可以在任何时间通过单独删除被删除,或选择"Empty Trash"。

移动扫描结果文件夹,选择左边的扫描检查框。一旦检查,额外的顶部下拉菜单就会出现。一个提供"More"选项包括重命名和标记扫描读取或未读。第二个允许您移动扫描到所需的文件夹.

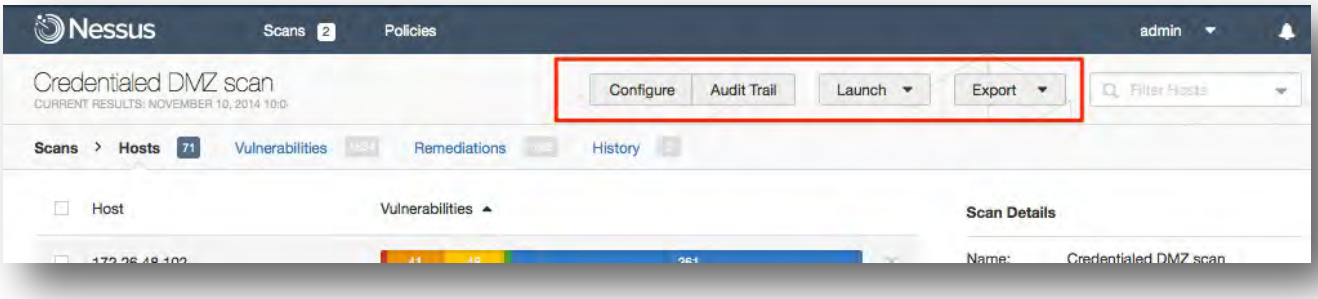


扫描结果和报表

Nessus 有一个广泛的界面查看扫描结果和生成报告。此外,您可以重新配置扫描,执行审计跟踪,启动扫描,或导出结果,查看报告。

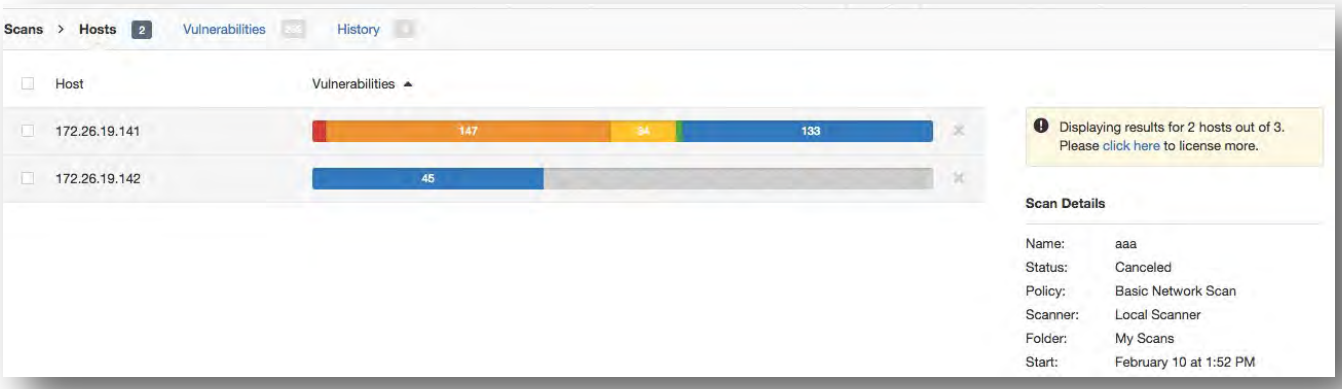
浏览扫描结果

标题的扫描结果显示,当前日期的结果,导航栏,扫描结果。扫描结果,上面有四个按钮处理扫描结果:



按钮/下拉	描述
Configure	导航会扫描设定。
Audit Trail	拉开审计跟踪对话。本节稍后审计跟踪。
Launch	启动扫描停两个选择:默认和自定义。自定义选项允许您定义不同的目标扫描,违约将与预定义的目标运行扫描。
Export	允许您保存扫描结果的四种格式:Nessus(.nessus)、HTML、CSV 或 Nessus DB。导出本节后的扫描结果。

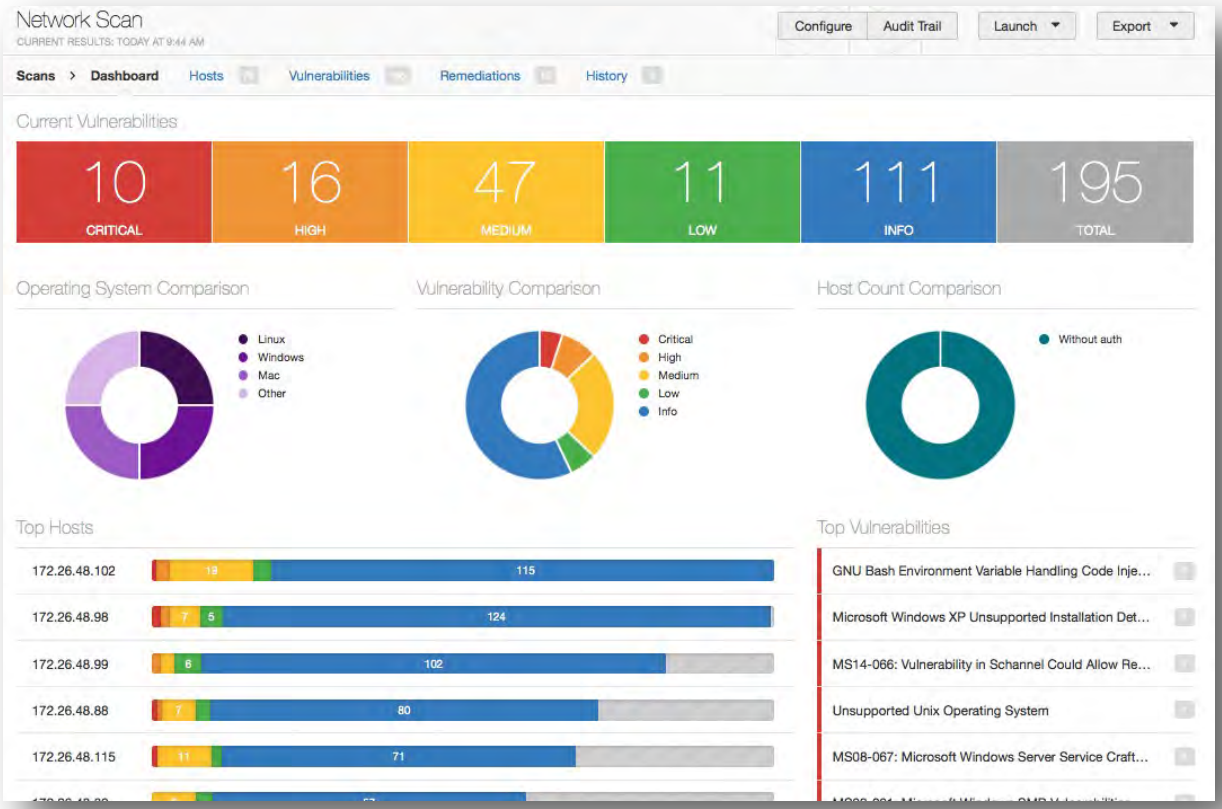
如果你主机扫描超过许可允许,Nessus 将显示一个警告来引导你联系站得住脚的获得更多许可证通过选择“点击这里”:



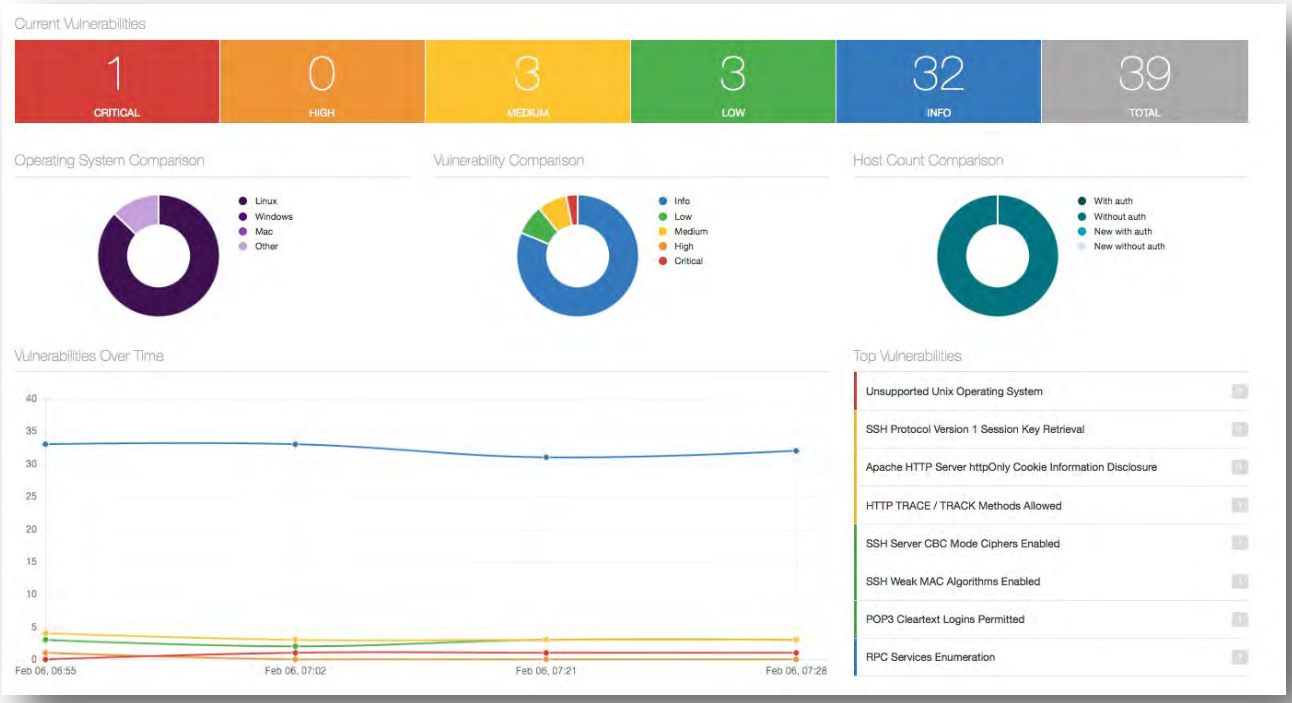
仪表盘

Nessus 经理可以为扫描结果显示仪表盘。仪表盘图形的扫描,包括:总结目前的漏洞的严重性和总,由操作系统漏洞,漏洞的严重性,主机扫描比较有和没有凭证。

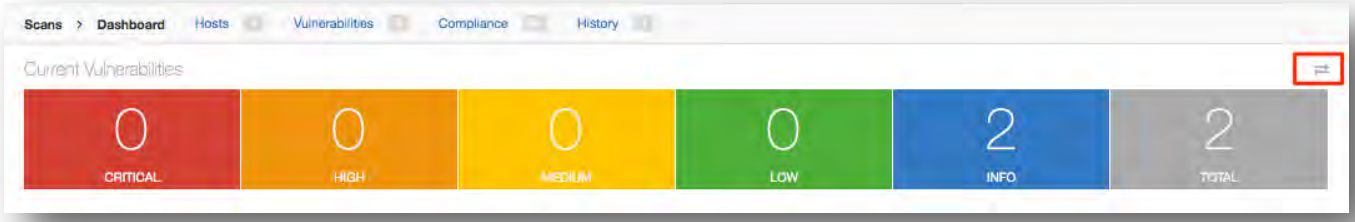
第一次运行扫描时,仪表板将显示漏洞数随着时间的推移和大漏洞发现:



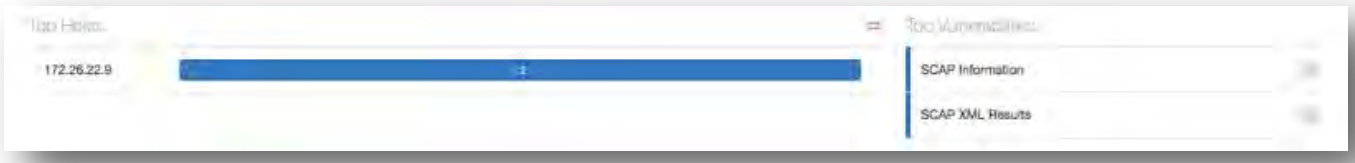
如果有多个扫描结果,最高主机表将被替换为根据时间的漏洞:



如果一个扫描包括合规结果,您将看到切换箭头上方的总数:

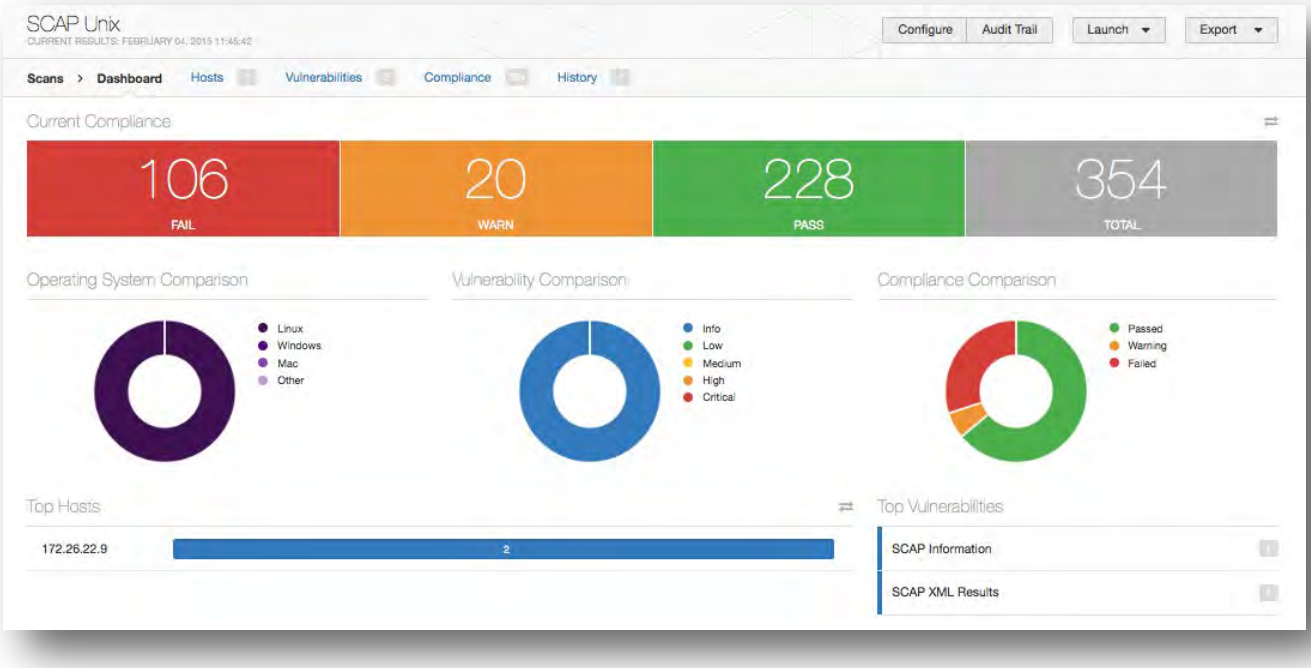


您还将看到最高漏洞旁的开关箭头:



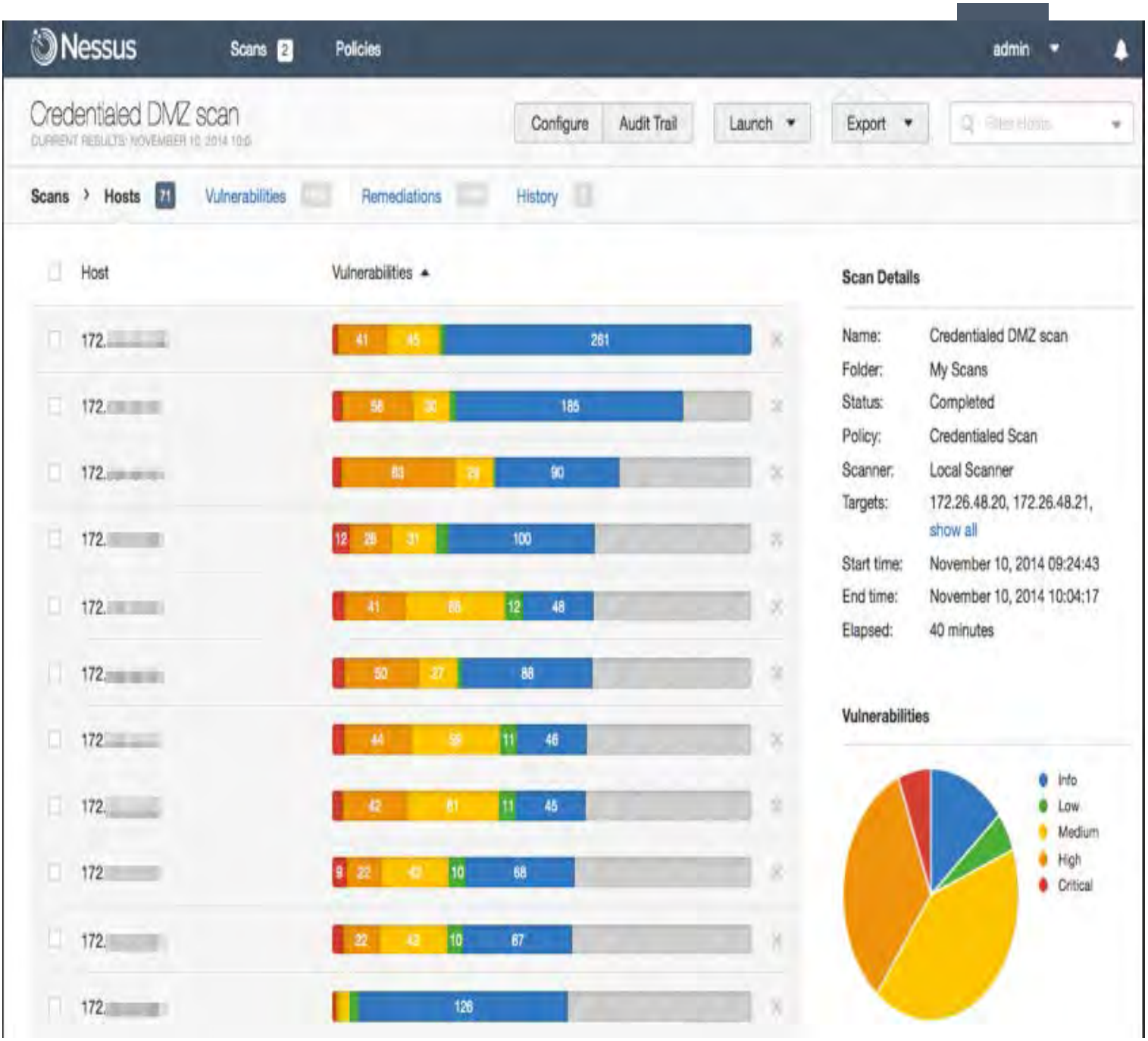
如果你鼠标的箭头切换,您将看到文本,导航将带你到漏洞数量或合规计数指示板:

合规化结果会显示如下:

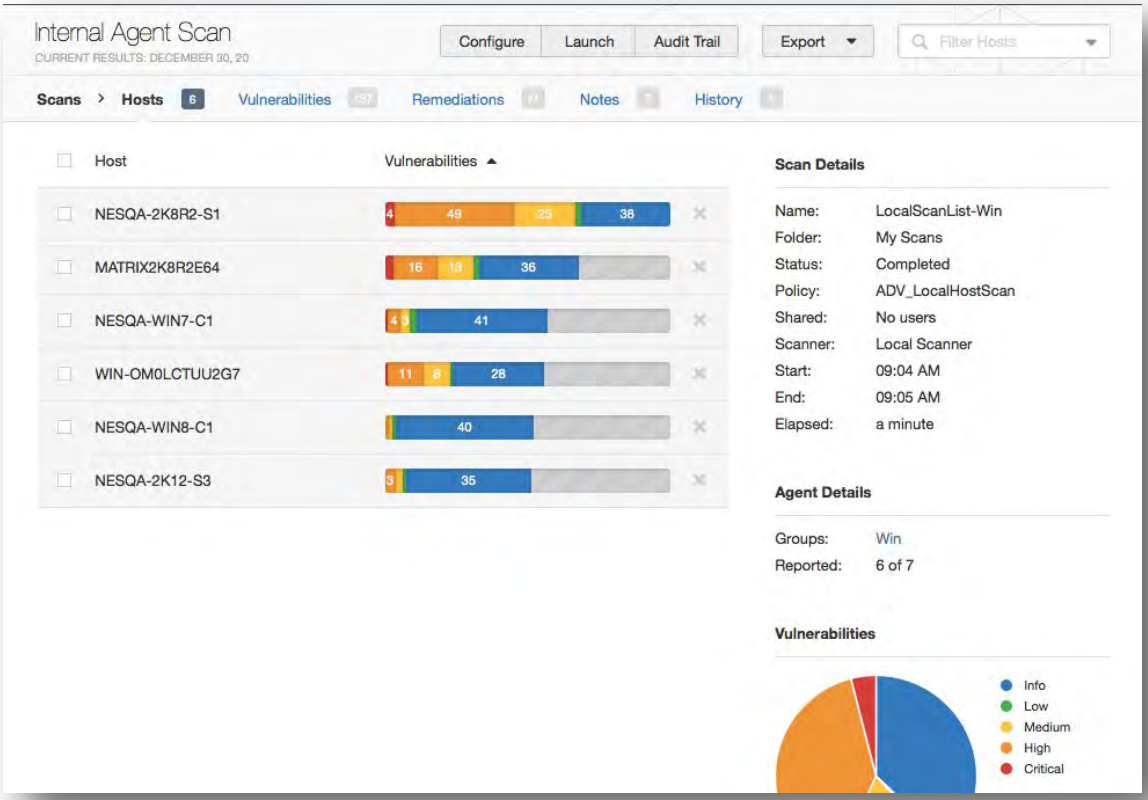


只扫描仪表板可从完成扫描。上传扫描默认不启用仪表板。

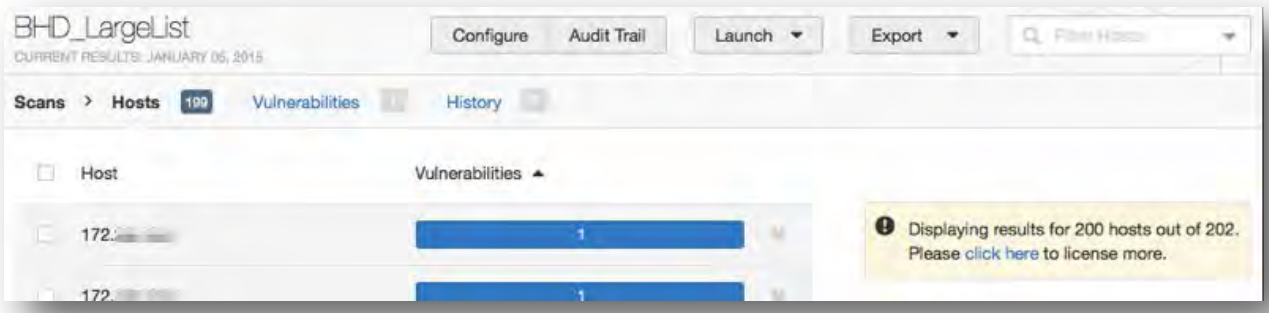
扫描结果可以通过漏洞或导航主机显示端口和特定漏洞的信息。默认视图/选项卡是由主机总结用不同颜色列表显示每个主机脆弱性的总结:



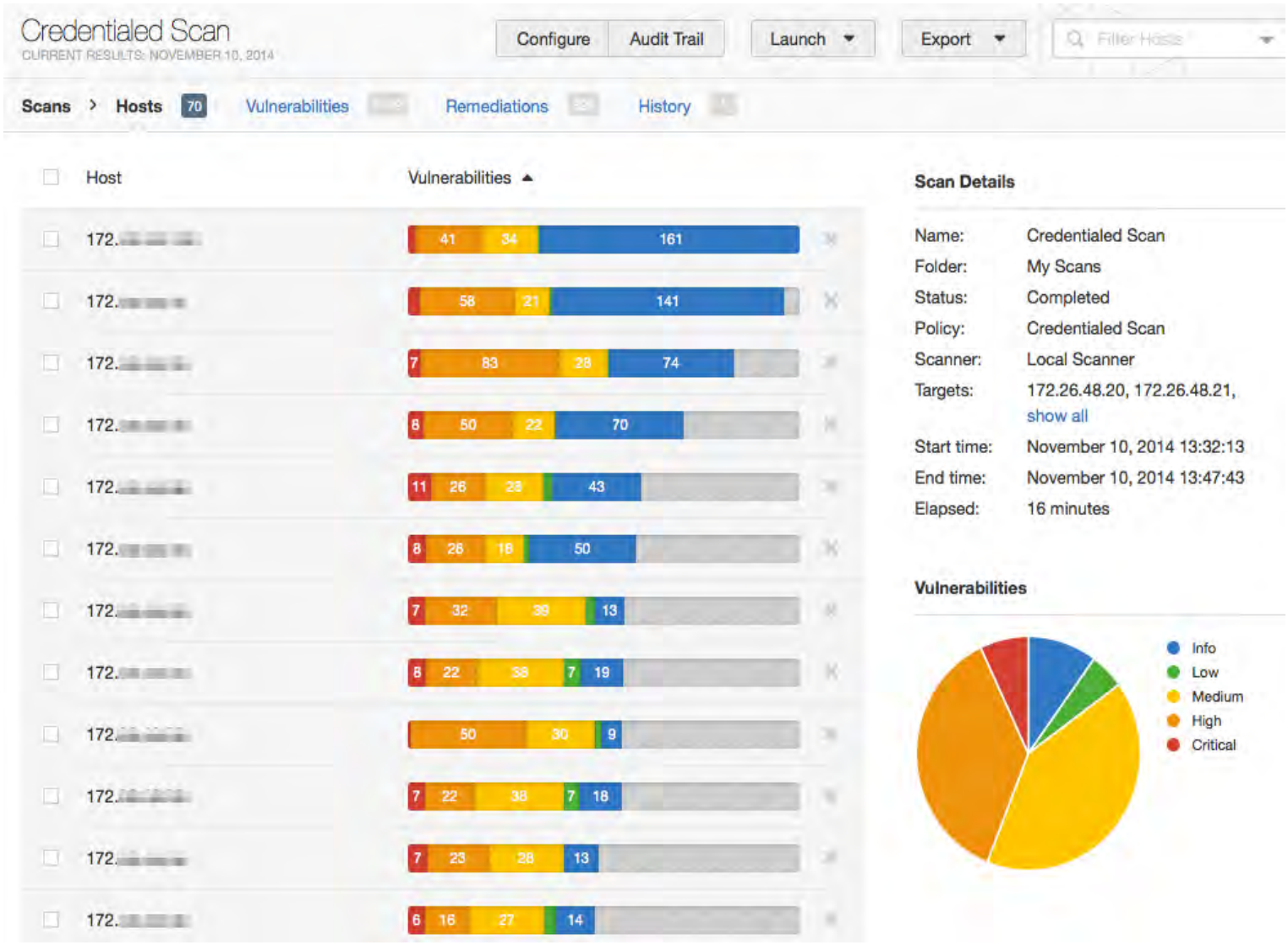
Nessus Agent 扫描结果导航和 Nessus 扫描器一样:



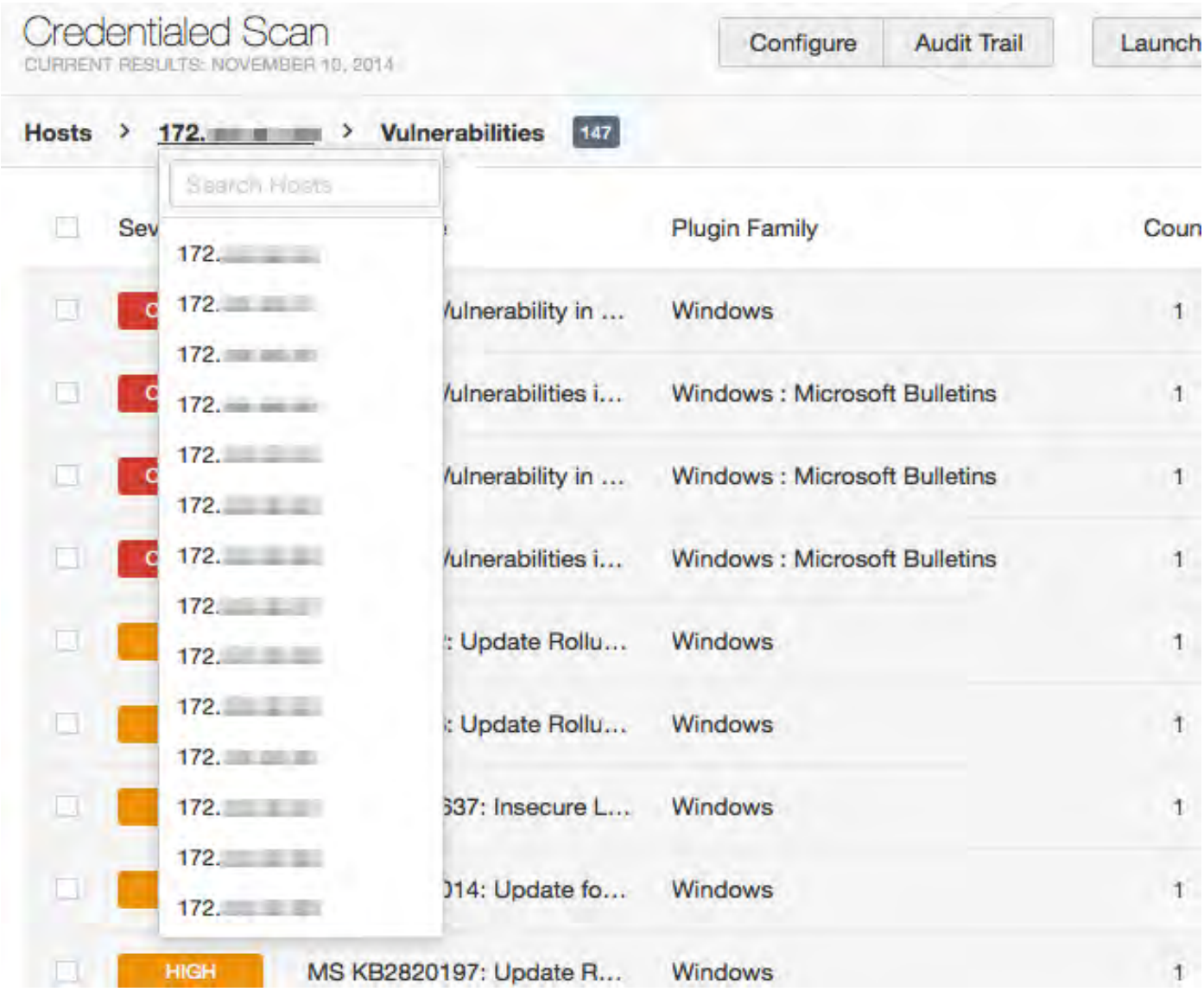
请注意,如果你超过许可通过扫描比分配主机,这一政策将会显示一个警告:



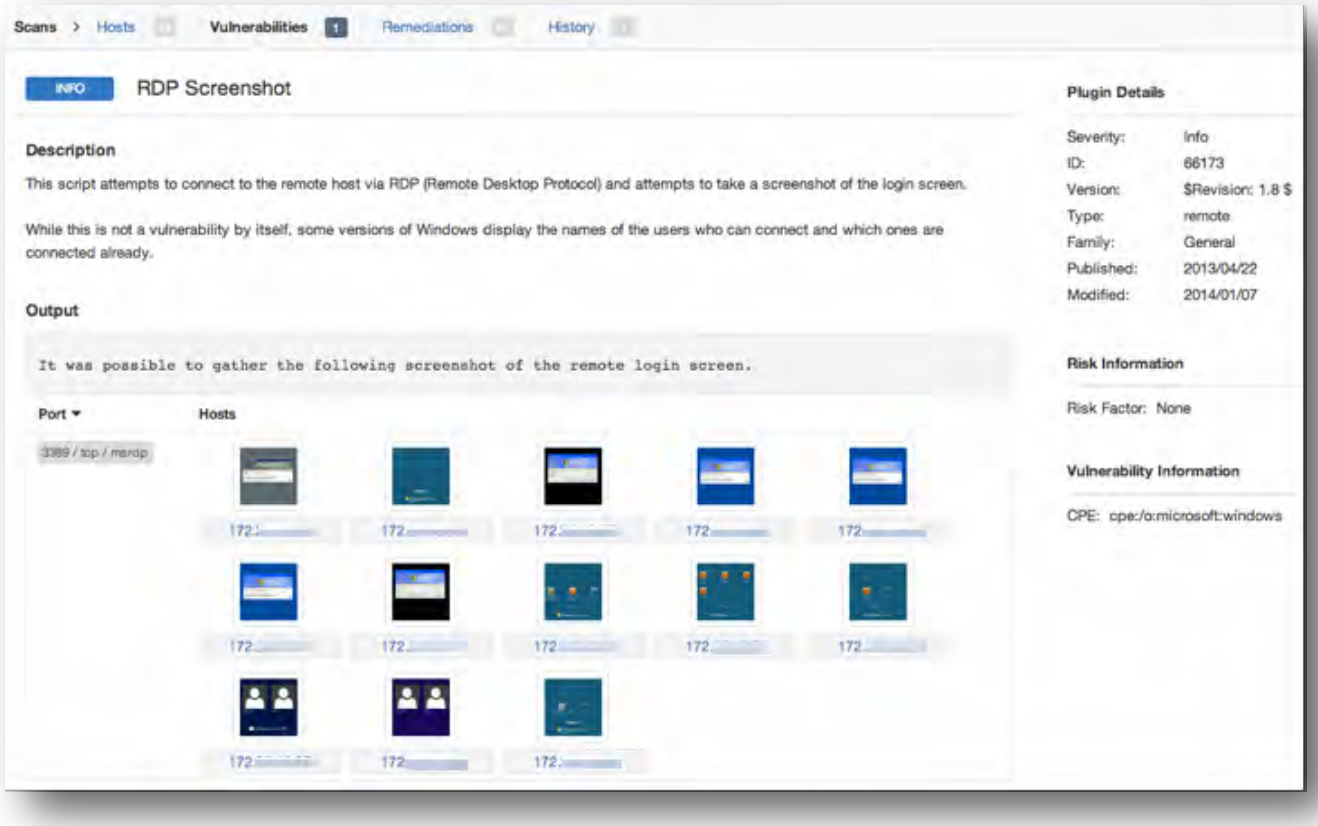
从“主机”查看每个概要总结将包含漏洞的细节或信息的发现以及主机的细节,提供一般信息一次主机扫描。如果选择“允许 Post-Scan 报告编辑”政策扫描主机可以通过选择从扫描结果中删除删除图标右边的主机详细信息。



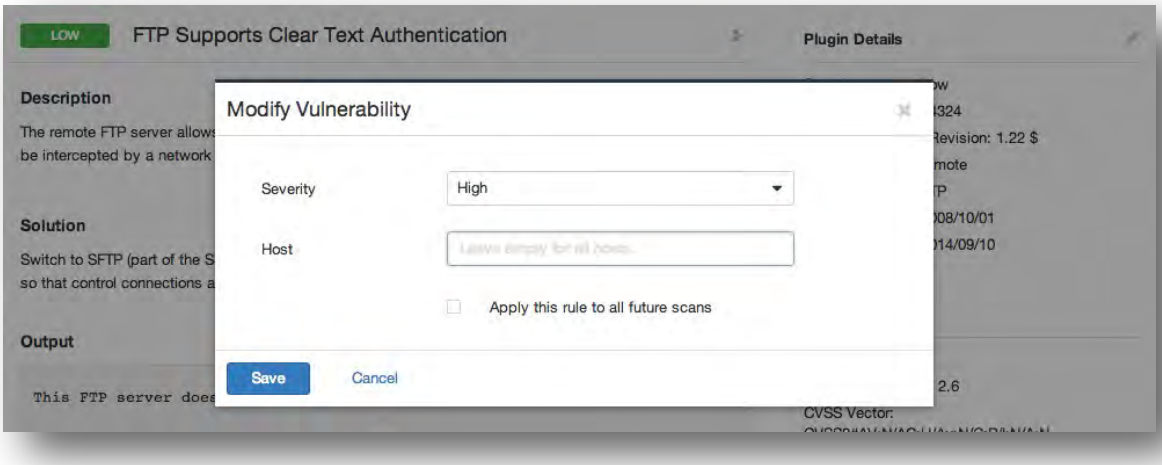
您已经选中后很快改变主机之间一个单击主机通过顶部的导航流来显示一个下拉菜单的其他主机。如果有许多主机一个搜索框可以快速主机位置:



点击一个漏洞通过“Hosts”或"Vlunerabilities”选项卡将显示漏洞信息包括一个描述,解决方案,引用,和任何可用的插件输出。插件的详细信息将显示在右边提供关于插件的附加信息和相关的脆弱性。从这个屏幕,笔图标右边的插件可以用来修改细节显示的脆弱性:

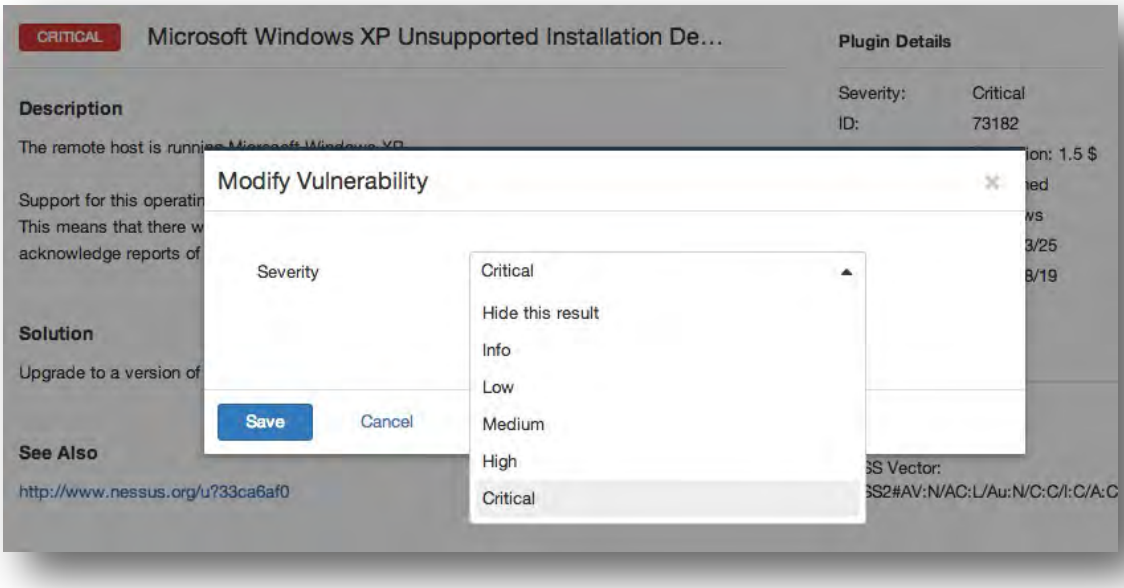


点击笔图标将显示一个对话框,如下所示:

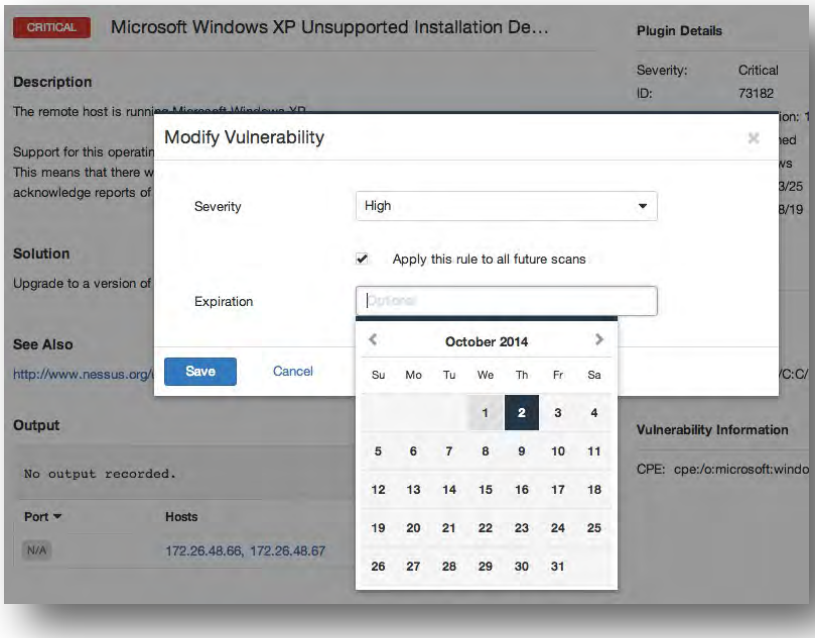


修改漏洞的主机输入对话只显示当你选择修改漏洞主机,而不是漏洞列表概述。

程度下拉菜单将使你分类的严重性等级权力漏洞问题,并把它藏的报告:



一旦更改,点击“保存”保存更改,应用它的脆弱性问题。此外,修改可应用于所有未来的报告通过单击选项。这样做会弹出一个对话框允许您设置一个可选的有效期修改规则:

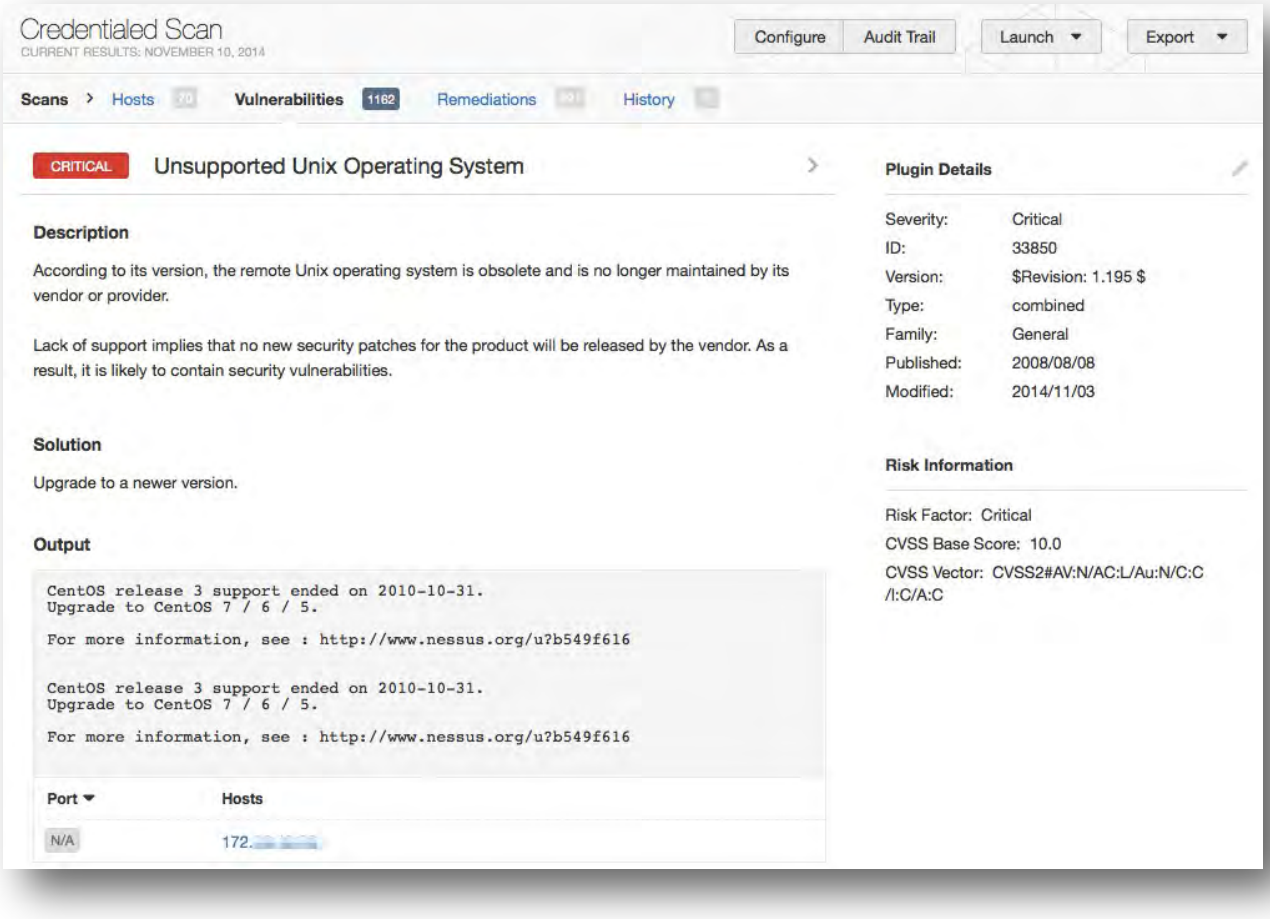


一个过期日期可以选择使用日历。在那个日期,指定的修改规则将不再适用于发现。

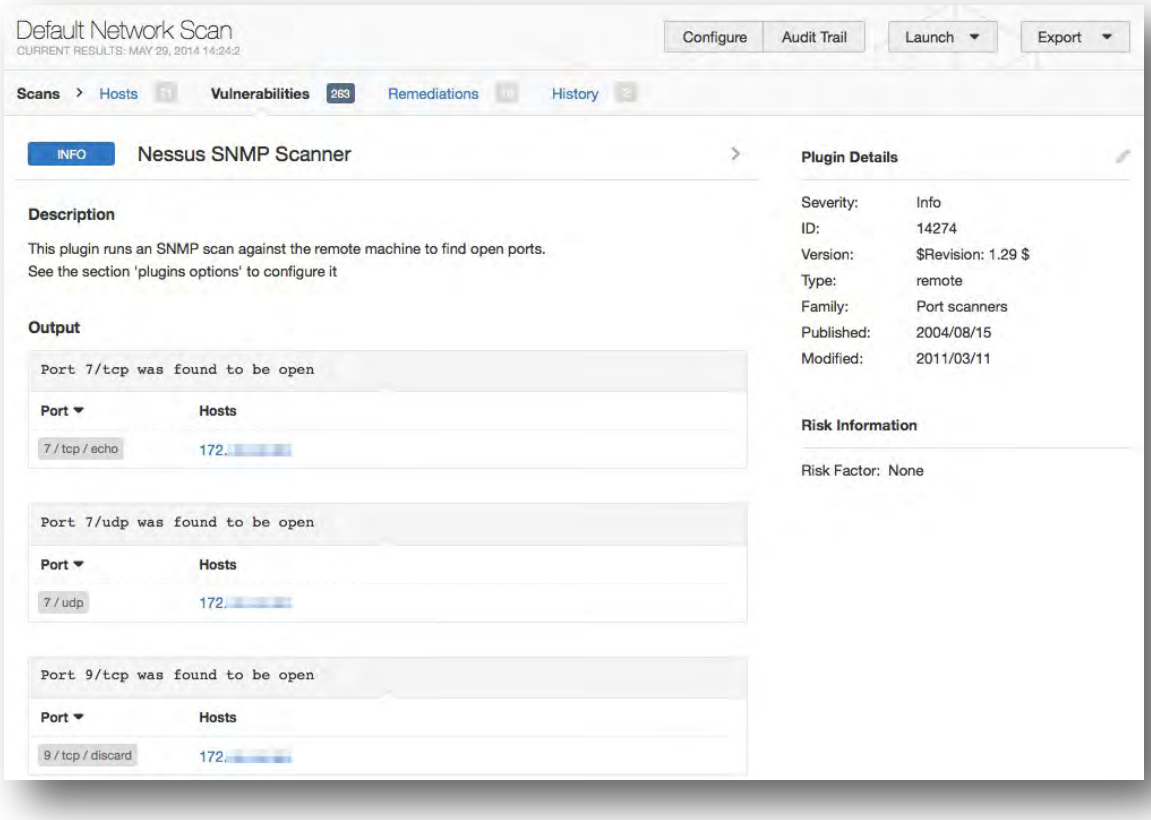
注意全局规则重铸插件风险/严重性可以在 Nessus 上建立在“用户配置文件”- >“插件规则”。

严重性评级来自相关的 CVSS 分数,0 是“信息”,不到 4 是“低”,不到 7 是“媒介”,不到 10 是“高”,将标记 CVSS 分数 10“至关重要的”。

选择顶部的“漏洞”选项卡将切换到漏洞的观点。这将通过漏洞而不是主机,对结果进行排序,包括主机的数量影响到右边。选择一个漏洞将提供相同的信息,但也包括影响主机底部的列表,连同相关的每个主机输出。



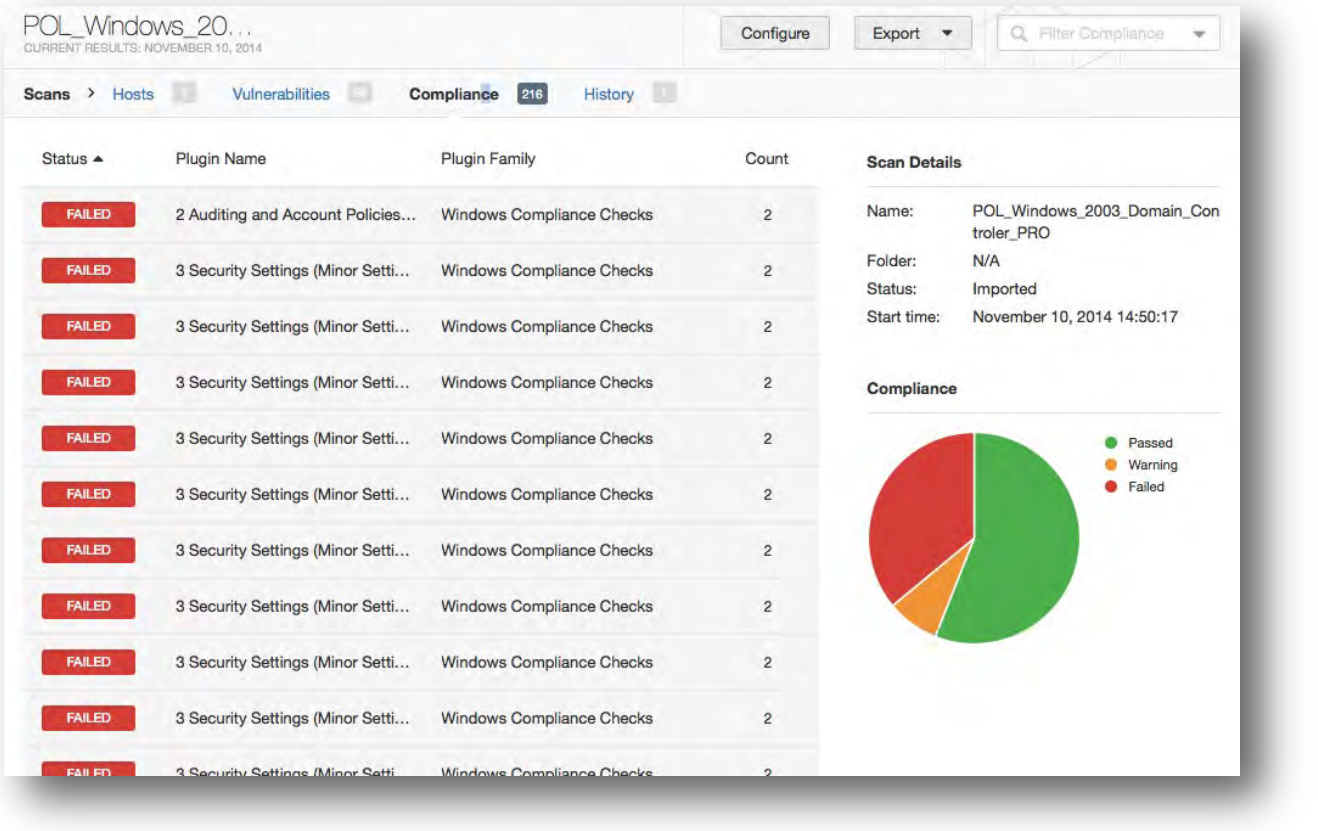
在这种情况下,一个主机有多个研究结果在不同的端口,将分解结果主机和端口的进一步分解:



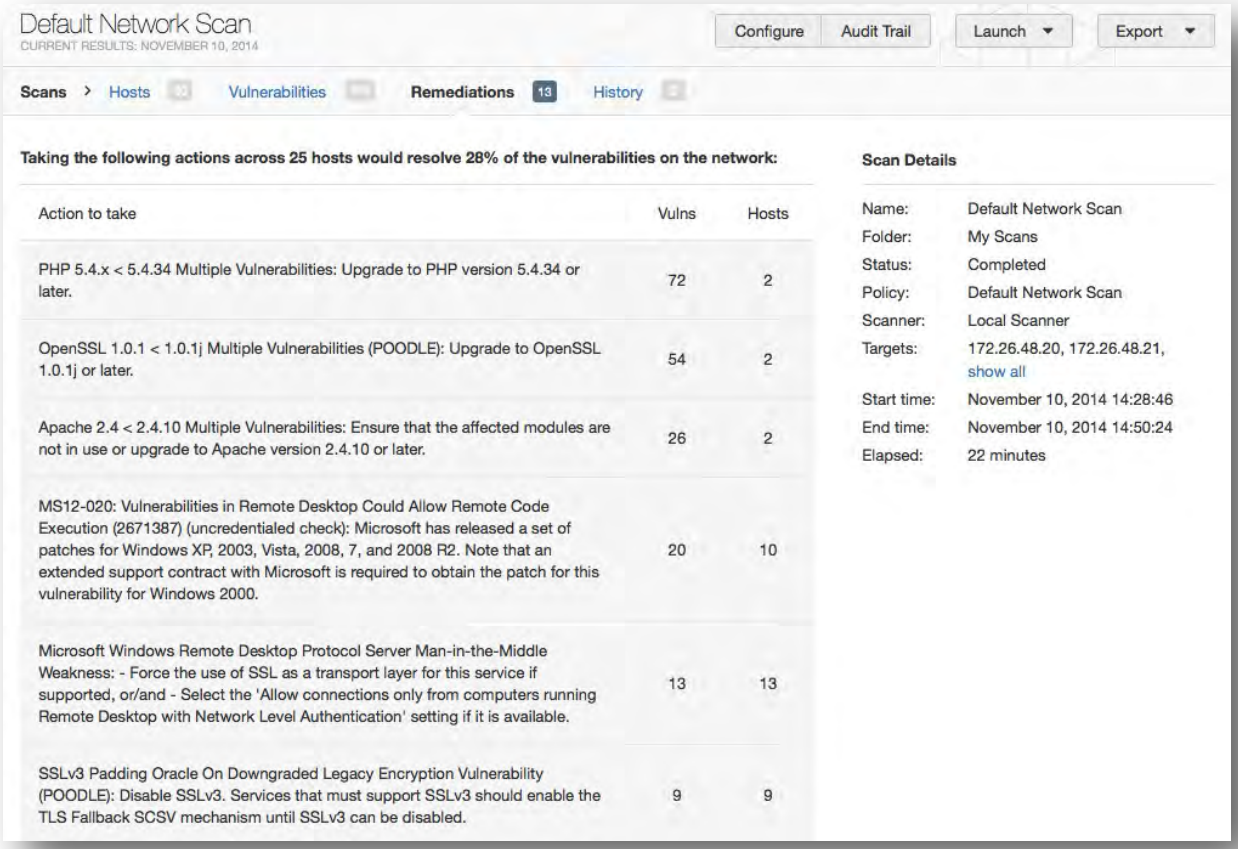
点击一个影响主机底部将加载基于主机的漏洞。

合规化结果

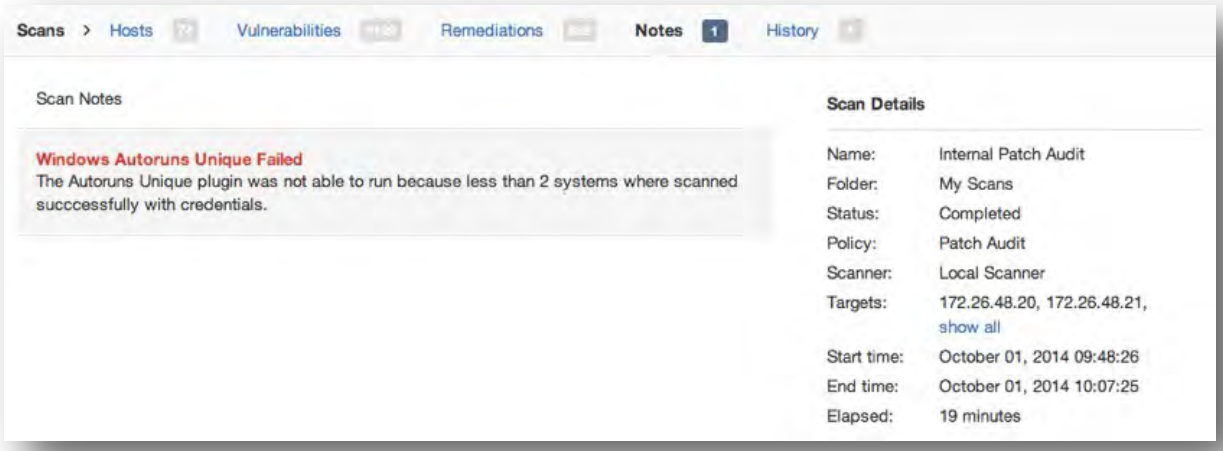
如果启动扫描,使用合规政策,结果会发现在一个单独的选项卡顶部称为“Compliance”:



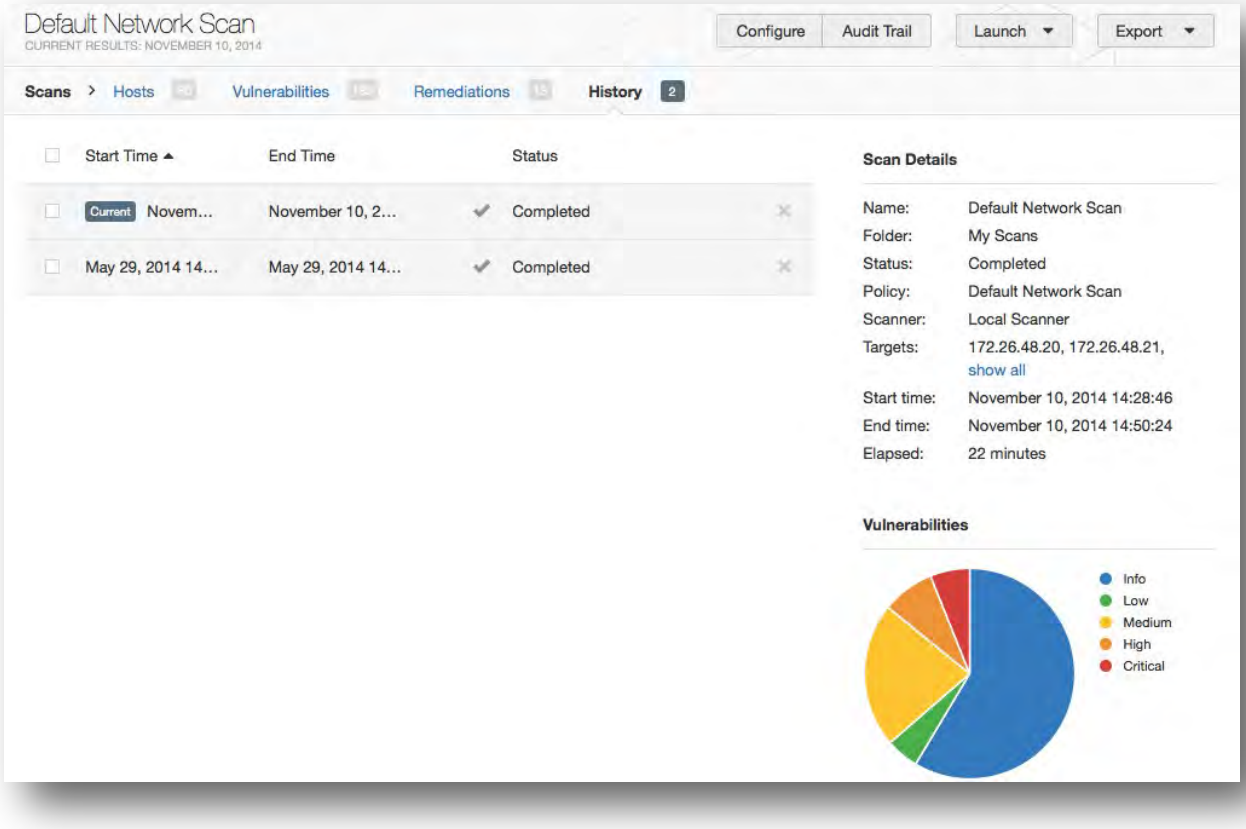
除了主机和漏洞标签、Nessus 提供了三个额外的标签。第一个是矫正补救选项卡提供摘要信息被发现的重大问题。这个建议的目的是为您提供最有效的缓解,将大大减少漏洞带来的风险:



第二个选项卡被称为笔记和提供建议来增强你的扫描结果或包含的警告:



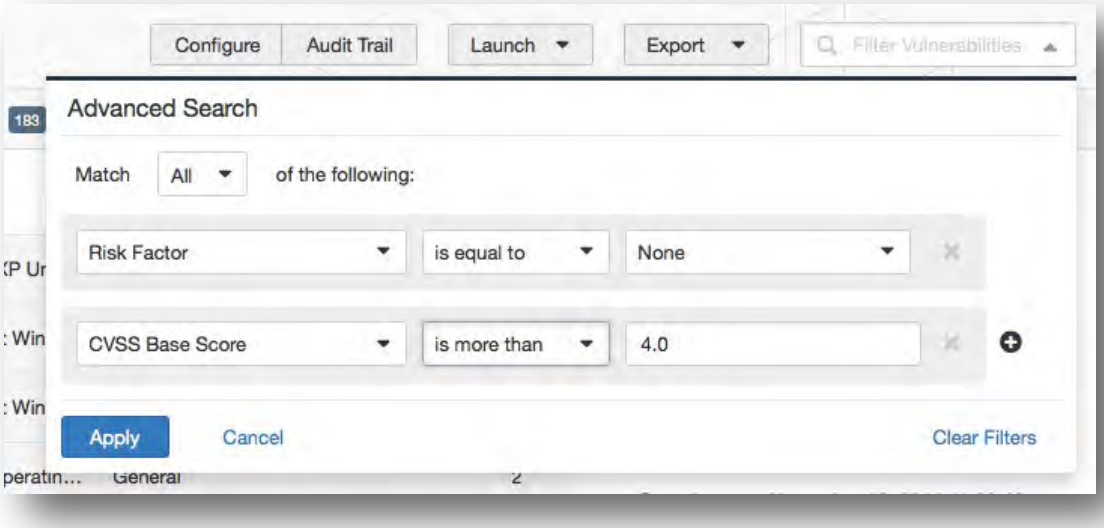
第三个选项卡是称为“History”,它显示了扫描和扫描列表的开始时间,结束时间,和地位。查看更早的扫描结果,选择列表中的扫描。“current”指示将更新显示您正在查看当前的扫描结果。



报表过滤器

Nessus 过滤器提供了一个灵活的系统协助显示特定的报告结果。过滤器可以用来显示结果基于漏洞的任何方面的发现。当使用多个过滤器,可以创建更详细的和定制的报告视图。

第一个过滤器类型是一个简单的文本字符串输入到“过滤漏洞”框右上角。在键入,Nessus 将立即开始筛选结果基于文本和标题的匹配结果。第二个过滤器类型是更全面,并允许您指定更多的细节。创建这种类型的滤波器,首先单击向下箭头右边的“过滤漏洞”框。可以从任何 report 选项卡创建过滤器。可以创建多个过滤器与逻辑,允许复杂的过滤。一个过滤器是通过选择插件创建的属性,一个过滤器参数,和一个值来过滤。当选择多个过滤器时,指定相应的关键字“任何”或“所有”。如果选择“所有”,则只匹配所有过滤器将显示结果:



一旦设置了一个过滤器,它可以单独通过点击右边的 X 删除。此外,可以在同一时间删除所有过滤器通过选择“Clear Filters”。报告过滤器允许各种各样的细粒度的控制标准的结果。以下过滤器属性将出现如果发现扫描结果。如果一个属性不存在的扫描结果,Nessus 会为了方便从过滤器抑制过滤器:

选项	描述
Plugin ID	筛选结果，如果插件 ID"等于"、"不等于"、"包含"不包含"给定的字符串 （eg. 42111）。
Plugin Description	筛选结果，如果插件描述"包含"不包含"一个给定的字符串 （eg."远程"）。
Plugin Name	筛选结果，如果插件名称"等于"，”不等于"，”包含“，或“不包含“给定字符。（eg.“Windows”）
Plugin Family	筛选结果，如果插件名称"等于"不等于"指定 Nessus 插件家族之一。通过下拉菜单中提供了可能的匹配项。
Plugin Output	筛选结果，如果插件描述"等于"、"不等于"、"包含"不包含"给定的字符串 （eg. "PHP"）
Plugin Type	筛选结果，如果插件类型"等于"不等于"两种类型的插件之一： 本地或远程。
Solution	筛选结果，如果插件解决方案"包含"不包含"一个给定的字符串 （如"升级"）。
Synopsis	筛选结果，如果插件解决方案"包含"不包含"给定的字符串 （eg."PHP"）。
Hostname	筛选结果，如果主机"等于"、"不等于"、"包含"不包含"一个给定的字符串 （eg. "192.168"或"实验室"）。
Port	筛选结果，如果端口"等于"、"不等于"、"包含"或"不包含"给定的字符串 （eg. "80"）。

Protocol	筛选结果，如果协议“等于”或“不等于”一个给定的字符串(e.g., “http”).
CPE	筛选结果，如果通用平台枚举(CPE)“等于”、“不等于”、“包含”或“不包含”一个给定的字符串(e.g., “Solaris”).
CVSS Base Score	筛选结果，如果 CVSS 基础分数“不足”，“大于”、“等于”、“不等于”、“包含”或“不包含”一个字符串 (e.g., “5”). 这个过滤器可以用于选择风险水平。严重性评级来自相关的 CVSS 分数,0 是“信息”,不到 4 是“低”,不到 7 是“媒介”,不到 10 是“高”,将标记 CVSS 分数 10“至关重要的”。
CVSS Temporal Score	筛选结果，如果 CVSS temporal score “小于”、“大于”、“等于”、“不等于”、“包含”或“不包含”一个字符串 (e.g., “3.3”).
CVSS Temporal Vector	筛选结果，如果 CVSS temporal vector “等于”、“不等于”、“包含”或“不包含”给定字符串(e.g., “E:F”).
CVSS Vector	筛选结果，如果 CVSS vector “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “AV:N”).
Vulnerability Publication Date	筛选结果，如果漏洞出版日期“早于”,“迟于”,“在”、“不在”、“包含”或“不包含”一个字符串 (e.g., “01/01/2012”). 注:按下按钮旁边的日期将弹出日期选择日历界面容易得多。
Patch Publication Date	筛选结果，如果漏洞补丁发布日期“小于”、“大于”、“等于”、“不等于”、“包含”或“不包含”一个字符串 (e.g., “12/01/2011”).
Plugin Publication Date	筛选结果，如果 Nessus 插件发布日期 “小于”、“大于”、“等于”、“不等于”、“包含”或“不包含”一个字符串 (e.g., “06/03/2011”).
Plugin Modification Date	筛选结果，如果 Nessus 插件修改日期 “小于”、“大于”、“等于”、“不等于”、“包含”或“不包含”一个字符串 (e.g., “02/14/2010”).
CVE	筛选结果，如果 CVE reference “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “2011-0123”).
Bugtraq ID	筛选结果，如果 Bugtraq ID “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “51300”).
CERT Advisory ID	筛选结果，如果 CERT Advisory ID (现称为 Technical Cyber Security Alert) “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “TA12-
OSVDB ID	筛选结果，如果 Open Source Vulnerability Database (OSVDB) ID “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “78300”).
Secunia ID	筛选结果，如果 Secunia ID “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “47650”).
Exploit Database ID	筛选结果，如果 Exploit Database ID (EBD-ID) 参考 “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “18380”).
Metasploit Name	筛选结果，如果 Metasploit name “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “xslt_password_reset”).

Exploited by Malware	筛选结果，如果一个漏洞的存在是利用恶意软件”等于“或”不等于“真或假。
IAVA	筛选结果，如果 IAVA 引用“等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., 2012-A-0008).
IAVB	筛选结果，如果 IAVB 引用“等于”、“不等于”、“包含”或“不包含”一个给定的字符串 (e.g., 2012-A-0008).
IAVM Severity	基于 IAVM 严重性级别过滤结果(e.g., IV).
IAVT	筛选结果，如果 IAVT 引用“等于”、“不等于”、“包含”或“不包含”一个给定的字符串 (e.g., 2012-A-0008).
See Also	筛选结果，如果 Nessus 插件“也看到”参考 “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “seclists.org”).
Risk Factor	过滤结果基于漏洞的风险因素(e.g., Low, Medium, High, Critical).
Exploits Available	过滤结果基于已知的漏洞有公共利用。
Exploitability Ease	筛选结果，如果可利用性缓解“等于”或“不等于”以下值:“利用可用”，“不需要利用”,或“没有可用已知漏洞”.
Metasploit Exploit Framework	筛选结果，如果 Metasploit 利用框架中的一个漏洞的存在“等于”或“不等于”真或假。
CANVAS Exploit Framework	筛选结果，如果在画布上利用框架的存在“等于”或“不等于”真或假。
CANVAS Package	过滤结果基于帆布包一个利用存在利用框架。选项包括油画、D2ExploitPack 或 White_Phosphorus。
CORE Exploit Framework	筛选结果，如果存在利用的核心开发框架“等于”或“不等于”真或假。
Elliot Exploit Framework	筛选结果，如果 Elliot 的开发利用框架的存在“等于”或“不等于”真或假。
Elliot Exploit Name	筛选结果，如果 Elliot 利用 “等于”、“不等于”、“包含”或“不包含”给定字符串 (e.g., “Typo3 FD”).
ExploitHub	筛选结果，如果 ExploitHub 网站上的利用的存在“等于”或“不等于”真或假。

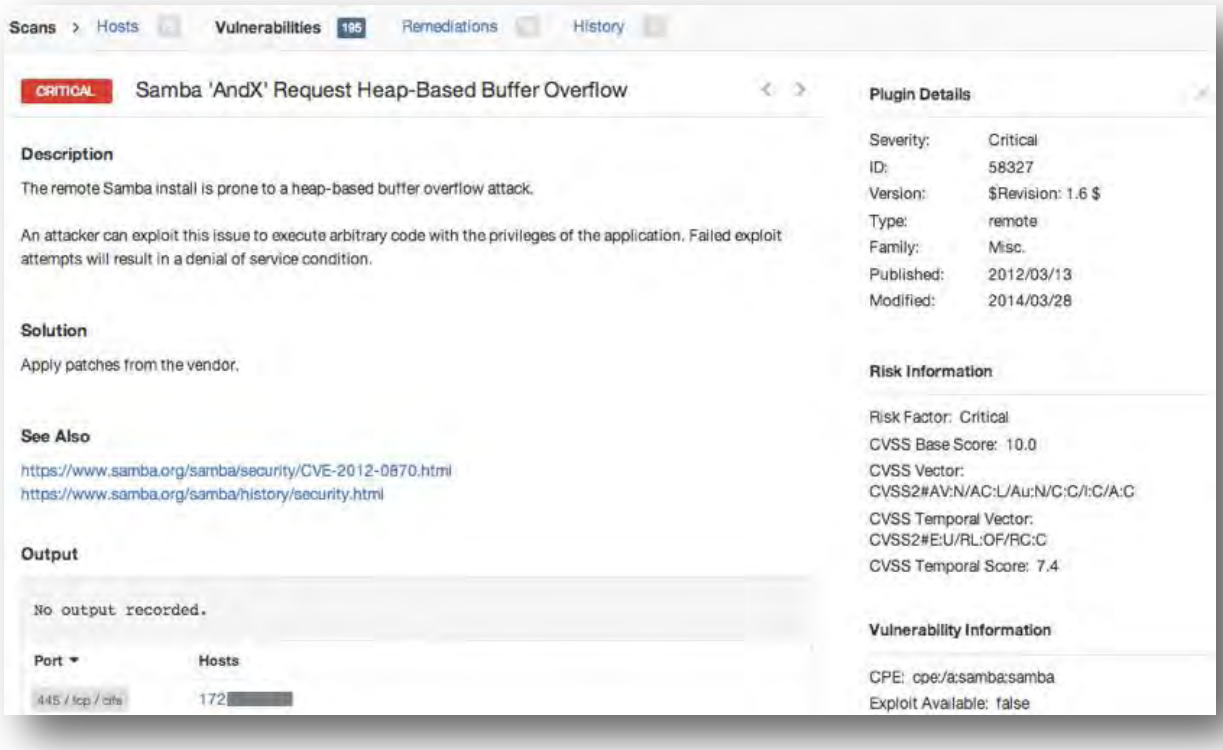
当使用一个过滤器,可以逗号分隔的字符串或数值来过滤基于多个字符串。例如,过滤结果只显示 web 服务器,您可以创建一个过滤器“港口”,选择“等于”,输入“80443、8000、8080”。这将向您展示的结果与这四个港口。

筛选标准是不区分大小写的
如果一个过滤器选项不可用,这意味着符合标准的报告包含什么。例如,如果“微软公报”不是过滤器下拉列表中,则没有发现漏洞,参考微软的公告。

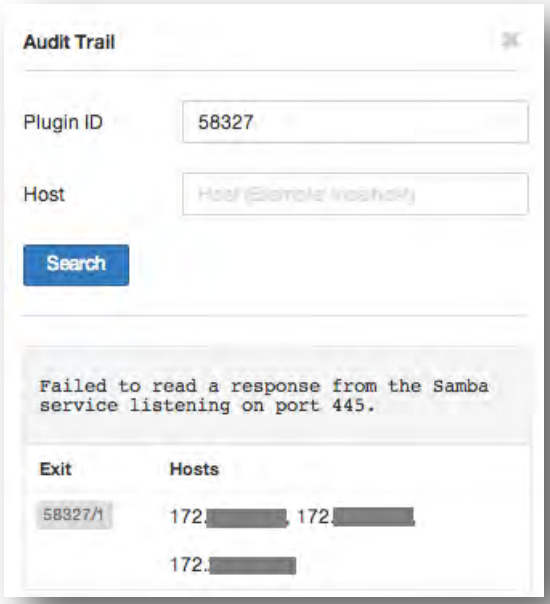
创建一个过滤器,扫描结果将被更新以反映新的过滤条件后选择“Apply”。“Filter Vulnerabilities”框中的向下箭头将会改变多少的数值表示过滤器目前正在应用。

一旦结果被过滤提供你想要的数据集,点击“Export Results“出口过滤的结果。收到一份报告的结果,删除所有过滤器和使用导出功能。

Nessus 扫描结果提供一个简洁的插件列表,在主机检测到的问题。但是,有些时候,您可能想知道为什么一个插件没有返回结果。“Audit Trail”功能将提供这一信息。首先点击位于上部右边的“Audit Trail”:



这将弹出审计跟踪对话框。首先进入的 ID 插件你想知道更多有关。点击“Search”和一个主机或主机列表将显示与查询。可选地,您可以提供一个主机 IP 初始查询结果限制到一个感兴趣的目标。一旦主机显示,点击一个显示信息插件显示未被出发的原因:

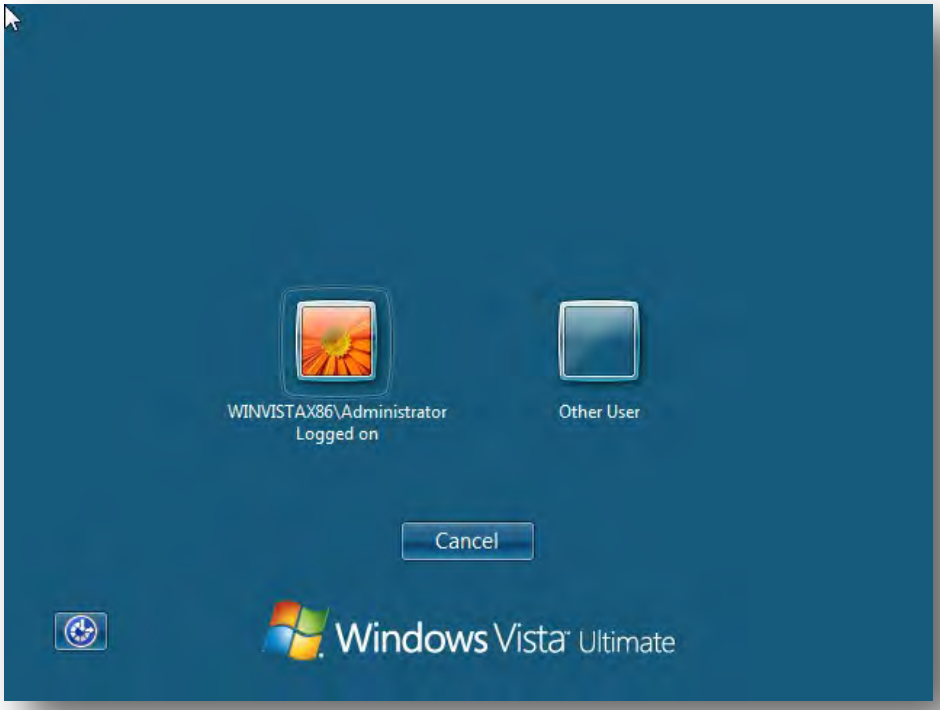


由于审计跟踪所需的资源,在某些情况下,只有部分将提供审计跟踪。一个扫描主机,完整的审计跟踪。如果扫描 2 和 512 台主机之间,一个完整的审计跟踪只有如果 Nessus 服务器超过 1 CPU 和 2 g 内存。扫描 512 多个主机总是会导致部分审计跟踪。

审计跟踪仅用于扫描是在主机上。它不会对进口扫描。

报表快照

Nessus 中也有能力采取截图漏洞扫描,并将它们包括在一份报告中。例如,如果 Nessus 发现运行 VNC 密码来限制访问,将采取截图显示会话和包含在报告中。在下面的示例中,发现了一个 VNC 的登录屏幕显示管理员登录系统:

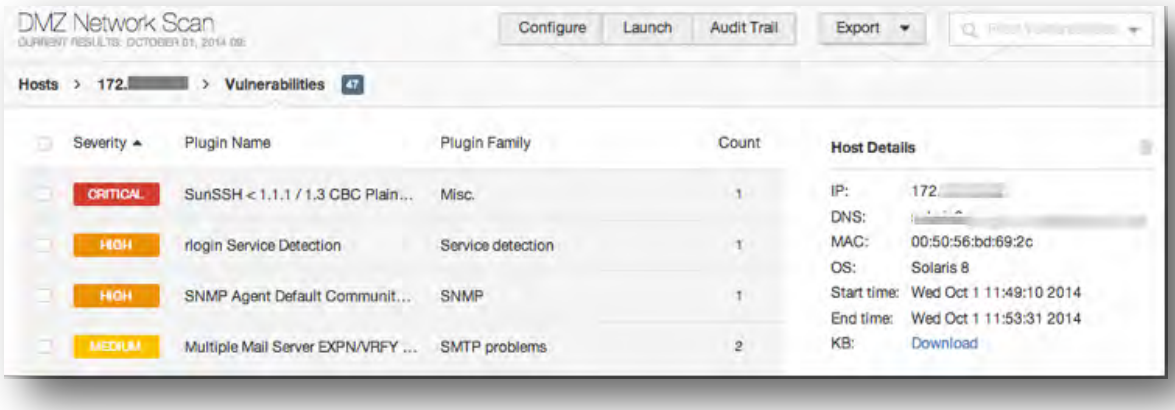


必须启用这个特性的“扫描 Web 应用程序”部分扫描策略,在“一般”。

知识库扫描

知识库(KB)保存每一次扫描完成。这是一个 ASCII 文本文件,其中包含一个日志信息相关的扫描,结果发现执行。KB 通常是有用的在你需要支持成立的情况,因为它允许支持人员理解 Nessus 做什么,和什么信息被发现。

下载 KB,选择一份报告,然后一个特定的主机。右边的主机名或 IP 有链接标题为“Host Details”。点击这个,主机详细信息之一是“KB”“现在”链接:

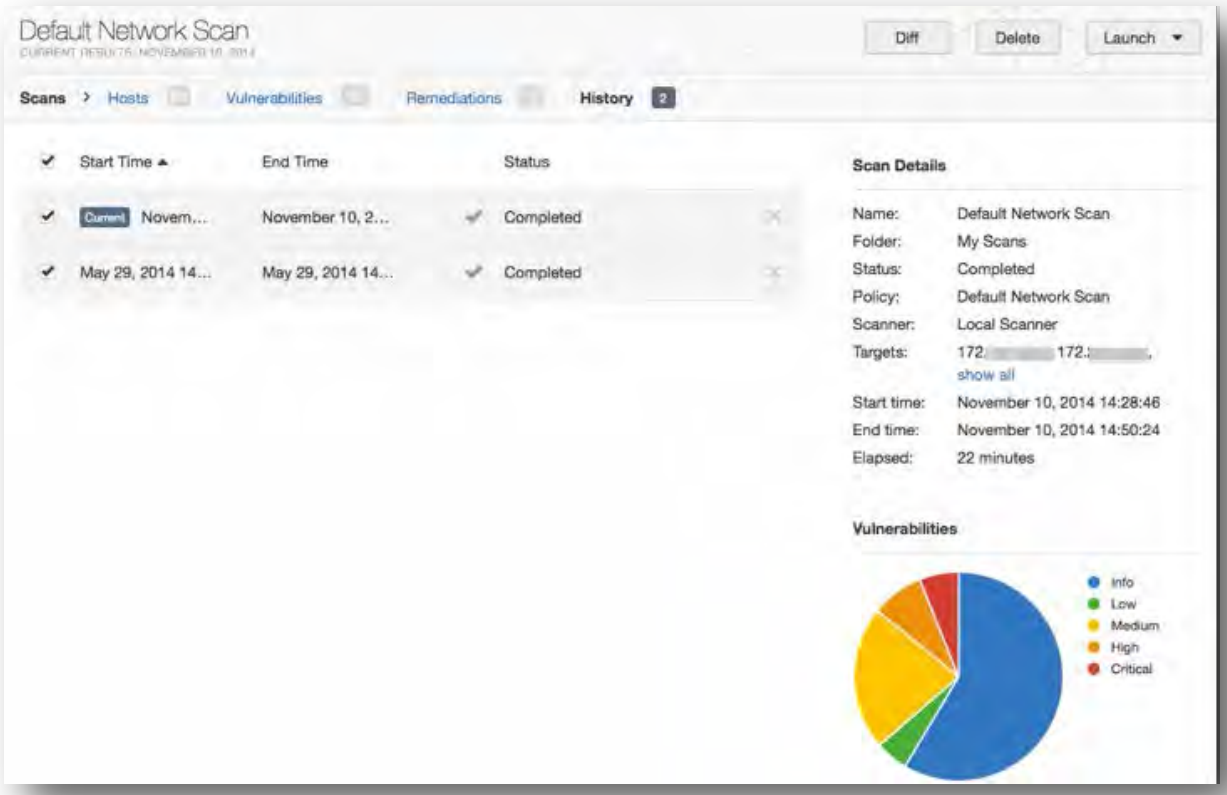


只扫描主机上执行相关的知识库。进口扫描不带知识库。

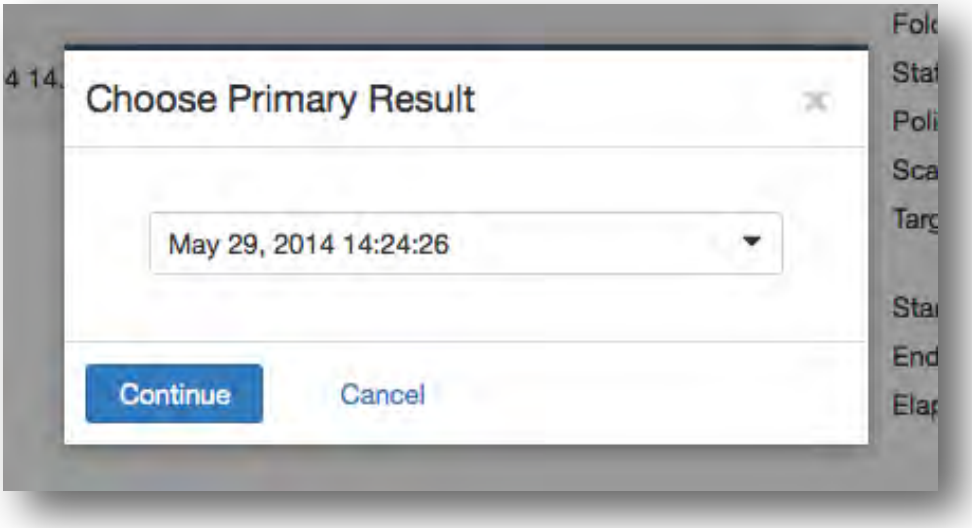
结果比对 (Diff)

Nessus,互相可以比较两个扫描报告显示任何差异。显示扫描的能力差异有助于指出一个给定的系统或网络如何改变随着时间的推移。这有助于在合规分析通过展示漏洞被矫正,如果发现系统漏洞发布新补丁,或者两个扫描可能不是针对相同的主机。

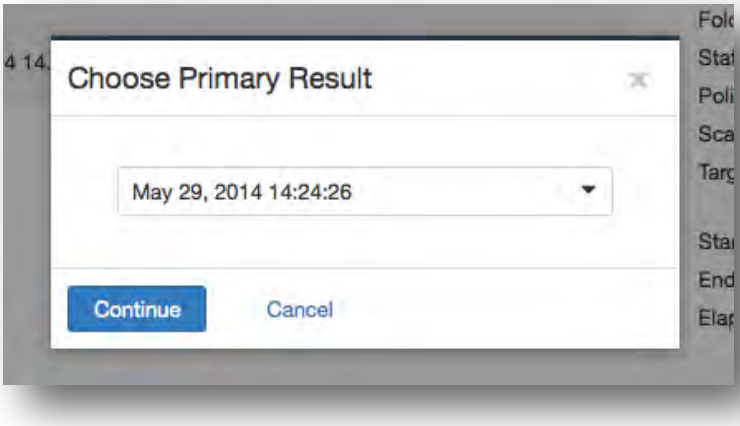
比较报告,首先从“Scans”选择扫描列表,点击“History”,检查报告你想比较,并选择右上角的“Diff”:



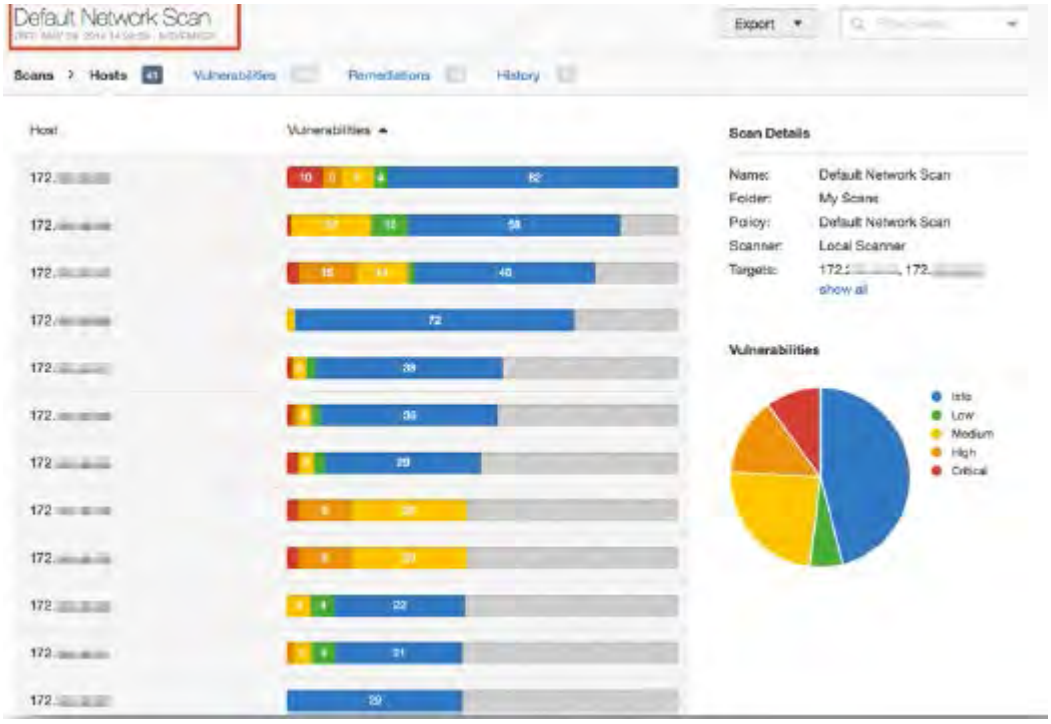
Nessus 将比较第一个报告选择第二个并产生一个结果列表,自第一个是不同的。比较功能自基线(即显示什么是新的。第一个报告选择),没有产生一个微分的两份报告。这种比较突出两个扫描中被发现或修复的漏洞。



在上面的示例中,“DMZ Network Scan”是一个未经身份验证的 DMZ 扫描,执行了几次。



报告结果会显示对比的差异结果并，并高亮显示漏洞信息 以下为没有发现 10 月 1 日扫描的差异报告。



报表管理

Nessus 提供多种方式来管理您的扫描报表.

报表的上传与导出

扫描结果可以从一个 Nessus 扫描器的扫描结果导出和导入到另一个 Nessus 扫描器中. 使用 “**Upload**” 和 “**Export**” 功能便捷的管理扫描任务，报表对比, 报表备份, 以及不同部门或组织的信息共享。.

用户可以通过该章节创建自己的报表: 主机信息汇总, 主机漏洞信息汇总, 修复建议, 漏洞库漏洞信息, 或者 合规性检查。默认为 HTML 格式. 如果扫描器所安装的主机安装了 JAVA, 用户可以导出 PDF 以及其他格式的报表，如： CSV, 或者 the Nessus DB.。通过使用报告过滤器和导出功能,用户可以自己选择创建动态报告。

Nessus DB 格式是一种专用的加密的文件格式。注意：NessusDB 文件包括所有可能的扫描数据,包括但不限于结果,审计跟踪信息以及其他附件信息.

导出扫描结果, 首先需要选择点击 “Scans” 界面. 进入下一个扫描界面, 然后点击 “Export” 下拉选项,选择你所需要的报表文件格式。

只有执行合规扫描，Nessus 可以导出 PDF 或 HTML 格式的合规扫描的信息. 从以前版本的导入的扫描 Nessus 不会以这种方式导出

可以下载以下几个格式的报告。注意：一些格式不允许章节的选择及所有的信息.

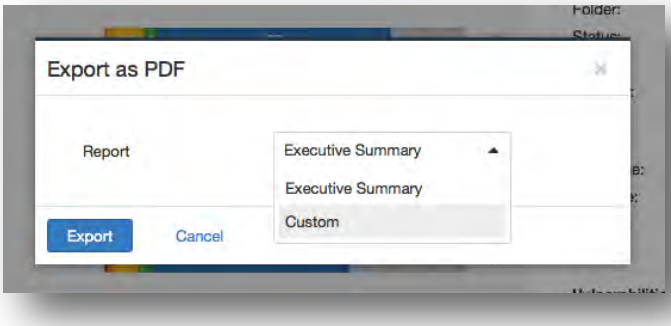
选项	描述
.nessus	基于 xml 的格式和 Nessus 4.2 及以后的实际标准。这种格式使用一组扩展的 XML 标记提取和解析信息更细粒度的。这种报告不允许选择章节.
Nessus DB	专有加密数据库格式用于 Nessus 5.2 及以后版本。其中包含一个扫描中的所有信息描述,包括审计跟踪和结果。当导出这种格式时,系统将提示您输入密码加密扫描的结果。.
HTML	使用标准的 HTML 生成的一份报告,允许选择章节。这份报告将在浏览器中使用一个新标签打开。
PDF	生成 PDF 格式的报告,允许选择章。根据报告的大小,PDF 生成可能需要花费几分钟的时间. Oracle Java (以前 SUN 公司的 Java) 是基于 Unix 的系统上所需的 PDF 报告功能.
CSV	逗号分隔值(CSV)导出,可以用来导入外部程序数据库、电子表格等。这份报告不允许选择章节。

然后选择一个报表的格式, 标准的浏览器将显示“**Save File**”, 根据你的选择将扫描结果保存在本地主机上。

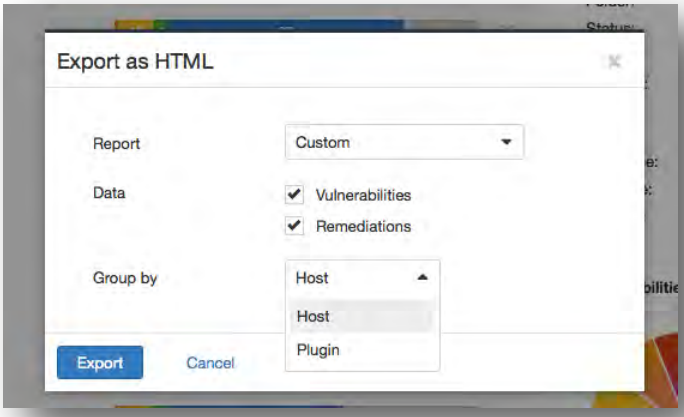
HTML and PDF 定制

HTML 和 PDF 格式, 当你选择 **Executive Summary** 或 **Custom**，Nessus 将显示一个下拉框。

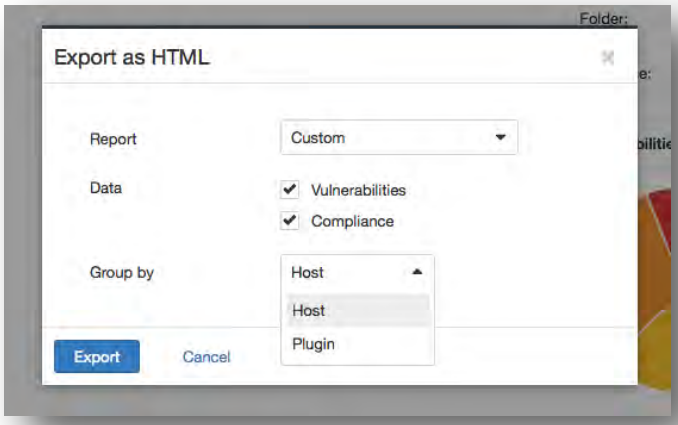
:



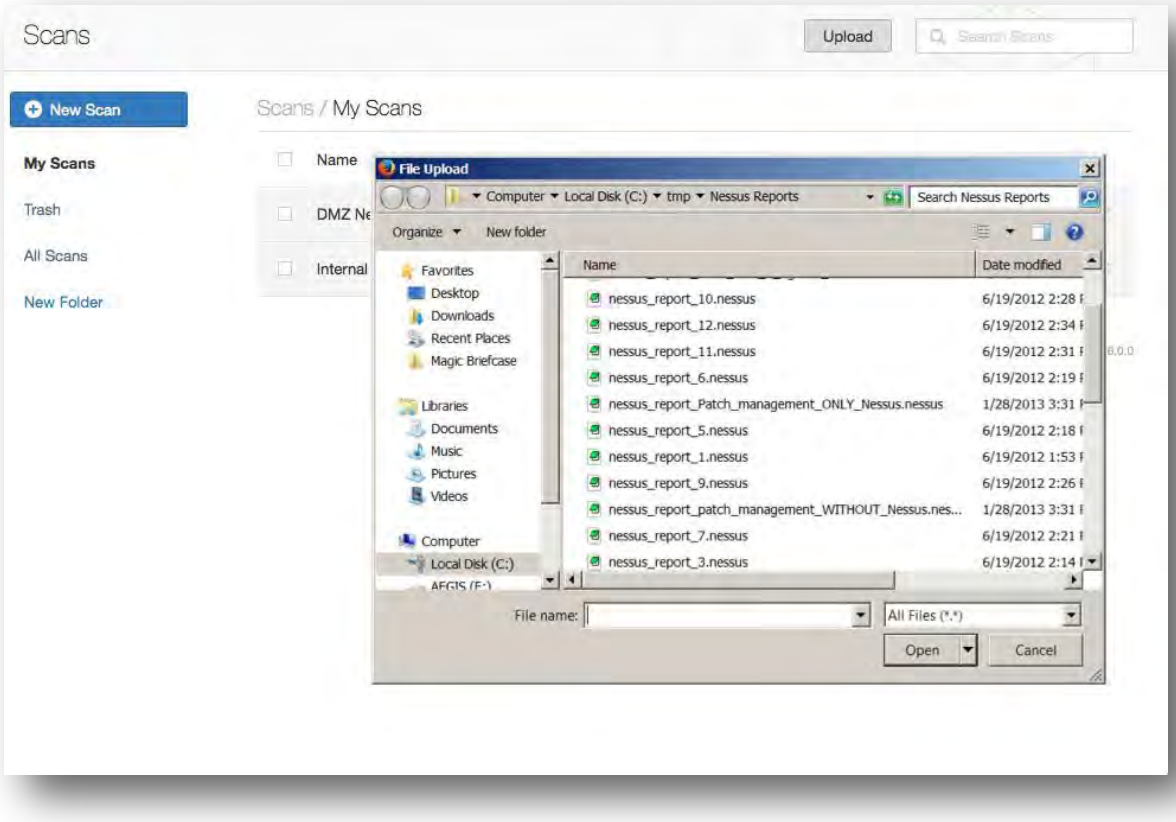
在用户订制中，通过下拉菜单指定需要在报表中包含的信息. 里面包含了漏洞信息、漏洞修复建议以及这些信息如何分组排序(根据主机或者根据漏洞):



注意：合规性扫描报告导出操作在 custom 报表有所不同：



导入报表, 点击“**Upload**” 按钮，在 “**Scans**”页面中的上方，将打开一个新的标签:



选择需要导入的 .nessus 扫描文件，然后点击 “Open”. Nessus 将解析文件信息并将漏洞信息展现在 “Scans” 界面中.

Nessus 文件格式

Nessus 使用两种特有的文件格式 (.nessus and .db) 由于扫描结果的导入和导出. **.nessus** 格式的文件有以下几种特点:

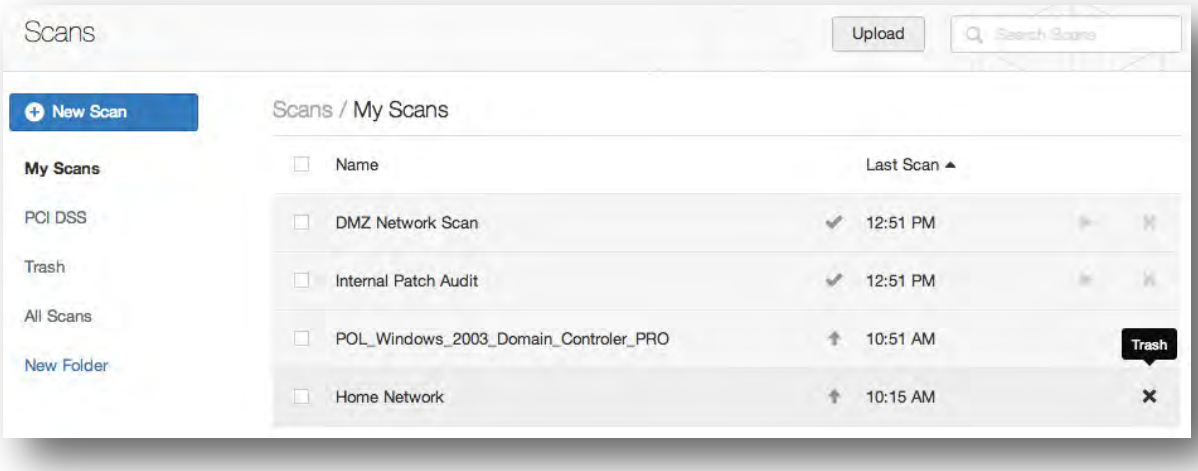
- 基于 XML,向前与向后的兼容,以及更容易的编辑性和实用性.
- 信息完整性:单独的一个 **.nessus** 文件包含了扫描目标的列表,用户定义的策略,以及扫描结果.
- 安全性: 文件中不保存任何密码信息. 而是, 一个密码的参考信息存储在本地主机上的一个安全的位置。

要创建一个包含了目标、策略和扫描结果.nessus 的文件，先创建一个策略并保存它. 再创建目标地址列表,最后执行扫描. 一旦扫描任务完成, 所有信息将通过“Scans”结果中，使用“Export”选项来保存在 .nessus 文件中. 更多**.nessus 文件**信息请参考 “Nessus v2 File Format” 文档 。

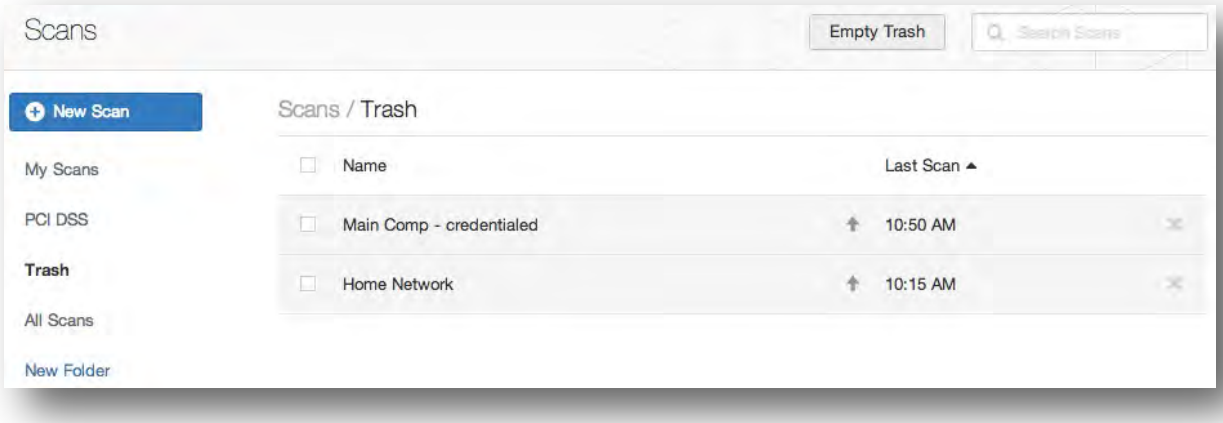
Nessus DB 格式 (.db)文件 包含了所有的扫描数据，并进行了加密。唯一可查看文件的方式是在上传报表时输入正确的密码。.

删除扫描结果

一旦完成了扫描结果, 你可以在有边的选项中点击 “X”将扫描结果移至“Trash”：



选择 “Trash” 文件夹,你可以永久删除扫描结果:



一旦删除将无法恢复！在删除之前使用“**Export**” 导出你的扫描结果.

PCI ASV 认可的 Nessus 企业云

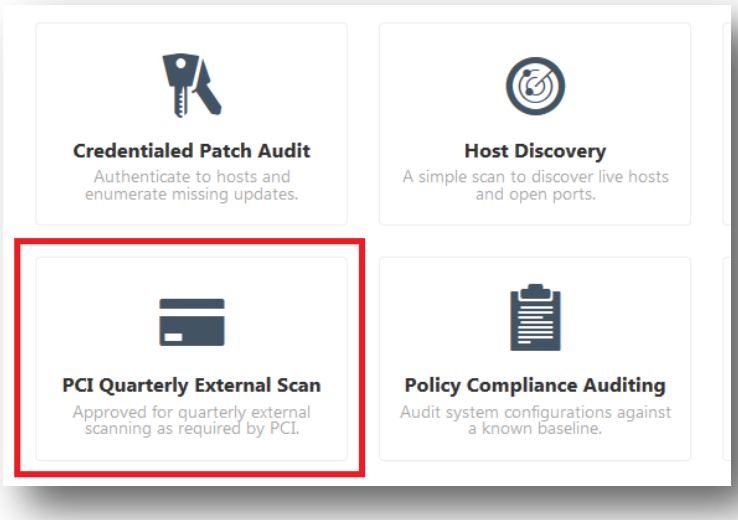
Tenable 网络安全公司是 PCI 认可的扫描提供商(ASV), 用于验证在 Internet 中的系统遵循 PCI 数据安全标准(PCI DSS)的某些方面的漏洞扫描. Nessus 企业云包括一个预构建静态的 PCI DSS 策略，PCI DSS v2.0 遵循每季度扫描一次的要求. 这些策略可能被商业应用 同时提供系统环境最初的基于 PCI DSS 需求的评估, 以及执行外部漏洞扫描并生成报告,验证是否合格。

Tenable 网络安全公司是 PCI DSS 认证及满足要求的的成员. 值得需要注意的是, 当客户需要经常使用 PCI DSS 扫描策略来检测他们的系统之前要提交验证信息到 Tenable，才会被认为是一次有效的 PCI ASV 扫描。允许客户将两个季度报告提交至 Tenable 网络安全公司。.

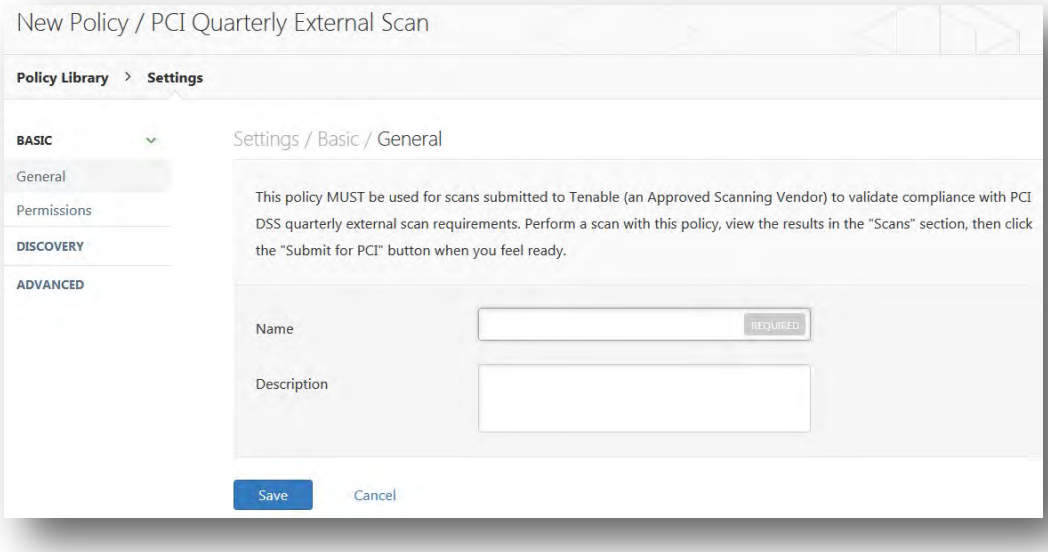
当登陆系统, 用户可以选择一个名称为 “PCI Quarterly External Scan” 的扫描策略，是满足 PCI ASV 大纲中 Guide v2.0 “ASV Scan Solution – 所需的组件”.

通过 Nessus 企业云验证系统是否符合 PCI DSS ASV,必须选择“PCI Quarterly External Scan”的扫描政策。

创建一个 PCI DSS ASV 扫描策略, 选择 “**Policies**” 然后点击 “**+ New Policy**”. 接下来, 点击“**PCI Quarterly External Scan**”:

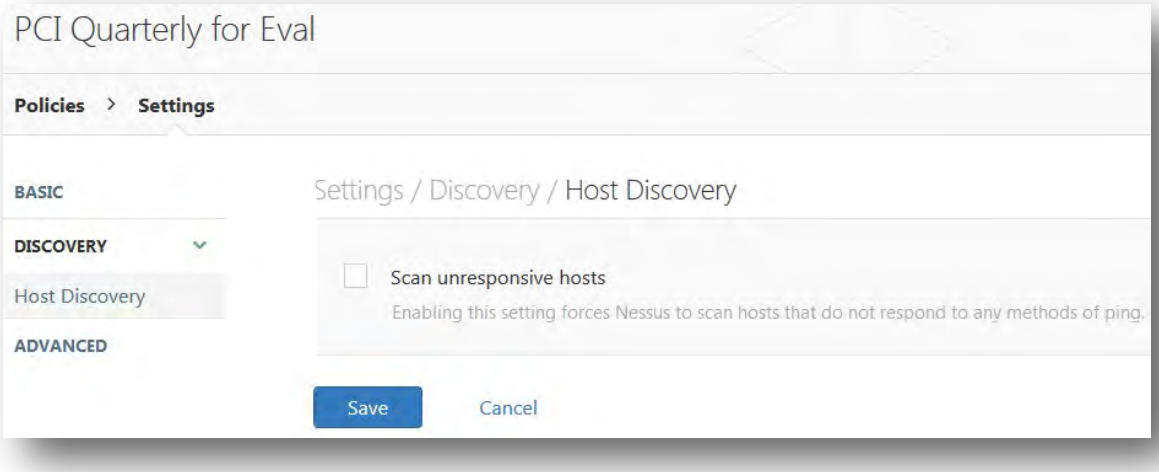


首先, 为你的 PCI 扫描输入名称和描述:

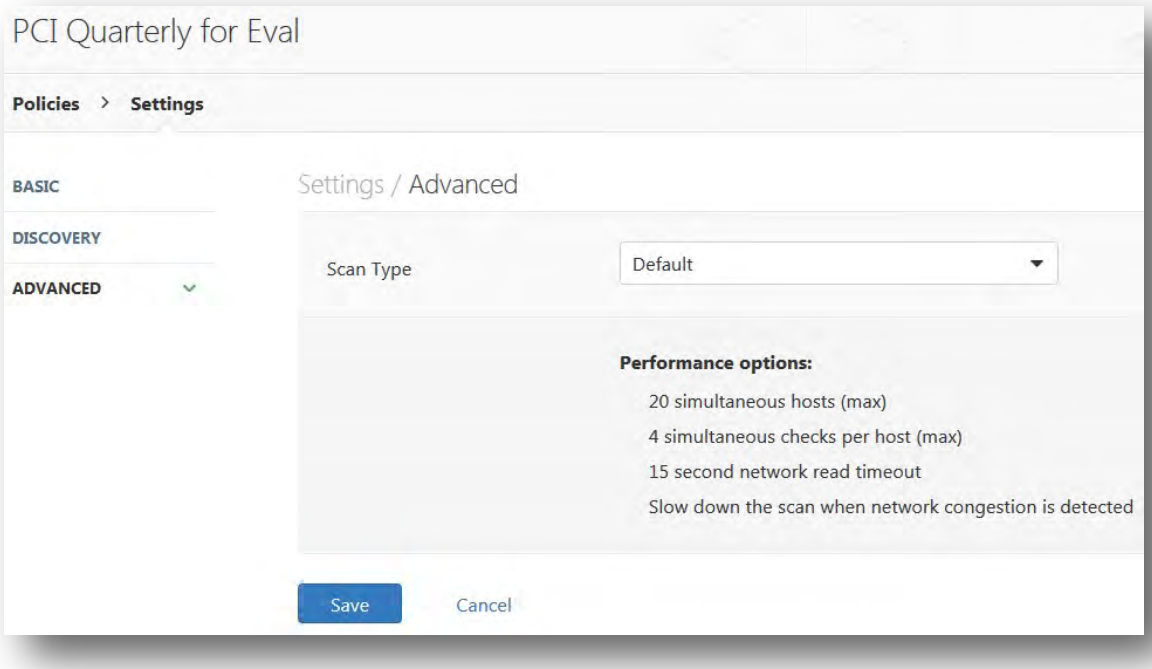


默认的扫描策略，已经配置专门为 PCI 遵从性扫描测试. 你可以根据需要配置一些额外的选项.

在 **Policies** 界面中, 选择你刚才创建的策略. **Discovery** 选项下面, 你可以选择 “Scan unresponsive hosts”:



在 **Advanced** 选项下面, 你可以对 “Scan Type”进行操作:

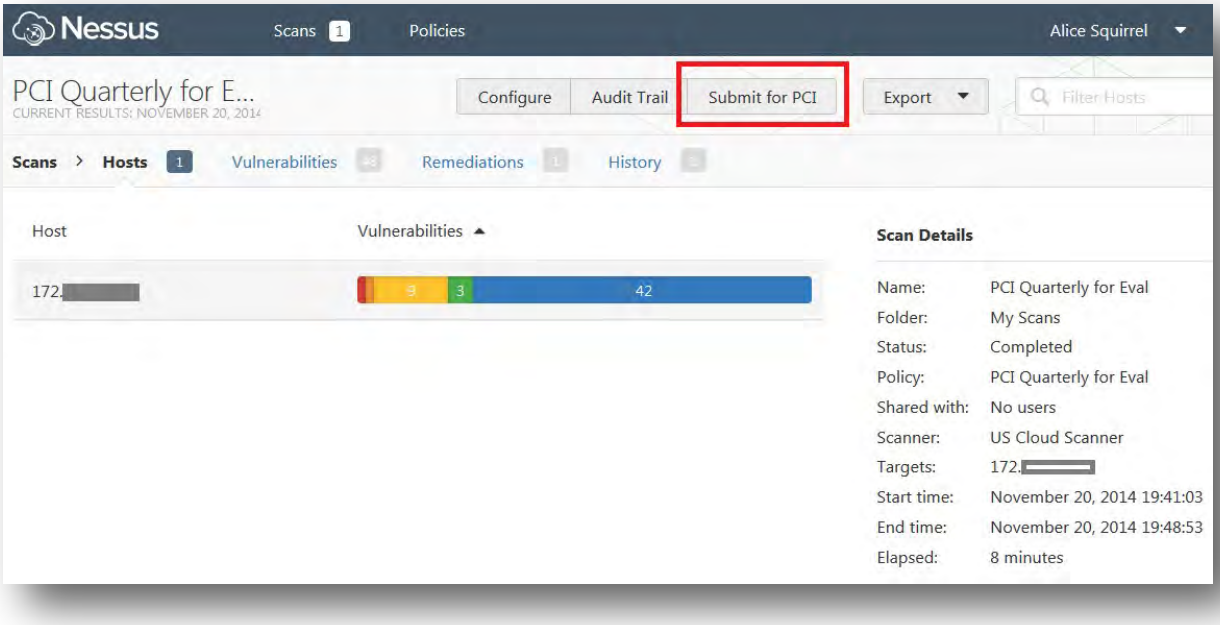


任何使用 PCI 季度外部扫描 策略模板创建的策略不能被编辑，进一步确保所需的测试都被执行。

查看提交的 PCI 扫描结果

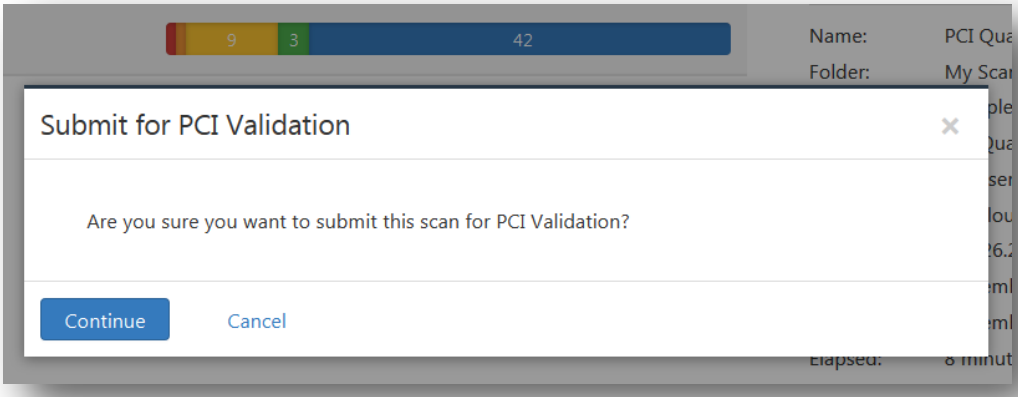
客户可以选择提交 PCI 扫描结果至 Tenable.

通过点击 “Submit for PCI”, 扫描结果将上传到 Nessus 企业云的一个管理部分，为客户进行查看, 同时会提示用户登陆服务产看经过从 PCI DSS 的角度进行分析的扫描结果.



Link to “Submit for PCI” (highlighted in red)

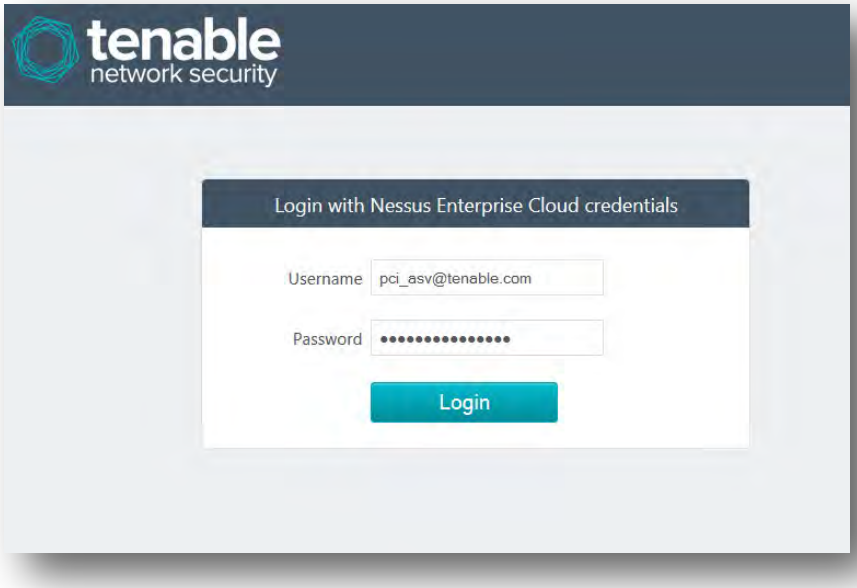
PCI-DSS ASV 超过 3 个月的扫描无法提交查看. 将无法显示 “Submit for PCI”选项。



Report Upload and PCI Validation Link Dialog Box

客户需要先将扫描结果提交上传至 Tenable 企业云，扫描结果与才能被彻底完整的查看. 报告内失败的审计结果，必须经过完整的 PCI 审查周期（限期 2 个季度）

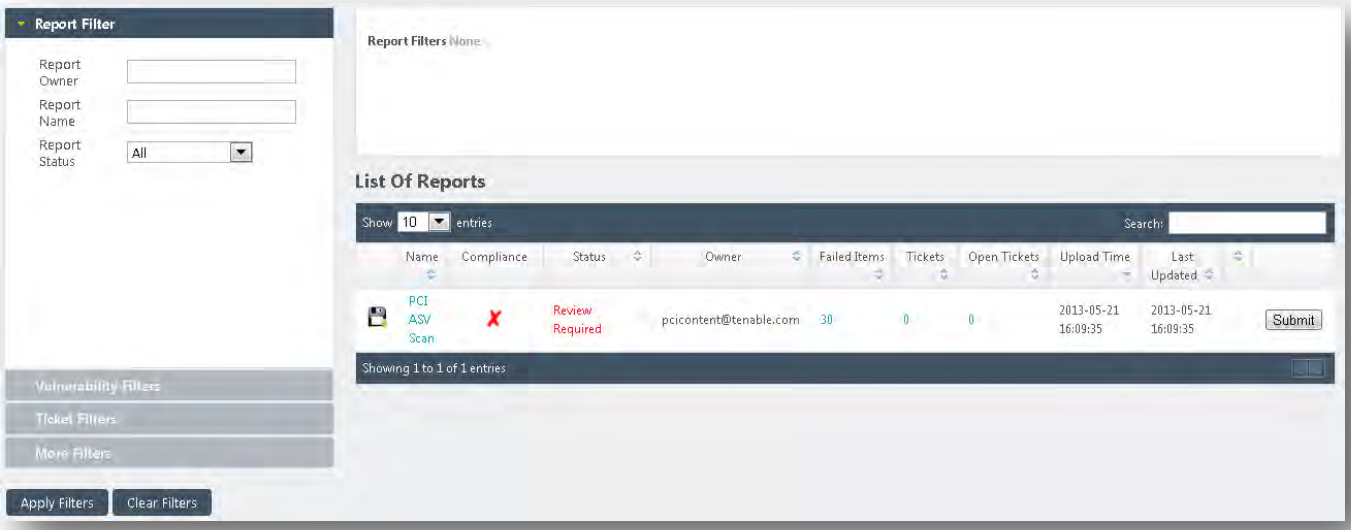
用户登陆查看接口



Nessus 企业云客户登陆界面

一旦登陆进入 PCI Validation user section,界面，可以看到一个提交到企业云的报告列表。

“Report Filter” 可以根据客户的需要过滤报表,包括 Owner、 Name, and Status.



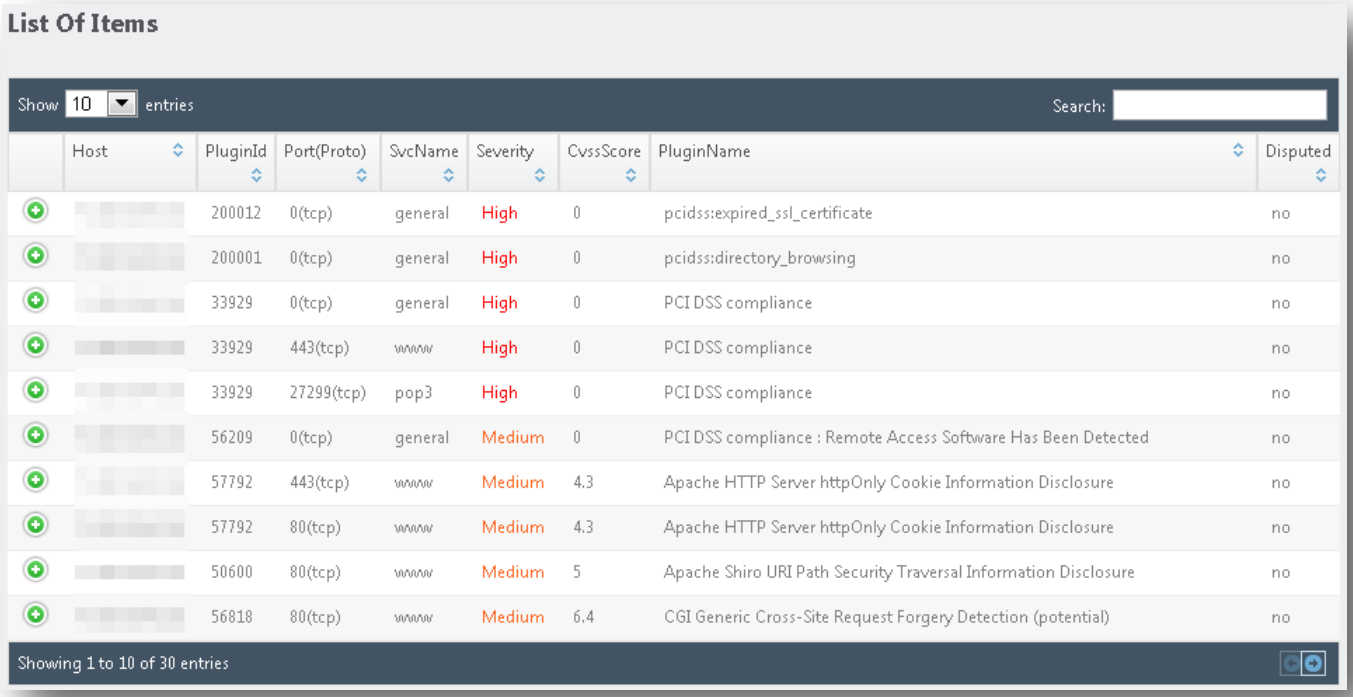
查看扫描结果

所有通过了 PCI DSS ASV 的评估结果, 所有的项目 (除了拒绝服务 (DoS)漏洞) 列为“Critical”, “High”, 以及 “Medium” (或 CVSS 的评分为 4.0 或以上) 所有的条目分为可修复或存在争议的情况, 所有有争议的项目必须得到解决, 接受成为例外, 确认为误报, 或者视为风险在可控范围之内. 所有的 “Critical”, “High”, or “Medium” 项目在 Nessus 企业云中都可以查看到相关细节。所有项目都会带有一个“Dispute”选项。

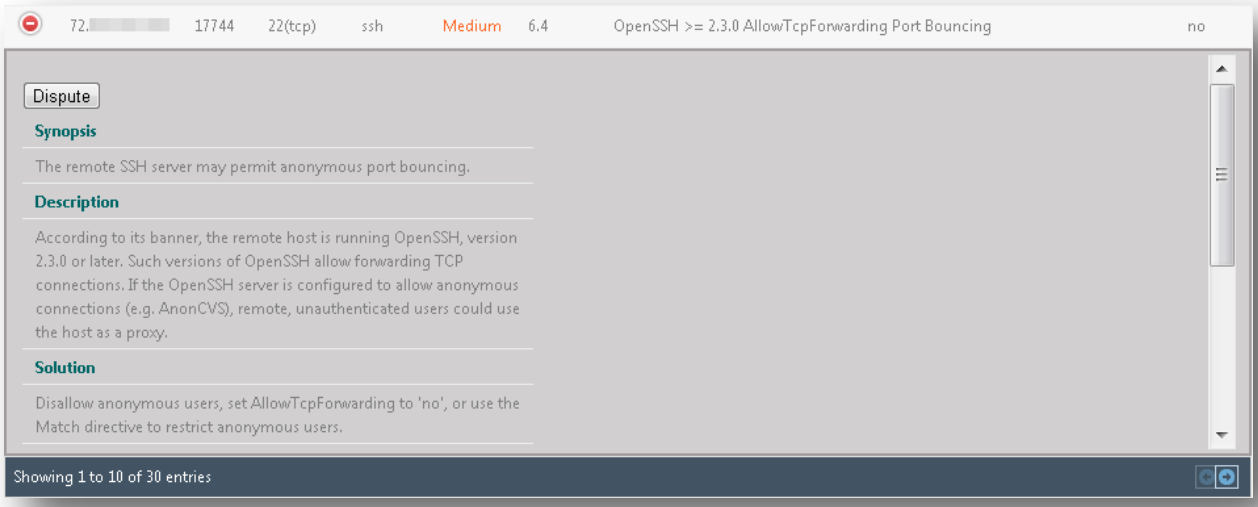
点击 “List of Reports” 里面的扫描名称，允许用户查看主机列表,每个主机上发现的漏洞的数量,按严重程度排序.

点击 “List of Reports” 里“Failed Items”的数字，将会显示一个需要被解决项目的列表。

Nessus 企业云客户负责提交报告给 Tenable 之前. “List of Reports”列表中 “Failed Items” 的选择可以允许你直接跳转到可能影响到PCI ASV 合规检测状态的项目.



使用在最左列的绿色的 “+” 按钮 查看单个漏洞的详细细节.

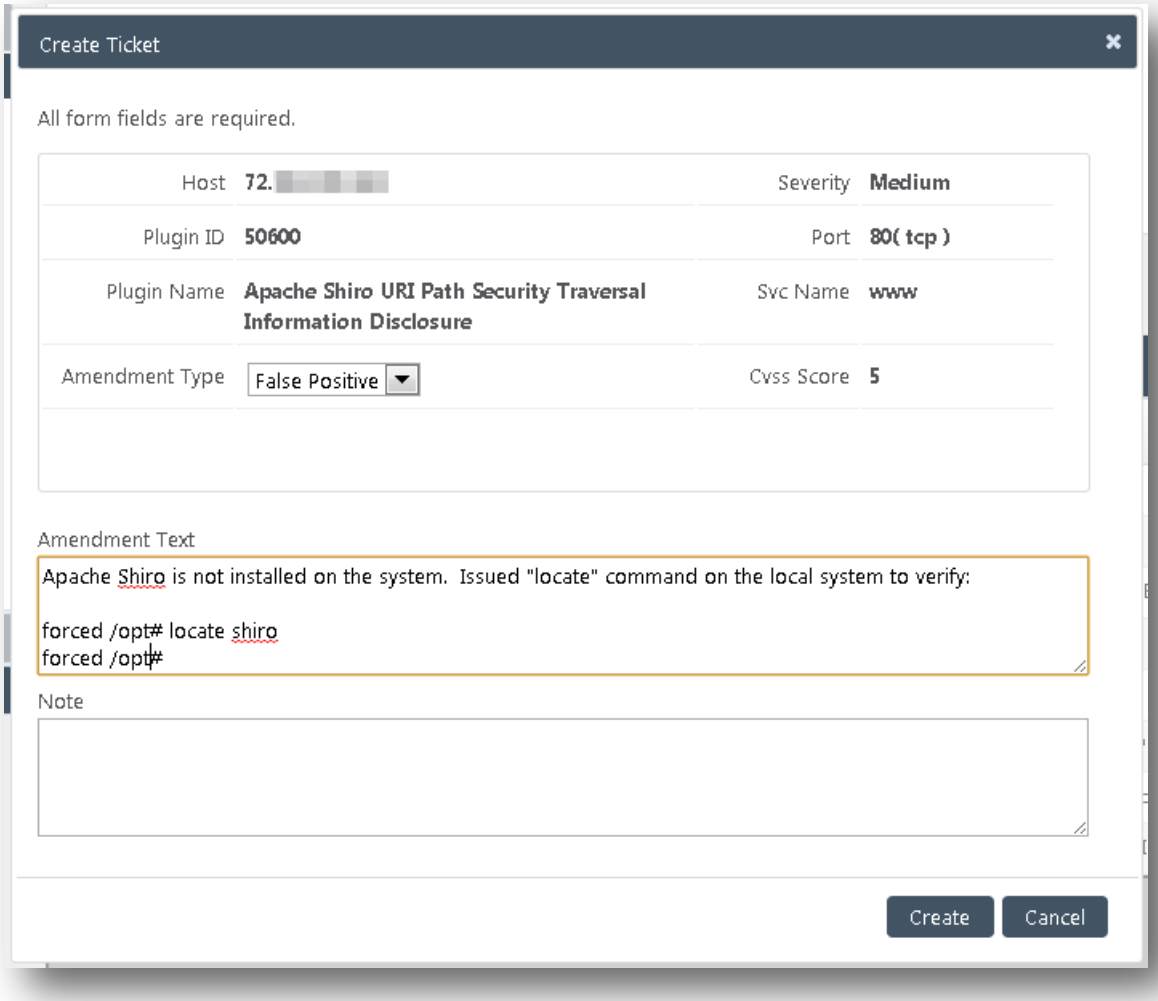


扫描报告描述“Dispute” 的功能

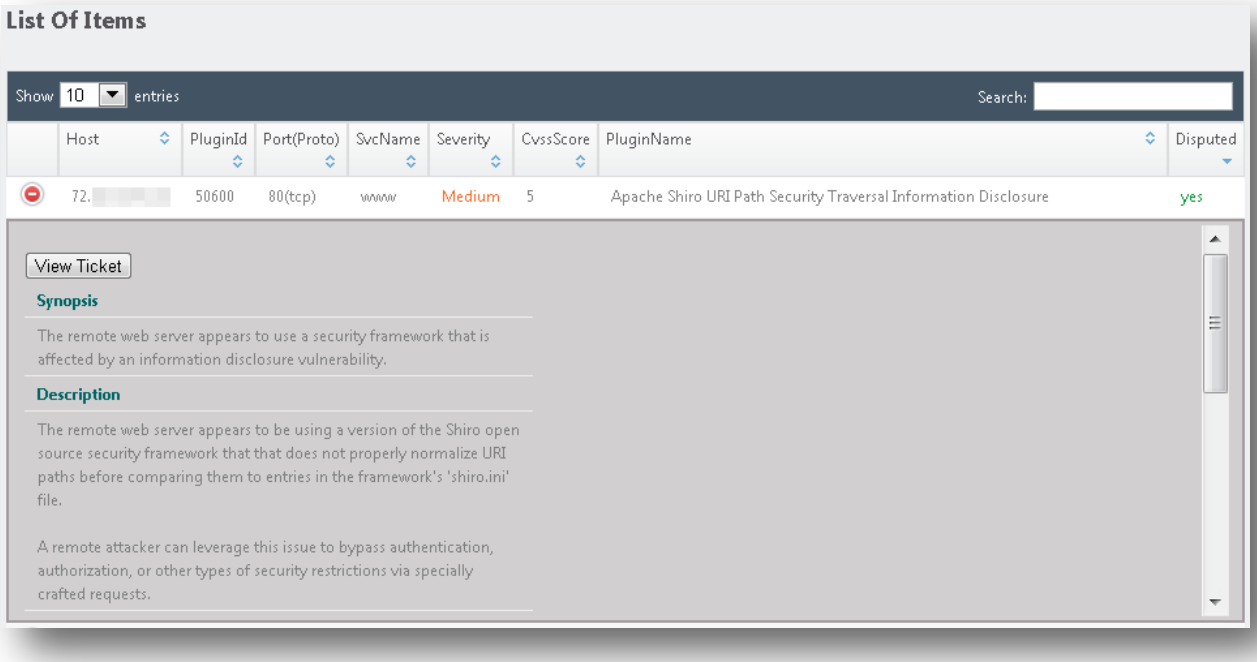
如上图所示，“Dispute”按钮显示为每个单独的项目，客户可以输入额外的漏洞修复细节，或者认为是扫描中的误报信息.

Disputing Scan 结果

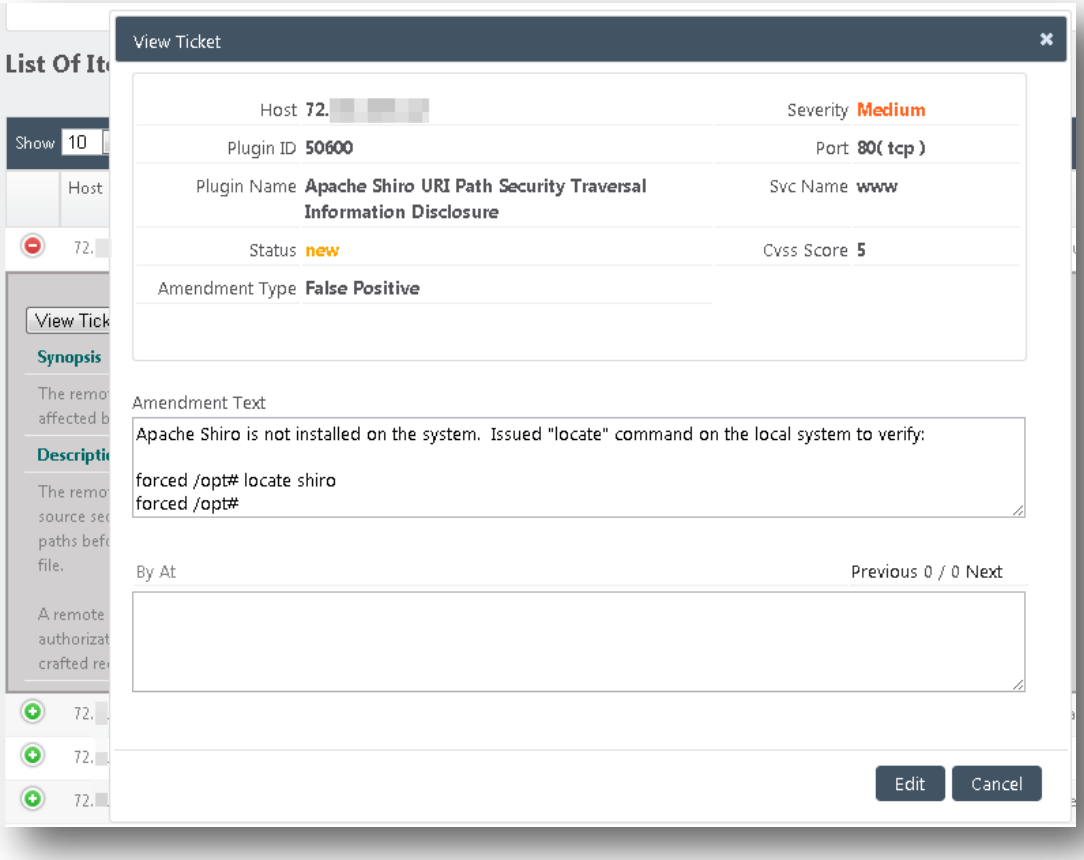
当一个项目存在争议时，“creat Ticket”可以创建 允许选择一向正确的修复类型, 添加文本的修复方案, 以及任务描述说明.



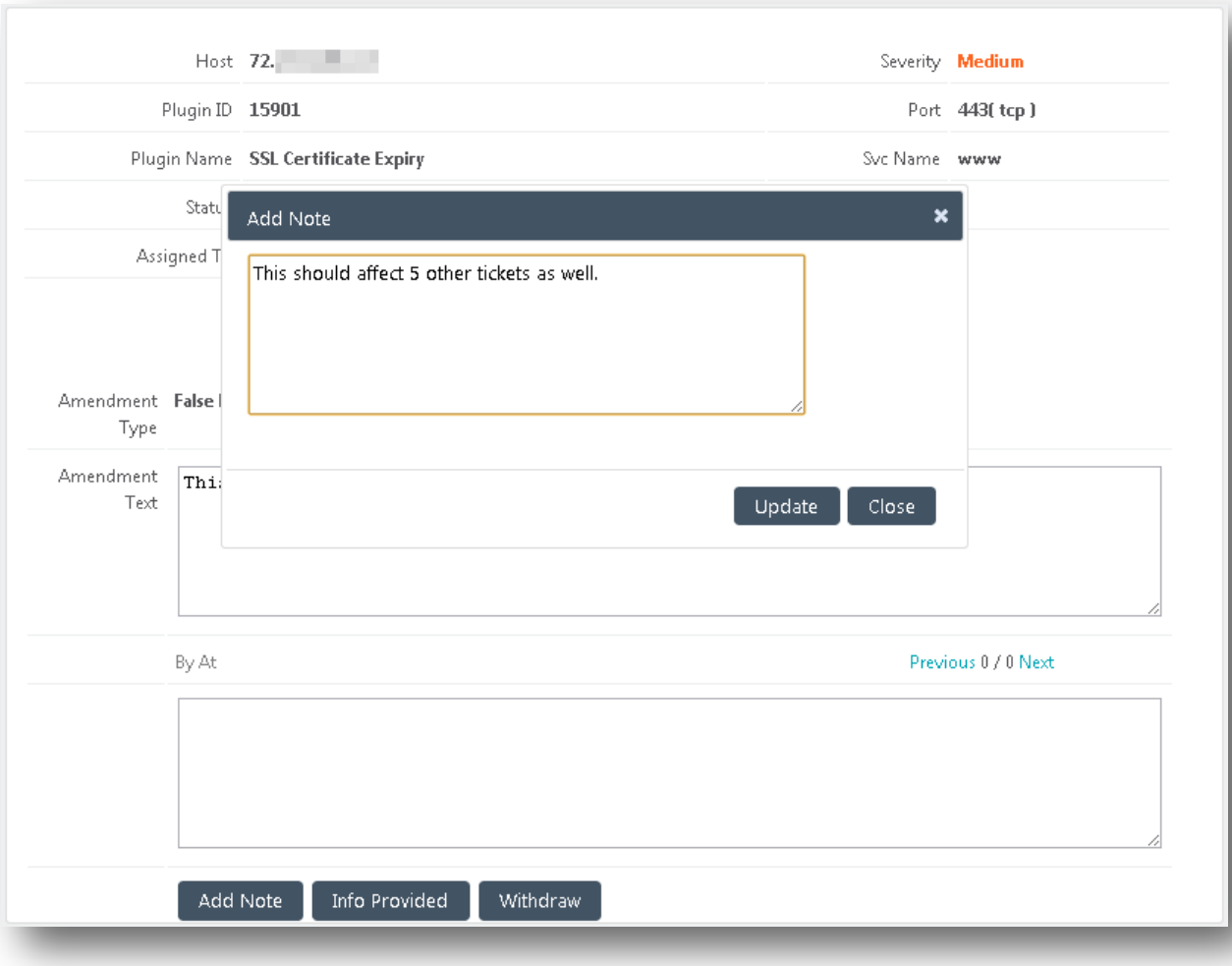
Ticket 创建了一个特定的项目，用户可以通过“View Ticket”选项来查看项目的问题



扫描报告项目描述“View Ticket”功能



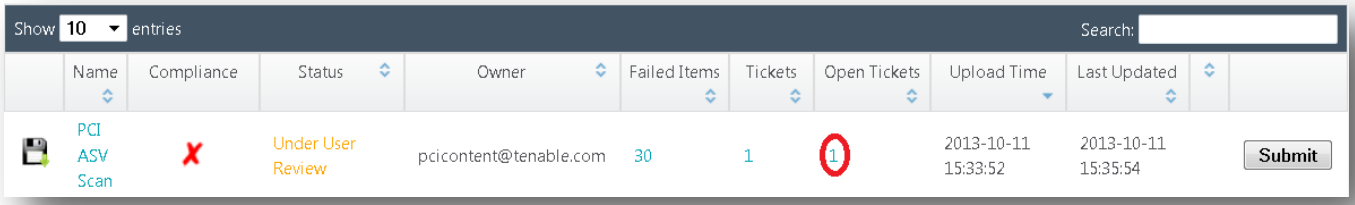
可以添加额外的评论通过单击“Edit”按钮,然后“Add Note”,通过点击“Update”进行更新



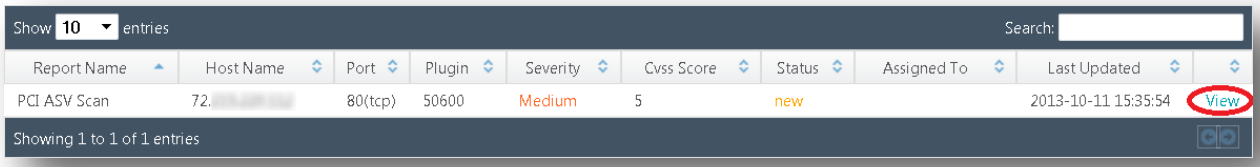
Plugin 33929, “PCI DSS Compliance”, 是一个管理的 plugin， 链接到其他的 plugins. 如果一个报告显示一台主机有许多不符合 PCI DSS, 解决有所失败的项目用 plugin 33930 “PCI DSS Compliance: Passed”.替代 plugin 33929 若存在有争议的或者例外的情况, 如果所有失败的报告项目确定为有争议的或定义为例外,可以给出基于所有其他报告问题解决的 plugin33929.

提交附件做为争议凭据

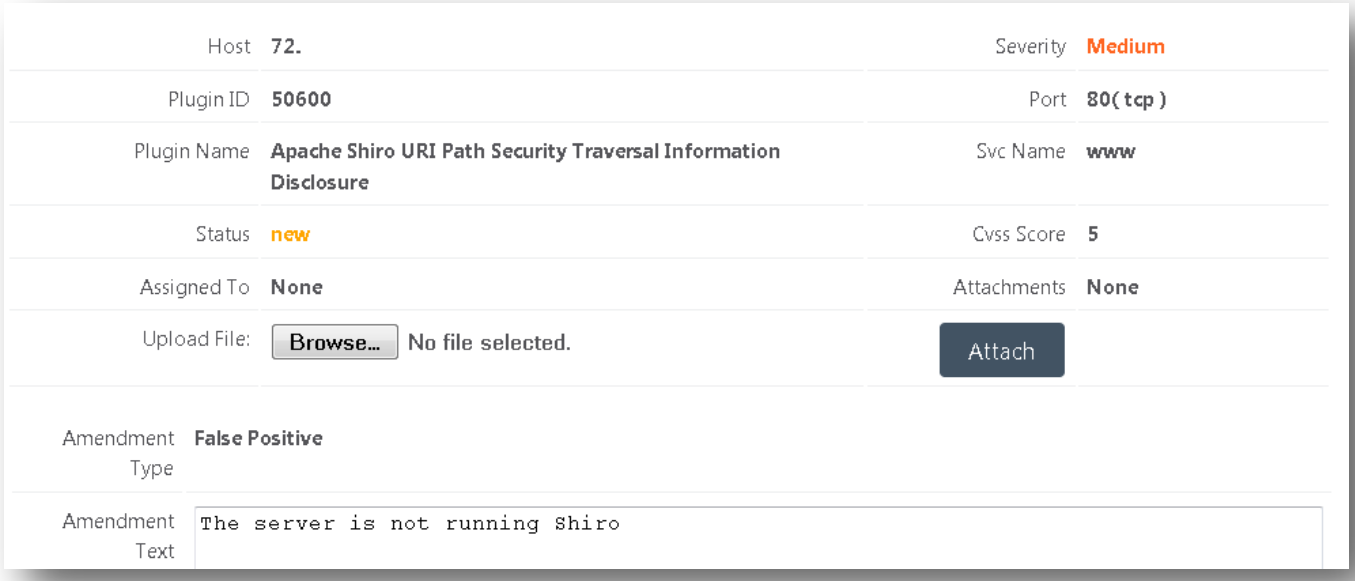
一旦建立了一个 Ticket, 可以作为附件提交证据. 创建 ticket 之后, 点击“Open Tickets”下面的数字来显示所有启用的 tickets



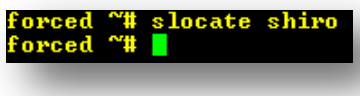
在 “List of Tickets” 界面中，点击 “View”:



当 ticket 界面显示时，“Upload File” 和 “Attach” 的选择将被显示:

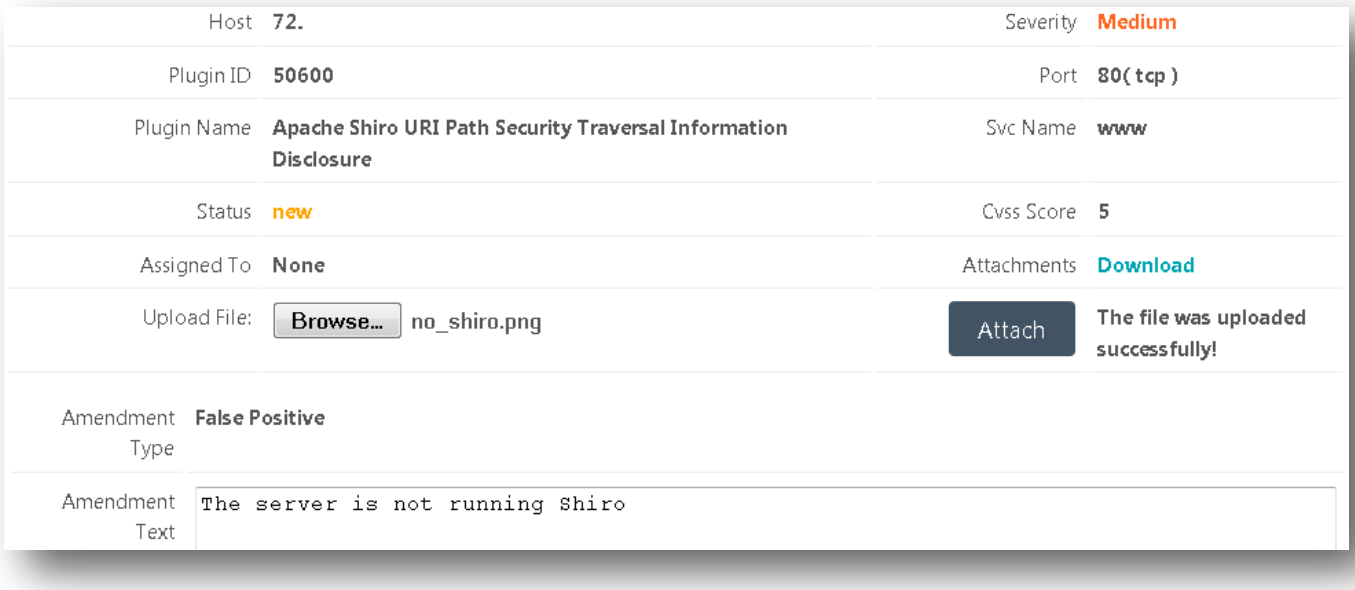


点击 “Browse…” 选择凭据文件 (screenshot, Word document, PDF, etc.) 进行上传:



Sample Evidence File (no_shiro.png)

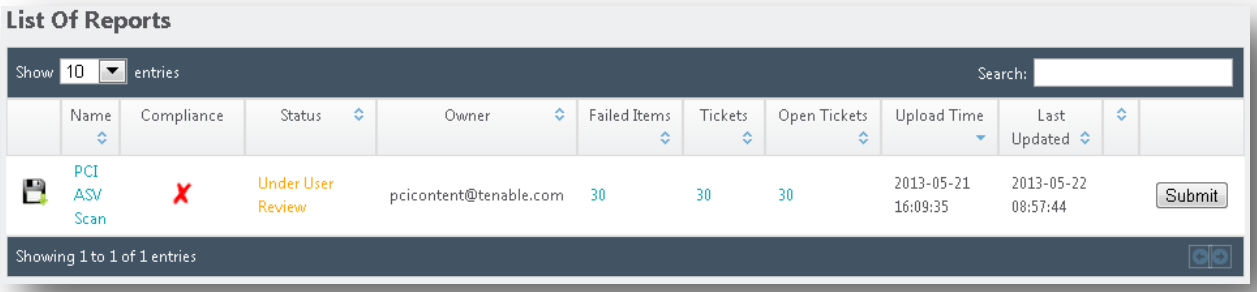
下一步，点击 “Attach” 添加附件到 Ticket 中. 当完成后界面将显示一条上传成功的消息:



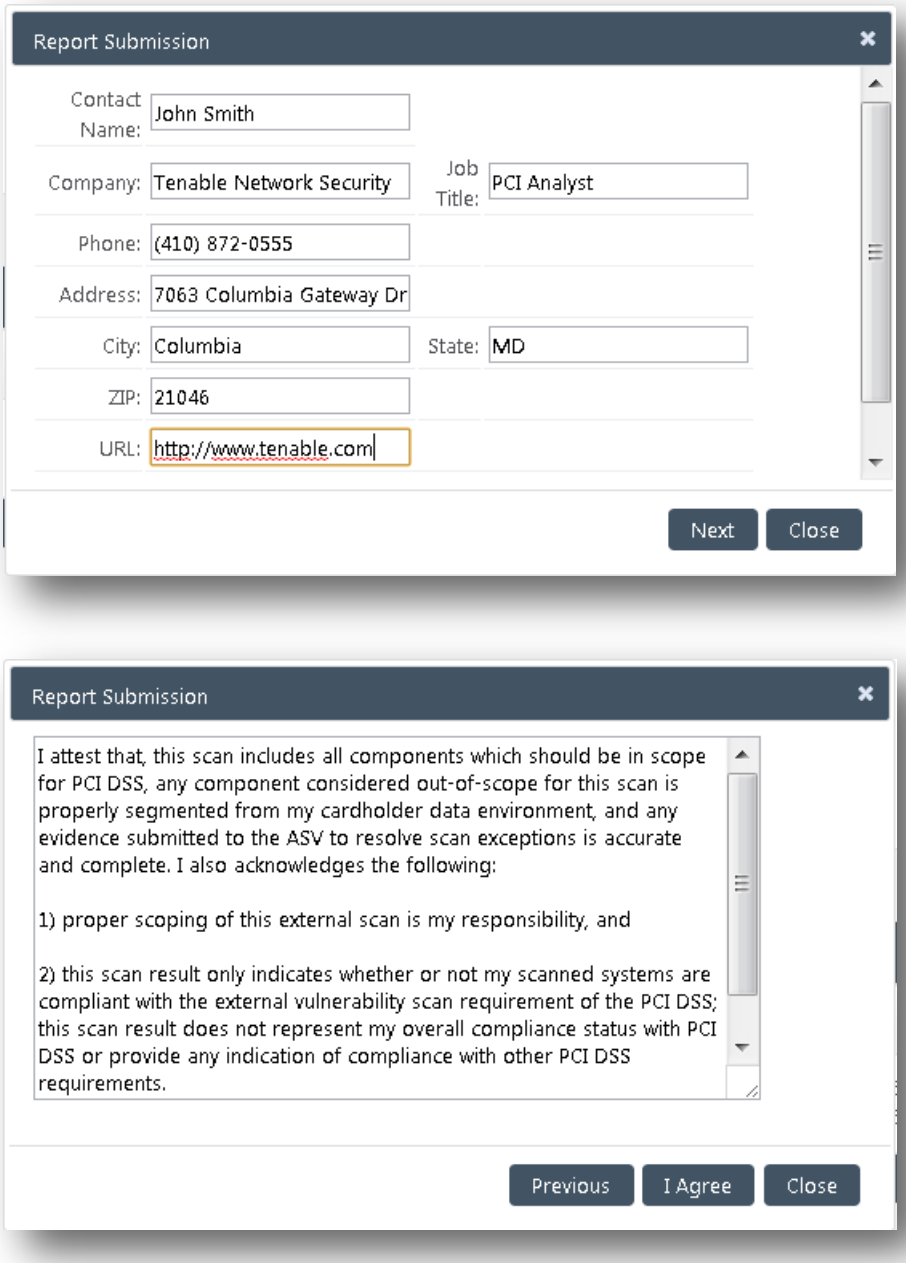
点击 “Download” 链接旁边的 “Attachments” 将显示所有附件的文件名:

提交扫描报告至 Tenable 进行检测

当所以的标签被显示为高亮的 “under user review” 项目, 该报告会发送到 Tenable Network Security for 做为 ASV 审查.

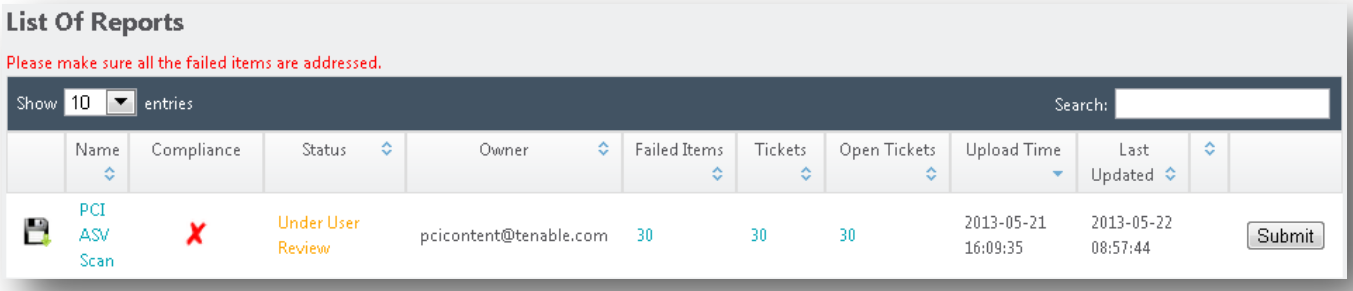


在报告提交审查前，用户必须要填写一份联系信息并同意包括强制 ASV 项目指南中描述的文本条款.

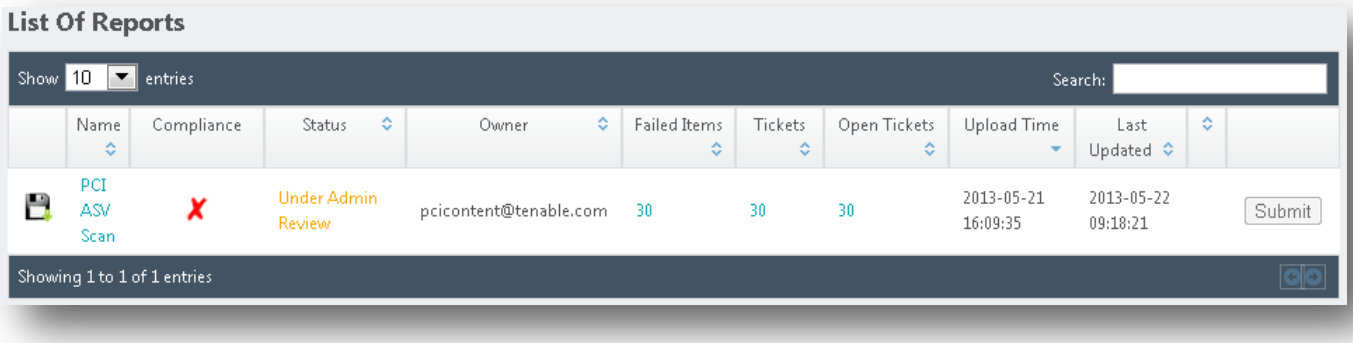


Report Submission Attestation Text

如果客户在提交 ASV 的审查审查报告前. 缺少相关信息，系统会进行提示确保所有的信息均已正确的填写。否则将无法提交至 Tenable Network Security 进行审查.



当报告最终提交到 Tenable Network Security 进行审查, 报告的状态将由 “Under User Review” 变为 “Under Admin Review” 同时 “Submit” 选项将无法点击(变为灰色) 用来防止重复提交.

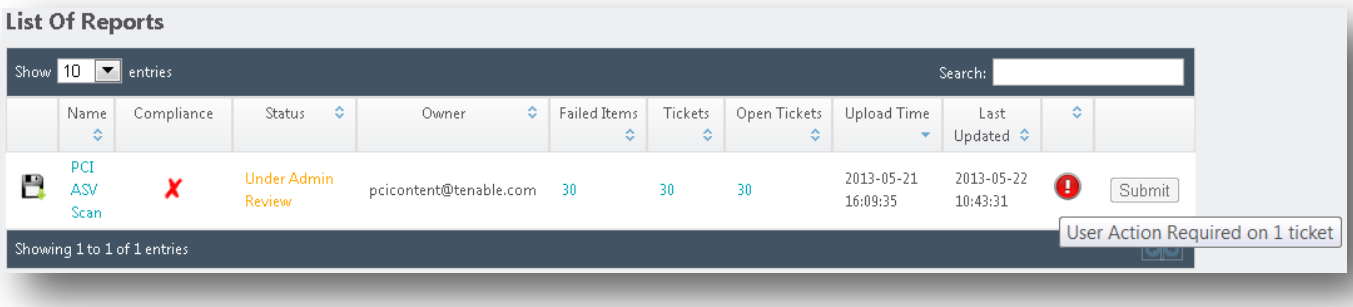


Submitted Report “Under Admin Review”

“Withdraw” 功能只有在成功将报告上传到 Tenable’s Nessus 企业云之后才是有效的. 请小心使用 “Withdraw” 功能; 撤销一个 Ticket 将会导致问题项目被标记为未解决（由于不确定的凭据）, 同时报告将被视为不一致的。

如果 Tenable Network Security 的工作人员 要求更多的信息或者要求用户进行操作,一个指标将出现在客户的报告列表。

如下所示:

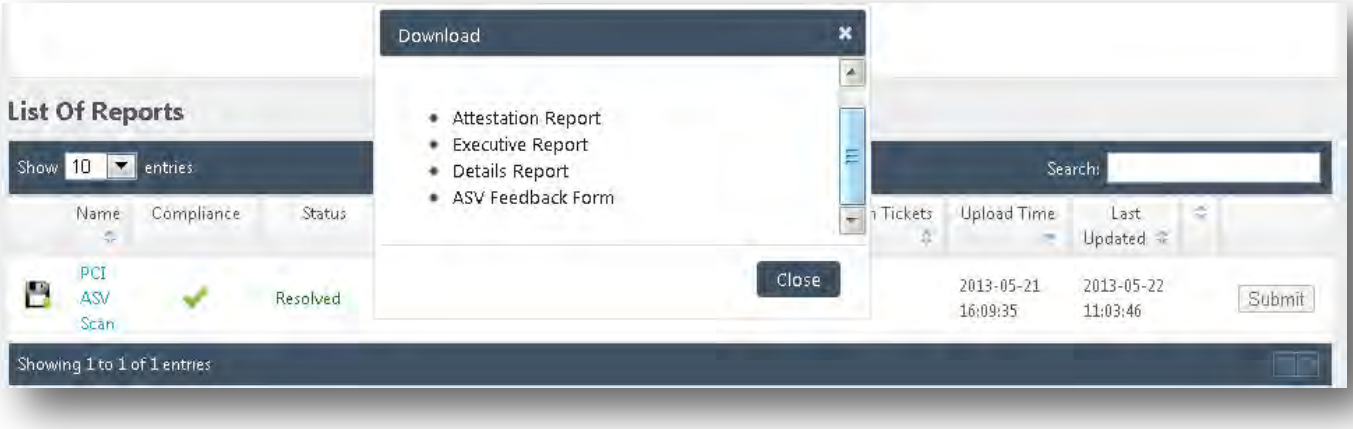


“User Action Required” Notification

Ticket 可以由用户修改和重新提交到 Tenable Network Security 进行进一步审查.

PCI ASV 报告格式

在 Tenable's Nessus 企业云中，一份报告状态变为 “compliance”, 用户可以在“Attestation Report”中选择查看报告的选项, “Executive Report”, 或者 “Detailed Report”.以及 ASV 的反馈信息. 这些操作可以通过 “Download” 图标列出每一份报告.



“Attestation Report”，“Executive Report”, 和 “Details Report”只为用户提供了 PDF 格式，不能进行编辑。.

Scan Customer Information		Approved Scanning Vendor Information	
Company:	Tenable Network Security	Company:	Tenable Network Security
Contact:	John Smith	Contact:	
Title:	PCI Analyst	Title:	Software Engineer
Telephone:	(410) 872-0555	Telephone:	4108720555
Email:	pcicontent@tenable.com	Email:	@tenable.com
Business Address:	7063 Columbia Gateway Drive	Business Address:	7063 Columbia Gateway Drive, Suite 100
City:	Columbia	City:	Columbia
State:	MD	State:	MD
ZIP:	21046	ZIP:	21046
URL:	http://www.tenable.com	URL:	www.tenable.com

Scan Status

- Compliance Status: **PASSED**
- Number of unique components scanned: **1**
- Number of identified failing vulnerabilities: **30**
- Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope: **0**
- Date scan completed: **Tue May 21 12:39:34 2013**
- Scan expiration date (90 days from date scan completed): **Mon Aug 19 12:39:34 2013**

Scan Customer Attestation

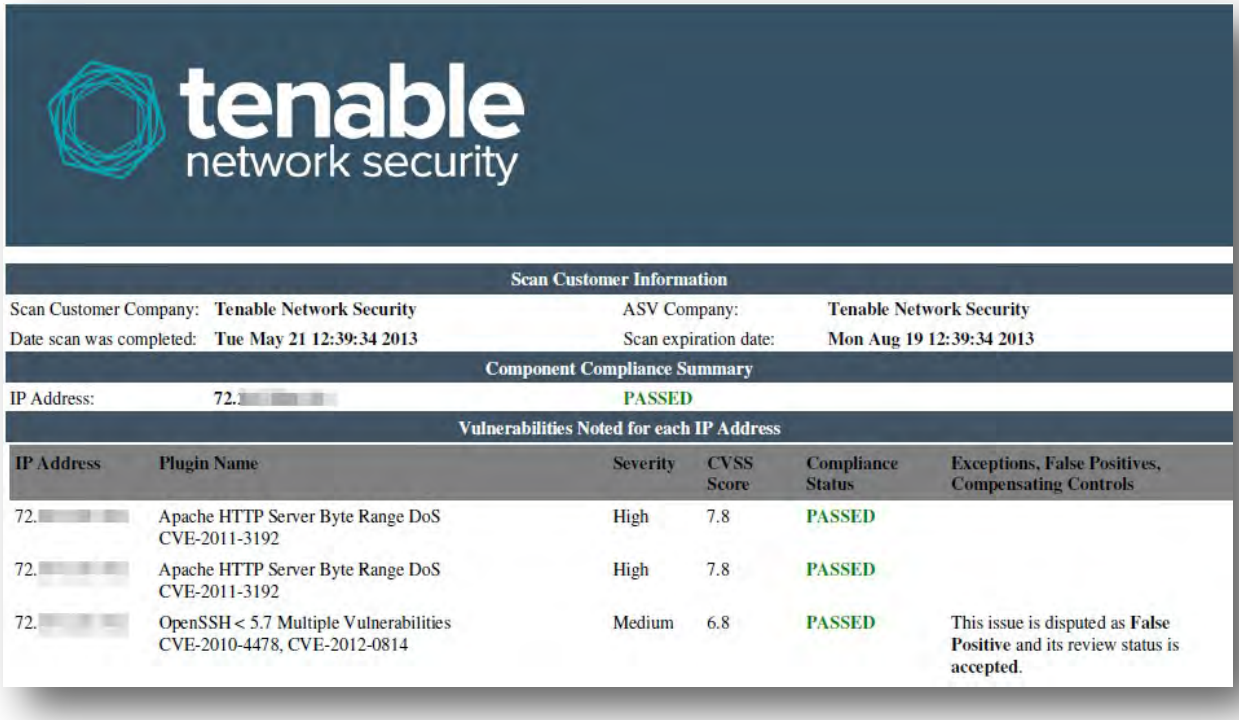
Tenable Network Security attests on **2013-05-22 09:18:21** that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements

ASV Attestation

R
L
:

This scan and report was prepared and conducted by **Tenable Network Security, Inc.** under certificate number "5049-01-02", according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. **Tenable Network Security, Inc.** attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by sshah@tenable.com.

Sa mple Attestation Report



tenable network security

Scan Customer Information			
Scan Customer Company:	Tenable Network Security	ASV Company:	Tenable Network Security
Date scan was completed:	Tue May 21 12:39:34 2013	Scan expiration date:	Mon Aug 19 12:39:34 2013

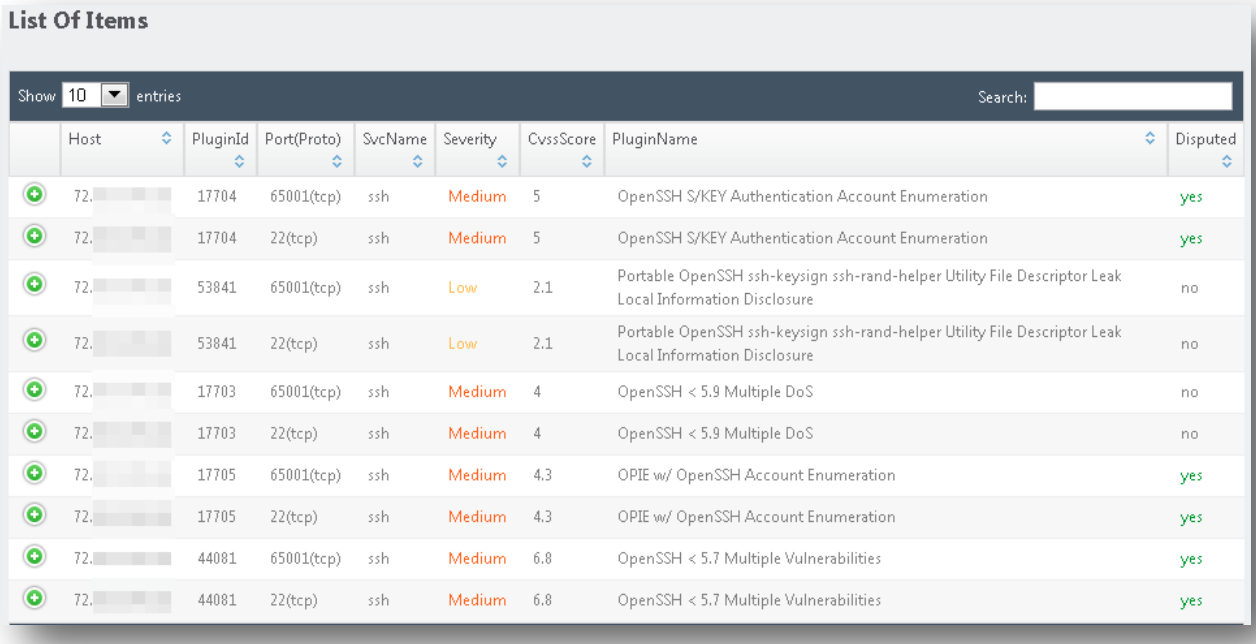
Component Compliance Summary		
IP Address:	72.	PASSED

Vulnerabilities Noted for each IP Address

IP Address	Plugin Name	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, Compensating Controls
72.	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	PASSED	
72.	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	PASSED	
72.	OpenSSH < 5.7 Multiple Vulnerabilities CVE-2010-4478, CVE-2012-0814	Medium	6.8	PASSED	This issue is disputed as **False Positive** and its review status is **accepted**.

Sample Executive Report

在基于 web 的接口的报告先选择一个报告名称,然后选择主机名, 可以显示选中的项目列表.



List Of Items

Show 10 entries Search:

Host	PluginId	Port(Proto)	SvcName	Severity	CvssScore	PluginName	Disputed
72.	17704	65001(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
72.	17704	22(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
72.	53841	65001(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no
72.	53841	22(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no
72.	17703	65001(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no
72.	17703	22(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no
72.	17705	65001(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes
72.	17705	22(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes
72.	44081	65001(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes
72.	44081	22(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes

"List of Items" Displayed in the Web Interface

关于柯力士信息安全

- 请从 Tenable **中国区唯一授权认证代理**<柯力士信息安全>获取产品介绍信息，点击链接：http://www.jw-assoc.com/products.html&c_id=82&d_id=131”；
- QQ 交流：柯力士信息安全交流群(156403892)；
- 微信获取第一手资料：柯力士信息安全

关于 Tenable

Tenable Network Security 提供持续的网络监控和漏洞识别, 降低风险,确保合规. 我们的产品包括 SecurityCenter Continuous View™, which 提供最全面 网络安全整体解决方案。Nessus®, 全球标准的检测和网络数据评估. 全球超过 20000 个组织在只用 Tenable 产品, 包括整个美国国防部和许多全球最大的公司和政府. 更多信息请访问 tenable.com.

欲了解更多信息

Tenable 有各种其他文档来详细描述 Nessus 的安装, 部署, 配置, 用户操作, 和整体测试:

- Nessus 6.3 Installation and Configuration Guide – 一步一步进行关于 Nessus Professional, Nessus Manager, Nessus Scanner, 和 Nessus Agents 的安装和配置
- Nessus 6.3 Command Line Reference –描述了 Nessus 命令行工具
- Nessus v6 SCAP Assessments –描述如何使用 Tenable 的 Nessus 生成 SCAP 内容审计以及查看和导出扫描结果
- Nessus Compliance Checks –高级指南， 了解和运行使用 Nessus 和 SecurityCenter 合规检查
- Nessus Compliance Checks Reference –全面指导Nessus合规检查语法
- Nessus v2 File Format – 描述, 介绍 Nessus 3.2 和 NessusClient 3.2 .nessus 格式的文件结构
- Nessus and Antivirus –概述了几种流行的安全软件如何与 Nessus 交互, 并提供建议或解决方案,允许软件更好的共存不损害您的安全或阻碍你的漏洞扫描工作
- Strategic Anti-malware Monitoring with Nessus, PVS, and LCE – 描述如何使用 Tenable's USM 平台检测各种恶意软件和识别和确定恶意软件感染的程度
- Real-Time Compliance Monitoring – 概述 Tenable's 如何解决用来协助会议许多不同类型的政府和金融监管
- Tenable Products Plugin Families –提供了一个描述和总结 Nessus 日志关联引擎,被动的漏洞扫描器的 Plugin
- SecurityCenter 管理员指导

其他在线资源如下:

- Nessus Discussions Forum: https://discussions.tenable.com/
- Tenable Blog: http://www.tenable.com/blog
- Tenable Podcast: http://www.tenable.com/podcast
- Example Use Videos: http://www.youtube.com/user/tenablesecurity
- Tenable Twitter Feed: http://twitter.com/tenablesecurity

请随时联系 Tenable 的 tenable@jw-assoc.com, sales@jw-assoc.com 或者访问我们的主页 http://www.jw-assoc.com。

您也可以直接致电柯力士获取更多信息，Nessus 销售直线：021-36567589，36567590；总机：021-36567588

附录 A – Windows 平台认证配置

先决条件

用户权限

一个很常见的错误是，创建一个本地帐户,没有足够远程登录和做任何有用的事的权限. 如果远程登录，一般需要 Windows 将分配新的本地账户“Guest”特权. 这可以成功远程漏洞审核. 另一个常见的错误是增加“Guest”访问的用户。这降低了您的 Windows 服务器的安全.

为本地和远程启用 Windows 登录审计

关于 Windows 凭据最重要的方面是,账户用于执行检查应该有权访问所有必需的文件和注册表项,并在许多情况下,这意味着需要管理权限. 如果不能提供带有管理权限的帐号，Nessus 最多检查系统的补丁情况。 虽然这仍是一个有效的方法来确定一个补丁安装,但不能与一些第三方补丁管理工具,可能忽视制定的关键政策。如果 Nessus 配置了管理权限,然后它会检查远程主机中版本的动态链接库文件(. dll),这是更加准确和有效的.

配置本地帐号

配置一个独立的 Windows 服务器凭证使用, 简单地创建一个独特的账户作为管理员.

确认帐号的默认配置不是默认的 “Guest only: local users authenticate as guest”. 反而应该为 “Classic: local users authenticate as themselves”.

配置服务器允许通过域登陆,“Classic” 安全模块应该被启用. 进行以下步骤的操作:

1. Open “Group Policy” by clicking on “start”, click “Run”, type “**`gpedit.msc`**” and then click “OK”.
2. Select Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
3. From the list of policies open “Network access: Sharing and security model for local accounts”.
4. In this dialog, select “Classic – local users authenticate as themselves” and click “OK” to save this.

这将导致当地域进行身份验证的用户,即使他们实际上不是真的身体的特定服务器上的。没有这样做,所有远程用户,甚至真实用户的域,将作为一个“Guest”和实际验证可能会没有足够的凭证进行远程审计.

注意 gpedit.msc 不可用于 Windows 7 Home, Tenable 不支持.

配置身份验证扫描的域帐户

创建一个 Windows 服务器的远程基于主机的域帐户审计，服务器必须首先 Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Windows 7, 和 Windows 8. 一般有五个步骤应该执行，为了便于扫描,同时保持安全意识.

Step 1: 创建安全组

首先，创建一个安全组，名称为 **Nessus Local Access**:

- Log onto a Domain Controller, open Active Directory Users and Computers.
- Create a security Group from **Menu** select **Action** -> **New** -> **Group**.
- Name the group **Nessus Local Access**. Make sure it has a "Scope" of **`Global`** and a "Type" of **`Security`**.
- Add the account you will use to perform Nessus Windows Authenticated Scans to the **Nessus Local Access** group.

Step 2: 创建组策略

接下来, 需要创建一个组策略，名称为 **Local Admin GPO**.

- Open the **Group Policy Management Console**.
- Right click on **Group Policy Objects** and select **New**.
- Type the name of the policy **Nessus Scan GPO**".

Step 3: 配置策略，添加 "Nessus Local Access" 组为管理员组

Here you will add the **Nessus Local Access** group to the **Nessus Scan GPO** policy and put them in the groups you wish them to use.

- Right click "**Nessus Scan GPO**" Policy then select **Edit**.
- Expand ***Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups***.
- In the Left pane on **Restricted Groups**, right click and select "**Add Group**".
- In the **Add Group** dialog box, select browse and type **Nessus Local Access** and then click "**Check Names**".
- Click **OK** twice to close the dialog box.
- Click **Add** under "***This group is a member of:***"
- Add the "**Administrators**" Group.
- Click **OK** twice.

Step 4: 确保适当的防火墙端口是打开的保证 Nessus 可以连接到主机

Nessus 使用 SMB (Server Message Block) 和 WMI (Windows Management Instrumentation) 我们需要确保 Windows 防火墙允许访问系统.

在 Windows 防火墙 Vista, 7, 8, 2008, 2008R2 and 2012 Windows 打开 WMI 访问权限

- Right click "**Nessus Scan GPO**" Policy then select **Edit**.

- Expand *Computer configuration|Policies|Windows Settings|Security Settings|Windows Firewall with Advanced Security|Windows Firewall with Advanced Security|Inbound Rules*
- Right-click in the working area and choose **New Rule...**
- Choose the Predefined option, and select **Windows Management Instrumentation (WMI)** from the drop-down list.
- Click on **Next**.
- Select the Checkboxes for:

- Windows Management Instrumentation (ASync-In)
- Windows Management Instrumentation (WMI-In)
- Windows Management Instrumentation (DCOM-In)

- Click on **Next**
- Click on **Finish**
- ***Note***: You can later edit the predefined rule created and limit the connection to the ports by IP Address and Domain

User so as to reduce any risk for abuse of WMI.

Step 5: 连接 GPO

- In Group policy management console, right click on the domain or the OU and select Link an Existing GPO
- Select the Nessus Scan GPO

配置 Windows 2008, Vista and 7

当执行身份验证的扫描与 Windows 2008,Vista 或 7 系统,有几个配置选项,必须启用:

1. Under **Windows Firewall** -> **Windows Firewall Settings**, "**File and Printer Sharing**" must be enabled.

2. Using the **`gpedit.msc`** tool (via the "Run.." prompt), invoke the **Group Policy Object Editor**. Navigate to **Local Computer Policy** -> **Administrative Templates** -> **Network** -> **Network Connections** - > **Windows Firewall -> Standard Profile** -> **Windows Firewall : Allow inbound file and printer exception**, and enable it.

3. While in the **Group Policy Object Editor**, navigate to **Local Computer Policy** -> **Administrative Templates** -> **Network** -> **Network Connections** -> **Prohibit use of Internet connection firewall on your DNS domain** and ensure it is set to either "Disabled" or "Not Configured".

4. The Remote Registry service must be enabled (it is disabled by default). It can be enabled manually for continuing audits, either by an administrator or by Nessus. Using plugin IDs 42897 and 42898, Nessus can enable the service just

for the duration of the scan.

Nessus has the ability to enable and disable the Remote Registry service. For this to work, the target must have the Remote Registry service set to "Manual" and not "Disabled".

Windows User Account Control (UAC) can be disabled alternatively, but that is not recommended. To turn off UAC completely, open the Control Panel, select "User Accounts" and then set "Turn User Account Control" to off. Alternatively, you can add a new registry key named "`LocalAccountTokenFilterPolicy`" and set its value to "1". This key must be created in the registry at the following location: **`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`**. For more information on this registry setting, consult the MSDN 766945 KB. In Windows 7 and 8, if UAC is disabled, then `EnableLUA` must be set to 0 in **`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`** as well.

附录 B – Enabling SSH Local Security Checks on Unix and Network Devices

This section is intended to provide a high-level procedure for enabling SSH between the systems involved in the Nessus credentialed checks. It is not intended to be an in-depth tutorial on SSH. It is assumed the reader has the prerequisite knowledge of Unix system commands.

Generating SSH Public and Private Keys

The first step is to generate a private/public key pair for the Nessus scanner to use. This key pair can be generated from any of your Unix systems, using any user account. However, it is important that the keys be owned by the defined Nessus user.

To generate the key pair, use **`ssh-keygen`** and save the key in a safe place. In the following example the keys are generated on a Red Hat ES 3 installation.

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
                                /home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Do not transfer the private key to any system other than the one running the Nessus server. When **`ssh-keygen`** asks you for a passphrase, enter a strong passphrase or hit the "Return" key twice (i.e., do not set any passphrase). If a passphrase

is specified, it must be specified in the Policies -> Credentials -> SSH settings options in order for Nessus to use key-based authentication.

Nessus Windows users may wish to copy both keys to the main Nessus application directory on the system running Nessus (**`C:\Program Files\Tenable\Nessus`** by default), and then copy the public key to the target systems as needed. This makes it easier to manage the public and private key files.

Creating a User Account and Setting up the SSH Key

On every target system to be scanned using local security checks, create a new user account dedicated to Nessus. This user account must have exactly the same name on all systems. For this document, we will call the user "nessus", but you can use any name.

Once the account is created for the user, make sure that the account has no valid password set. On Linux systems, new user accounts are locked by default, unless an initial password was explicitly set. If you are using an account where a password had been set, use the "**`passwd -l`**" command to lock the account.

You must also create the directory under this new account's home directory to hold the public key. For this exercise, the directory will be **`/home/nessus/.ssh`**. An example for Linux systems is provided below:

```
# passwd -l nessus
# cd /home/nessus
# mkdir .ssh
#
```

For Solaris 10 systems, Sun has enhanced the "**passwd(1)**" command to distinguish between locked and non-login accounts. This is to ensure that a user account that has been locked may not be used to execute commands (e.g., cron jobs). Non-login accounts are used only to execute commands and do not support an interactive login session. These accounts have the "NP" token in the password field of **/etc/shadow**. To set a non-login account and create the SSH public key directory in Solaris 10, run the following commands:

```
# passwd -N nessus
# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

Now that the user account is created, you must transfer the key to the system, place it in the appropriate directory and set the correct permissions.

From the system containing the keys, secure copy the public key to system that will be scanned for host checks as shown below. 192.1.1.44 is an example remote system that will be tested with the host-based checks.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

You can also copy the file from the system on which Nessus is installed using the secure FTP command, "**sftp**". Note that the

file on the target system must be named "`authorized_keys`".

Do not use the **no-pty** option in your "`authorized_keys`" file for SSH authentication. This can impact the SSH
credentialed scans.

Return to the System Housing the Public Key

Set the permissions on both the **/home/nessus/.ssh** directory, as well as the **authorized_keys** file.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Repeat this process on all systems that will be tested for SSH checks (starting at "Creating a User Account and Setting up the SSH Key" above).

Test to make sure that the accounts and networks are configured correctly. Using the simple Unix command "**id**", from the Nessus scanner, run the following command:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

If it successfully returns information about the `nessus` user, the key exchange was successful.

Enabling SSH Local Security Checks on Network Devices

In addition to using SSH for local security checks, Nessus also supports local security checks on various network devices. Those network devices currently include Cisco IOS devices, F5 networks devices, Huawei devices, Junos devices, and Palo Alto Networks devices.

Network devices that support SSH require both a username and password. Currently, Nessus does not support any other forms of authentication to network devices.

See your appropriate network device manual for configuring SSH support.