# 使用Qualys配置ISE 2.1以威脅為中心的NAC(TC-NAC)

# 目錄

簡介 必要條件 需求 採用元件 設定 高級流程圖 配置Qualys雲和掃描器 步驟1.部署Qualys Scanner 步驟2.配置Qualys掃描器 配置ISE 步驟1.調整Qualys雲設定以便與ISE整合 步驟2.啟用TC-NAC服務 步驟3.配置Qualys介面卡與ISE VA框架的連線 步驟4.配置授權配置檔案以觸發VA掃描 步驟5.配置授權策略 驗證 身分識別服務引擎 **Qualys Cloud** 疑難排解 ISE上的調試 典型問題 參考資料

# 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



### 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

Vulnerability Management V										
Dashboard Scans		Reports	Remediation	Assets	KnowledgeBase	Users				
Scans	Scans	Maps	Schedules	Appliances	Option Profiles	Authe				
New 🗸 Search Scanner Appliance					D					
Virtual Scanner Appliance Replace Scanner Appliance				:	20539994589436					
Download										

### 選擇Download Image Only,然後選擇適當的分發

	6
ense(s) available. Choose one of the	e options below to get started.
Download Image Only	I Have My Image
I want to download the virtual image now and configure my scanner later.	I'm ready to complete the configuration of my scanner.
Download	Continue >
	ense(s) available. Choose one of the Download Image Only I want to download the virtual image now and configure my scanner later. Download

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.noa
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。

QUALYS' ENTERPRISE								
Vulnerability Management ~				8	🛐 Nep 🗸 Expensionershuk (socke) 🗸 Lapod			
Dashboard Scane Reports Remediati	on Assets KnowledgeBase Users							
Scane Scane Maps Schedules	Applances Option Profiles Authentication	Search Lists Setup						
Nex w Basth					1 1-242 D 0 = 11 III			
Applance	. 0	LAN IP WAN IP Pulling	Scarver	Signatures	Last Update			
Anneyt, salys	20530094589408	10.62.145.82 10.62.145.80 180 seconds	8339-1	233642	06/27/2014 at 23:95:30 (SMT+0400) (SA)			

# 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

/SS Setup	20
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	U
Cancel	Save

 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。

			Launch Help	2	-
ust be employees or contractor	rs of your company who are bound	to confidentiality obligations as pro	tective as those contained in the Qualys	\$8	
> User Role					
> Licer Pole: *	Harris				
>	manager				
> Allow access to:	GUI 🗹 API				
Business Unit: *	Unassigned	•			
	New Business Unit				
					ñ
	ust be employees or contractor          >       User Role: *         >       Allow access to:         >       Business Unit: *	ust be employees or contractors of your company who are bound	User Role: * Manager Alow access to: OUI OPI Business Unit: * Unassigned New Business Unit	use be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Quary          >       User Role: *       Manager         Allow access to:       •       •         >       •       •         New Business Unit: *       Unassigned       •         New Business Unit:       •       •	Ver Role:     User Role:     Image:     Allow access to:     Image:     Imag

•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

New Hosts	Launch Help	Ø	×
General Information:	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		
Cancel	A	bb	

### 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。

Deployment Nodes List > ISE21-3ek	
Edit Node General Settings Profiling Configura	ition
Hesterne TCE31-3ak	
EOON ISE21-3ek	vamala com
IP Address 10 62 145 2	E C
Node Type Identity Ser	vices Engine (ISE)
Personas	
✓ Administration	Role STANDALONE Make Primary
Monitoring	Personas Personas Other Monitoring Node
✓ Policy Service	
C Enable Session Services	Include Node in Node Group None *
C Enable Profiling Service	
C Enable Threat Centric NAC Serv	ice 🕢

## 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。

dentity Services Eng	gine Home	Context Visibility	<ul> <li>Operations</li> </ul>	Policy	▼ Admini	istration	Work Centers	
System Identity Manag	ement   Network	Resources + Device	Portal Management	pxGrid S	ervices	Feed Sen	vice + PassiveID	Threat Centric NAC
Third Party Vendors								
Vendor Instances > New Input fields marked with an asterisk (*) are required.								
Vendor •	Qualys : VA				Ŧ			
Instance Name *	QUALYS_VA							
			a	ancel	ave			

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

dentity Services Engine		Home Context Vis	sibility • Operations	Policy     Administration	Work Centers	
<ul> <li>Syste</li> </ul>	m Identity Management	Network Resources	Device Portal Managemen	t pxGrid Services + Feed S	ervice + PassiveID	* Threat Centric NAC
Third Pa	arty Vendors					
Vende	or Instances					
CR	efresh 🕂 Add 📋 Trash •	C Edit				▼ Filter ▼ • •
	Instance Name	Vendor Name	Туре	Hostname	Connectivity	Status
	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
	QUALYS_VA	Qualys	VA		Disconnected	Ready to configure

### 帳戶應該是具有管理員許可權的帳戶,按一下**下一步**。

dudu cisco	Identity Services Engine	Home	Context	Visibility	<ul> <li>Operations</li> </ul>	Policy	▼ Adm	inistration	• Work Centers		
<ul> <li>Syst</li> </ul>	em Identity Management	Network	Resources	Device	Portal Management	pxGrid S	ervices	+ Feed Ser	vice + PassiveID	* Threat Centric NAC	
Third P	Party Vendors										
Vende Ente Enabl addre	or Instances > QUALYS_VA or Qualys Configuration e CVSS Scoring in Qualys (Re ss of your endpoints in Qualys	Details ports->Setup- (Assets > Hos	>CVSS Scori It Assets)	ng>Enable	e CVSS Scoring) and	add the IP					
RES	T API Host										
qu	ualysguard.qg2.apps.qualys.co	m									
The	hostname of the Qualys platfo	rm where you	r account is lo	ocated.							
RES	T API Port										
44	43										
The	port used by the REST API ho	st.									
lice	mama										
CS	c2ek										
User	r account with Manager priviles	es to the Qua	lys platform.								
Dae	surved										
Pass	aword of the user.										
HTT	P Proxy Host										
Onti	onal HTTP Provy Host, Require	s provy port a	iso to be set.								
opo	on an interest of the second second	a bronk bour o									
нт	P Proxy Port										
Opti	onai HTTP Proxy Port. Require	s proxy host al	so to be set.								
						_					
					Car	cel Nex	đ				

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。

Identity Services Engine	Home	Context	Visibility	Operations	Policy	▼ Ad	ministration	→ Wo	rk Centers	
System Identity Management	Network	Resources	+ Device	Portal Management	pxGrid Se	rvices	Feed Ser	rvice	PassiveID	Threat Centric NAC     ■
Third Party Vendors										
venoor instances > QUALTS_VA										
Scanner Mappings										
Default Scanner										
ekomeyc_qualys						*				
Default scanner to use for scans.										
PSN to Scanner Mapping Map Policy Service Node (PSN) to a	Qualys scan	ner appliance.	This confi	guration ensures tha	t the selected	I				
Map ISE21-3ek to:	on the PSN	withon auchors	des une enc	pon.						
× ekorneyc_qualys										
				Car	icel Next					

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。

ence Id	entity Services Engine	Home Context	Visibility • Operations	Policy      Administration	Work Centers	
<ul> <li>System</li> </ul>	n Identity Management	Network Resources	Device Portal Manageme	ant pxGrid Services + Feed Se	rvice + PassiveID	▼ Threat Centric NAC
Third Pa	rty Vendors					
Vendo © Re	r Instances fresh + Add 會Trash	• © Edit				Ÿ Filter ▼ Q ▼
	Instance Name	Vendor Name	Туре	Hostname	Connectivity 5	Status
×	Instance Name	Vendor Name	Туре	Hostname	Connectivity	Status
0	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected /	Active
$\Box$	QUALYS_VA	Qualys	VA.	qualysguard.qg2.apps.qualys.com	Connected /	Active @
					Knowledge in-progress	e base download s

### 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。

dentity Services Engine	Home  Context Visibility  Operations  Policy  Administration  Work Centers
Authentication Authorization Profil	ing Posture Client Provisioning   Policy Elements
Dictionaries + Conditions * Result	5
0	
Authentication	Authorization Profile Authorization Profile
- Authorization	Name 14 Care
<ul> <li>Authorization</li> </ul>	Name VA_Scan
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT T
Profiling	Network Device Profile 🗮 Cisco 💌 🕀
+ Posture	Service Template
<ul> <li>Client Provisioning</li> </ul>	Track Movement
r Ginetit Provisioning	Passive identity Tracking (1)
	* Common Tasks
	Assess Vulnerabilities
	Adapter Instance QUALYS_VA   *
	48
	Trigger scan if the time since last scan is greater than 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。

intication	Authorization Profiling P	osture Client Provi	ioning > Policy Ele	ments			
the Autho	Policy rization Policy by configuring rules	based on identity gro	ps and/or other condi	tions. Drag and drop ru	ies to change	the order.	
loy Expon	lgo to Administration > System > ule Applies *	sackup & Hestore > P	sicy Export Page				
ception	s (1)						
Status	Rule Name	Cond	ions (identity groups a	and other conditions)		1	Permissions
<b>X</b>	Exception Rule	i Threa	Qualys-CVSS_Base	Score GREATER 8		then	Quarantine
	Wireless Black List Default	i Black	ist AND Wireless_Ao	cess		then	Blackhole_Wireless_Aco
						-	
	Profiled Cisco IP Phones	- Cisco	IP-Phone			Unen	Cisco_IP_Phones
2	Profiled Non Cisco IP Phones	if Non_	lisco_Profiled_Phone:	5		then	Non_Cisco_IP_Phones
0	Compliant_Devices_Access	ii (Netw	ork_Access_Authentic	ation_Passed AND Co	mpliant_Devic	ces) then	PermitAccess
0	Employee_EAP-TLS	I (Wire MAC)	iss_802.1X AND BYC in_SAN )	D_is_Registered AND	EAP-TLS AN	D then	PermitAccess AND BYOC
0	Employee_Onboarding	i (Wire	ISS_802.1X AND EAP	-MSCHAPv2)		then	NSP_Onboard AND BYO
2	WI-FI_Guest_Access	i (Guer	Flow AND Wireless,	MAB)		then	PermitAccess AND Gues
2	WI-FI_Redirect_to_Guest_Login	i Wirel	ss_MAB			then	Cisco_WebAuth
	Basic_Authenticated_Access	if Netwo	rk_Access_Authentica	ation_Passed		then	VA_Scan
	Default	if no mate	es, then DenyAo	cess			

# 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。

cisco Identity Ser	vices Engine	9 Home	+ Context Visib	illy • Oper	ations + Policy	+ Administration + Wor	k Centers					License Warning	۸.	٩,	0	£.	0
- RADIUS TC-N	AC Live Logs	+ TACACS	Reports + Trou	bleshoot + A	daptive Network Contr	ol .											
Live Logs Live Se	esions																
					-							-					
									Refrech	Every 1 minute	• Show	Latest 20 records	•	Vithin	Last 241	ours	•
CRebesh ORe	set Repeat Cour	ns A Export 7	5 <b>-</b>												¥ rise		۰۰
Time		Status	Details	Repeat	Identity	Endpoint ID	End	spoint P	Author	ntication Policy	1	Authorization Polic	у			Auth	orizatio
		Auth Pase 📩	×		Meetity	C0.4A.00.14.8D.4B	×	(point Profil	Asthe	etication Policy		Authorization Policy				Aub	visation
Jun 28, 2016 07:25:10.5	PM IN	•			alce	C0:4A.00:14:8D:48	Mic	rowsh-Wo	Default	>> Dot1X >> Defau	k 1	Default >> Exception R	ale			Quara	etine
Jun 28, 2016 07:25:07.0	K5 PM		.0			C0.4A.00.14.8D.48											
Jun 28, 2016 07:06:23.4	87 PM				alce 🕈	C0:4A:00:14:8D:48 💠	1794	LINK-Dr	Defailt	>> Dot1X >> Defa	k	Default >> Basic_Aath	officati	et,Acc	-	10,5	-

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。

identity dervices Engine	Home *CO	next visibility	serations + Policy	<ul> <li>Administration</li> </ul>	Work Centers		License Warning A	
points Network Devices								
CHORODAT COUNT	DV OUCO							
ENDPOINT COUNT	BT CVSS							
Number of Endpoints Affecte							1	
						1	10	
0				VSS Score			-	
• · · · · · · · · · · · · · · • • • • •	2	3	4	5 6	7	8 9	10	
0	2 h+ Gilli AN	3	4 4 400 * Cear Threats &	5 6 Vulnezbilities Export •	7 Import + MDM Actio	8 9 RowsPage 1 1	10 N	FIGo 1 Total Pic
Refere + Add E Tree	2 A + G'lin AN Usemame	3 Change Authoriza IPv4 Address	4 4 dos * Cour Threats & Walnerability	5 6 Vulnenbillies Export • r Source	7 Import * MEM Action Score	8 9 RowsPage 1 • ns * Revoke Certificate Location	Connectivity	Go 1 Total Ro Y Filter * C Hostname
Referent + Add B Trus MAC Address	2 A * & Bdit AN Usemame Usemame	3 C+ Charge Autoriza IPv4 Address IPv4 Address	4 4 4 4 4 Vulnerability Vulnerability	5 6 Vulnenbilities Export • Source Source	7 Import * MDM Actio Score Score	8 9 PowsPage 1 9 m.* Revoke Certificate Location Location	TO TO TO TO TO TO TO TO TO TO	File Go 1 Total Ro Y Filer * C Hostname
0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1           0         1	2 & * & disk ANO Usemame Usemame alore	3 C+ Charge Authoriza IPv4 Address IPv4 Address IDv4.Address 10.62.148.63	4 4 4 4 Vulnerability QD-90783	5 6 Vulnenihilitis Export + Source Source Quelys	7 Import * MEM Action Score 9.3	8 9 RowsPage 1 • ms * Reveix Certificate Location Location Location	Connectivity Connectivity Disconnected	V Filter * C Hostname Romane skoncyo PC
Add Trans     Add Trans     MAC Address     MAC Address     MAC Address     MAC Address     MAC Address	2 dr & Bits ANC Usemanne Usemanne alce	3 C+ Osege Autoria IPv4 Address IPv4 Address ID42.148.63	4 4 4 4 4 4 4 4 4 4 4 4 4 4	5 6 Vulnenshillies Export * / Source Source Qualys Qualys	7 Import * MDM Action Score 9.3 9.4	8 9 RowsPage 1 • ms * Revoke Certificate Location Location Location	Connectivity Connectivity Disconnected	V Filer + C Hostname Romane demain PC
Add B Tree     MAC Address     MAC Address     MAC Address     Co4A.00148048	2 dr Cildi AN Usemame Usemane alce	3 C* Charge Authorizz IPv4 Address IPv4 Address 10.62.148.63	4 4 4 4 4 4 4 4 4 4 4 4 4 4	5 6 Vulneshiltio Export • r Source Source Quetys Quetys	7 Import * MDM Action Score 9.3 9.4 4.7	8 9 PowsPage 1 1 ss * Revoke Contificate Location Location Location	Connectivity Connectivity Disconnected	Go 1 Total Po     Triter *      G     Hostname     skoneyo PC
0         1           0         1           0         1           0         4.44           0         MAC Address           1         MAC Address           1         MAC Address           1         Co.4A.00.14.80.48	2 A * G bit AND Usemame Usemame alce	3 C* Change Authorizz IPv4 Address IPv4 Address IPv4 Address I0.62.148.63	4 ton * Cour Threats & Vulnerability QID-90783 QID-90783 QID-90882 QID-90882	5 6 Vulneshilties Export *	7 Import * MDM Action Score 9.3 9.4 4.7 7.3	8 9 PowsPage 1 9 m * Revoke Certificate Location Location Location	Connectivity Connectivity Disconnected	P Co 1 Total Po     V Piter * C     Hostname     Instrame     ekonego PC

## 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。

cisco Identit	y Services Engine	Home	▼ Context Visibility	<ul> <li>Operations</li> </ul>	Policy	Administration	<ul> <li>Work Centers</li> </ul>
Endpoints	Network Devices						
Endpoints >	C0:4A:00:14:8D:4B						
C0:4A:0	0:14:8D:4B	0 Q	8				
Ę	MAC Address: C0 Username: alice Endpoint Profile: I Current IP Addres Location:	):4A:00:14:8 Microsoft-We as: 10.62.148	D:4B orkstation .63				
Attrit	outes Authentication	n Threa	ats Vulnerabilities				
QID-90783							
Title:	Microsoft Windows Ren	note Desktop I	Protocol Remote Code Exe	cution Vulnerability	(MS12-020)		
CVSS score:	9.3						
CVEIDS:	CVE-2012-0002,CVE-2	012-0152,					
Reported by:	Qualys						
Reported at:							
QID-38173							
Title:	SSL Certificate - Signate	are 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

**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。

ence ider	tity Services Engine	Home + Context V	ability •Operat	ions + Policy	+ Adm	inistration + Work Cent	675	License V	Varning 🔺 🔍	0 2	. 0
+ RADIUS	TC-NAC Live Logs	TACACS Reports + T	roubleshoot + Ad	aptive Network Cont	NOR						
Threat Cen	tric NAC Livelog										
C Retroh	A Export To • • • Pa	und .								Y Filter -	0-
Time	•	Endpoint ID	Username	Incident type	Ven	Old Authorization p	New Authorization	Authorization rule matched	Details		
×		Endpoint ID	Usemane	Incident type	Vende	Old Authorization profile	New Authorization profile	Autorization rule matched			
Tue A	un 28 2016 12:25:32 GMT-05	C0.4A.00.14.8D.48	alice	valuerability	Qualys	VA_Scan	Quarantine	Exception Rale	CVS5_Bas CVS5_Ten	_Score: 9.4 poral_Score: 7.2	,

# **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

<b>QUALYS'</b> ENTERPR	RISE							
Vulnerability Management	*					🖂 🖄	Help 🛩 Eugene Kor	meychuk (csc2ek) 🛩 🛛 Logout
Dashboard Scans	Reports Remediation	Assets K	KnowledgeBase	Users				
Scans Scans	Maps Schedules	Appliances	Option Profiles	Authentication	Search Lists Setup			
Actions (0)	ech Filters w						4 1 - 13 of 13	
Title				Targets	User	Reference	Date	- Status
C (selicen				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

<b>QUALYS'</b> ENTER	PRISE									
Vulnerability Manageme	nt v i							S 🔂	Help 🛩 🛛 Eugene Kor	neychuk (csc2ek) 🛩 🛛 Logout
Dashboard Scan	Reports	Remediation	Assets	KnowledgeBase	Users					
Scans Scan	Maps	Schedules	Appliances	Option Profiles	Authentication	Search List	s Setup			
Actors (0)	Search Filters 1	<							4 1 + 13 of 13	D • •
Title					Targets	Us	er	Reference	Date	- Status
C IseScan					10.62.148.63	Eu	gene Korneychuk	scan/1467134073.04090	05/25/2016	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**。

							S 1	Help 🛩 Eugene I	lomeythuk (csc2ek) ~	Lo
ashboard Scar	ns Reports	Remediation	Assets	KnowledgeBase	Users					
Scans Sca	ns Maps	Schedules	Appliances	Option Profiles	Authentication	Search Lists Setup				
tions (1) 🔍 New 🗤	Search Filters w	9						4 1 - 13 of 13	D Ov	
Title					Targets	User	Reference	Date	- Status	
IseScan					10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Finished	8
IseScan					10.201.228.107	Eugene Korneychuk	scan/1467132757.03967	06/28/2016	Finished	5
IseScan					10.201.228.102	Eugene Korneychuk	scan/1467131435.03855	06/28/2016	Finished	5
IseScan					10.62.148.89	Eugene Korneychuk	scan/1464895232.91271	06/02/2016	Finished	Ę
IseScan					10.62.148.71	Eugene Korneychuk	scan/1464855593.86436	06/02/2016	Finished	8
IseScan					10.62.148.71	Eugene Korneychuk	scan/1454850315.85548	06/02/2016	Finished	Ę
IseScan					10.62.148.71	Eugene Komeychuk	scan/1464847674.85321	06/02/2016	Finished	5
IseScan					10.62.148.71	Eugene Komeychuk	scan/1464841736.84337	06/02/2016	Finished	5
IseScan					10.62.148.71	Eugene Korneychuk	scan/1464836454.83651	06/02/2016	Finished	5
eview									Actions	-
alnerability Scan - rpet: 1 IP(s)	IseScan									
can launched by Eugene P	(omeychuk (csc2ek) 1	Start: 06/28/2016 at 2	11:16:55 (OMT+0	400) I Ended: 05/28/2016 at	21:22:17 (GMT+0400)   Scen	Finished (30:05:22)				
ummary Scanner(s) are fin	shed. Results from this	s scan have been pror	cessed.							

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)

🗸 Vulner	rabilities (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
- > <b>=</b>	1	ICMP Timestamp Request
Potent	tial Vulneral	bilities (1) 🕀 🖂

# 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** 

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System      Identity Management	Network Resources      Device Portal Management pxGrid Services      Feed Service      PassiveID      Threat Centric NAC
Deployment Licensing + Certificat	es   Logging   Maintenance Upgrade Backup & Restore   Admin Access   Settings
0	
Local Log Settings	Node List > ISE21-3ek.example.com Debug Level Configuration
Remote Logging Targets	besty teref configuration
Logging Categories	/ Edit Careet to Default
Message Catalog	Component Name   Log Level Description
Debug Log Configuration	val O
Collection Filters	O va-runtime DEBUG Vulnerability Assessment Runtime messages
	O va-service 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-adb0627f30248ad0","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_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"QUALYS_VA","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
- <u>技術支援與文件 Cisco Systems</u>
- 影片:採用Qualys的ISE 2.1
- Qualys文檔