用Qualys配置ISE 2.1威胁中心NAC (TC-NAC)

Contents

Introduction

本文描述如何用在身份服务引擎(ISE) 2.1的Qualys配置威胁中心NAC。威胁中心网络访问控制(TC-NAC)功能enable (event)创建授权策略的您根据从威胁和弱点适配器接收的威胁和弱点属性。

Prerequisites

Requirements

Cisco建议您有这些题目基础知识：

- Cisco身份服务引擎
- Qualys ScanGuard

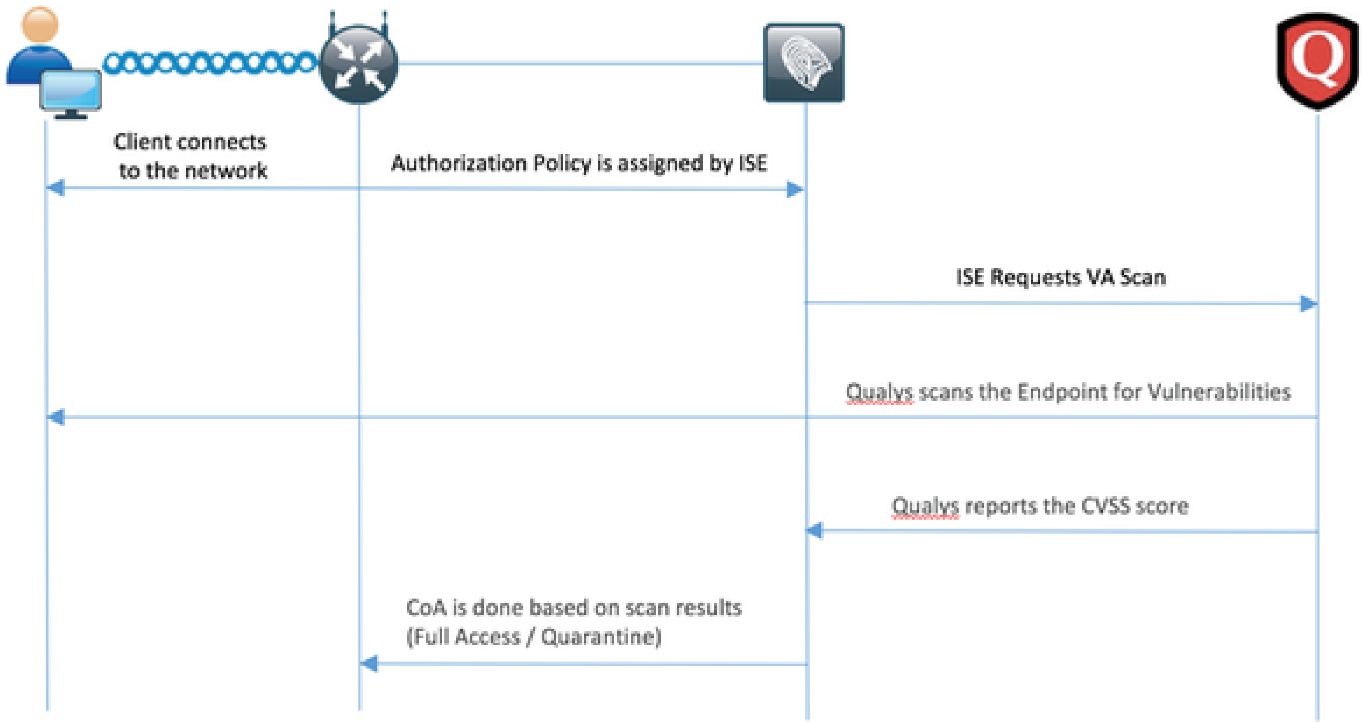
Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco身份服务引擎版本2.1
- 无线局域网控制器(WLC) 8.0.121.0
- Qualys卫兵扫描程序8.3.36-1，签名2.3.364-2
- Windows 7服务包1

Configure

高级流程图



这是流：

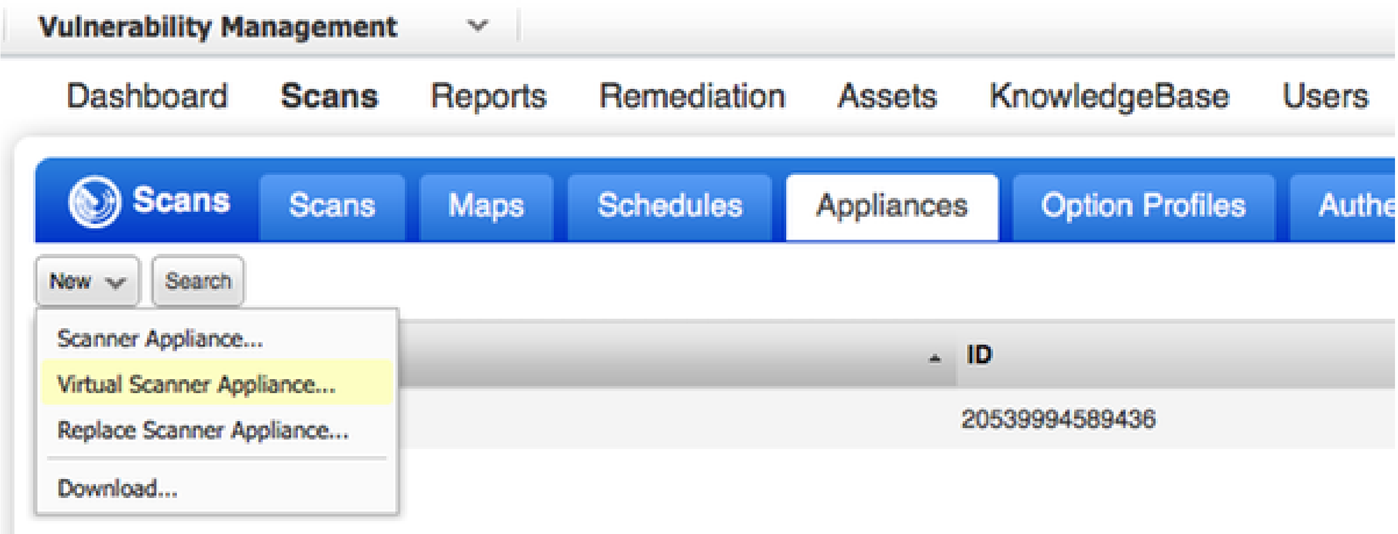
1. 客户端连接到网络，有限享用产生，并且配置文件与**估计**被启用的复选框分配的**弱点**
2. PSN节点传送系统消息到MNT节点确认的认证发生了，并且VA扫描是授权策略的结果
3. MNT节点提交扫描给TC-NAC节点(使用Admin WebApp)使用此数据， ：
   - MAC地址
   - IP地址
   - Scan interval
   -被启用的定期扫描
   -产生PSN
4. Qualys TC-NAC (封装在码头工人容器)与Qualys Cloud联络(通过其余API)若需要触发扫描
5. Qualys Cloud指示Qualys扫描程序扫描终端
6. Qualys扫描程序发送扫描的结果到Qualys Cloud
7. 扫描的结果被退还到TC-NAC ：
   - MAC地址
   -所有CVSS评分
   -所有弱点(QID，标题， CVEIDs)
8. TC-NAC更新与所有数据的PAN从第7.步。
9. 若需要CoA根据被配置的授权策略被触发。

配置Qualys Cloud和扫描程序

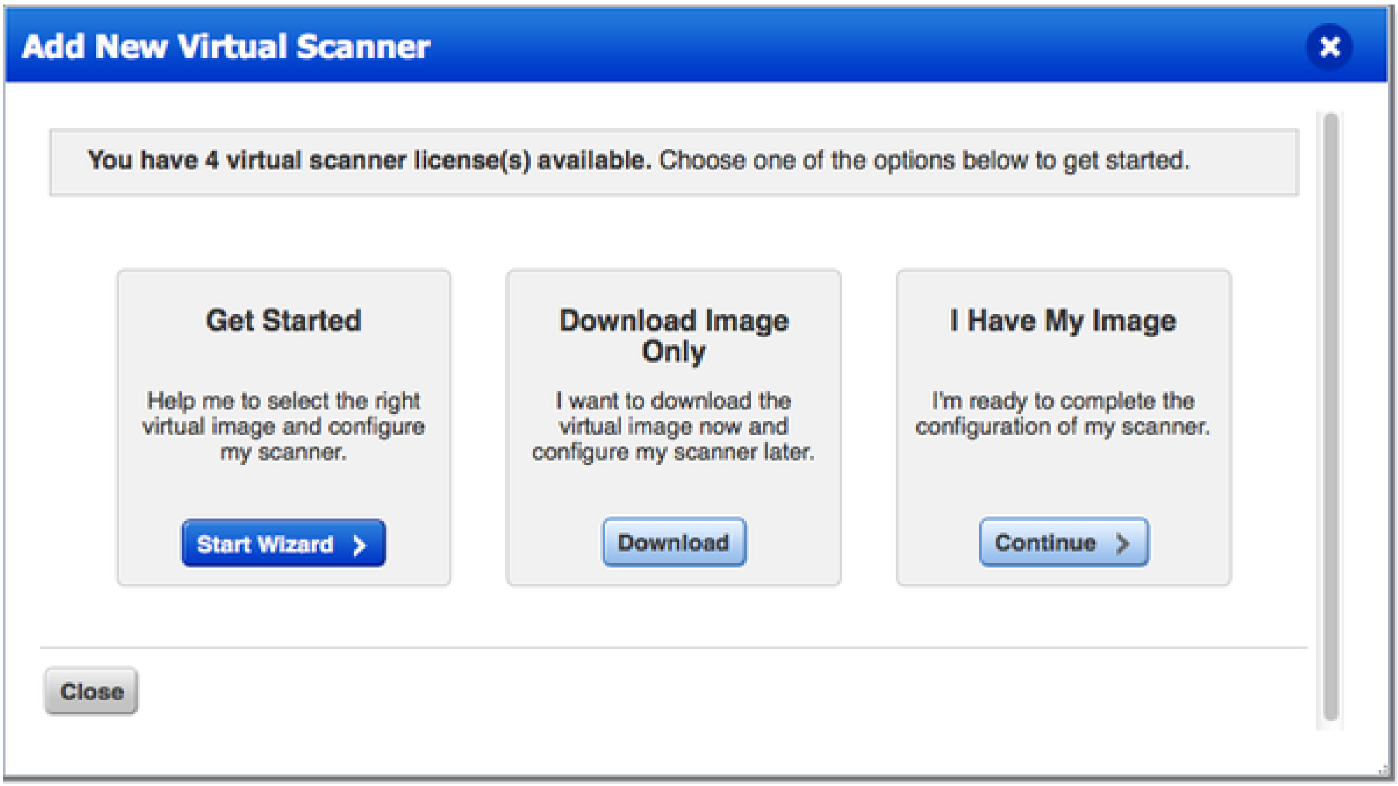
警告：在本文的Qualys配置为实验室目的被执行，请与设计注意事项的Qualys工程师协商

步骤1.配置Qualys扫描程序

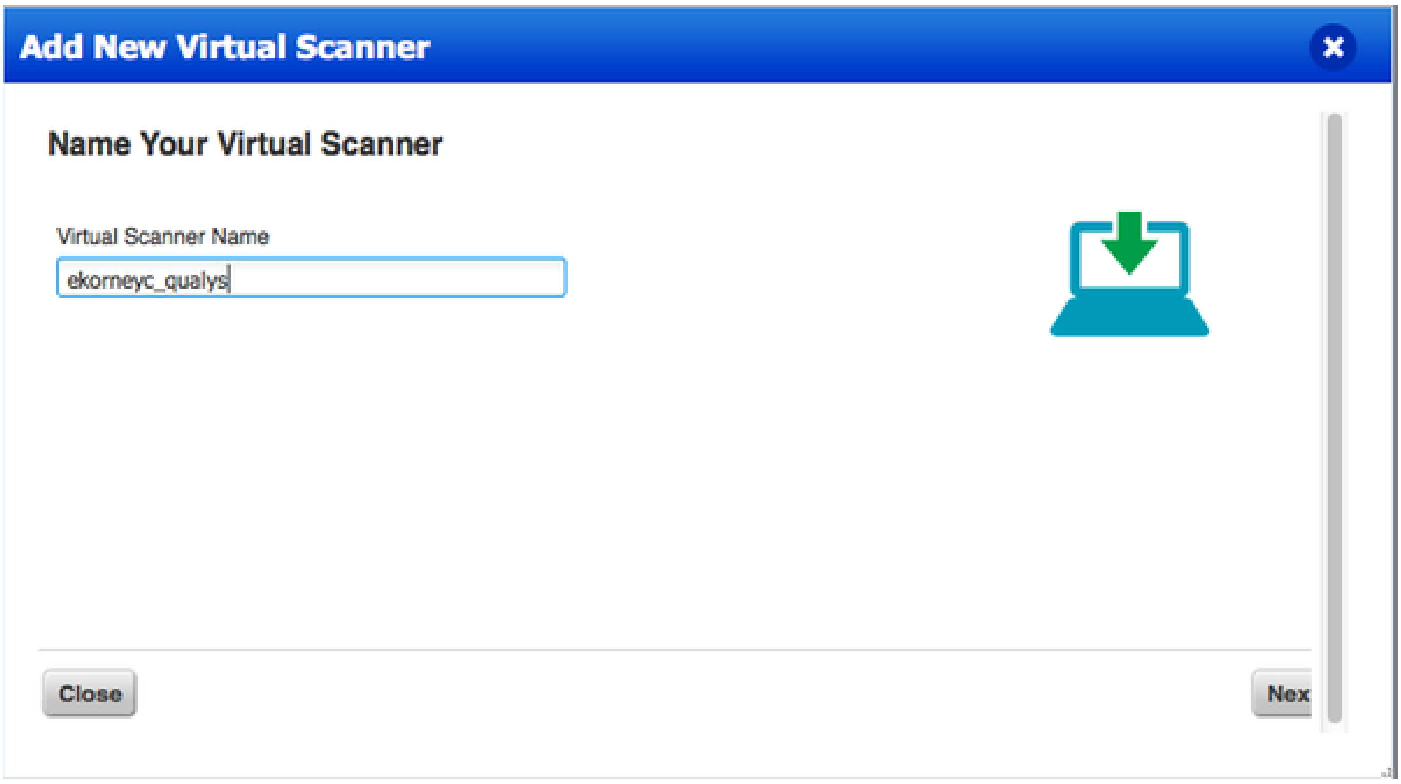
Qualys扫描程序可以从卵文件配置。登陆对Qualys网云并且连接对扫瞄>工具并且选择新>虚拟扫描程序工具



选择**仅下载镜像**并且选择适当的分配



要获得启动代码您可以去扫瞄>工具，并且选择新>虚拟扫描程序工具和选择**我有我的镜像**

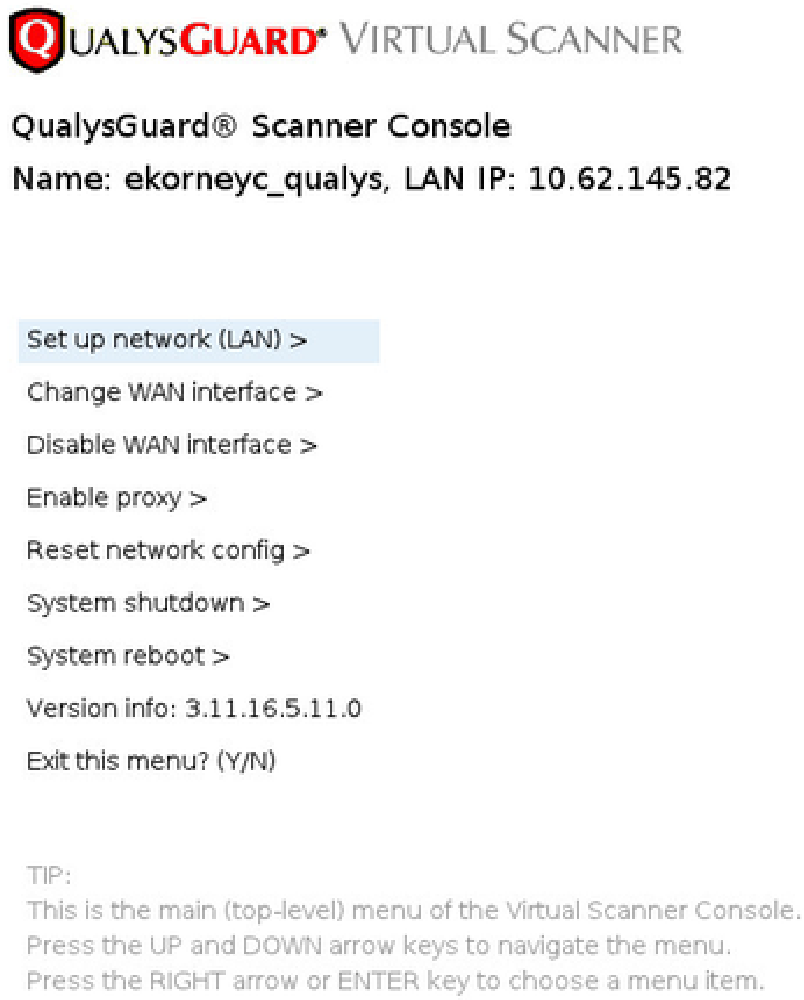


在输入扫描程序名字后产生您以后将使用您的授权码。

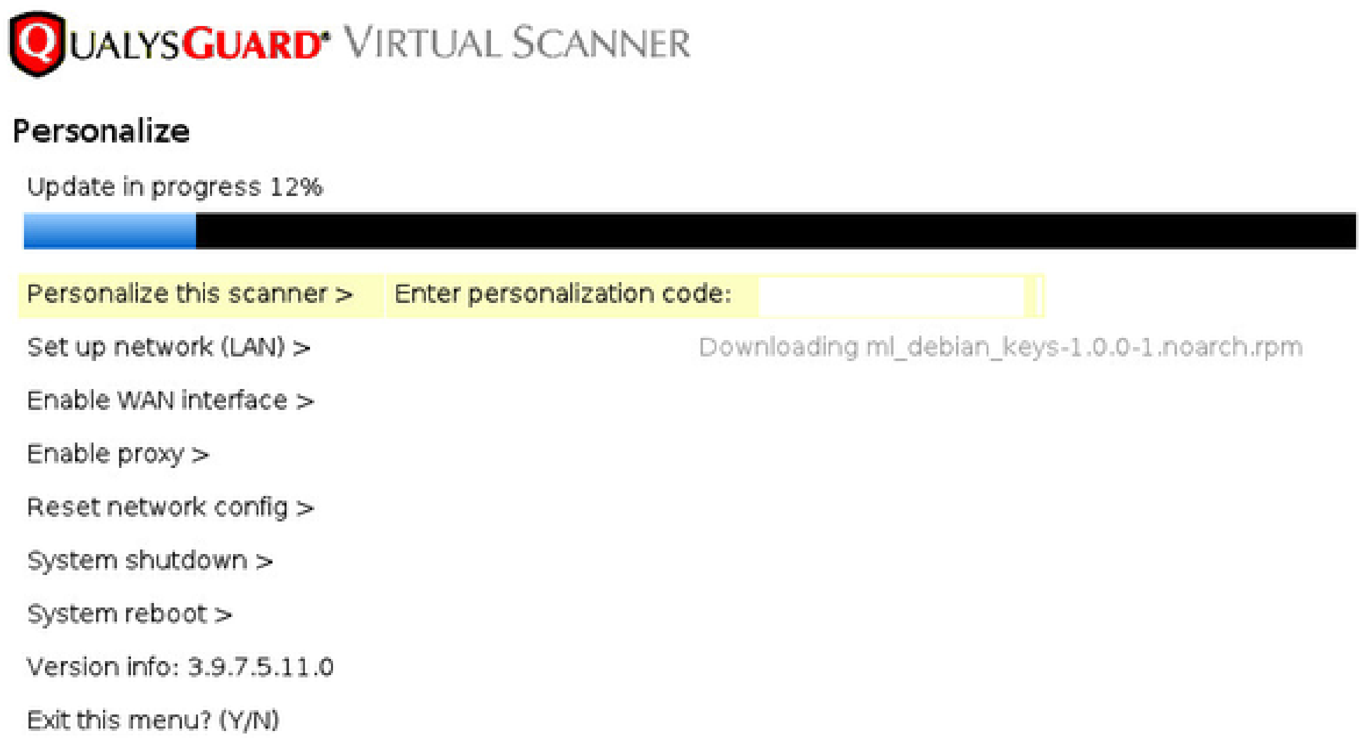
步骤2.配置Qualys扫描程序

配置在您的选择虚拟化平台的卵。一旦完成，请配置那些设置：

- 建立网络(LAN)
- 广域网接口设置(如果使用两个接口)
- 代理设置(如果使用代理)
- 个性化此扫描程序

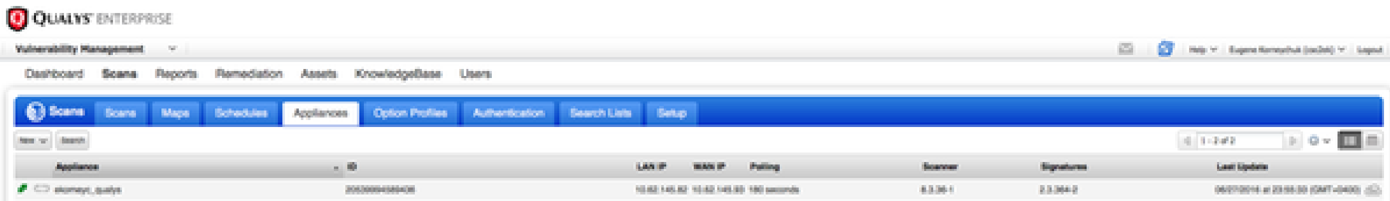


之后扫描程序连接到Qualys并且下载最新的软件和签名。



要验证扫描程序被连接您能连接到扫瞄>工具。

绿色在左边的被连接的符号表明扫描程序准备好，您能也看到LAN IP、广域网扫描程序的IP、版本和签名。

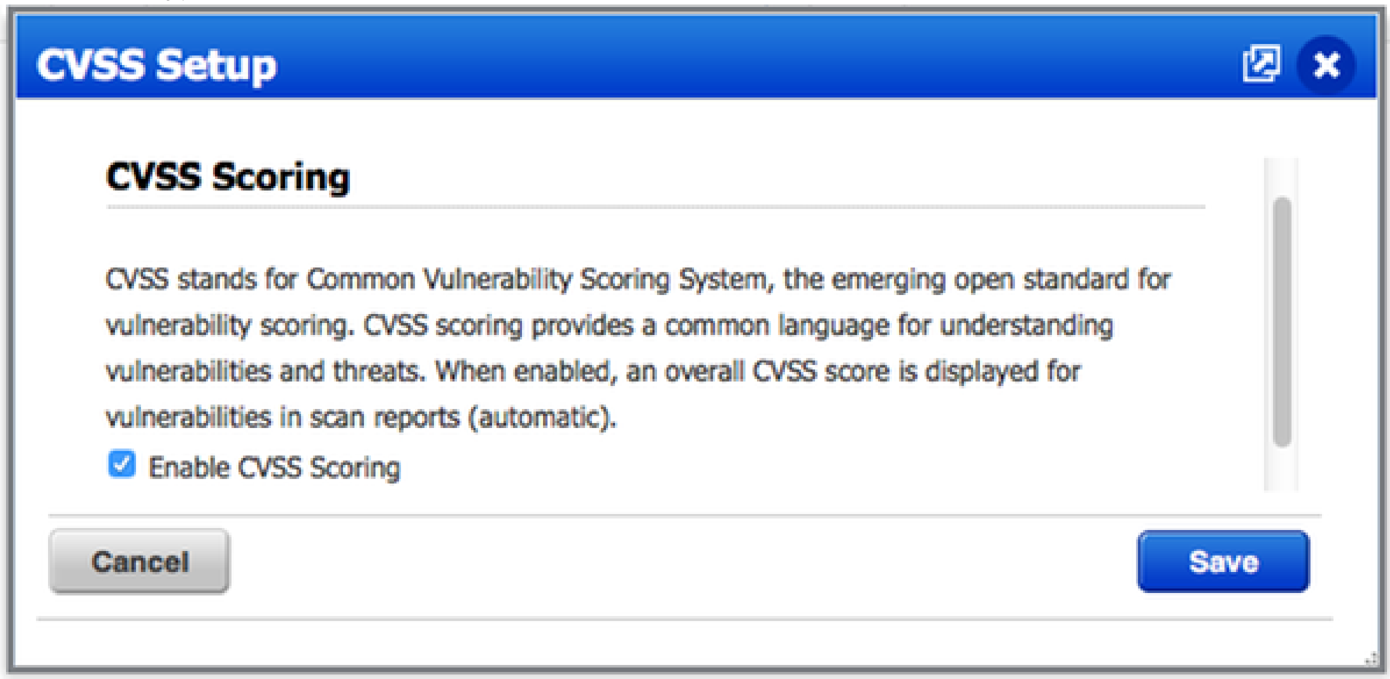


配置ISE

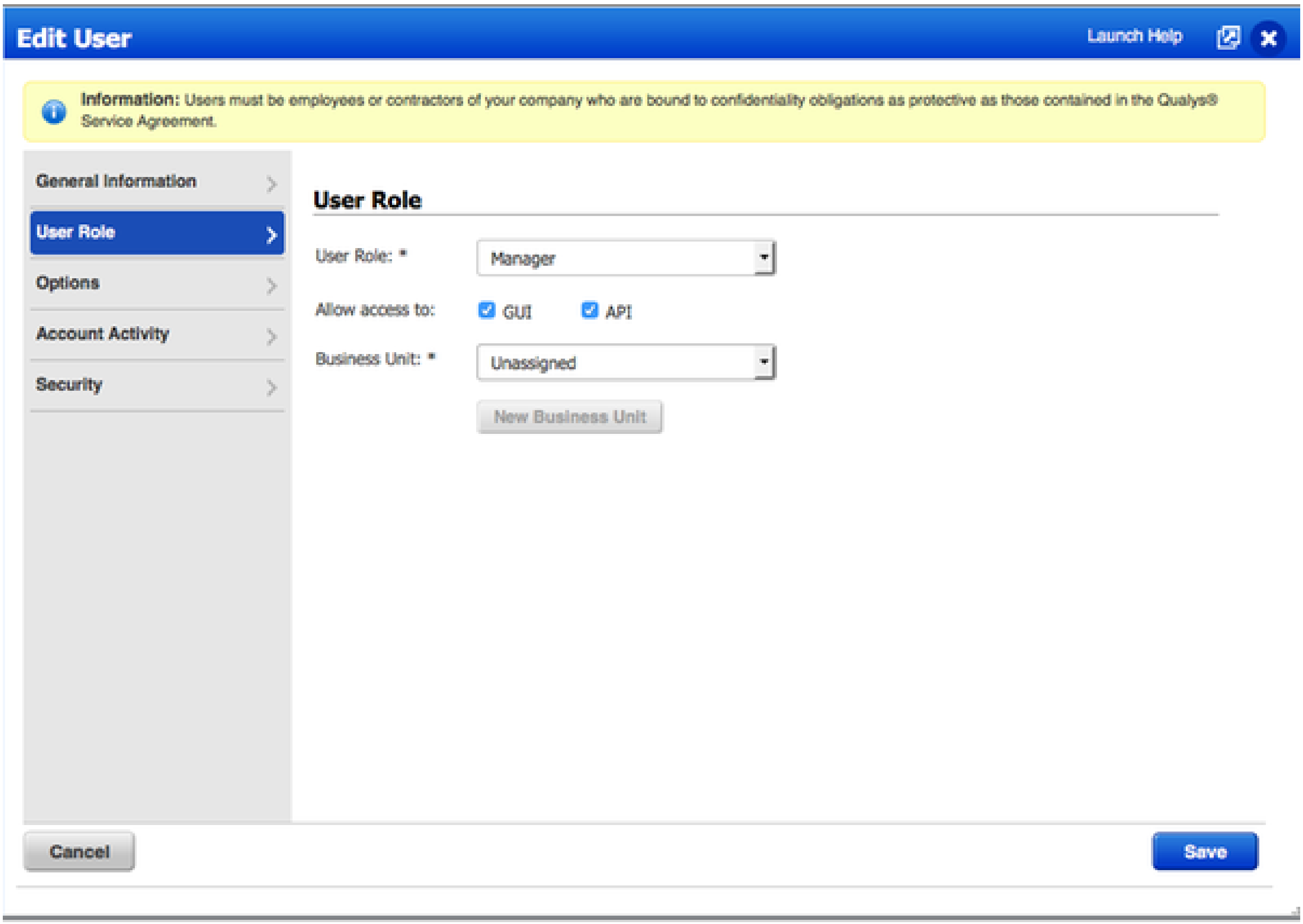
虽然您配置了Qualys扫描程序和Cloud，您必须仍然调整Cloud设置优良确定与ISE工作的集成。请注释，它应该执行，在您通过GUI前配置适配器，因为下载包含CVSS计分的信息库，在第一次后配置适配器。

步骤1.调整集成的Qualys Cloud设置与ISE

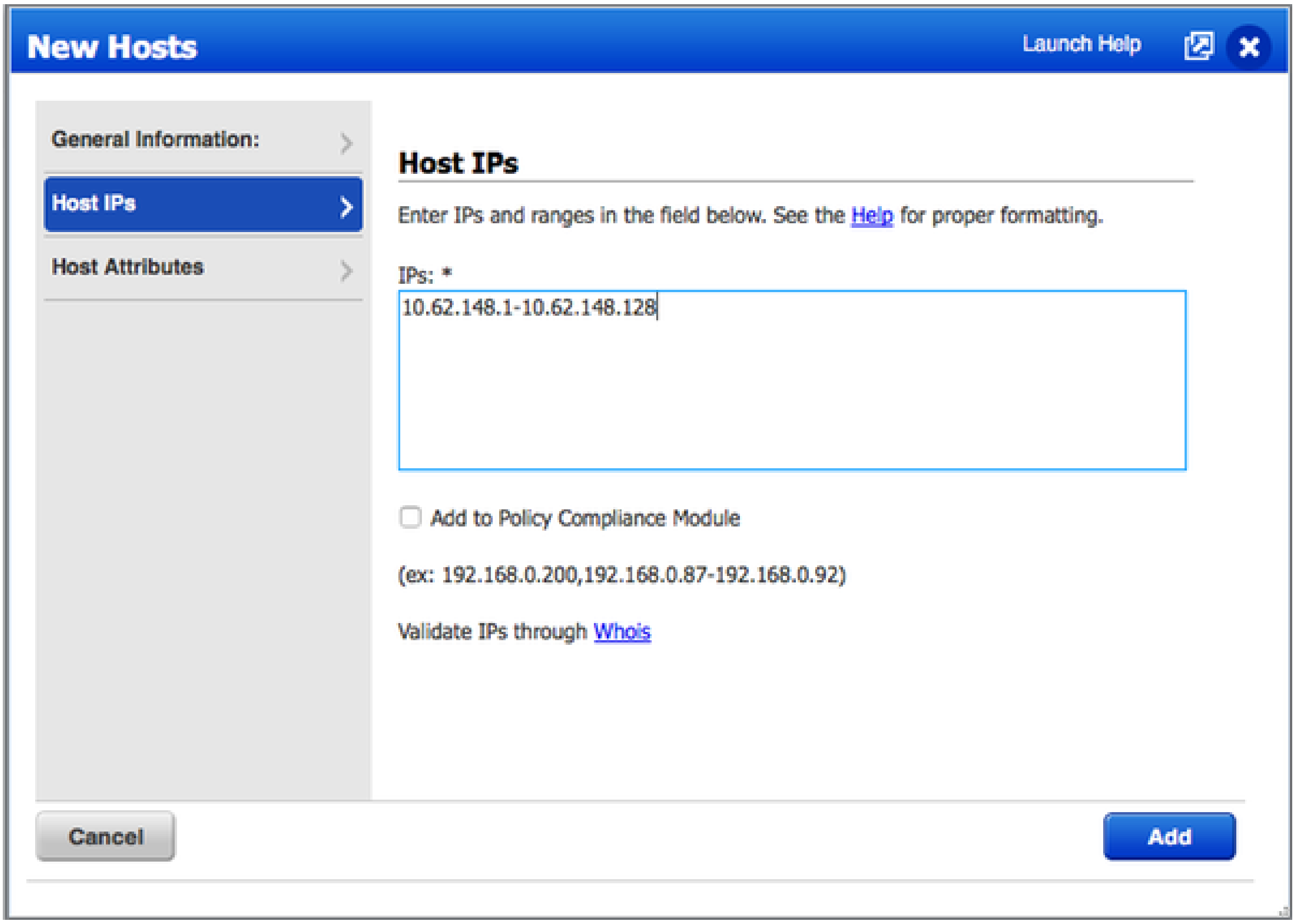
- 计分在弱点Management>报告的Enable (event) CVSS >设置> CVSS > Enable (event) CVSS计分



- 保证用于适配器配置的用户凭证有管理器权限。选择您的用户从左顶部角落并且点击**用户配置文件**。您应该有在**用户角色的**管理器权利。



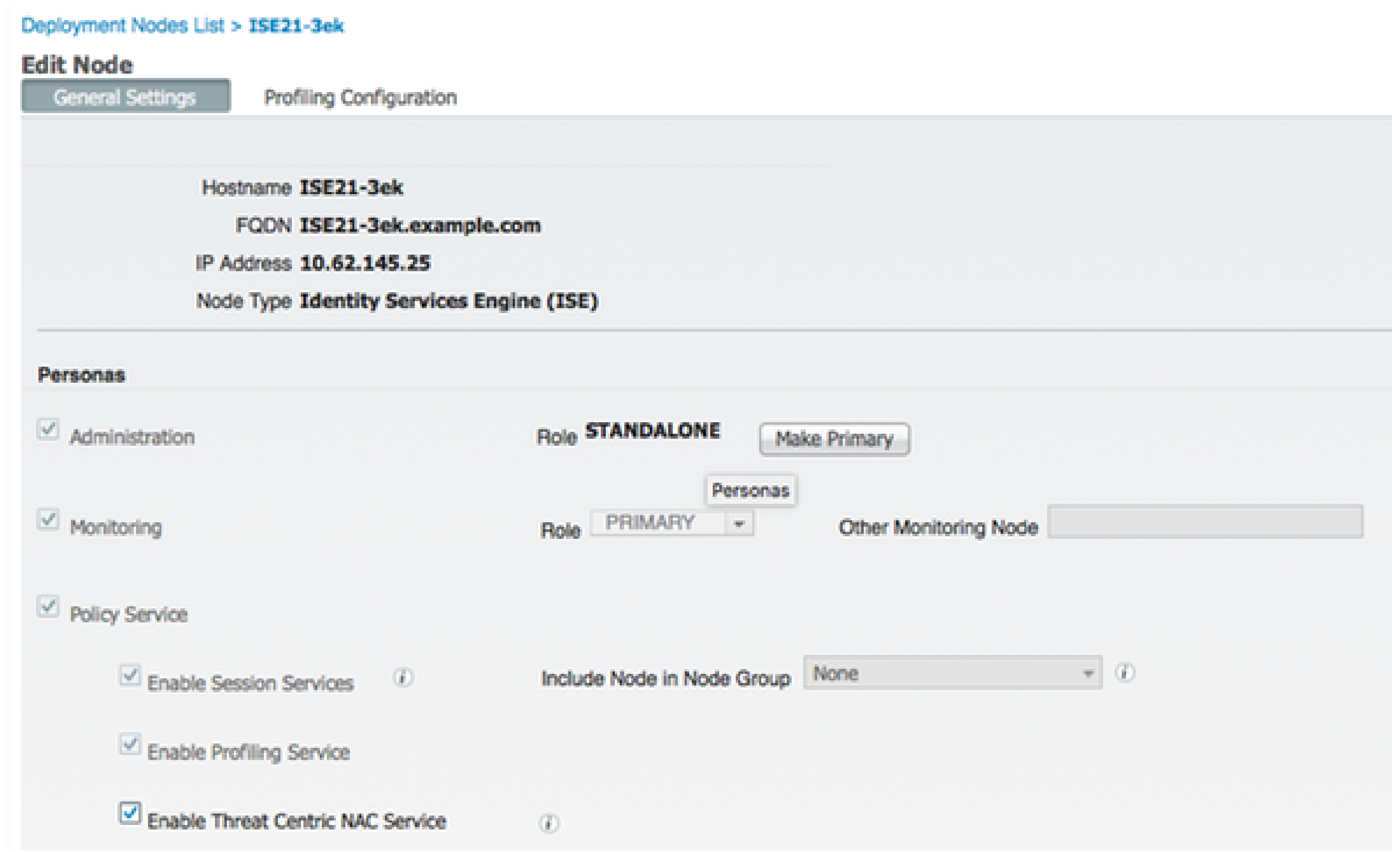
- 保证要求弱点评估终端的IP地址/子网被添加到在弱点Management>资产>主机资产>New > IP被跟踪的主机的Qualys



步骤2. Enable (event) TC-NAC服务

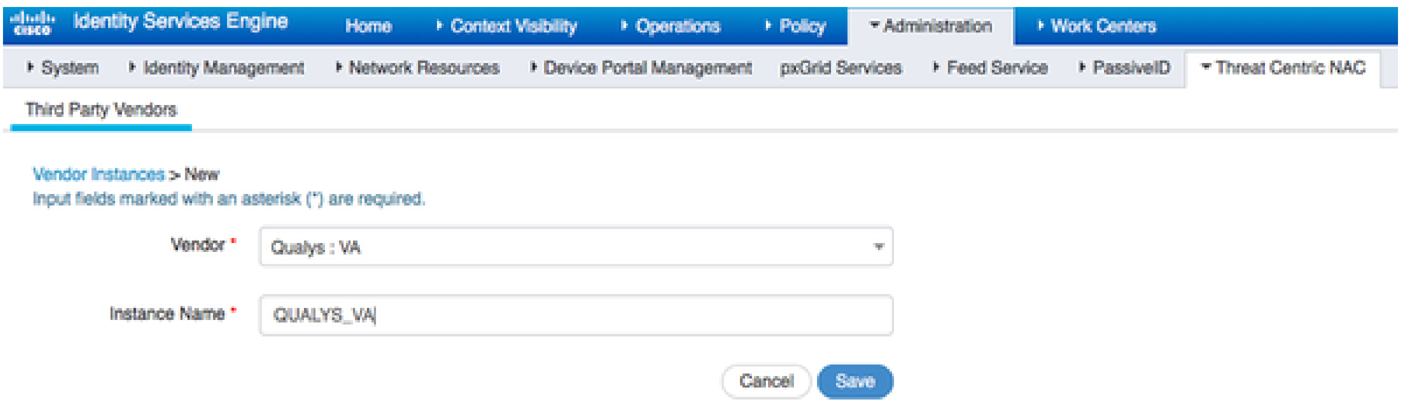
在Administration >配置> Edit下的Enable (event) TC-NAC服务节点。检查 **Enable (event)威胁中心NAC服务** 复选框。

Note:只可以有每配置一个TC-NAC节点。

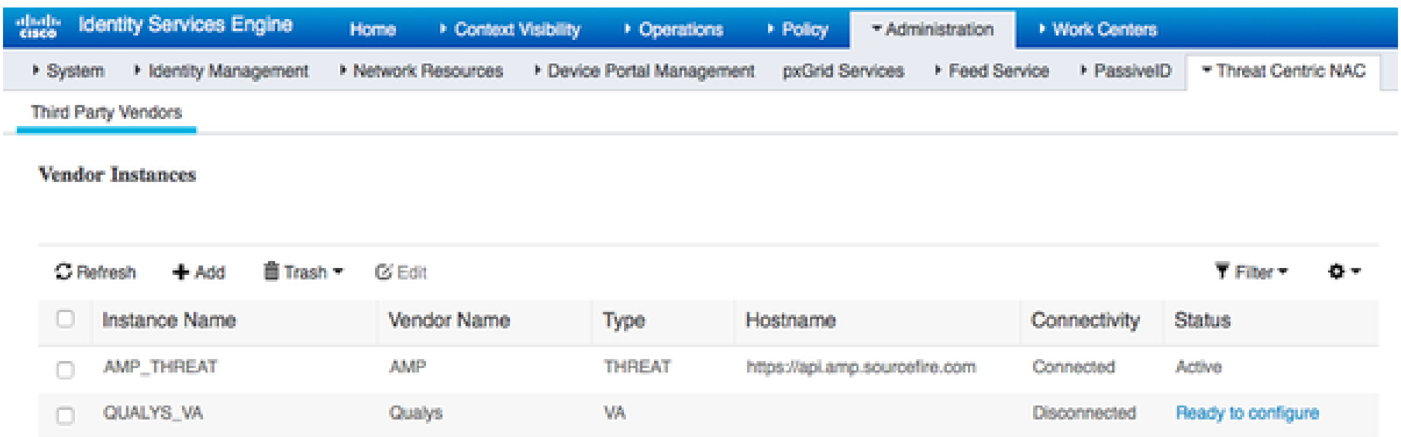


步骤3.配置Qualys适配器连接对ISE VA框架

连接对中心的Administration >的威胁NAC >第三方供应商>Add。点击**“Save”**。

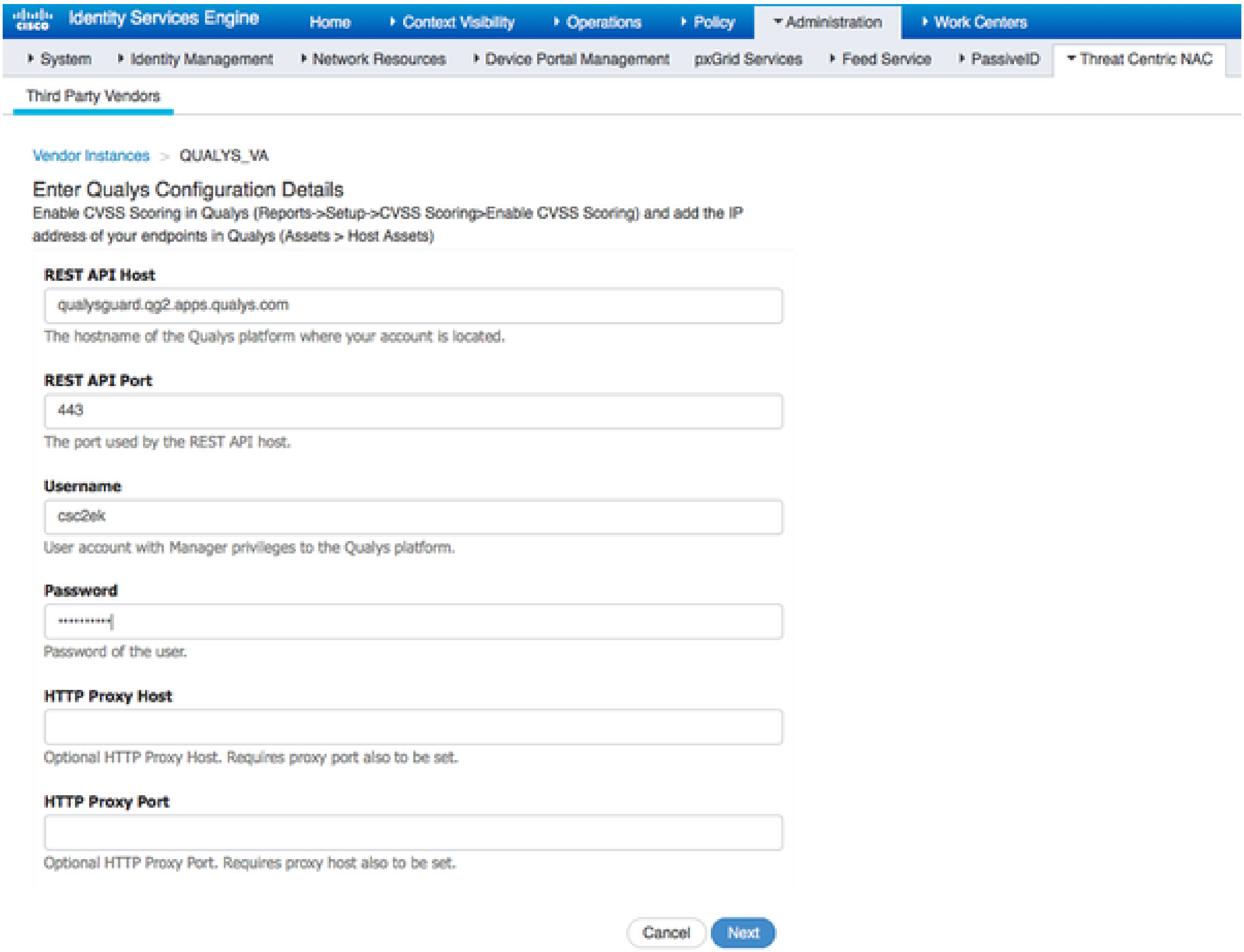


当Qualys实例过渡**准备配置**状态，请点击**准备好配置**在状态的选项。

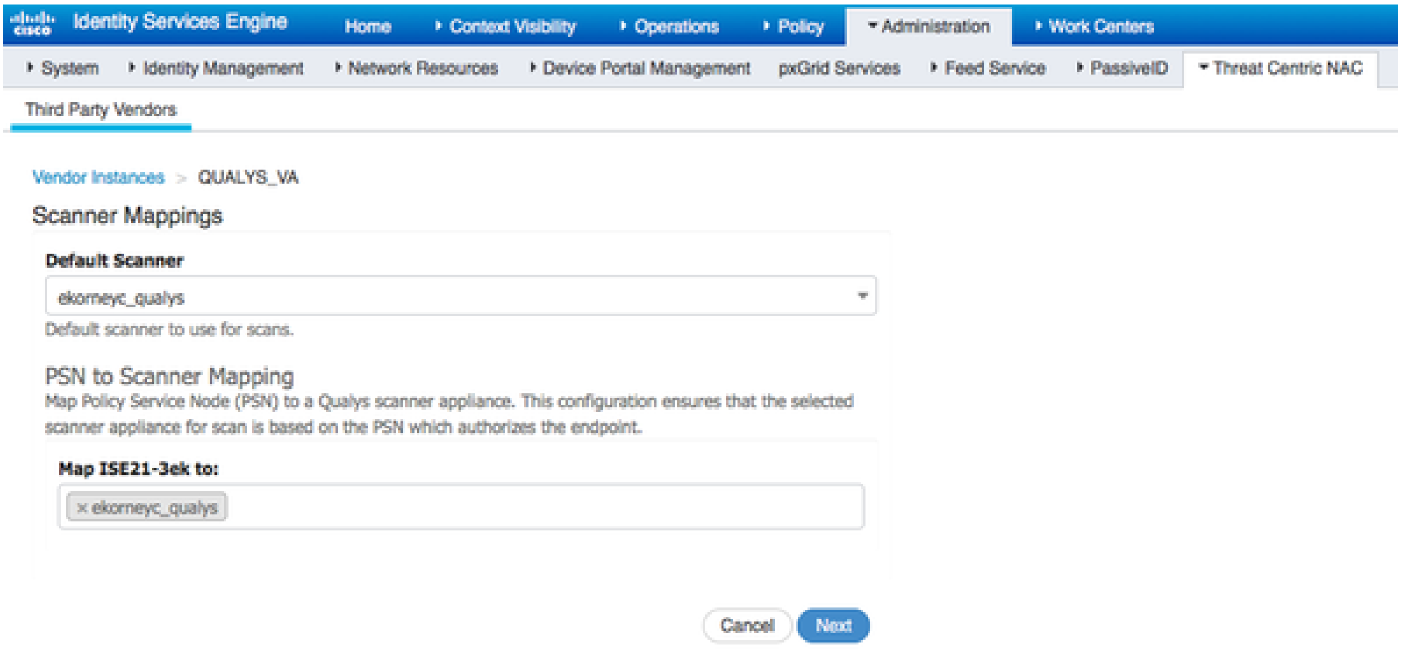


其余API主机应该是您使用Qualys Cloud，找出您的帐户的那个。在本例中-qualysguard.qg2.apps.qualys.com

帐户应该是那个有管理器权限，**其次**点击。

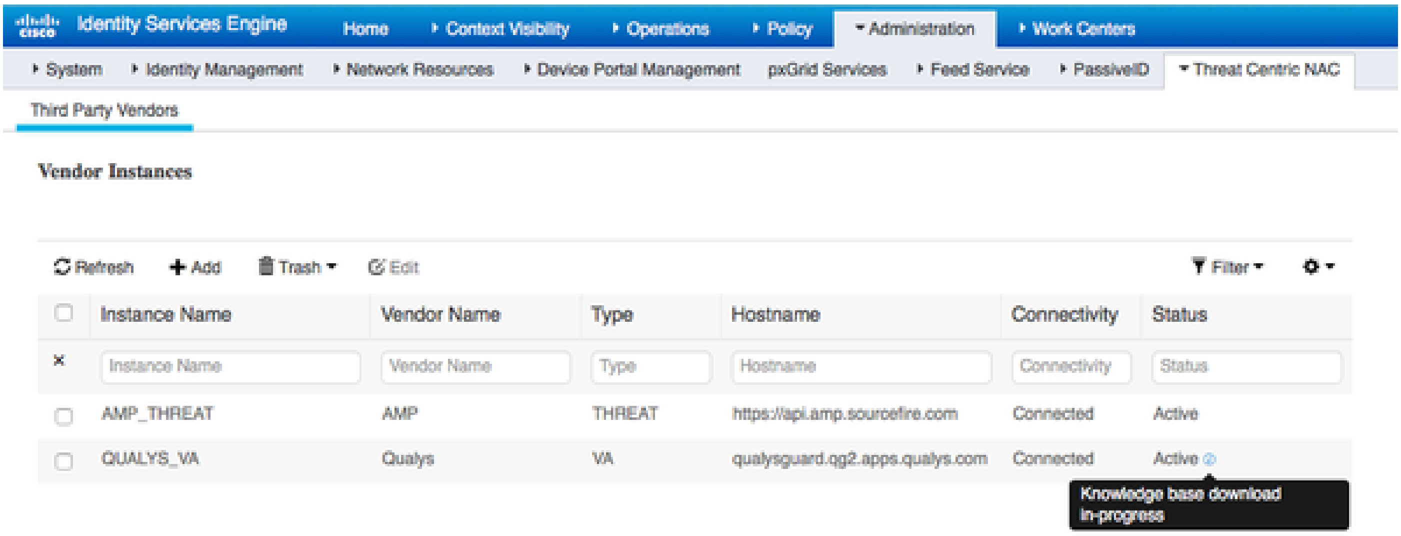


ISE下载关于被连接到Qualys Cloud的扫描程序的信息，您能配置PSN到在此页的扫描程序映射。它保证核准终端的所选的扫描程序根据PSN被选择。



先进的设置是有大量文件证明的在ISE 2.1管理指南，链路可以在本文的References部分找到。**其次**点击并且**完成**。Qualys对激活状态和知识库下载的实例转变开始。

Note:只可以有每配置一个Qualys实例。



步骤4.配置授权配置文件触发VA扫描

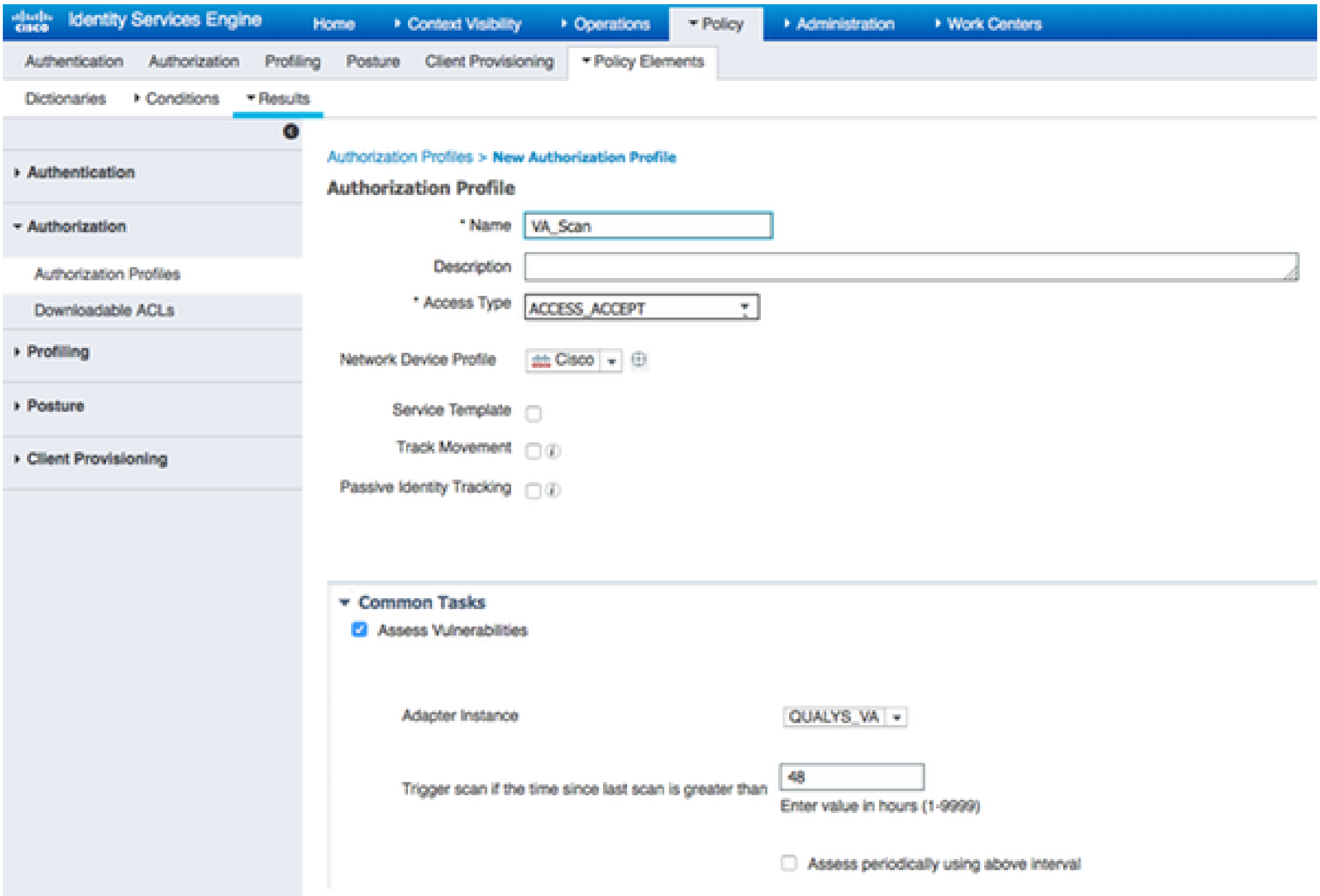
连接对策略>Policy元素>结果>授权>授权配置文件。添加新配置文件。在**普通的任务下请**选择**弱点评估**复选框。
应该根据您的网络设计选择根据要求scan interval。

授权配置文件包含那些AV对：

cisco-av-pair = on-demand-scan-interval=48
cisco-av-pair = periodic-scan-enabled=0
cisco-av-pair = va-adapter-instance=796440b7-09b5-4f3b-b611-199fb81a4b99

他们被发送到在访问接受信息包内的网络设备，虽然真正目的他们将告诉应该触发扫描的MNT节点

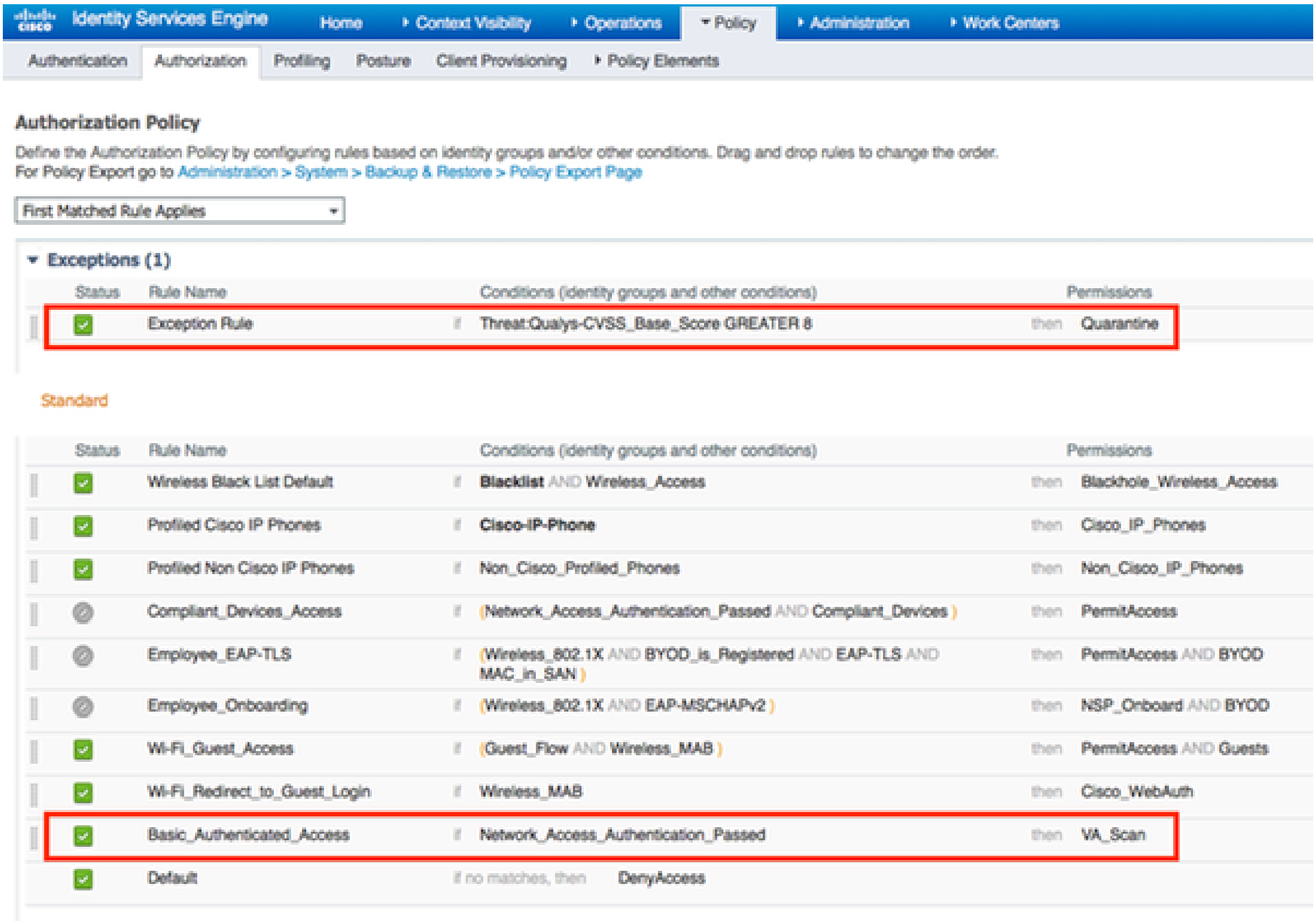
。MNT指示TC-NAC节点与Qualys Cloud联络。



步骤5.配置授权策略

- 配置授权策略使用被配置的新的授权配置文件在第4.步连接对策略>授权>授权策略，找出**Basic_Authenticated_Access**规则并且点击**Edit**。从**PermitAccess**更改权限到新建立的**标准的VA_Scan**。这导致所有用户的一弱点扫描。点击**“Save”**。

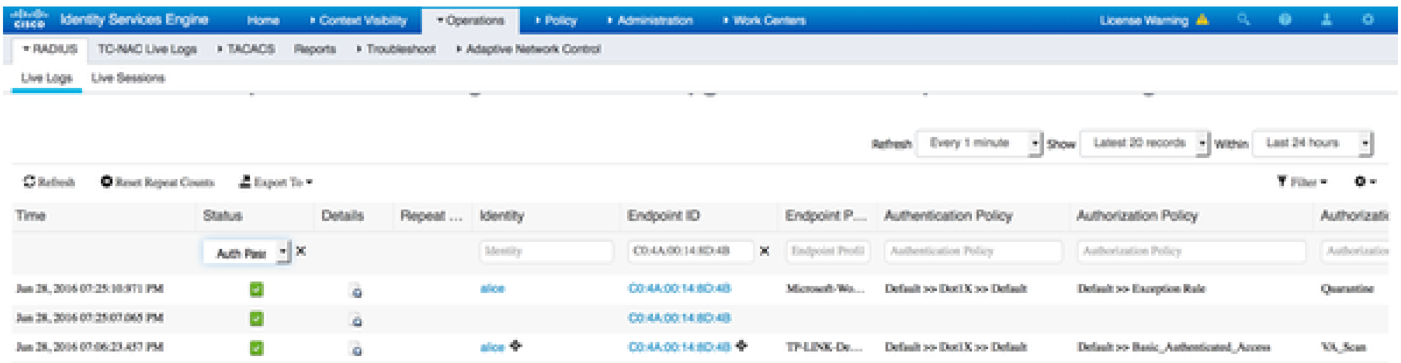
- 创建Quarantined机器的授权策略。连接对策略>授权>授权策略>例外并且创建**例外规则**。点击情况>创造新的条件(Advanced选项) >选择属性，把并且选择**威胁移下来**。扩展**威胁**属性并且选择**Qualys-CVSS_Base_Score**。更改运算符到**极大比**并且根据您的安全策略输入值。**检疫**授权配置文件应该产生有限享用易受攻击机器。



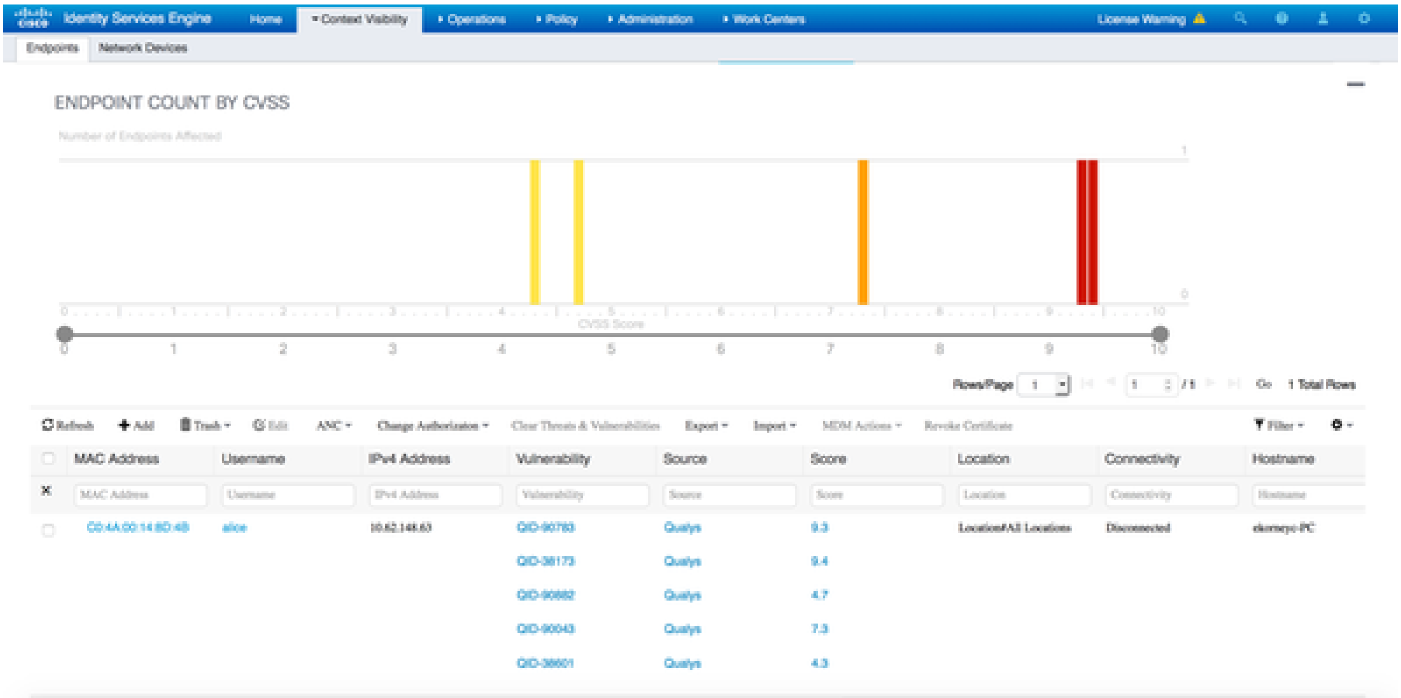
Verify

身份服务引擎

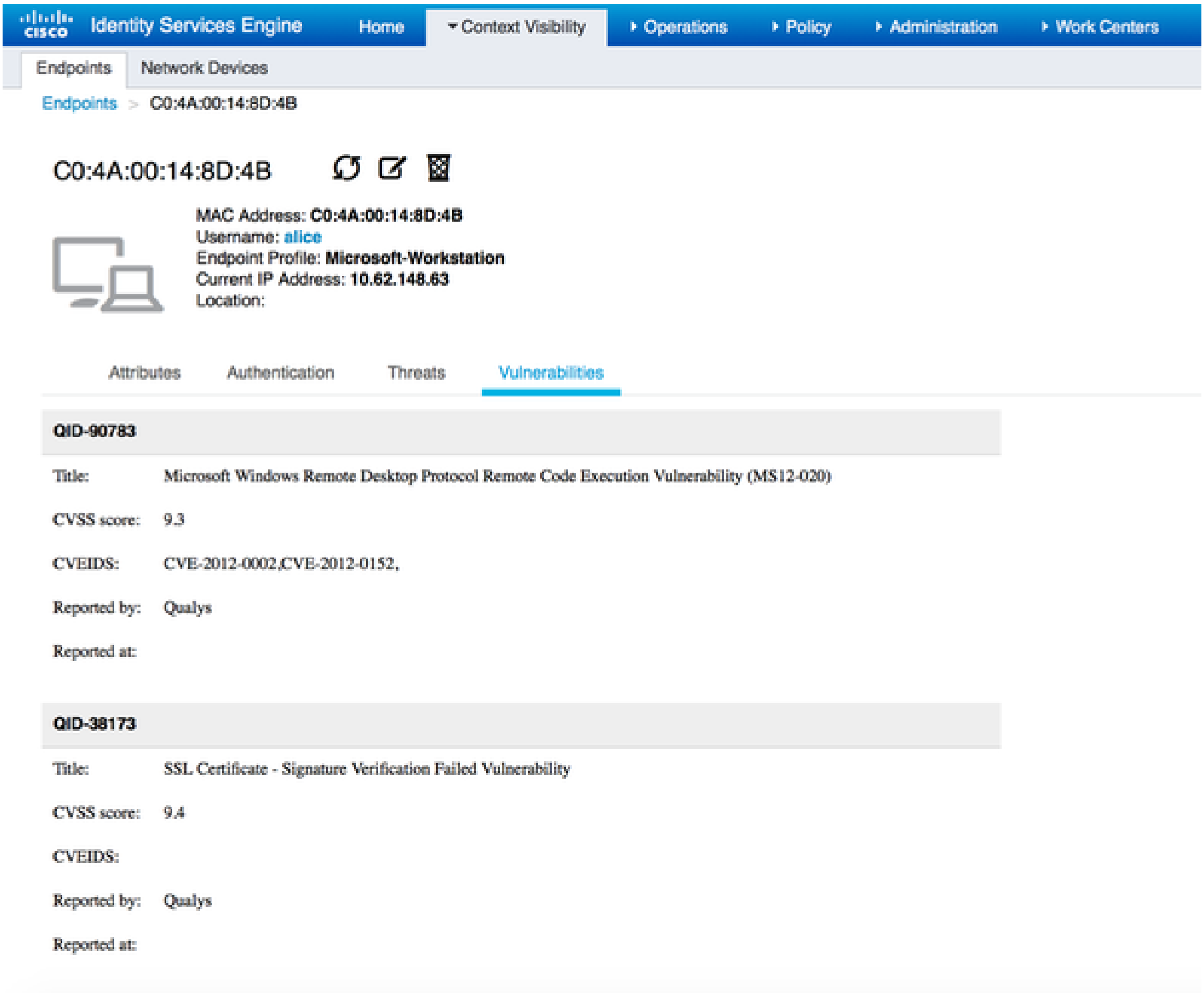
第一个连接触发VA扫描。当扫描完成时， CoA再验证被触发运用新的策略，如果被匹配。



为了验证发现了哪些弱点，请连接对上下文公开性>终端。每终端弱点检查与评分产生它由Qualys。



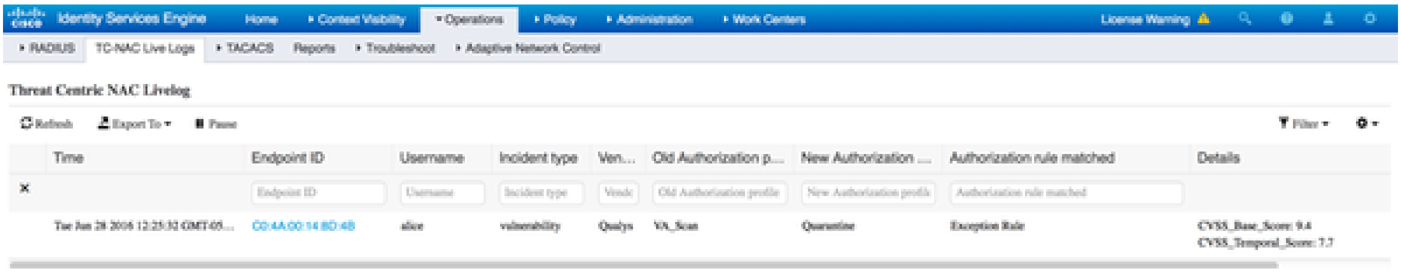
当选择特定的终端时，关于每个弱点的更多详细资料出现，包括**标题**和CVEID。



在操作> TC-NAC中居住日志，您能看到老与在CVSS_Base_Score的策略被运用的新的授权和详细

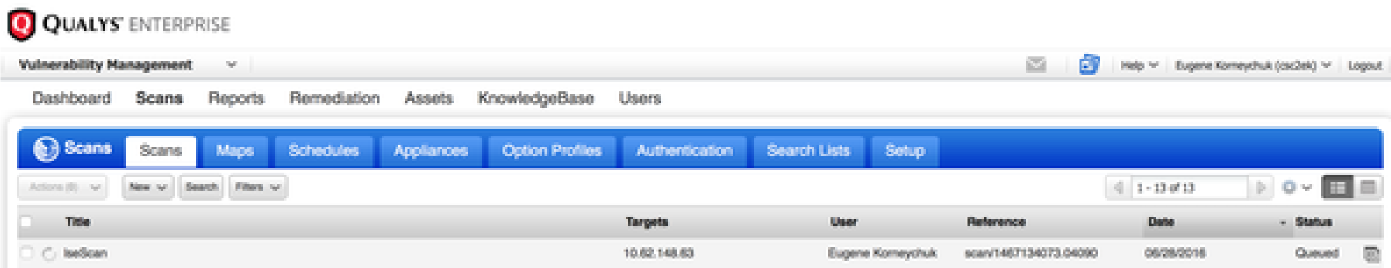
资料。

Note:授权情况根据CVSS_Base_Score完成，等于在终端发现的最高的弱点评分。

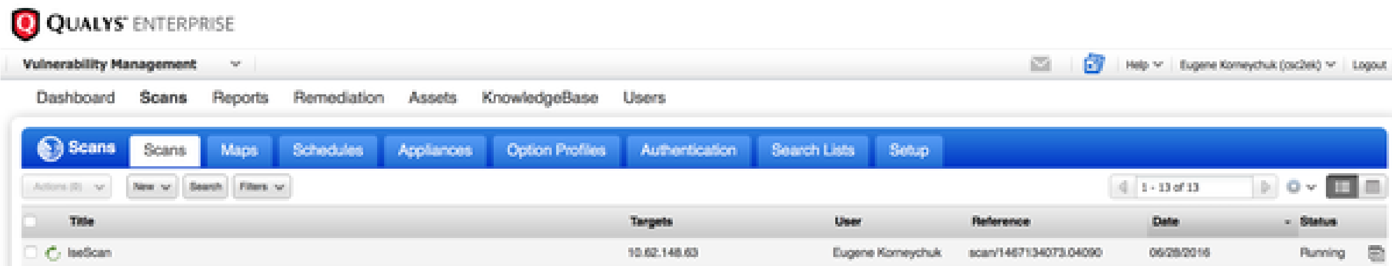


Qualys Cloud

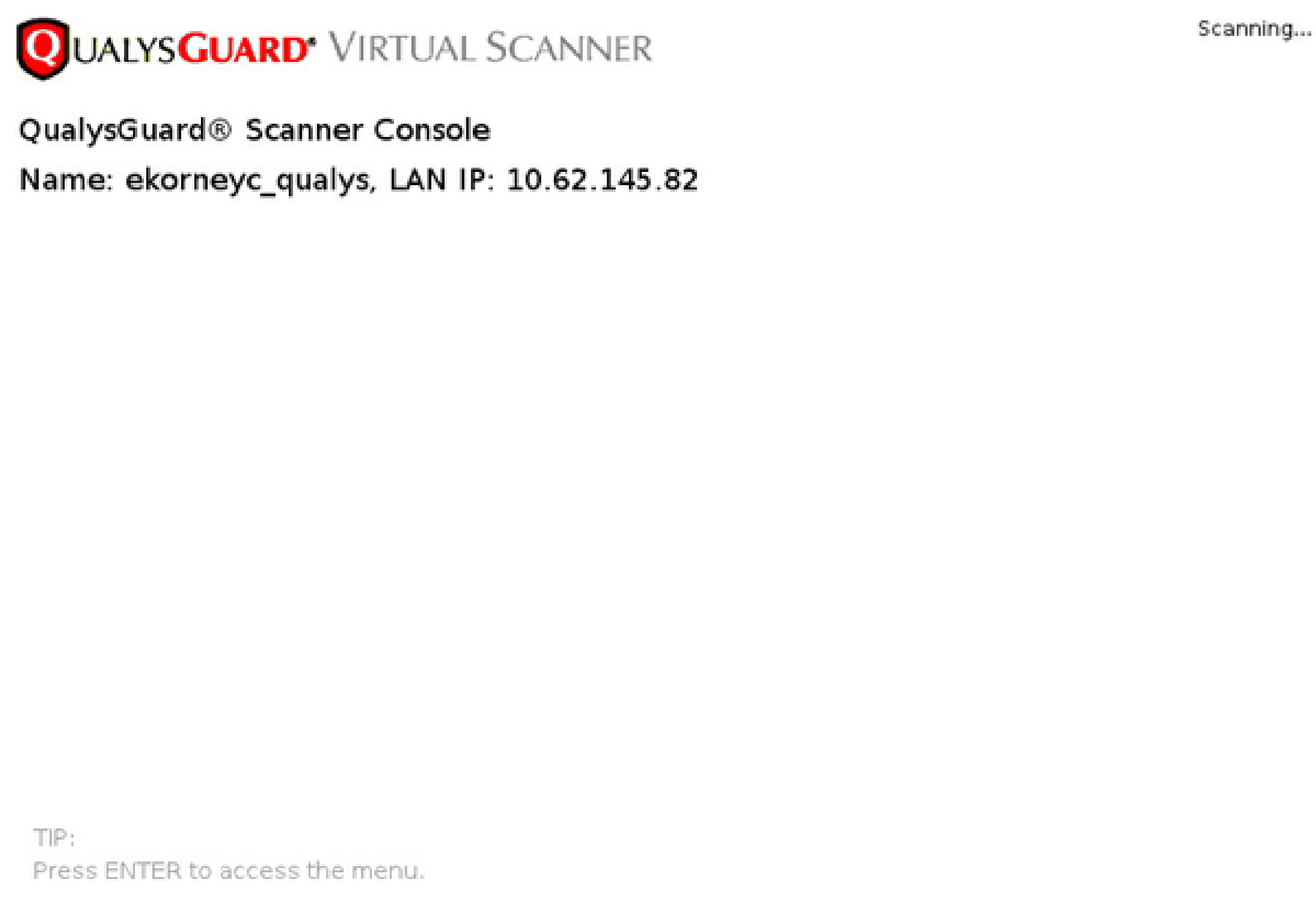
当VA扫描由TC-NAC Qualys时触发排队扫描，它能查看在扫瞄>扫瞄



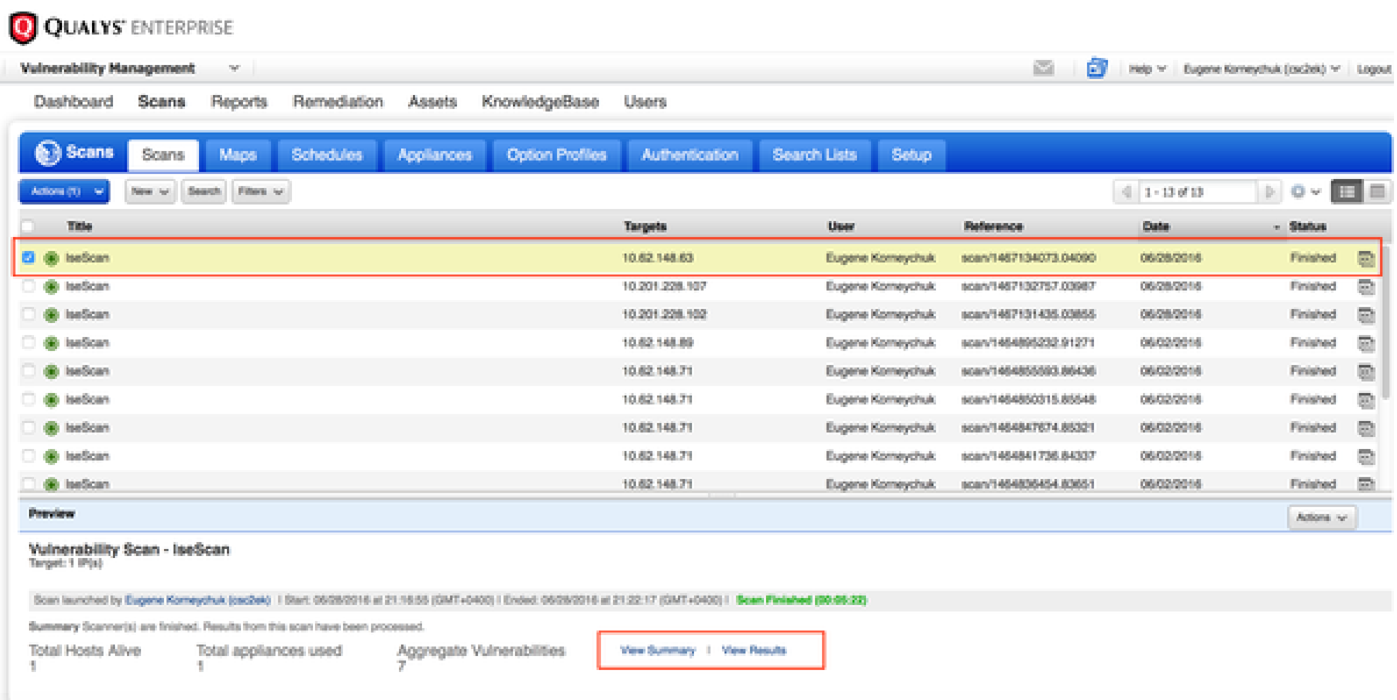
之后它过渡了到运行，意味着Qualys网云指示Qualys扫描程序进行实际扫描



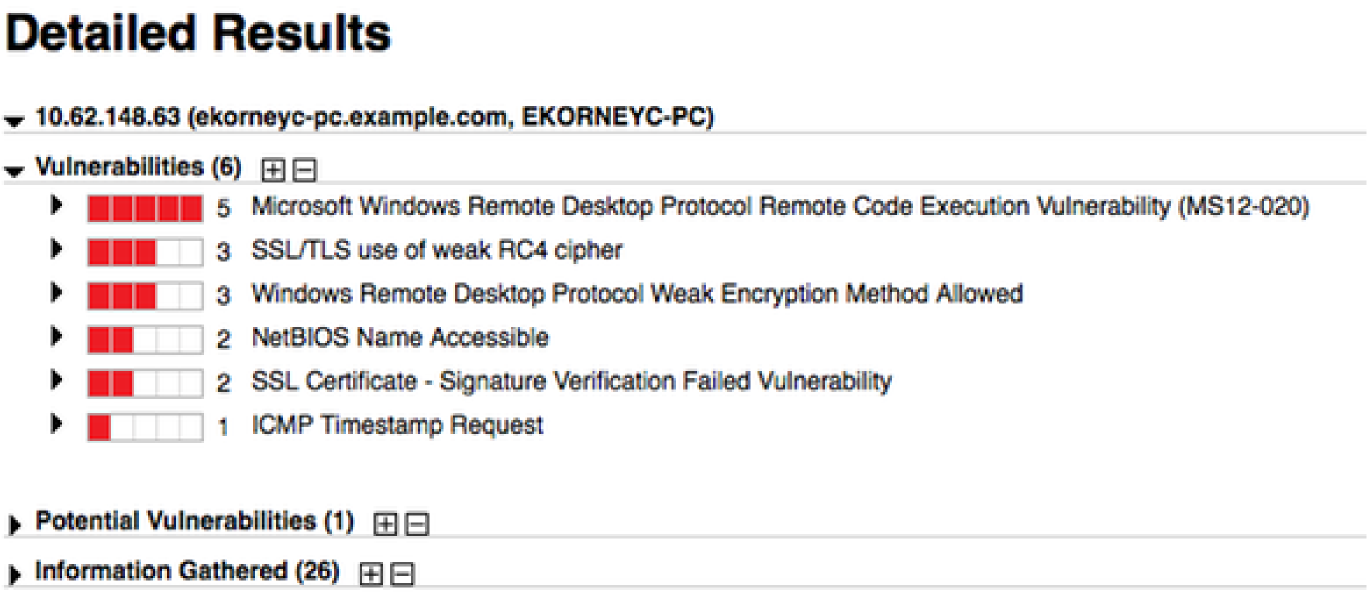
当扫描程序执行扫描时，您应该看到“扫描…”在Qualys卫兵的右上角符号



一旦扫描执行过渡了到完成陈述。您能查看结果在扫瞄>扫瞄，挑选必需的扫描和点击**视图汇总**或**视图结果**。



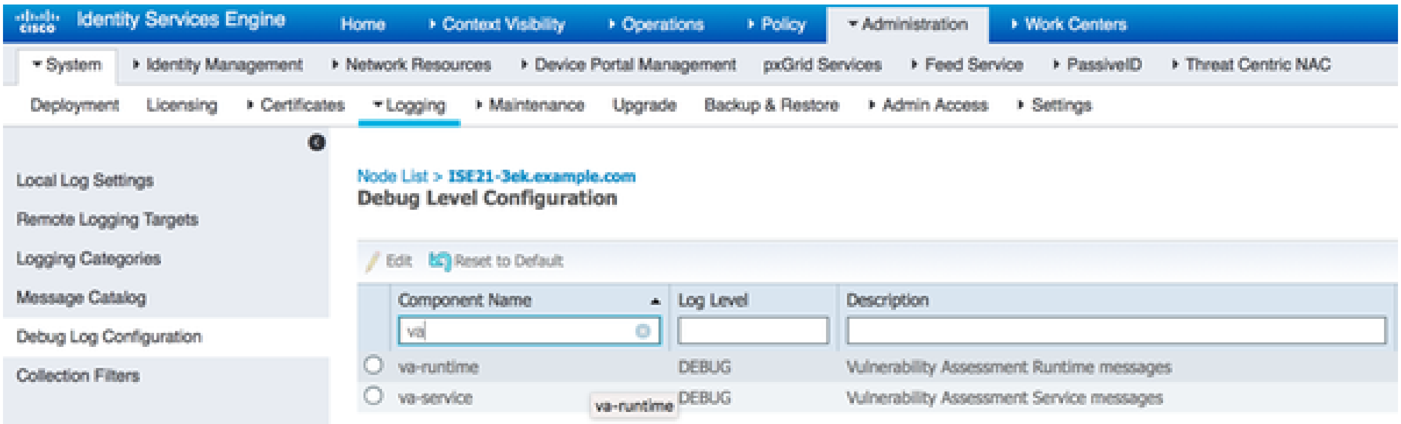
在报告您能看到**详细的结果**，被发现的弱点显示。



Troubleshoot

在ISE的调试

为了在ISE的关闭调试连接对管理>System >记录>调试日志配置，挑选TC-NAC节点并且更改**日志级别VA运行时间**和VA**服务**组件**调试**



将被检查的日志- varuntime.log。您能直接地从ISE CLI盯梢它：

```
ISE21-3ek/admin# show loggingvaruntime.log
```

TC-NAC码头工人接收的指令执行特定的终端的扫描。

```
2016-06-28 19:06:30,823[Thread-70][] va.runtime.admin.mnt.EndpointFileReader -      - VA VA
[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScan
Enabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
199fb81a4b99","psnHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}]
2016-06-28 19:06:30,824[Thread-70][] va.runtime.admin.vaservice.VaServiceRemotingHandler -      -
VA Mnt
{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScanE
nabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
199fb81a4b99","psnHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}
```

一旦结果收到在上下文目录存储所有弱点数据。

```
2016-06-28 19:25:02,020[pool-311-thread-8][] va.runtime.admin.vaservice.VaServiceMessageListener
-     -VaService
[{"macAddress":"C0:4A:00:14:8D:4B","ipAddress":"10.62.148.63","lastScanTime":1467134394000,"vulnerabilities":["{\"vulnerabilityId\":\"QID-90783\",\"cveIds\":\"CVE-2012-0002,CVE-2012-0152,\",\"cvssBaseScore\":\"9.3\",\"cvssTemporalScore\":\"7.7\",\"vulnerabilityTitle\":\"Microsoft Windows(MS12-020)\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-38173\",\"cveIds\":\"\",\"cvssBaseScore\":\"9.4\",\"cvssTemporalScore\":\"6.9\",\"vulnerabilityTitle\":\"SSL-Vulnerability\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-90882\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.7\",\"cvssTemporalScore\":\"4\",\"vulnerabilityTitle\":\"WindowsAllowed\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"vulnerabilityTitle\":\"SMBRequired\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-38601\",\"cveIds\":\"CVE-2013-2566,CVE-2015-2808,\",\"cvssBaseScore\":\"4.3\",\"cvssTemporalScore\":\"3.7\",\"vulnerabilityTitle\":\"SSL/TLSRC4SMB \” \ “vulnerabilityVendor \” \ “Qualys \ “}”]}]
2016-06-28 19:25:02,127[pool-311-thread-8][] va.runtime.admin.vaservice.VaServiceMessageListener
-     - VA db lastscantime 1467134394000 mac C0:4A:00:14:8D:4B
2016-06-28 19:25:02,268[pool-311-thread-8][] va.runtime.admin.vaservice.VaAdminServiceContext -
   - VA jsonPRI LAN
2016-06-28 19:25:02,272[pool-311-thread-8][] va.runtime.admin.vaservice.VaPanRemotingHandler -
  - VA {C0:4A:00:14:8D:4B=[{"vulnerabilityId":"QID-90783","cveIds":"CVE-2012-0002,CVE-2012-0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft Windows (MS12-020)","vulnerabilityVendor":"Qualys"} {"vulnerabilityId":"QID-38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL-”
“vulnerabilityVendor” “Qualys”}{"vulnerabilityId":"QID-90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows”
“vulnerabilityVendor” “Qualys”} {"vulnerabilityId":"QID-90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMBSMB”
“vulnerabilityVendor” “Qualys”} {"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLSRC4”
“vulnerabilityVendor” “Qualys”}]}
```

将被检查的日志- vaservice.log。您能直接地从ISE CLI盯梢它：

```
ISE21-3ek/admin# show loggingvaservice.log
```

弱点评估请求被提交给适配器

```
2016-06-28 17:07:13,200[endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil -     -
VA SendSyslog systemMsg
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-NAC.ServiceName","Vulnerability” “TCNAC.Status” “VA” “TCNAC.Details” “VAprocessing","TC-NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IpAddress","10.62.148.63","TC-NAC.AdapterInstanceUuid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

AdapterMessageListener检查每5分钟扫描的状态，直到完成。

```
2016-06-28 17:09:43,459[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number 100"}
2016-06-28 17:14:43,760[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number 001"}
```

```
2016-06-28 17:19:43,837[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number 001"}
2016-06-28 17:24:43,867[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number 001"}
```

适配器是获得QID， CVE'S与CVSS评分一起

```
2016-06-28 17:24:57,556[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
{"requestedMacAddress":"C0:4A:00:14:8D:4B","scanStatus":"ASSESSMENT_SUCCESS","lastScanTimeLong":
1467134394000,"ipAddress":"10.62.148.63","vulnerabilities":[{"vulnerabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL-
Vulnerability","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
Required","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-90783","cveIds":"CVE-2012-
0002,CVE-2012-
0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft Windows(
RC4cipher","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
MS12-020)","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-
2566,CVE-2015-
2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLSSMB”
“vulnerabilityVendor” “Qualys"}]}
2016-06-28 17:25:01,282 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -IRF
{"C0:4A:00:14:8D:4B":[{"vulnerability":{"CVSS_Base_Score":9.4,"CVSS_Temporal_Score":7.7},"time-
stamp":1467134394000,"title":"Vulnerability","vendor":"Qualys"}]}
2016-06-28 17:25:01,853[endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -     -
VA SendSyslog systemMsg
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability” “TCNAC.Status” “VA” “TCNAC.Details” “VA;5","TC-
NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IpAddress","10.62.148.63","TC-
NAC.AdapterInstanceUuid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-
NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

典型的问题

问题1. ISE获得与CVSS_Base_Score 0.0和CVSS_Temporal_Score的弱点报告0.0，而Qualys Cloud报告包含被发现的弱点。

问题：

当检查从Qualys您能看到时的Cloud的报告发现了弱点，然而在ISE您看不到他们。

在vaservice.log看到的调试：

```
2016-06-02 08:30:10,323 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -IRF
{"C0:4A:00:15:75:C8":[{"vulnerability":{"CVSS_Base_Score":0.0,"CVSS_Temporal_Score":0.0},"time-
stamp":1464855905000,"title":"Vulnerability","vendor":"Qualys"}]}
```

解决方案：

是cvss的评分的原因零是二者之一没有弱点或cvss计分未在Qualys Cloud被启用，在您通过UI前配置适配器。包含cvss的信息库，在配置适配器第一次后，计分被启用的功能下载。您在ISE必须保

证CVSS计分是启用的前面，适配器实例被创建了。它可以执行在弱点Management>报告下>设置> CVSS > Enable (event) CVSS计分

问题2. ISE从Qualys Cloud不取得结果回到，即使正确的授权策略被击中了。

问题：

被更正的授权策略被匹配了，如果请触发VA扫描。尽管该事实扫描没有执行。

在vaservice.log看到的调试：

```
2016-06-28 16:19:15,401[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
(Body:'[B@6da5e620(byte[311])'MessageProperties [headers= {} timestamp=nullmessageId=null
userId=nullappId=nullclusterId=nulltype=nullcorrelationId=null replyTo=null
contentType=application/octet-stream contentEncoding=null contentLength=0
deliveryMode=PERSISTENT expiration=null priority=0 redelivered=false
receivedExchange=irf.topic.va-reports receivedRoutingKey= deliveryTag=9830 messageCount=0])
2016-06-28 16:19:15,401[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -
{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"Error
trigeringon1904IPscanning.","lastScanTimeLong":0,"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15,771[SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -     -Macaddress:24:77:03:3D:CF:20 IP
Address(DB) 10.201.228.102
2016-06-28 16:19:16,336[endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -     -
VA SendSyslog systemMsg
[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability" "TCNAC.Status" "VA" "TCNAC.Details" "trigering1904IP
scanning.","TC-NAC.MACAddress","24:77:03:3D:CF:20","TC-NAC.IpAddress","10.201.228.102","TC-
NAC.AdapterInstanceUuid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-
NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

解决方案：

Qualys Cloud表明终端的IP地址没有资格扫描，请保证您添加了终端的IP地址到弱点Management>资产>主机资产>New > IP被跟踪主机

参考

- 思科身份服务引擎管理员指南，版本2.1
- Technical Support & Documentation - Cisco Systems
- 视频：与Qualys的ISE 2.1
- Qualys文档