使用Qualys配置ISE 2.1以威脅為中心的NAC(TC-NAC)

目錄

簡介

本文檔介紹如何使用身份服務引擎(ISE)2.1上的Qualys配置以威脅為中心的NAC。威脅中心網路訪問控制(TC-NAC)功能允許您根據從威脅和漏洞介面卡接收的威脅和漏洞屬性建立授權策略。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 思科身分識別服務引擎
- Qualys ScanGuard

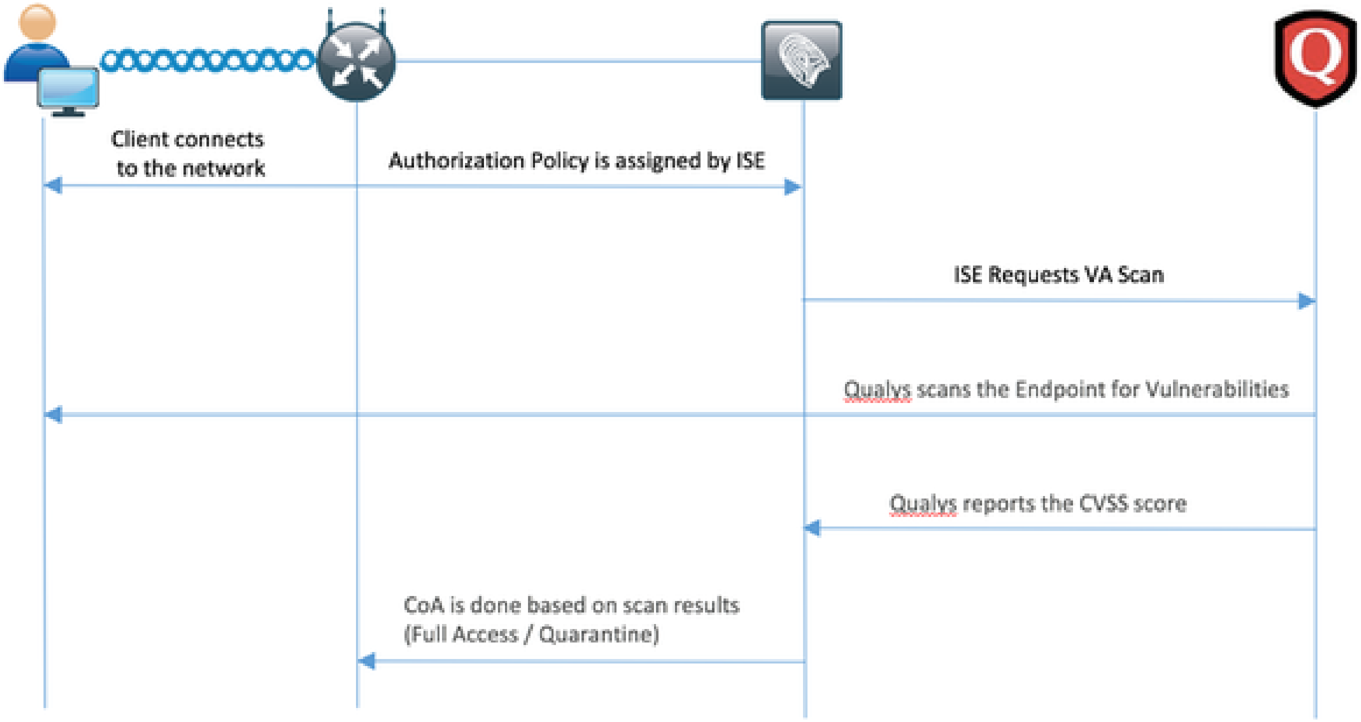
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.1
- 無線區域網路控制器(WLC)8.0.121.0
- Qualys防護掃描器8.3.36-1，簽名2.3.364-2
- Windows 7 Service Pack 1

設定

高級流程圖


Client connects
to the network
Authorization Policy is assigned by ISE
ISE Requests VA Scan
Qualys scans the Endpoint for Vulnerabilities
Qualys reports the CVSS score
CoA is done based on scan results
(Full Access / Quarantine)

以下是流程：

1. 客戶端連線到網路，提供受限訪問並分配啟用了**Assess Vulnerabilities**覈取方塊的配置檔案
2. PSN節點向MNT節點傳送系統日誌消息，確認發生了身份驗證，並且VA掃描是授權策略的結果
3. MNT節點使用以下資料向TC-NAC節點（使用管理WebApp）提交SCAN:
   -MAC 地址
   -IP 位址
   — 掃描間隔
   — 定期掃描已啟用
   — 始發PSN
4. Qualys TC-NAC（封裝在Docker容器中）與Qualys Cloud通訊（通過REST API）以觸發掃描（如果需要）
5. Qualys Cloud指示Qualys Scanner掃描終端
6. Qualys Scanner將掃描結果傳送到Qualys Cloud
7. 掃描結果將傳送回TC-NAC:
   -MAC 地址

— 所有CVSS分數
— 所有漏洞（QID、標題、CVEID）

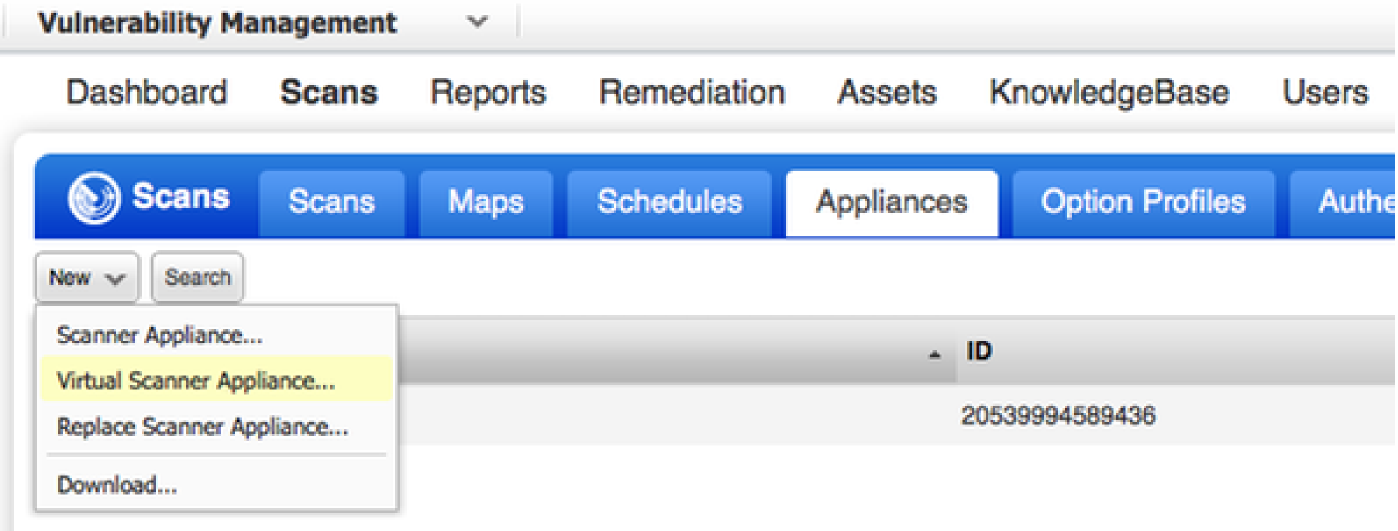
8. TC-NAC使用步驟7中的所有資料更新PAN。
9. 如果需要，將根據配置的授權策略觸發CoA。

配置Qualys雲和掃描器

注意：本文檔中的Qualys配置用於實驗目的，請諮詢Qualys工程師以瞭解設計注意事項

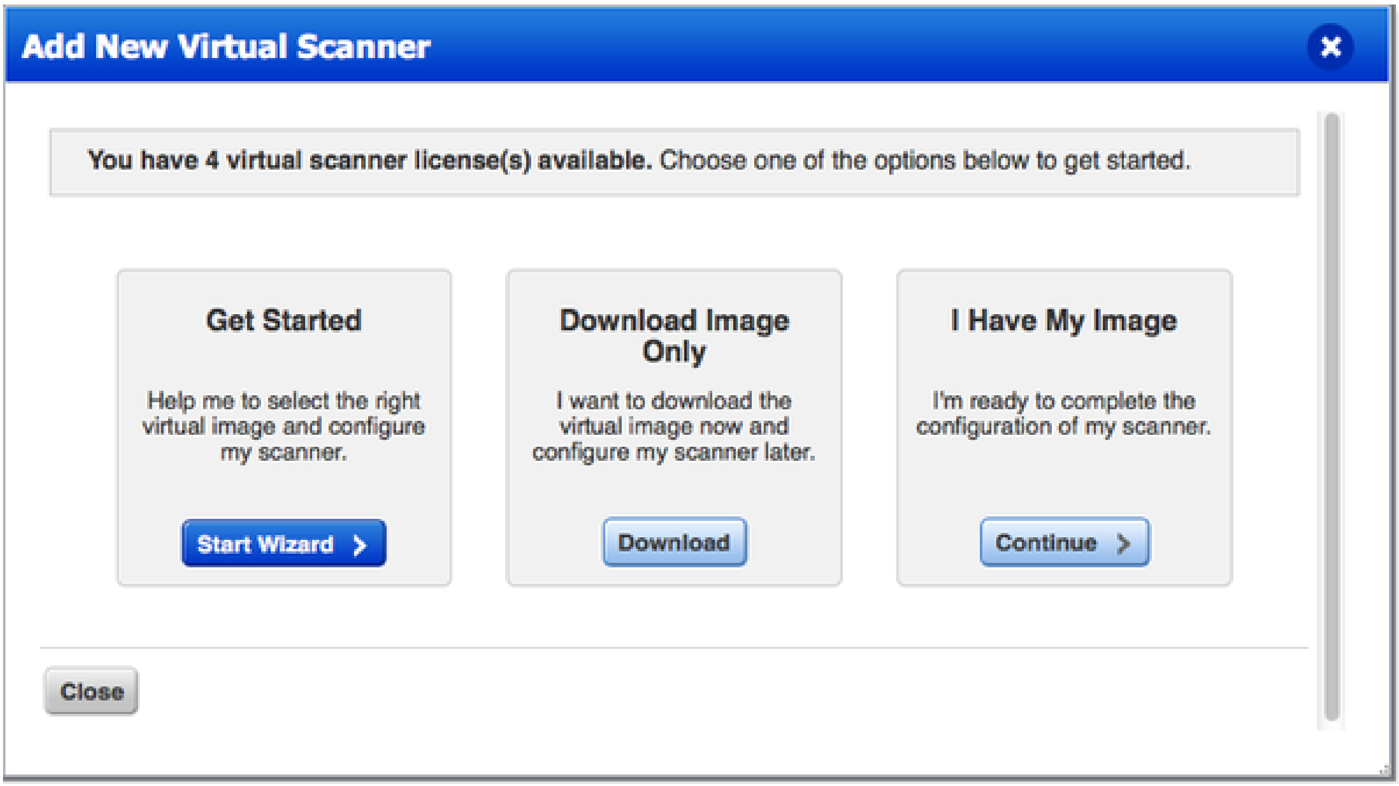
步驟1.部署Qualys Scanner

Qualys掃描器可以從OVA檔案部署。登入到Qualys雲並導航到Scans > Appliances並選擇New > Virtual Scanner Appliance



選擇**Download Image Only**，然後選擇適當的分發

輸入掃描器名稱后，您將獲得授權碼，稍後將使用該授權碼。


Add New Virtual Scanner

You have 4 virtual scanner license(s) available. Choose one of the options below to get started.

Get Started

Help me to select the right virtual image and configure my scanner.

Start Wizard >

Download Image Only

I want to download the virtual image now and configure my scanner later.

Download

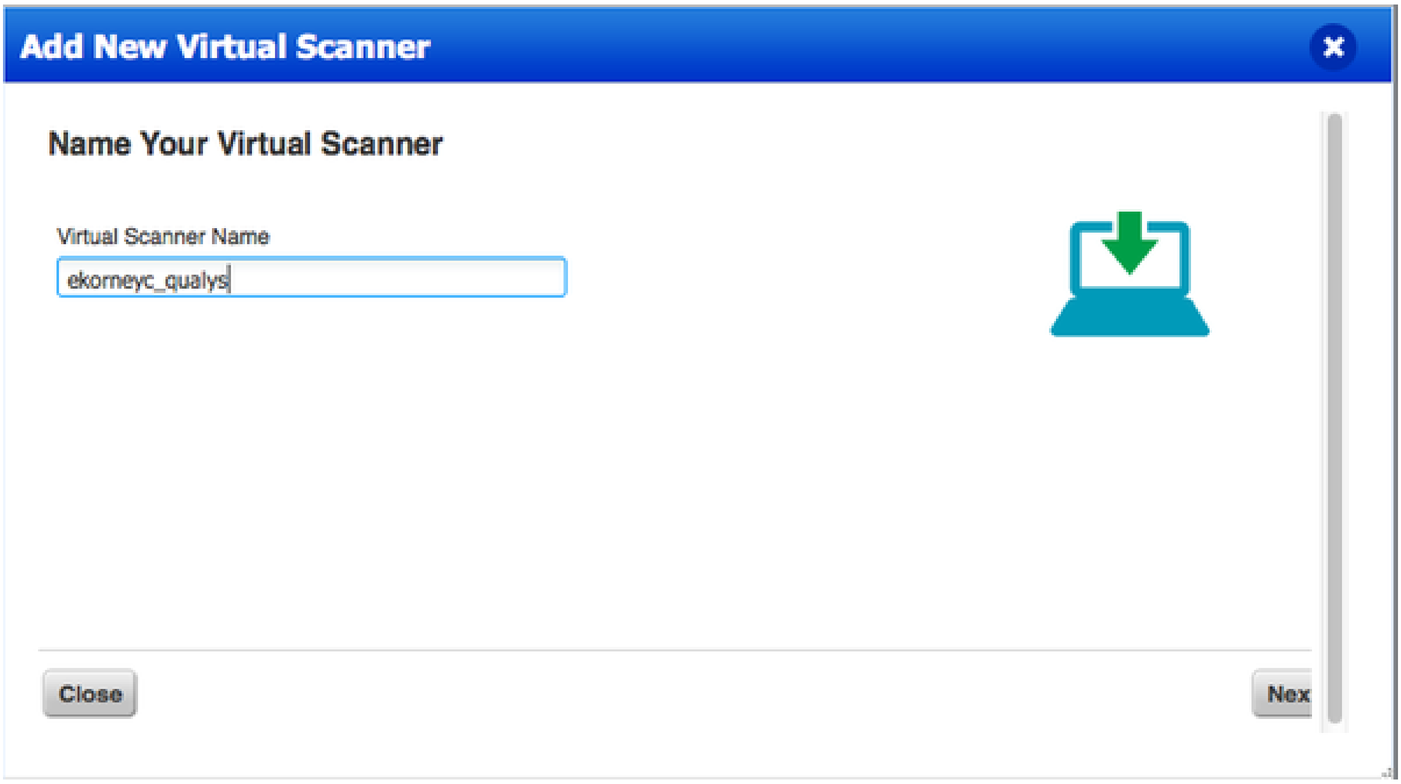
I Have My Image

I'm ready to complete the configuration of my scanner.

Continue >

Close

要獲取啟用代碼，您可以轉至Scans > Appliances，然後選擇New > Virtual Scanner Appliance，然後選擇**I Have My Image**


Add New Virtual Scanner

Name Your Virtual Scanner

Virtual Scanner Name

ekorneyc_qualys

Close

Nex

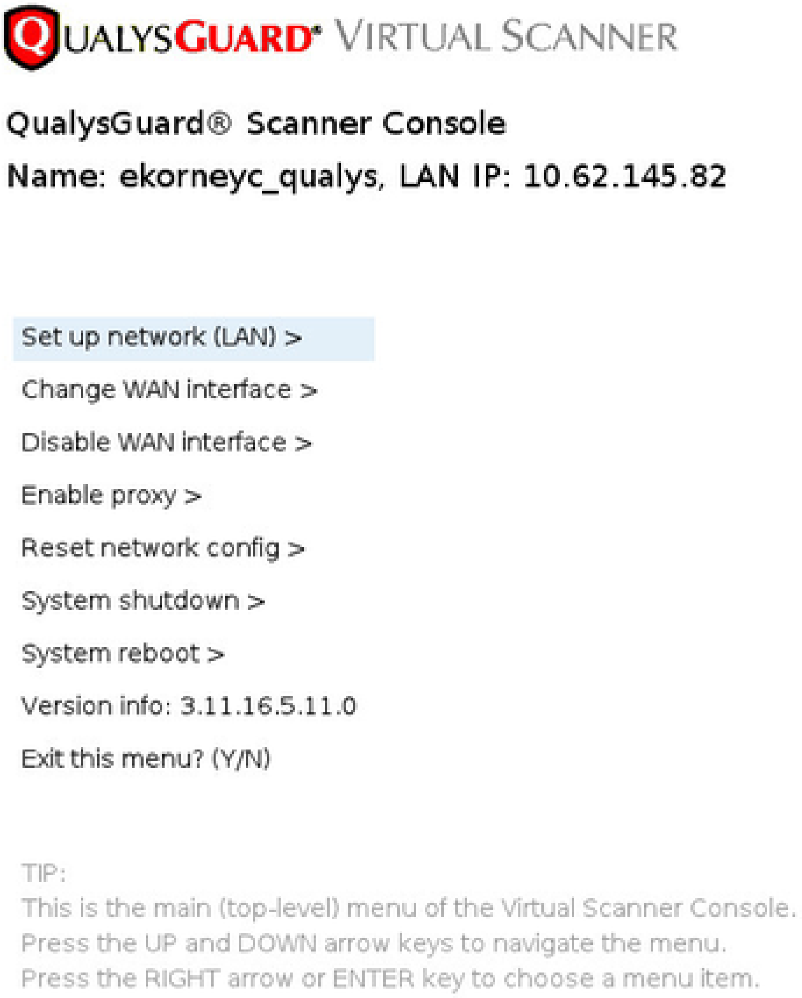
輸入掃描器名稱后，您將獲得授權碼，稍後將使用該授權碼。

步驟2.配置Qualys掃描器

在您選擇的虛擬化平台上部署OVA。完成後，配置這些設定：

- 設定網路(LAN)

- WAN介面設定（如果您使用兩個介面）
- 代理設定（如果您使用代理）
- 個人化此掃描器



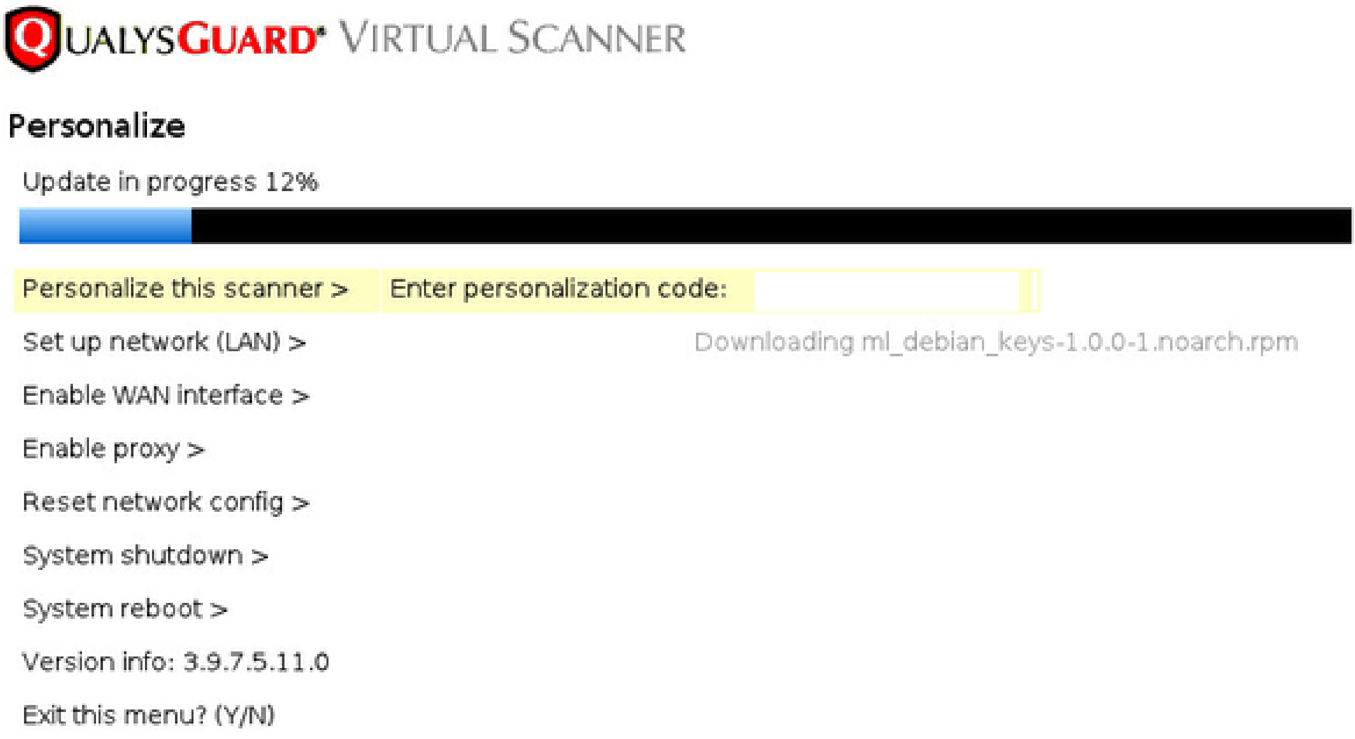
QUALYSGUARD® VIRTUAL SCANNER

QualysGuard® Scanner Console
Name: ekorneyc_qualys, LAN IP: 10.62.145.82

```
Set up network (LAN) >
Change WAN interface >
Disable WAN interface >
Enable proxy >
Reset network config >
System shutdown >
System reboot >
Version info: 3.11.16.5.11.0
Exit this menu? (Y/N)
```

TIP:
This is the main (top-level) menu of the Virtual Scanner Console.
Press the UP and DOWN arrow keys to navigate the menu.
Press the RIGHT arrow or ENTER key to choose a menu item.

之後，掃描器連線到Qualys並下載最新的軟體和簽名。



Personalize

Update in progress 12%

Personalize this scanner > Enter personalization code:

Set up network (LAN) > Downloading ml_debian_keys-1.0.0-1.noarch.rpm

Enable WAN interface >

Enable proxy >

Reset network config >

System shutdown >

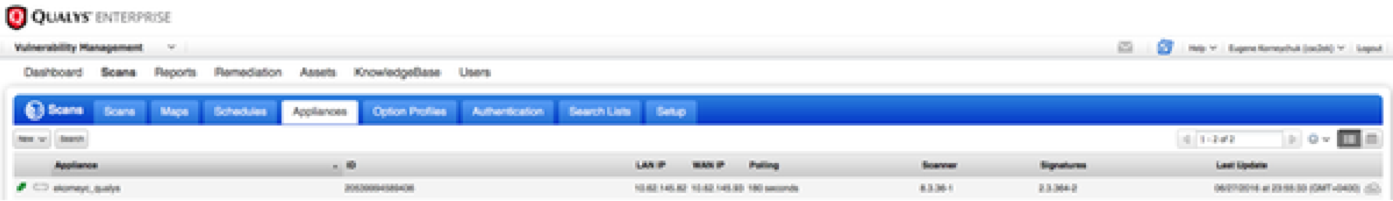
System reboot >

Version info: 3.9.7.5.11.0

Exit this menu? (Y/N)

要驗證掃描器是否已連線，可以導航到Scans > Appliances。

左側的綠色連線符號表示掃描器已準備就緒，您還可以看到LAN IP、WAN IP、掃描器版本和簽名
。



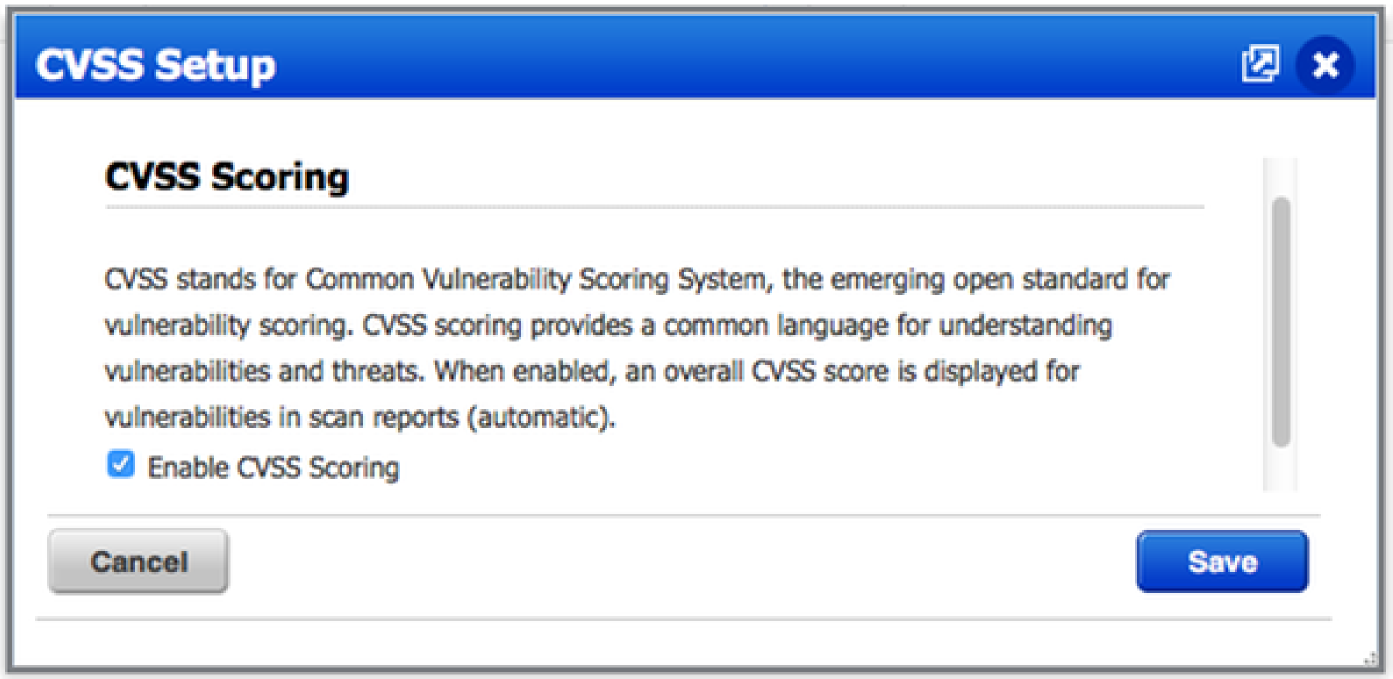
Appliance	ID	LAN IP	WAN IP	Polling	Scanner	Signatures	Last Update
ekomeyc_qualys	[illegible]	10.62.145.82	10.62.145.83	180 seconds	8.3.36-1	2.3.364-2	[illegible]

配置ISE

雖然您已配置Qualys Scanner和雲，但仍需調整雲設定以確保與ISE的整合工作正常。注意，應在通過GUI配置介面卡之前執行此操作，因為在首次配置介面卡之後會下載包含CVSS評分的知識庫。

步驟1.調整Qualys雲設定以便與ISE整合

- 在漏洞管理>報告>設定> CVSS >啟用CVSS計分時啟用CVSS計分



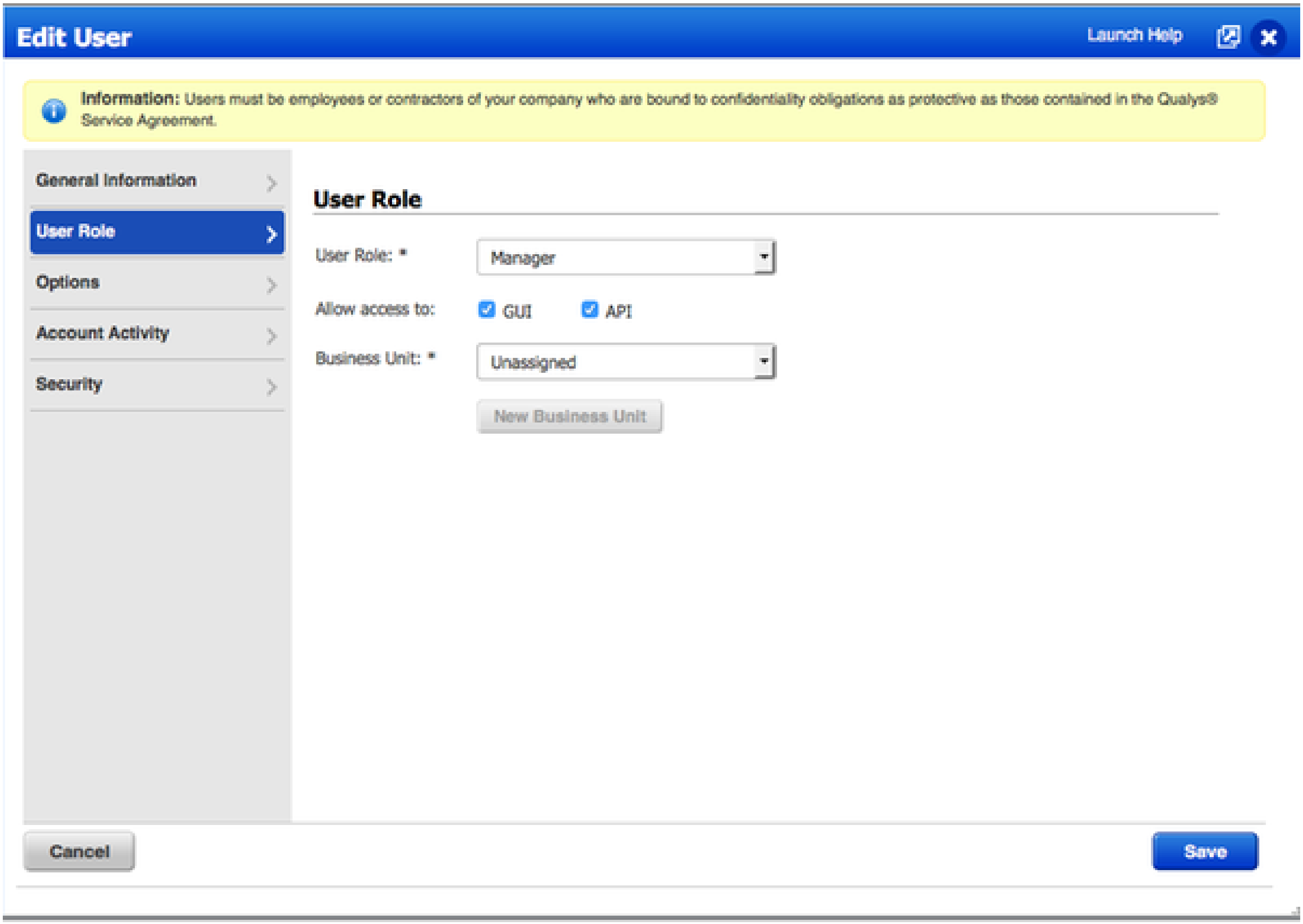
CVSS Setup

CVSS Scoring

CVSS stands for Common Vulnerability Scoring System, the emerging open standard for vulnerability scoring. CVSS scoring provides a common language for understanding vulnerabilities and threats. When enabled, an overall CVSS score is displayed for vulnerabilities in scan reports (automatic).

☑ Enable CVSS Scoring

- 確保在介面卡配置中使用的使用者憑證具有管理員許可權。從左上角選擇使用者，然後按一下 **User Profile**。您應該具有使用者角色中的**管理員許可權。**



Edit User

Information: Users must be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Qualys® Service Agreement.

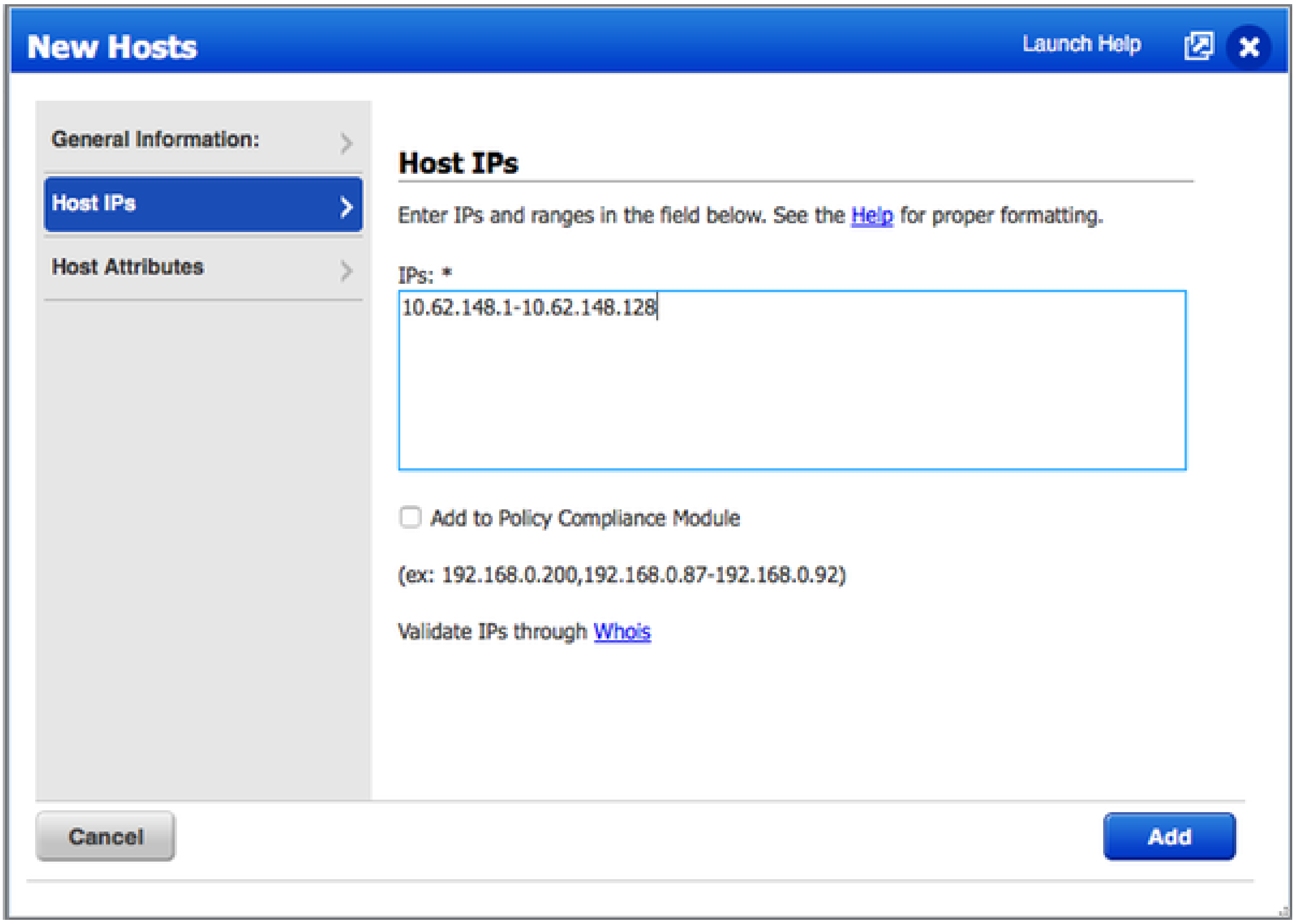
User Role

User Role: * Manager

Allow access to: ☑ GUI ☑ API

Business Unit: * Unassigned

- 確保需要漏洞評估的終端的IP地址/子網新增到Qualys中的Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts



Host IPs

Enter IPs and ranges in the field below. See the Help for proper formatting.

IPs: *
10.62.148.1-10.62.148.128

□ Add to Policy Compliance Module

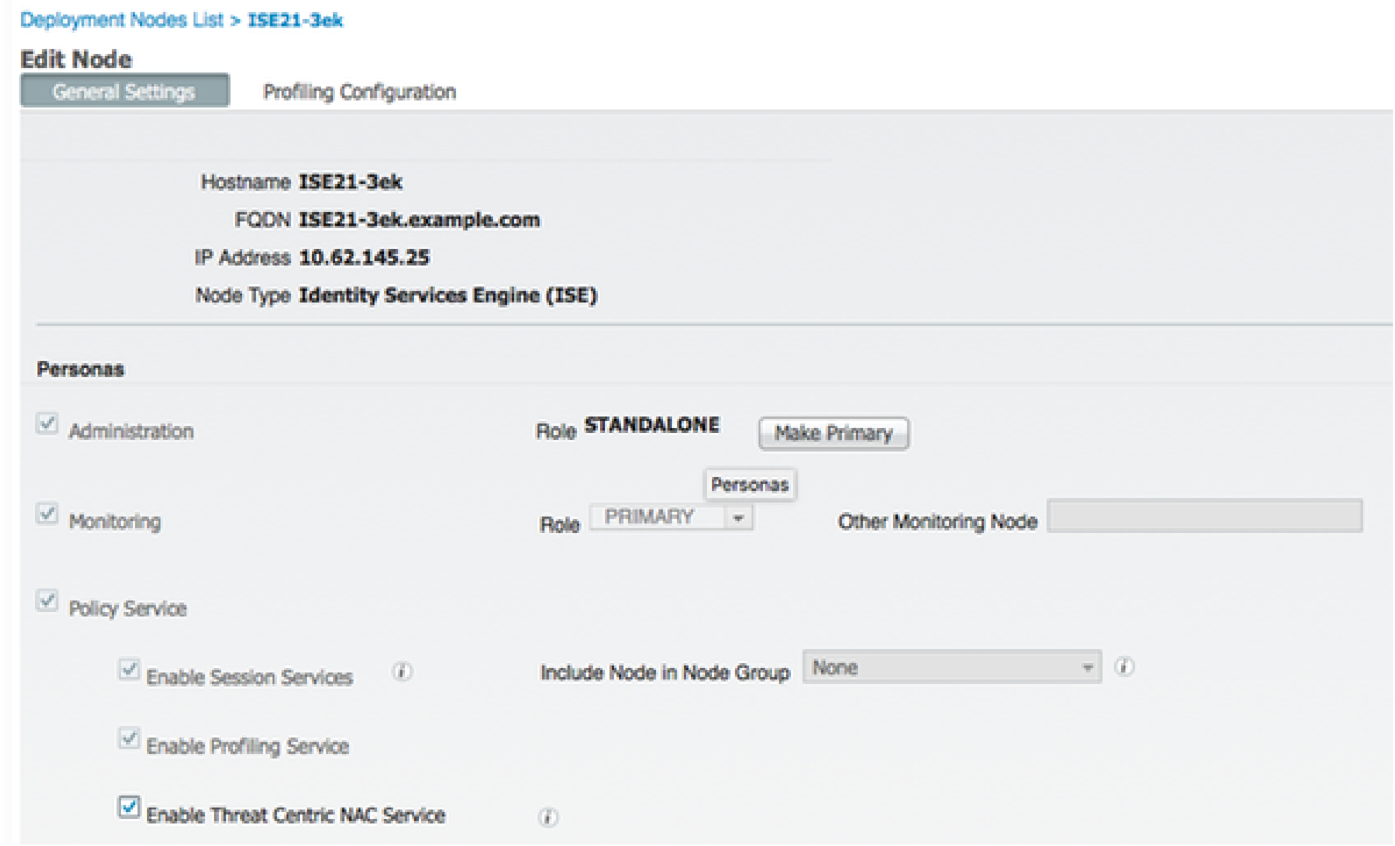
(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through WhoIs

步驟2.啟用TC-NAC服務

在管理>部署>編輯節點下啟用TC-NAC服務。支票 **啟用以威脅為中心的NAC服務** 覈取方塊。

附註：每個部署只能有一個TC-NAC節點。



Hostname **ISE21-3ek**

FQDN **ISE21-3ek.example.com**

IP Address **10.62.145.25**

Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **STANDALONE**

☑ Monitoring — Role PRIMARY — Other Monitoring Node

☑ Policy Service

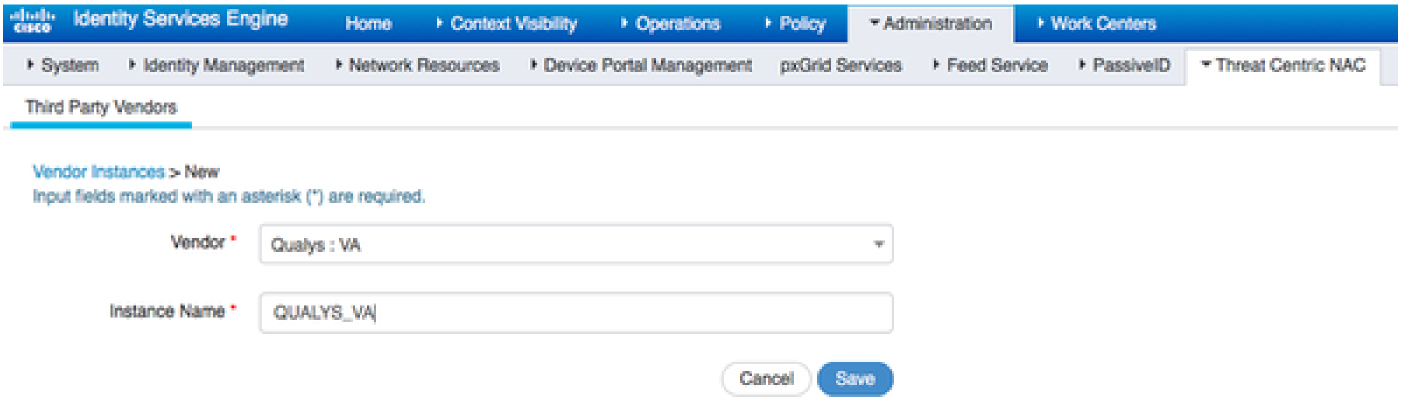
☑ Enable Session Services — Include Node in Node Group None

☑ Enable Profiling Service

☑ Enable Threat Centric NAC Service

步驟3.配置Qualys介面卡與ISE VA框架的連線

導航到Administration > Threat Centric NAC > Third Party Vendors > Add。按一下**Save**。

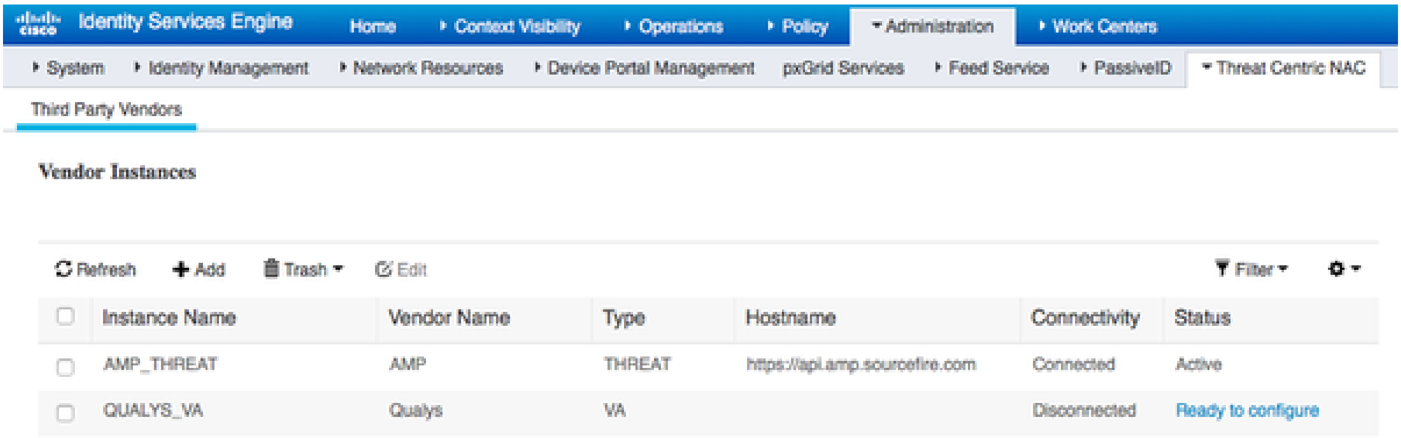


Vendor Instances > New
Input fields marked with an asterisk (*) are required.

Vendor * Qualys : VA

Instance Name * QUALYS_VA

當Qualys例項轉變為**Ready to configure狀態**時，按一下**Status中的Ready to configure**選項。

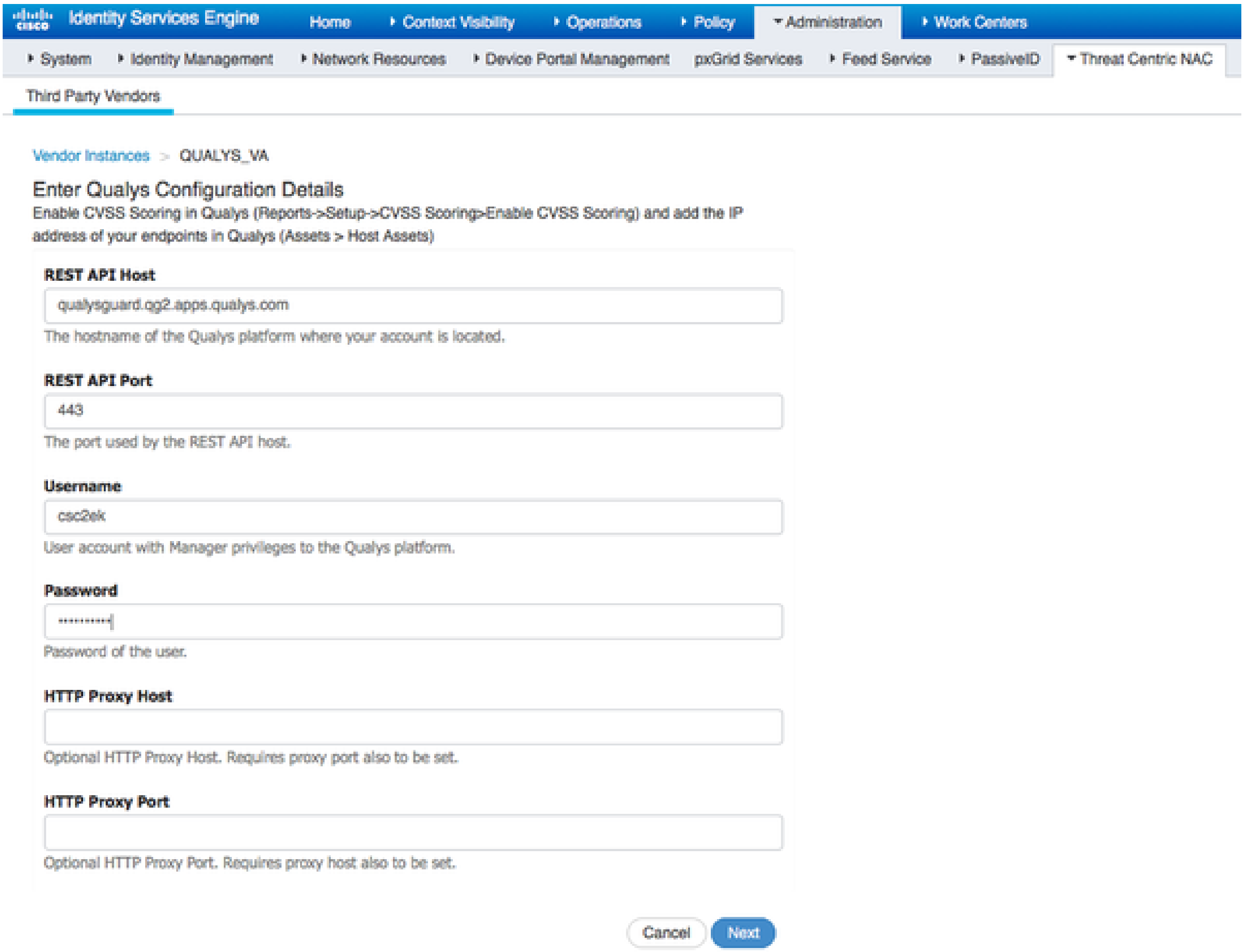


Vendor Instances

□	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
□	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
□	QUALYS_VA	Qualys	VA		Disconnected	Ready to configure

REST API主機應該是您的帳戶所在的Qualys Cloud所使用的主機。在此示例中 — qualysguard.qg2.apps.qualys.com

帳戶應該是具有管理員許可權的帳戶，按一下**下一步**。



Enter Qualys Configuration Details

Enable CVSS Scoring in Qualys (Reports->Setup->CVSS Scoring>Enable CVSS Scoring) and add the IP address of your endpoints in Qualys (Assets > Host Assets)

REST API Host

qualysguard.qg2.apps.qualys.com

The hostname of the Qualys platform where your account is located.

REST API Port

443

The port used by the REST API host.

Username

csc2ek

User account with Manager privileges to the Qualys platform.

Password

••••••••••

Password of the user.

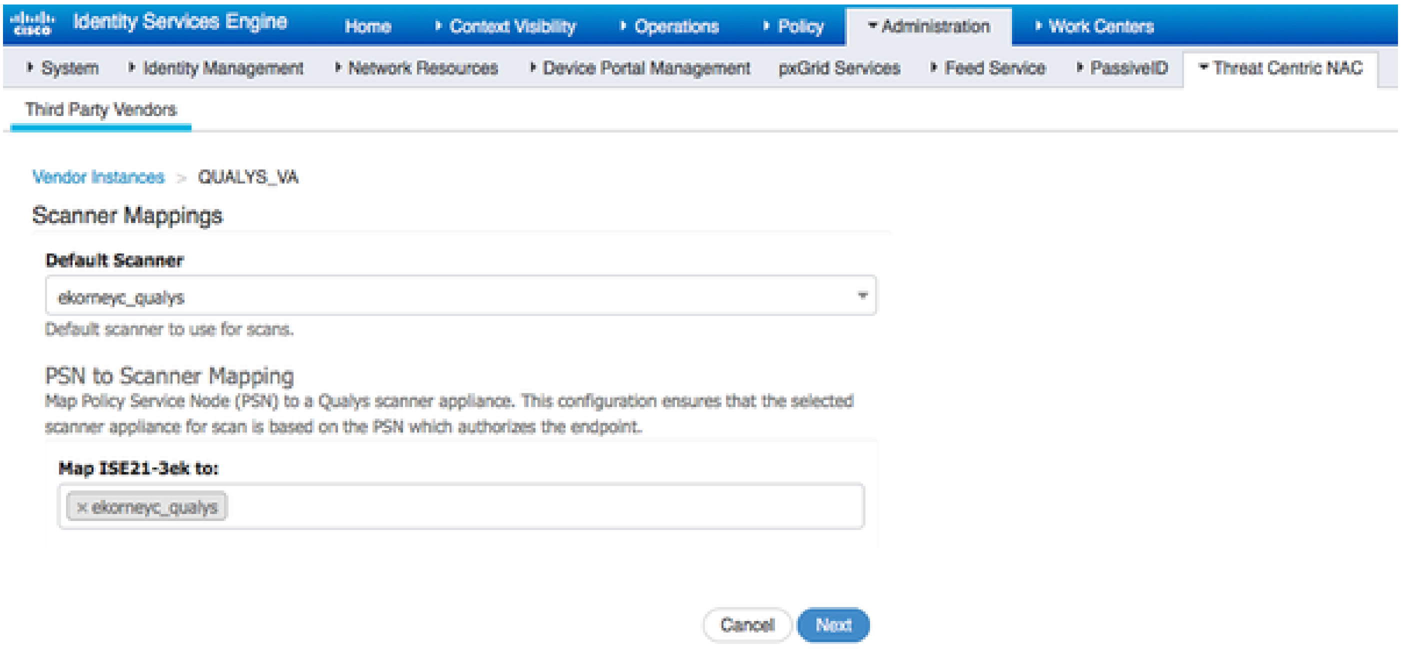
HTTP Proxy Host

Optional HTTP Proxy Host. Requires proxy port also to be set.

HTTP Proxy Port

Optional HTTP Proxy Port. Requires proxy host also to be set.

ISE下載有關連線到Qualys雲的掃描器的資訊，您可以在此頁上配置PSN到掃描器的對映。它確保基於授權端點的PSN來選取選定的掃描器。



Vendor Instances > QUALYS_VA

Scanner Mappings

Default Scanner

ekorneyc_qualys

Default scanner to use for scans.

PSN to Scanner Mapping

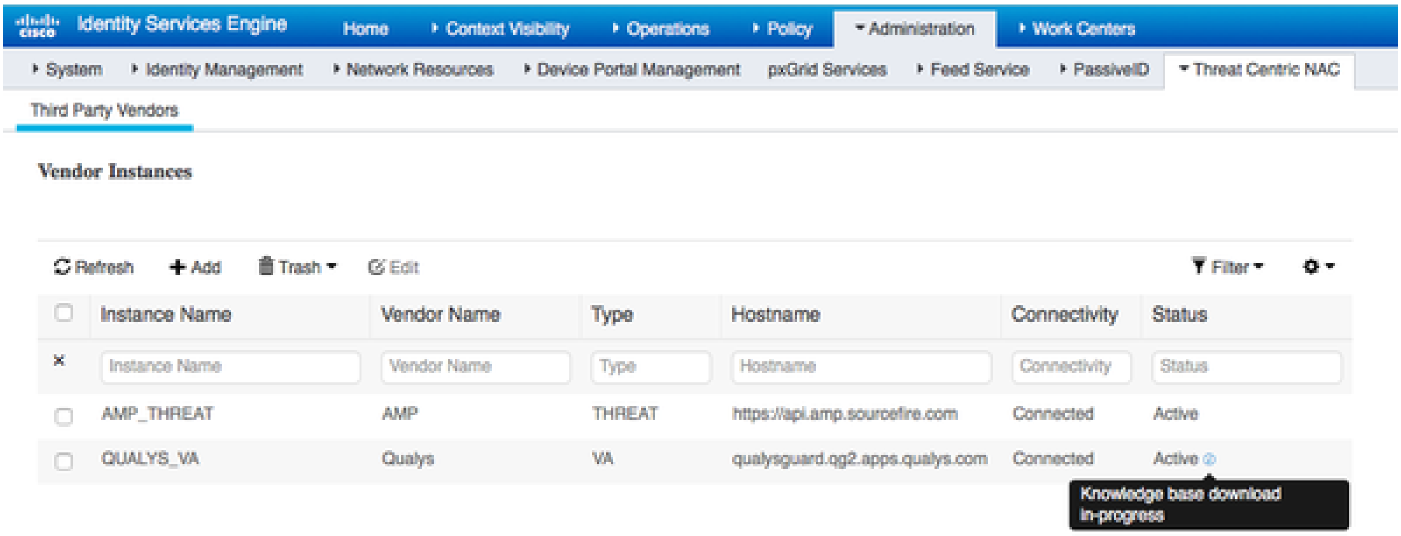
Map Policy Service Node (PSN) to a Qualys scanner appliance. This configuration ensures that the selected scanner appliance for scan is based on the PSN which authorizes the endpoint.

Map ISE21-3ek to:

× ekorneyc_qualys

高級設定在ISE 2.1管理指南中有詳細記錄，可以在本文檔的參考部分找到連結。按一下**Next**和**Finish**。Qualys例項轉換為**活動**狀態，並開始下載知識庫。

> **附註**：每個部署只能有一個Qualys例項。



Vendor Instances

□	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
×	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
□	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
□	QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

Knowledge base download in-progress

步驟4.配置授權配置檔案以觸發VA掃描

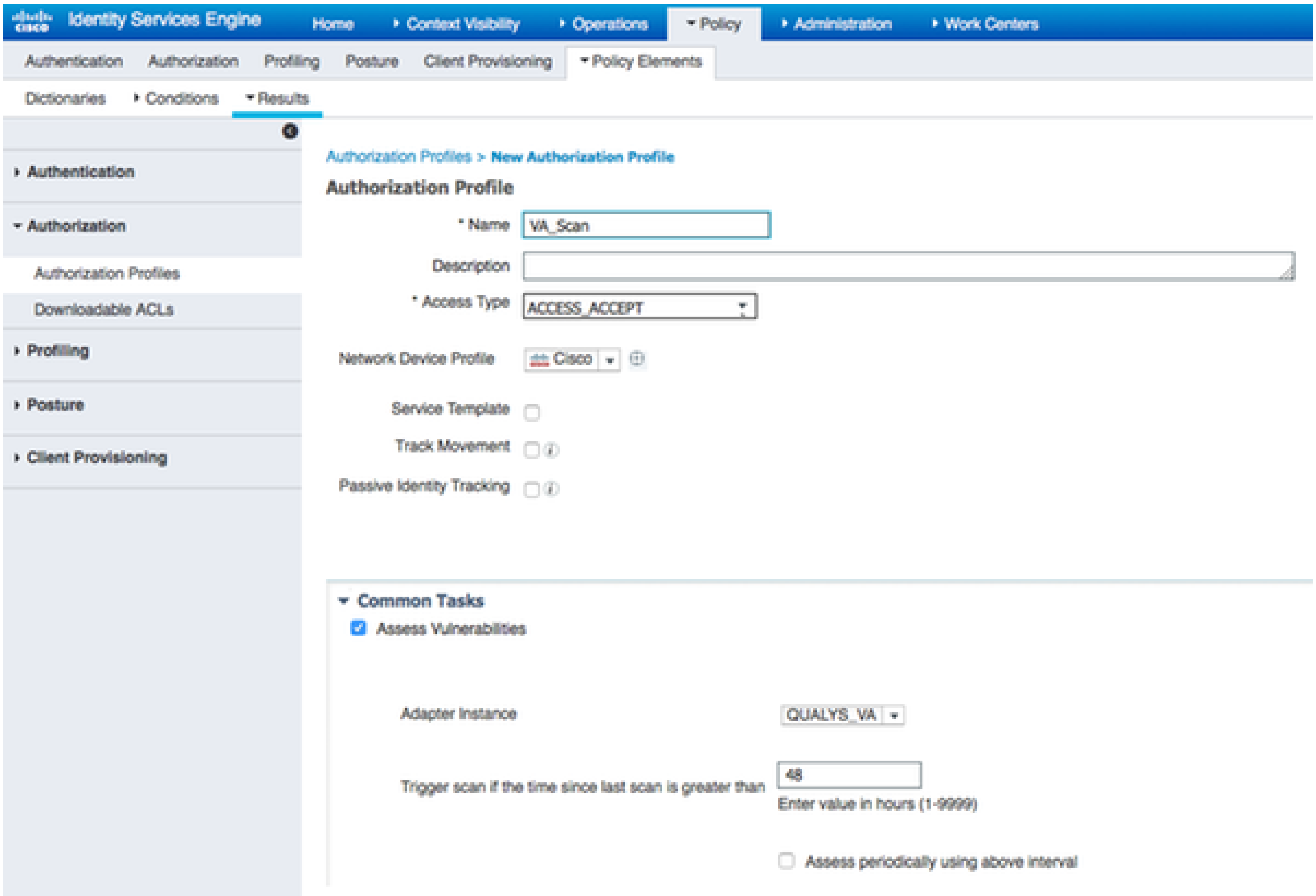
導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。新增新配置檔案。在**Common Tasks**下，選中**Vulnerability Assessment**覈取方塊。
應根據網路設計選擇按需掃描間隔。

授權配置檔案包含這些av對：

```
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
```

它們被傳送到訪問接受資料包中的網路裝置，儘管它們的真正目的是告知MNT節點應該觸發掃描。

MNT指示TC-NAC節點與Qualys Cloud通訊。



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: VA_Scan

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

☑ Assess Vulnerabilities

Adapter Instance: QUALYS_VA

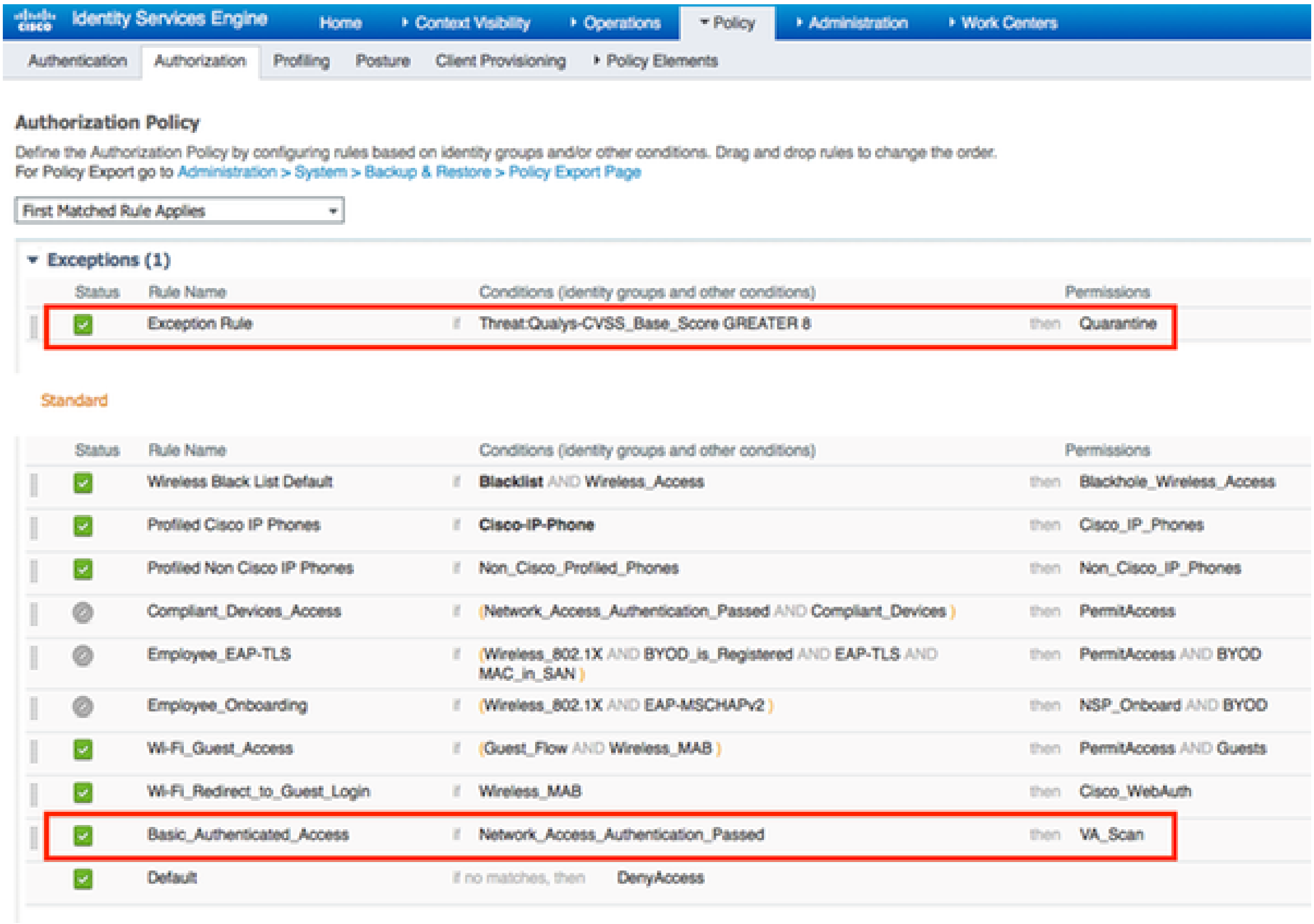
Trigger scan if the time since last scan is greater than: 48

Enter value in hours (1-9999)

□ Assess periodically using above interval

步驟5.配置授權策略

- 配置授權策略以使用步驟4中配置的新授權配置檔案。導航到Policy > Authorization > Authorization Policy，找到**Basic_Authenticated_Access**規則，然後按一下**Edit**。將許可權從**PermitAccess**更改為新**建立的標準VA_Scan**。這會導致對所有使用者進行漏洞掃描。按一下**Save**。
- 為隔離的電腦建立授權策略。導航到Policy > Authorization > Authorization Policy > Exceptions並建立**Exception Rule**。按一下條件>建立新條件（高級選項）>選擇屬性，向下滾動並選擇**威脅**。展開**Threat**屬性並選擇**Qualys-CVSS_Base_Score**。將運算子更改為**大於**，然後根據您的安全策略輸入一個值。**隔離**授權配置檔案應授予對易受攻擊的電腦的有限訪問許可權。



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Exception Rule	if	Threat:Qualys-CVSS_Base_Score GREATER 8	then	Quarantine

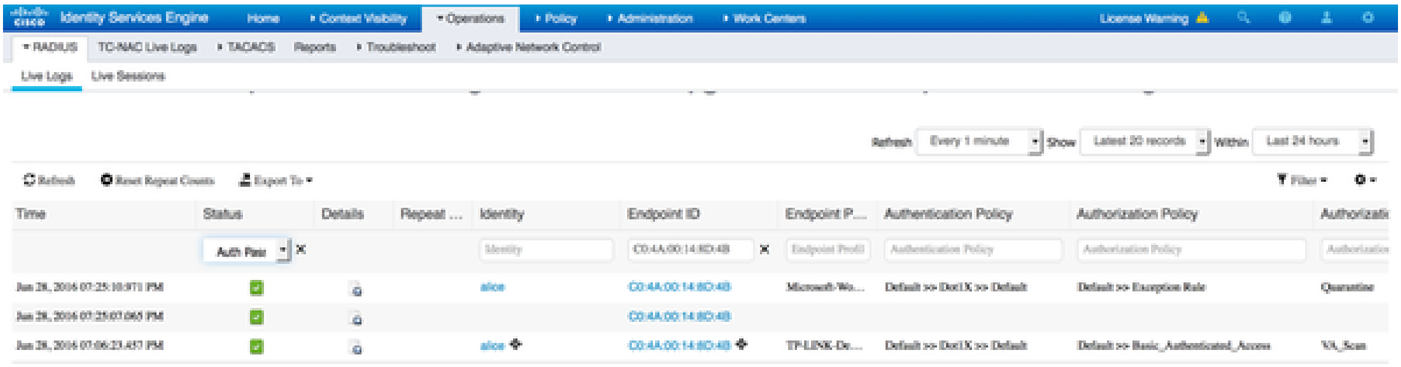
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
○	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess
○	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD
○	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD
✓	Wi-Fi_Guest_Access	if	(Guest_Flow AND Wireless_MAB)	then	PermitAccess AND Guests
✓	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	VA_Scan
✓	Default	if no matches, then	DenyAccess		

驗證

身分識別服務引擎

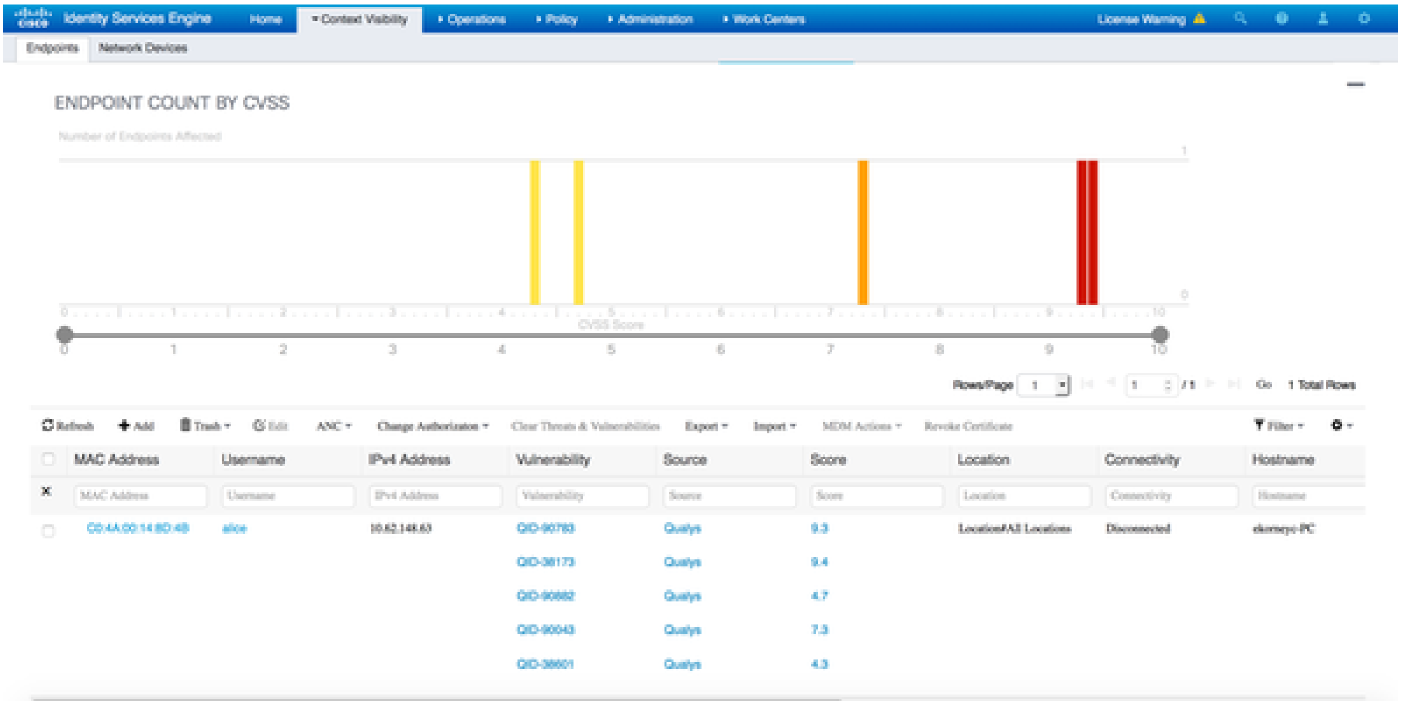
第一個連線觸發VA掃描。掃描完成後，如果匹配了CoA Reauthentication，將觸發CoA Reauthentication應用新策略。



Refresh: Every 1 minute　Show: Latest 20 records　Within: Last 24 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
	Auth Pass			Identity	C0:4A:00:14:8D:4B	Endpoint Profil	Authentication Policy	Authorization Policy	Authorizatio
Jun 28, 2016 07:25:10.971 PM	✓			alice	C0:4A:00:14:8D:4B	Microsoft-Wo...	Default >> Dot1X >> Default	Default >> Exception Rule	Quarantine
Jun 28, 2016 07:25:07.065 PM	✓				C0:4A:00:14:8D:4B				
Jun 28, 2016 07:06:23.457 PM	✓			alice	C0:4A:00:14:8D:4B	TP-LINK-De...	Default >> Dot1X >> Default	Default >> Basic_Authenticated_Access	VA_Scan

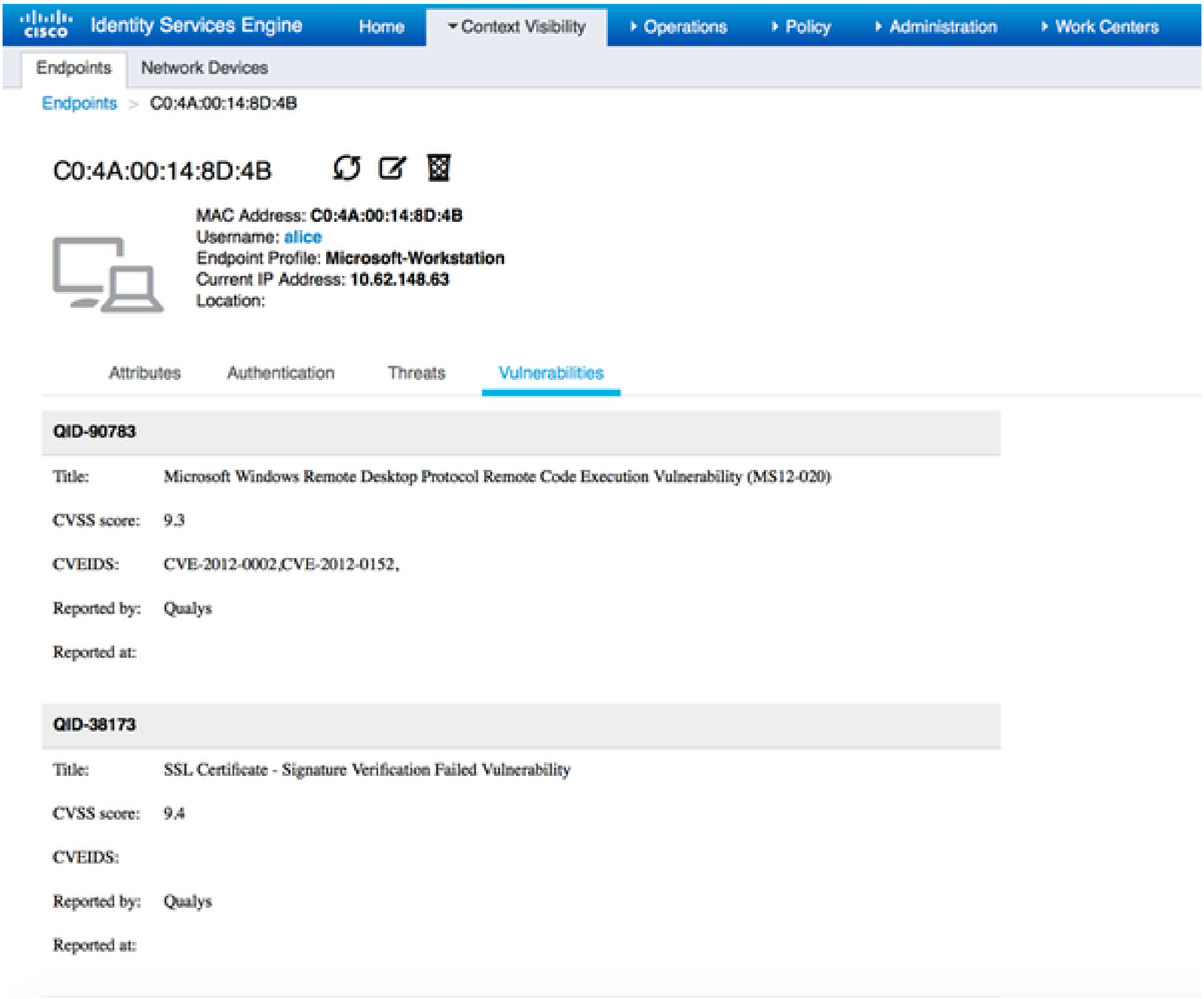
要驗證檢測到哪些漏洞，請導航至Context Visibility > Endpoints。使用Qualys為其提供的分數檢查每個終端的漏洞。



ENDPOINT COUNT BY CVSS

MAC Address	Username	IPv4 Address	Vulnerability	Source	Score	Location	Connectivity	Hostname
C0:4A:00:14:8D:4B	alice	10.62.148.63	QID-90783	Qualys	9.3	Location#All Locations	Disconnected	ekorneyc-PC
			QID-38173	Qualys	9.4			
			QID-90882	Qualys	4.7			
			QID-90043	Qualys	7.3			
			QID-38601	Qualys	4.3			

選擇特定端點時，會顯示有關每個漏洞的更多詳細資訊，包括**標題**和CVEID。



C0:4A:00:14:8D:4B

MAC Address: **C0:4A:00:14:8D:4B**
Username: **alice**
Endpoint Profile: **Microsoft-Workstation**
Current IP Address: **10.62.148.63**
Location:

QID-90783

Title: Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

CVSS score: 9.3

CVEIDS: CVE-2012-0002,CVE-2012-0152,

Reported by: Qualys

Reported at:

QID-38173

Title: SSL Certificate - Signature Verification Failed Vulnerability

CVSS score: 9.4

CVEIDS:

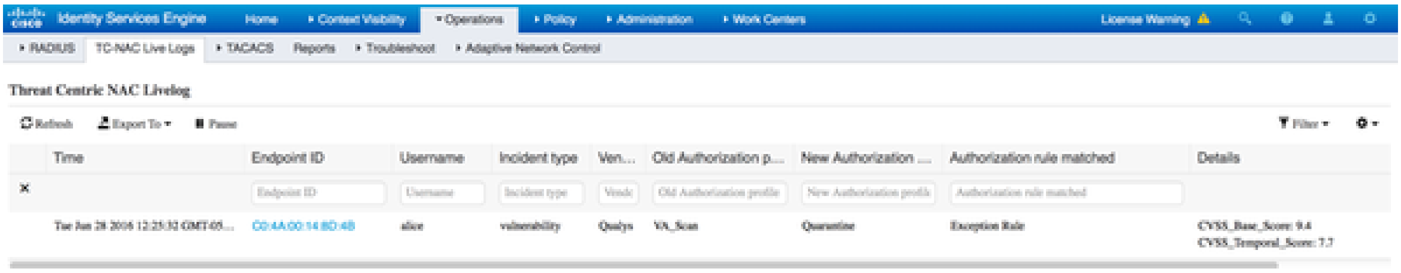
Reported by: Qualys

Reported at:

在Operations > TC-NAC Live Logs中，您可以檢視應用的舊授權策略和新授權策略以及

CVSS_Base_Score的詳細資訊。

> **附註**：授權條件基於CVSS_Base_Score完成，CVSS_Base_Score等於終端上檢測到的最高漏洞得分。

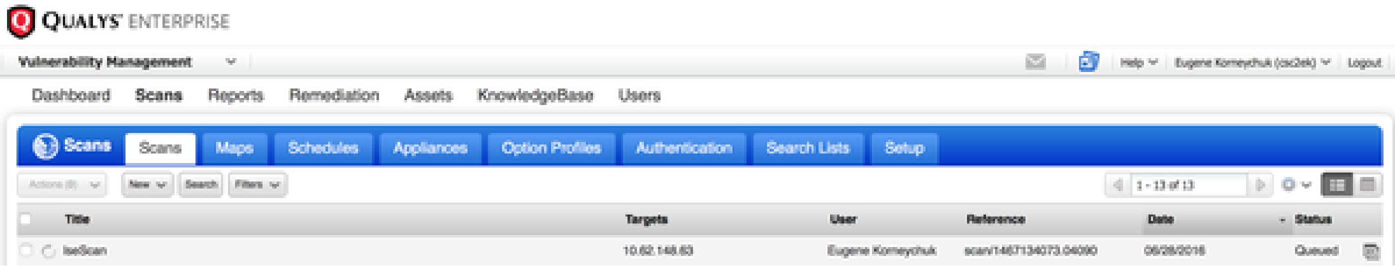


Threat Centric NAC Livelog

Time	Endpoint ID	Username	Incident type	Ven...	Old Authorization p...	New Authorization ...	Authorization rule matched	Details
Tue Jun 28 2016 12:25:32 GMT-05...	C0:4A:00:14:8D:4B	alice	vulnerability	Qualys	VA_Scan	Quarantine	Exception Rule	CVSS_Base_Score: 9.4 CVSS_Temporal_Score: 7.7

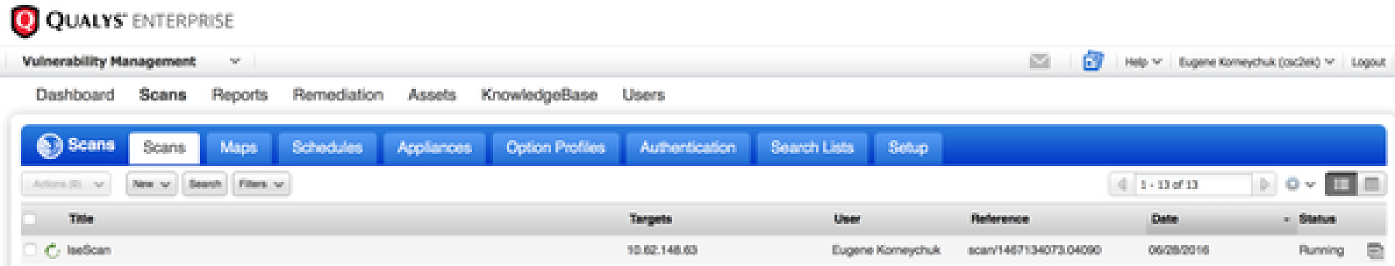
Qualys Cloud

當TC-NAC Qualys隊列將掃描觸發VA掃描時，可以在「掃描」>「掃描」中檢視該掃描



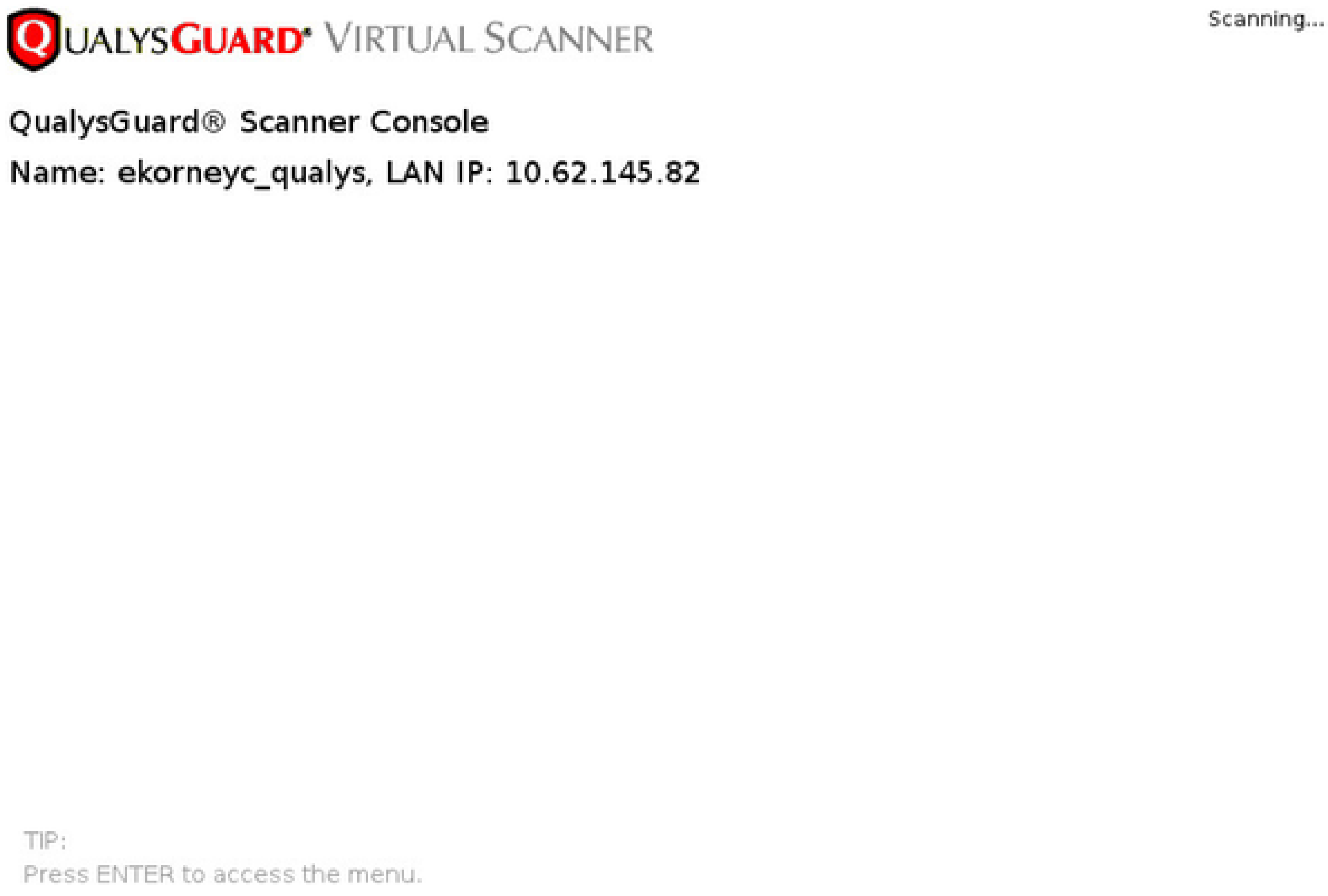
Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Queued

之後，它轉換到Running，這意味著Qualys cloud已指示Qualys Scanner執行實際掃描



Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Running

掃描器執行掃描時，您應該看到「Scanning...」 在Qualys Guard的右上角簽名

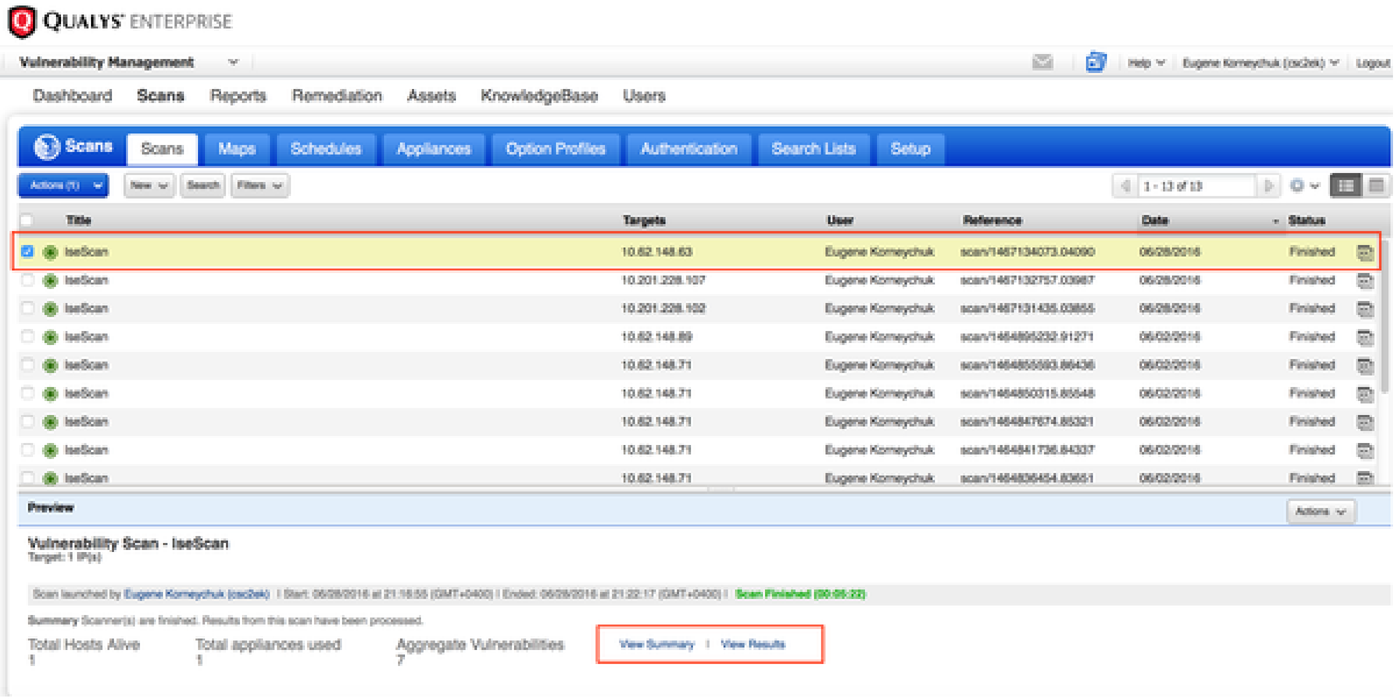


QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

掃描完成後，其將轉換為「完成」狀態。您可以在掃描>掃描時檢視結果，選擇所需的掃描，然後按一下**檢視摘要**或**檢視結果**。



	Title	Targets	User	Reference	Date	Status
☑	IseScan	10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Finished
□	IseScan	10.201.228.107	Eugene Korneychuk	scan/1467132757.03987	06/28/2016	Finished
□	IseScan	10.201.228.102	Eugene Korneychuk	scan/1467131435.03855	06/28/2016	Finished
□	IseScan	10.62.148.89	Eugene Korneychuk	scan/1464895232.91271	06/02/2016	Finished
□	IseScan	10.62.148.71	Eugene Korneychuk	scan/1464855593.86436	06/02/2016	Finished
□	IseScan	10.62.148.71	Eugene Korneychuk	scan/1464850315.85548	06/02/2016	Finished
□	IseScan	10.62.148.71	Eugene Korneychuk	scan/1464847674.85321	06/02/2016	Finished
□	IseScan	10.62.148.71	Eugene Korneychuk	scan/1464841736.84337	06/02/2016	Finished
□	IseScan	10.62.148.71	Eugene Korneychuk	scan/1464836454.83651	06/02/2016	Finished

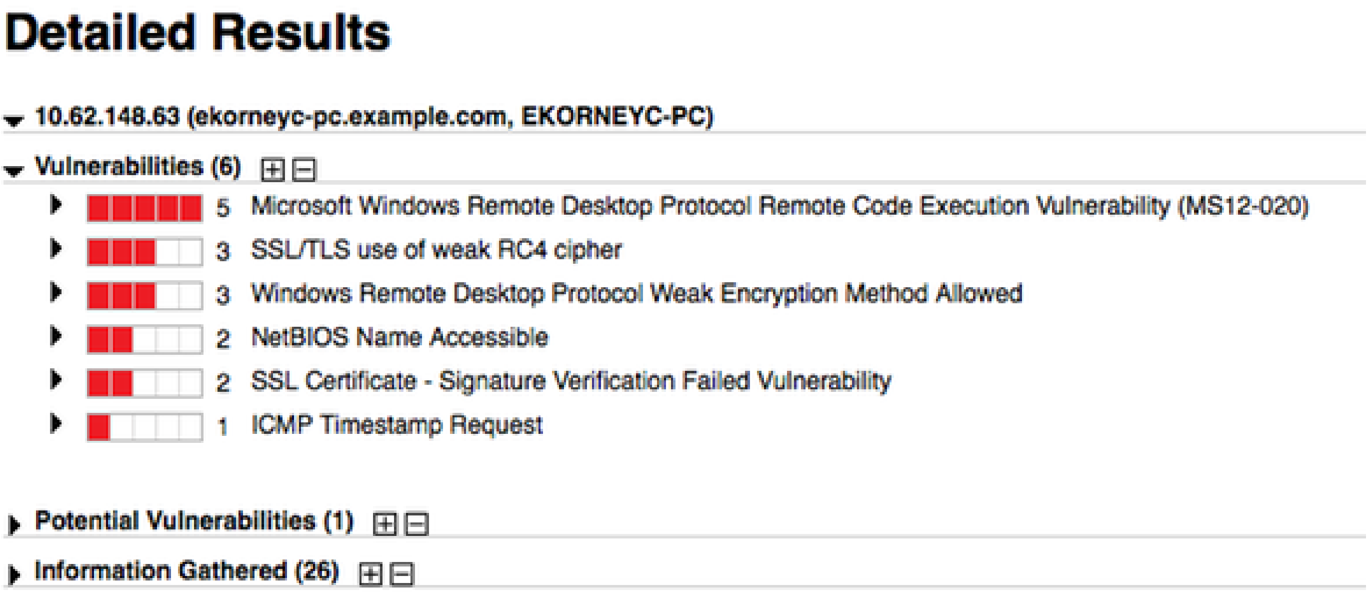
Vulnerability Scan - IseScan
Target: 1 IP(s)

Scan launched by Eugene Korneychuk (csc2ek) | Start: 06/28/2016 at 21:16:55 (GMT+0400) | Ended: 06/28/2016 at 21:22:17 (GMT+0400) | Scan Finished (00:05:22)

Summary Scanner(s) are finished. Results from this scan have been processed.

Total Hosts Alive	Total appliances used	Aggregate Vulnerabilities
1	1	7

在報告本身中，您可以看到**詳細結果**，其中顯示了檢測到的漏洞。



Detailed Results

10.62.148.63 (ekorneyc-pc.example.com, EKORNEYC-PC)

Vulnerabilities (6)

- 5 Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- 3 SSL/TLS use of weak RC4 cipher
- 3 Windows Remote Desktop Protocol Weak Encryption Method Allowed
- 2 NetBIOS Name Accessible
- 2 SSL Certificate - Signature Verification Failed Vulnerability
- 1 ICMP Timestamp Request

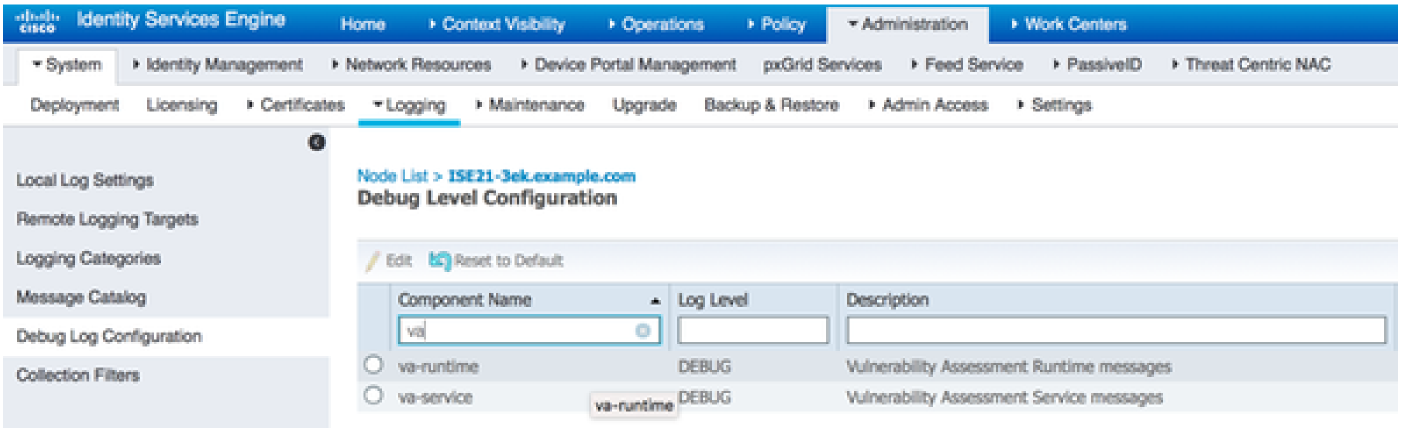
Potential Vulnerabilities (1)

Information Gathered (26)

疑難排解

ISE上的調試

若要在ISE上啟用調試，請導航到Administration > System > Logging > Debug Log Configuration，選擇TC-NAC Node，並將**Log Level va-runtime**和**va-service**元件更改為**DEBUG**



Node List > ISE21-3ek.example.com

Debug Level Configuration

	Component Name	Log Level	Description
	va		
○	va-runtime	DEBUG	Vulnerability Assessment Runtime messages
○	va-service	DEBUG	Vulnerability Assessment Service messages

要檢查的日誌 — varuntime.log。您可以直接從ISE CLI對其進行跟蹤：

```
ISE21-3ek/admin# show logging application varuntime.log tail
```

TC-NAC Docker收到對特定端點執行掃描的指令。

```
2016-06-28 19:06:30,823 DEBUG [Thread-70][] va.runtime.admin.mnt.EndpointFileReader -:::::- VA:
[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScan
Enabled":false"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
199fb81a4b9","psnHostName":"ISE 21-3ek","heartBeatTime":0,"lastScanTime":0}]
2016-06-28 19:06:30,824 DEBUG [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-
199fb81a4b9","psnHostName":"ISE 1-3ek","heartBeatTime":0,"lastScanTime":0}
```

收到結果後，它會將所有漏洞資料儲存在上下文目錄中。

```
2016-06-28 19:25:02,020 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::: — VaService
[{"macAddress":"C0:4A:00:14:8D:4B","ipAddress":"10.62.148.63","lastScanTime":1467134394000,"vuln
erabilities":["{\"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\": .4\"\"cvssTemporalScore\":\"6.9\"
\"vulnerabilityTitle\":\"SSL Certificate - Signature Verification Failed Vulnerability\"
\"vulnerabilityVendor\":\"Qualys\"}""{\"vulnerabilityId\":\"QID-90882\"\"cveIds\":\":\"4.7\"
\"cvssTemporalScore\":\"\"\"Windows\",\"\":\"Qualys\"}","{\"\":\"QID-
90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"\":\"SMBSMB
\",\"\" \"Qualys\"}","{\"ID\":\"QID-38601\",\"cveIds\":\"CVE-2013-2566,CVE-2015-
2808,\",\"cvssBaseScore\":\"4.3\",\"cvssTemporalScore\":\"3.7\",\"\"SSL/TLSRC"
,\"vulnerabilityVendor\":\"Qualys\"}"]}]
2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::- VA:lastscantime:1467134394000
mac:C0:4A:00:14:8D:4B
2016-06-28 19:25:02,268 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaAdminServiceContext -::::- VA:elastic search jsonpri-lan
2016-06-28 19:25:02,272 DEBUG [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
(MS) 12-020)","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL —
","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId-90882","cveIds":","cvss
BaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90043","cveIds":","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
Signing DisabledSMB Signing Not Required", vulnerabilityVendor":"Qualys"},
{"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-
2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLSRC4
","vulnerabilityVendor":"Qualys":"Qualys"}]
```

要檢查的日誌 — vaservice.log。您可以直接從ISE CLI對其進行跟蹤：

```
ISE21-3ek/admin# show logging application vaservice.log tail
```

漏洞評估請求已提交至介面卡

```
2016-06-28 17:07:13,200 DEBUG [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil -
::::- VA SendSyslog systemMsg
:[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA request submitted to
adapter","TC-NAC.Details","VA request submitted to adapter for processing","TC-
NAC.MACAdress","C0:4A:00:14:D:B","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每5分鐘檢查一次掃描的狀態，直到掃描完成。

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

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

介面卡獲得QID、CVE以及CVSS分數

```
2016-06-28 17:24:57,556 DEBUG [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 9","vulnerabilityTitle":"SSL
Certificate - Signature Verification Failed
Vulnerability","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90043","cveIds":","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
Signing Disabled or SMB Signing Not
Required","vulnerabilityVulnerabilityVendor":"Qualys"},{"VulnerabilityId" 90783","cveIds":"CVE-
2012-0002,CVE-2012-
0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft Windows
(MS12-020)","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID" -38601","cveIds":"CVE-2013-
2566,CVE-2015-
2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLSRC4
","vulnerabilityVendor":"Qualys"},{"vulnerabilityId-90882","cveIds":"
"cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
","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-
time ":1467134394000,"title":"Vulnerability","vendor":"Qualys"}]}
2016-06-28 17:25:01,853 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
::::- VA SendSyslog systemMsg
:[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA","TC-NAC.Details","VA
5","TC-NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IpAddress","10.62.148.63","TC-
NAC.AdapterInstanceUid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-NAC.Vendor1 name""Qualys""TC-
NAC.AdapterInstanceName""QUALYS_VA"]}]
```

典型問題

問題1. ISE獲得CVSS_Base_Score為0.0且CVSS_Temporal_Score為0.0的漏洞報告，而Qualys Cloud報告包含檢測到的漏洞。

問題：

從Qualys Cloud檢查報告時，您可以看到檢測到的漏洞，但在ISE上您看不到它們。

在vaservice.log中顯示的調試：

```
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_Temal_Score":0},"time-time
":1464855905000,"title":"Vulnerability","vendor":"Qualys"}]}
```

解決方案：

cvss分數為零的原因可能是，在您通過UI配置介面卡之前，它沒有漏洞或者未在Qualys雲中啟用cvss評分。首次配置介面卡後，將下載包含已啟用cvss計分功能的知識庫。您必須確保以前啟用了CVSS計分，在ISE上建立介面卡例項。可以在Vulnerability Management > Reports > Setup > CVSS > Enable CVSS Scoring下完成

問題2. ISE不會從Qualys雲獲取結果，即使已點選正確的授權策略。

問題：

已匹配更正的授權策略，應觸發VA掃描。儘管如此，沒有進行任何掃描。

在vaservice.log中顯示的調試：

```
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::: — (
'[B@6da5e620(byte[311])'MessageProperties [headers={}, timestamp=null messageId=null userId=null
appId=null clusterId=null type=null correlationId=null replyTo=null
contentType=application/octet-stream contentEncoding=null contentLength=0,
deliveryMode=PERSISTENT expiration=null priority=0, redelivered=false
receivedExchange=iringKey=, deliveryTag.va-Tag=, 98 0, messageCount=0])
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::: —
{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"1904:
IP","lastScanTimeLong":0,"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15,771 DEBUG [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 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
::::- VA SendSyslog systemMsg
:[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA Failure","TC-
NAC.Details","1904:IP","TC-NAC.MACAddress","24:77:03:3D:CF:20","TC-
NAC.IpAddress","10.201.228.102","TC-NAC.AdapterInstanceUid","796440b7-09b5-4f3b-b611-199a88
4b99","TC-NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

解決方案：

Qualys Cloud表示終端的IP地址不符合掃描條件，請確保已將終端的IP地址新增到Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts

參考資料

- 思科身份服務引擎管理員指南2.1版
- 技術支援與文件 - Cisco Systems
- 影片：採用Qualys的ISE 2.1
- Qualys文檔