Qualys で ISE 2.1 脅威中心型 NAC(TC-NAC)を設定する

目次

はじめに <u>前提条件</u> 要件 <u>使用するコンポーネント</u> 設定 高レベル フロー図 Qualys クラウドとスキャナの設定 <u>手順1:Qualysスキャナの導入</u> 手順2: Qualys スキャナの設定 ISE の設定 <u>手順1:ISE との統合のための Qualys クラウドの調整</u> 手順 2: TC-NAC サービスの有効化 <u>手順 3:Qualys アダプタの ISE VA フレームワークへの接続の設定</u> ステップ 4: VA スキャンをトリガーするための許可プロファイルの設定 ステップ5:許可ポリシーの設定 確認 **Identity Services Engine** Qualys クラウド トラブルシューティング ISE でのデバッグ よくある問題 参考資料

概要

このドキュメントでは、Identity Services Engine(ISE)2.1上で Threat-Centric NAC with Qualys を設定する方法を説明します。 Threat Centric Network Access Control(TC-NAC)機能を使用すると、許可ポリシーを、驚異および脆弱性アダプタから受け取る脅威と脆弱性の属性に基づいて作成することができます。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco Identity Service Engine
- Qualys ScanGuard

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Service Engine バージョン 2.1
- ワイヤレス LAN コントローラ (WLC) 8.0.121.0
- QualysGuard スキャナ 8.3.36-1、シグネチャ 2.3.364-2
- Windows 7 Service Pack 1

設定

高レベル フロー図



フローは次のとおりです。

- 1. クライアントがネットワークに接続すると、限定的なアクセスが付与され、[Assess Vulnerabilities] チェックボックスがオンになったプロファイルが割り当てられます。
- 2. PSN ノードが MNT ノードに Syslog メッセージを送信し、許可が行われたことと、VA スキャンが許可ポリシーの結果であることを確認します。
- MNT ノードは、次のデータを使用して、TC-NAC ノードに(Admin WebApp を使用して)
 SCAN を送信します。
 - MAC Address
 - IP アドレス
 - スキャン間隔
 - 有効化されている定期的なスキャン
 - 発信元 PSN
- 4. Qualys TC-NAC(Docker コンテナにカプセル化されています)は、Qualys クラウドと (REST API 経由で)通信し、必要に応じてスキャンをトリガーします。

5. Qualys クラウドは、エンドポイントをスキャンするよう Qualys スキャナに指示します。

- 6. Qualys スキャナは、スキャンの結果を Qualys クラウドに送信します。
- 7. 次のスキャン結果が TC-NAC に返送されます。
 - MAC Address
 - すべての CVSS スコア
 - すべての脆弱性(QID、タイトル、CVEID)
- 8. TC-NAC は、ステップ 7 のすべてのデータを PAN に反映します。
- 9. 設定されている許可ポリシーに従い、必要に応じて CoA がトリガーされます。

Qualys クラウドとスキャナの設定

注意: このドキュメントに記載する Qualys の設定は、ラボの目的のために行うものです。 設計上の考慮事項については、Qualys エンジニアに相談してください。

ステップ1: Qualys スキャナの導入

Qualys スキャナは OVA ファイルから導入できます。 Qualys クラウドにログインし、[Scans] > [Appliances and select New] > [Virtual Scanner Appliance] の順に移動します。

Vulnerability Ma	nagement	~					
Dashboard Scans		Reports Remediation		Assets	KnowledgeBase	Users	
Scans	Scans	Maps	Schedules	Appliances	Option Profiles	Authe	
New 🗸 Search							
Scanner Appliance					ID		
Virtual Scanner App	liance						
Replace Scanner Appliance					20539994589436		
Download							

[Download Image Only] を選択し、適切な配布方法を選択します。

Add N	New Virtual Scanner			×
V	ou have 4 virtual compar licens	cole) available. Choose one of the	options below to get started	
R	ou nave 4 virtual scamer licens	se(s) available. Choose one of the	options below to get started.	11
	Get Started	Download Image Only	I Have My Image	
	Help me to select the right virtual image and configure	I want to download the virtual image now and	I'm ready to complete the configuration of my scanner.	
	my scanner.	configure my scanner later.		
	Start Wizard >	Download	Continue >	
				-1-
Clos	e .			

[Scans] > [Appliances and select New] > [Virtual Scanner Appliance] に移動して [I Have My Image] を選択し、アクティベーション コードを取得します。

Add New Virtual Scanner	×
Name Your Virtual Scanner	
Virtual Scanner Name ekorneyc_qualys	
Close	Nex

スキャナ名を入力すると、後で使用する認証コードが付与されます。

手順2: Qualys スキャナの設定

OVA を選択した仮想化プラットフォームに展開します。 完了したら、次の設定を行います。

•ネットワーク(LAN)のセットアップ

- •WAN インターフェイスの設定(2つのインターフェイスを使用する場合)
- •プロキシの設定(プロキシを使用する場合)
- •スキャナのパーソナライズ

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.

その後、スキャナが Qualys に接続され、最新のソフトウェアとシグネチャがダウンロードされ ます。



Personalize

Update in progress 12%

Personalize this scanner >	Enter personalization code:
Set up network (LAN) >	Downloading ml_debian_keys-1.0.
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)	

スキャナが接続されているか確認するには、[Scans] > [Appliances] に移動します。

左側に緑色の接続中サインが表示されていれば、スキャナの準備は整っています。LAN IP、WAN IP、スキャナのバージョン、およびシグネチャも表示されています。

QUALYS' ENTERPRISE					
Vulnerability Hanagement 🔍				8	🛐 No 🗸 Expre Konsythak (solde) 🗸 Exped
Dashboard Scans Reports	Remediation Assets KnowledgeBase Users				
Scana Scana Mapa	Schedules Appliances Option Profiles Authentication	Search Lists Setup			
Nex w Seath					4 1-2#2 () O = 10 (0)
Applance	. 0	LAX P WAX P Puting	Scanner	Signatures	Last Update
ekoneyt, suitys	20530004589408	10.62.145.82 10.62.145.80 100 seconds	83361	233642	06/27/2014 at 23:55:30 (SMT-0400) 🐵

ISE の設定

Qualys スキャナと Qualys クラウドの設定が完了していても、ISE との統合が問題なく機能する ようにするには、クラウドの設定を調整する必要があります。 この作業は、GUI を使用してアダ プタを設定する前に行ってください。理由は、CVSS スコアを含むナレッジ ベースは、アダプタ の初回設定の後にダウンロードされるためです。

ステップ1: ISE との統合のための Qualys クラウドの調整

• [Vulnerability Management] > [Reports] > [Setup] > [CVSS] > [Enable CVSS Scoring] の順に 選択し、CVSS スコアを有効にします。

VSS Setup	2
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	
Cancel	ave

• アダプタ設定で使用するユーザ クレデンシャルに管理者権限があることを確認します。 左上 の角から自分のユーザを選択し、[User Profile] をクリックします。 [User Role] に表示される 自分の権限が [Manager] であることを確認します。

dit User			Launch Help	20
Information: Users Service Agreement.	must be employees or contracto	rs of your company who are bound to confidential	ity obligations as protective as those contained in the Qualy	68
General Information) User Role			
Jser Role	> Liter Role: *	Manager		
Options	>	Manager		
ecount Activity	Allow access to:	GUI API		
ecurity	>	Unassigned		
Cancel			s	ave

• [Vulnerability Management] > [Assets] > [Host Assets] > [New] > [IP Tracked Hosts] で、脆弱 性評価を必要とするエンドポイントの IP アドレス/サブネットが Qualys に追加されているこ とを確認します。

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	ld	

手順 2: TC-NAC サービスの有効化

[Administration] > [Deployment] > [Edit Node] で、TC-NAC サービスを有効化します。 チェック [Enable Threat Centric NAC Service] チェックボックスにマークを付けます。

注: TC-NAC ノードは、導入ごとに 1 つだけ存在します。

Deployment Nodes List > ISE21-3ek	
Edit Node General Settings Profiling Configuration	
Hostnama TSE21-3ak	
FOON ISE21-3ek example	com.
IP Address 10.62.145.25	
Node Type Identity Services End	gine (ISE)
Personas	
✓ Administration	Role STANDALONE Make Primary
	Personas
Monitoring	Role PRIMARY
Policy Service	
C Enable Session Services	Include Node in Node Group None *
C Enable Profiling Service	
Enable Threat Centric NAC Service	\odot

手順 3: Qualys アダプタの ISE VA フレームワークへの接続の設定

[Administration] > [Threat Centric NAC] > [Third Party Vendors] > [Add] の順に移動します。 [Save] をクリックします。

cisco	Identity Services	s Engine	Home	 Context Visib 	ility • Operations	Policy	▼ Ad	Iministration	• We	ork Centers	
+ S	ystem 🔸 Identity N	lanagement	Network i	Resources + D	Device Portal Manager	nent pxGrid S	Services	Feed Se	ervice	PassiveID	Threat Centric NAC ■
Thir	d Party Vendors										
Ve	ndor Instances > New out fields marked with	r an asterisk (*)	are required								
	Vendo	Qualys	: VA				٣				
	Instance Nam	e. QUAL	YS_VA								
						Cancel	iave				

Qualys インスタンスが [Ready to configure] 状態に遷移したら、[Status] 列で [Ready to configure] オプションをクリックします。

dentity Services Engine	Home	 Operations 	Policy Administra	ation Vork Centers	
System Identity Management	Network Resources + Devic	ce Portal Management	t pxGrid Services + F	eed Service + Passivel	Threat Centric NAC
Third Party Vendors					
Vendor Instances					
C Refresh + Add	C Edit				▼ Filter • • •
Instance Name	Vendor Name	Type H	lostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.co	m Connected	Active
QUALYS_VA	Qualys	VA		Disconnected	Ready to configure

[REST API Host] には、Qualys クラウドに使用する、自分のアカウントがあるホストを設定します。 この例では、「qualysguard.qg2.apps.qualys.com」が設定されています。

アカウントに管理者権限があることを確認し、[Next] をクリックします。

cisco	Identity Services Engine	Home	Context Visibil	ity Operations	Policy	▼ Administrat	ion 🔸	Work Centers		
+ Sys	tem Identity Management	Network I	Resources D	evice Portal Managemen	t pxGrid S	ervices + Fe	ed Service	PassiveID	Threat Centric NAC	1
Third	Party Vendors									
Ven Ent Enal addr	for Instances > QUALYS_VA er Qualys Configuration I ble CVSS Scoring in Qualys (Rep ess of your endpoints in Qualys (Details orts->Setup-> Assets > Host	CVSS Scoring>Ei t Assets)	nable CVSS Scoring) and	i add the IP					
R	ST API Host									
	ualysguard.qg2.apps.qualys.com									
Th	e hostname of the Qualys platform	n where your	account is located							
RE	ST API Port									
-	143									
Th	e port used by the REST API host									
Us	ername									
	sc2ek									
Us	er account with Manager privilege	s to the Qual	ys platform.							
Pa	ssword									
1										
Pa	isword of the user.									
н	TP Proxy Host									
Op	tional HTTP Proxy Host. Requires	proxy port al	so to be set.							
н	TP Proxy Port									
00	tional HTTP Proxy Port, Requires	proxy host als	so to be set.							
54	and a second sec	and the de								
				(Ca	voel Mer					

ISE により、Qualys クラウドに接続されているスキャナに関する情報がダウンロードされます。 このページでは、PSN to Scanner Mapping を設定することができます。 この設定により、エン ドポイントを承認する PSN に基づいてスキャナが選択されるようにできます。

ite Identity Services Engine	Home	Context	Visibility	 Operations 	Policy	▼ Ad	ministration	→ Wo	rk Centers	
System Identity Management	Network	Resources	+ Device	e Portal Managemen	t pxGrid S	ervices	 Feed Se 	rvice	PassiveID	▼ Threat Centric NAC
hird Party Vendors										
Scanner Mannings										
Default Scanner										
ekomeyc qualys						Ŧ				
Default scanner to use for scans.										
PSN to Scanner Mapping Map Policy Service Node (PSN) to a scanner appliance for scan is based	Qualys scan on the PSN	ner appliance. which authori	. This conf zes the en	iguration ensures the dpoint.	t the selecter	đ				
Map ISE21-3ek to:										
× ekorneyc_qualys										
				Ca	Nex					

詳細設定については、『ISE 2.1 管理者ガイド』を参照してください。このガイドへのリンクは、 このドキュメントの「参照」の項に記載されています。 [Next] と [Finish] をクリックします。 Qualys インスタンスが [Active] 状態になり、ナレッジ ベースのダウンロードが開始します。

注: Qualys インスタンスは、導入ごとに1つだけ存在します。

lt Id	lentity Services Engine	Home Context Visit	bility • Operations	Policy Administration	• Work Centers	
Syster	m Identity Management	Network Resources	Device Portal Manager	ment pxGrid Services + Feed Se	rvice Passivel	D Threat Centric NAC
ird Pa	urty Vendors					
endo	or Instances					
CR	efresh 🕂 Add 📋 Trash	• G'Edit				▼ Fiter • •
0	Instance Name	Vendor Name	Туре	Hostname	Connectivity	Status
×	Instance Name	Vendor Name	Туре	Hostname	Connectivity	Status
0	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
0	QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active @
					Knowle	dge base download

手順4: VA スキャンをトリガーするための許可プロファイルの設定

[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。 新しいプロファイルを追加します。 [Common Tasks] で、[Vulnerability Assessment] チェックボ ックスをオンにします。 オンデマンドのスキャン間隔は、ネットワーク設計に従って選択します。

許可プロファイルには、次の AV ペアが含まれています。

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 これらは、Access-Accept パケットでネットワーク デバイスに送信されます。ただし、これらの 実際の目的は、MNT ノードにスキャンのトリガーが必要になったことを通知することです。 MNT は、TC-NAC ノードに Qualys クラウドと通信するよう指示します。

dentity Services Engine	tome Context Visibility Operations Policy Administration Work Centers	
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements	
Dictionaries + Conditions • Results		
Authentication	Authorization Profiles > New Authorization Profile Authorization Profile	
- Authorization	*Name VA_Scan	
Authorization Profiles	Description	2
Downloadable ACLs	* Access Type ACCESS_ACCEPT *	
Profiling	Network Device Profile 🗮 Cisco 💌 🕀	
Posture	Service Template	
Client Provisioning	Track Movement	
	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	

ステップ5:許可ポリシーの設定

- ステップ 4 で設定した新しい許可プロファイルが使用されるよう、許可ポリシーを設定します。[Policy] > [Authorization] > [Authorization Policy] に移動し、
 [Basic_Authenticated_Access] ルールを選択し、[Edit] をクリックします。 [Permissions] を、(PermitAccess] から新しく作成した [Standard VA_Scan] に変更します。 これにより、脆弱性スキャンが全ユーザに対して実行されるようになります。 [Save] をクリックします。
- 検疫マシンの許可ポリシーを作成します。 [Navigate to Policy] > [Authorization] > [Authorization Policy] > [Exceptions] に移動し、[Exception Rule] を作成します。 [Conditions] > [Create New Condition (Advanced Option)] > [Select Attribute] をクリックし、画面を下へス クロールして [Threat] をクリックします。 [Threat] 属性を展開し、[Qualys-CVSS_Base_Score] を選択します。 演算子を [Greater Than] に変更し、セキュリティ ポリ シーに従って値を入力します。 許可プロファイル [Quarantine] では、脆弱なマシンには限定 的なアクセスが付与されるようにする必要があります。

- Contrary	Services Engline Home	Context Visibility Operations Policy Administration	Work Centers
entication	Authorization Profiling Post	ure Client Provisioning + Policy Elements	
	B-U-		
orization	n Policy	and an identity and an address that are different formation of the second data and the second s	
licy Export	2 go to Administration > System > Bac	sed on identity groups and/or other conditions. Drag and drop rules to change to kup & Restore > Policy Export Page	ne order.
Matched R	le Arolies *		
xception	s (1)		
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
×.	Exception Rule	Threat:Qualys-CVSS_Base_Score GREATER 8	then Quarantine
andard			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
1	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Acce
2	Profiled Cisco IP Phones	Cisco-IP-Phone	then Cisco_IP_Phones
2	Profiled Non Cisco IP Phones	I Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
0	Compliant_Devices_Access	I (Network_Access_Authentication_Passed AND Compliant_Device	s) then PermitAccess
0	Employee_EAP-TLS	I (Wreless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOC
0	Employee_Onboarding	<pre>// (Wireless_802.1X AND EAP-MSCHAPv2)</pre>	then NSP_Onboard AND BYO
	WI-FI_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Gues
	WI-FI_Redirect_to_Guest_Login	i Wireless_MAB	then Cisco_WebAuth
-	Basis Authenticated Assess	Network Access Authentication Passed	Data MA Case
×.	basic_Authenticated_Access		men wa_ocan

確認

Identity Services Engine

初回の接続により、VA スキャンがトリガーされます。 スキャンが終了すると CoA 再認証がトリ ガーされ、新しいポリシーが、一致していれば適用されます。

cisco Iden	tity Services Engin	e Home	Context Visible	• Opera	tions Policy	Administration	Work Ce	ntens				License Warning	A (۹.	0	£ 0	
* RADIUS	TC-NAC Live Logs	+ TACACS	Reports + Trout	sleshoot + Ac	deptive Network Contr	ol .											
Live Logs	Live Sessions																
												-					
									Refresh	Every 1 minute	• Show	Latest 20 records	• wes	in L	ast 24 ho		J
C Rebesh	O Reset Repeat Cou	as Lapor	To •												¥ Filter	•	•
Time		Status	Details	Repeat	Identity	Endpoint ID		Endpoint P	Auth	entication Policy		Authorization Policy	1			Authoriz	atic
		Auth Pase 📩	×		Mentity	C0.4A.00.14.8D.4B	×	Endpoint Profil	Asth	estication Policy		Autorization Policy				Authoria	ation 1
Jun 28, 2016 0	7:25:10:971 PM				alce	C0:4A:00:14:8D:48		Microsoft-Wo	Defaul	t >> Dot1X >> Defa	à.	Default >> Exception R	de :			Quarantin	
Jun 28, 2016 0	0.25.07.065 PM					C0.4A.00.14.8D.48											
Jan 28, 2016 0	7:06:23:457 PM				alce 🕈	C0:44:00:14:80:48	*	TP-LINK-Dr	Defea	t >> Dot1X >> Defa	a	Default >> Basic_Aathe	sticated_	Access		O. Scan	

どの脆弱性が検出されたか確認するには、[Context Visibility] > [Endpoints] に移動します。 各エンドポイントの脆弱性を Qualys が与えたスコアで確認します。

Rently Services Engine Hon	* Context Visibility	Operations	Poley P	Administration + Work	Centers		License Warning	-
oints Network Devices								
ENDPOINT COUNT BY CVS	S							
Number of Endpoints Affected							1	
							0	
0	2] 3			core				
0 l 1 l 0 1	2 3	4	CVSS 5	icore 6	7	8 9		
0 1	2 3	4	CV55 5	icore 6	7	8 9	18	
0 1	2 3	4	CV55.5 5	6	7	8 9 PowsPage 1 •	10 10 11 10	⊨ Go 1Tptal
0 1 1 Internet + Add 🛢 Treek + @ 1	2 3	4 Authorizatos * Cic	cords 5	6 nbilities Export * In	7 nport = MDM Actions =	8 9 RowsPage 1 1		⊢ Go 1 Total ▼ Filter +
tehesh +Add BTresh+ Gill MAC Address Useman	2 3 2 3 6 ANC+ Charge 0 IPv4 Ad	4 Authorizatos * Co Idress W	CVSS 5 5 eer Threes & Vulner Auherability	6 nbilition Export = In Source	7 nport * MEM Actions * Score	8 9 RowsPage 1 1	Connectivity	Filer *
Trank + Add Trank + G ii MAC Address Usernar MAC Address Usernar	2 3 2 3 8 ANC + Osege 0 IPv4 Ad	4 Authorizatos = Cir Sdress W dress 3	Cross 5 5 eer Threats & Vulner Autnerability Vulnerability	6 nbillio Expot = In Source Source	7 pert * MDM Actions * Score Score	8 9 PowsPage 1 Revola Certificate Location Location	Connectivity	P Go 1 Total T Filter + Hostname
	2 3 2 3 8 ANC + Osmpr 0 IPv4 Ad 10.62.141	4 Autorizatos * Cla Sdress W Idress V 163 O	CVISS 5 5 eer Throots & Vulner Authenability Vulnerability 20-50783	6 nbilities Export = In Source Source Costys	7 sport * MDM Actions * Score 0.3	8 9 PowsPage 1 Revolar Certificate Location Location Location Location	Connectivity Connectivity Disconnected	Fl Ge 1 Total F Filter * Hostname Hostname ekemeje PC
Truch + Add Truch + GFR MAC Address Usernam MAC Address Usernam MAC Address Usernam	2 3 2 3 8 ANC+ Osepr e IPv4 Ad 10.6234	4 Authorizatos * Cla Sdress W Liferen V Li63 G	Cristi S 5 ear Threats & Velace Adherability Velacebility 20-90783 20-38173	6 nbilition Export = In Source Coultys Outlys	7 port * MDM Actions * Score 9.3 9.4	8 9 PowsPage 1 Revolar Certificate Location Location Location Location	Connectivity Connectivity Decomented	Co 1 Total Y Filter * Hostname Restaure ekenspo PC
	2 3 2 3 8 ANC+ Osege e IPv4 Ad IPv4 Ad 10.62349	4 Authorizatos * Cla Sdress W threas %	Crisis is 5 for Threats & Value Admenability Valuerability 20-90783 20-90783 20-90783	6 abilition Export = In Source Coulys	7 port * MDM Actions * Score 9.3 9.4 4.7	8 9 PowsPage 1 Revoke Certificate Location Location Location Location	Connectivity Connectivity Disconnected	F Go 1 Total Y Filter + Hostname ekenspo-PC
T T	2 3 2 3 8 ANC+ Osege 9 IPv4 Ad 10.62349	4 Authorizatos * Cla Sdress W threas ? KAO Q Q	Crisis is 5 for Threats & Value Authorability Valuerability 200-90783 200-90882	6 nbilitio Export = In Source Custys Custys Custys Custys	7 port * MDM Actions * Score 0.3 0.4 4.7	8 9 PowsPage 1 Revoke Certificate Location Location Location Location	Connectivity Connectivity Disconnected	F Go 1 Total Y Filter + Hostname ekenego-PC
Image: Second	2 3 2 3 8 ANC+ Osege e IPv4 Ad IDv4.Ad 10.62349	4 Authorizatos * Cla Sdress W threas ? KAO C C C C C C C C C C C C C C C C C C C	S S S S S S S S S S S S S S	6 nbilitio Export = In Source Custys Custys Custys Custys Custys	7 sport * MDM Actions * Score 9.3 9.4 4.7 7.3	8 9 PowsPage 1 Revoke Certificate Location Location Location Location	Connectivity Connectivity Disconnected	F Go 1 Total Y Filter * Hostname ekengo-PC

特定のエンドポイントを選択すると、[Title] や [CVEIDS] など、各脆弱性の詳細が表示されます。

cisco	Identity	Services Engine	Home		 Operations 	Policy	Administration	 Work Centers
Endp	oints N	letwork Devices						
Endp	points >	C0:4A:00:14:8D:4B						
C	0:4A:00	0:14:8D:4B	0 G	8				
Ę		MAC Address: C0 Username: alice Endpoint Profile: I Current IP Addres Location:	:4A:00:14:8 Aicrosoft-W s: 10.62.148	D:4B forkstation 1.63				
	Attrib	utes Authentication	Thre	ats Vulnerabilities				
QI	0-90783							
Titl	e:	Microsoft Windows Ren	ote Desktop	Protocol Remote Code Exec	cution Vulnerability	(MS12-020)		
CV	SS score:	9.3						
CV	EIDS:	CVE-2012-0002,CVE-20	012-0152,					
Rep	ported by:	Qualys						
Rep	ported at:							
QI	0-38173							
Titl	e:	SSL Certificate - Signatu	re Verification	n Failed Vulnerability				
CV	SS score:	9.4						
CV	EIDS:							
Rep	ported by:	Qualys						
Rep	ported at:							

[Operations] > [TC-NAC Live Logs] では、適用された新旧の許可ポリシーと CVSS_Base_Score

注: 許可条件は、CVSS_Base_Score に基づいて設定されます。CVSS_Base_Score は、エンドポイントについて検出された最大の脆弱性スコアと同じ値です。

ence ld	entity Services Engine	Home + Context Val	•Operatio	ns + Policy	+ Adm	inistration + Work Cente	613	License	e Warning 🔺	9, O	٤.,	0
+ RADIU	S TC-NAC Live Logs >	TACACS Reports + Tro	ubleshoot > Adap	ptive Network Cont	rol							
Threat C	entric NAC Livelog											
C Refred	Laport To • ■ Par	-								Y File		o -
Te	ne	Endpoint ID	Username	Incident type	Ven	Old Authorization p	New Authorization	Authorization rule matched	Detail			
×		Endpoint ID	Usersame	Incident type:	Vende	Old Authorization profile	New Authorization profile	Autorization rule matched				
Te	e Jun 28 2016 12:25:32 GMT-05.	C0.4A.00.14.8D.48	alice	valuerability	Qualys	VA_Scat	Quarantine	Exception Rale	CV55, CV55,	Base_Score: 9.4 Temporal_Score:	7.7	

Qualys クラウド

VA スキャンが TC-NAC でトリガーされると、Qualys はスキャンをキューに入れます。これは [Scans] > [Scans] で確認できます。

C	QUALYS' ENTERPI	RISE											
	Vulnerability Management	v								🖂 🙆	Help 🛩 Eugene Ko	neychuk (csc2ek) 🗸 🛛 L	nogout
	Dashboard Scans	Reports	Remediation	Assets	KnowledgeBase	Users							
	Scans Scans	Maps	Schedules	Appliances	Option Profiles	Authentication	Search L	sts	Setup				
	Actions (0) - w	In Files v									4 1-13 of 13	D 0 - 1	
	Title					Targeta		User		Reference	Date	- Status	
	C (belicen					10.62.148.63		Eugene Ki	omeychuk	scarv1467134073.04090	06/28/2016	Queued	

その後、状態が [Running] に遷移します。これは、Qualys クラウドが Qualys スキャナに実際の スキャンを実行するよう指示したことを意味します。

(🗿 QUALYS'	ENTERP	RISE												
	Vulnerability Ma	nagement	~								S 1	Help 🗸	Eugene Korney	chuk (csc2ek) 🛩	Logout
	Dashboard	Scans	Reports	Remediation	Assets	KnowledgeBase	Users								
	Scans Scans	Scans	Maps	Schedules	Appliances	Option Profiles	Authentication	Search L	ists	Setup					
	Actions (0)	Nex v 8	each Filers -	-								(i) 1+1	0 of 13	D • • 🛙	
	Title						Targets		User		Reference	De	te .	- Status	
	🗆 🖒 IseGcan						10.62.148.63		Eugene	Korneychuk	scan/1467134073.04090	06/	28/2016	Runnin	. 8

スキャナによるスキャンの実行中は、[Scanning...] という サインが QualysGuard の右上の隅に 表示されます。



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

TIP: Press ENTER to access the menu.

スキャンが完了すると、[Finished] 状態に遷移します。 結果を表示するには、[Scans] > [Scans] で必要なスキャンを選択して、[View Summary] または [View Results] をクリックします。

Dashboard Sca	ns Reports	Remediation	Assets	KnowledgeBase	Users					
Scans Sca	ns Maps	Schedules	Appliances	Option Profiles	Authentication	Search Lists Setup				
Actions (1) 🔍 New 👓	Seath Files 1	*						4 1 - 13 of 13	Þ 0 - 1	
Title					Targets	User	Reference	Date	- Status	
IseScan					10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Finished	1
IseScan					10.201.228.107	Eugene Korneychuk	scan/1467132757.03987	06/28/2016	Finished	6
IseScan					10.201.228.102	Eugene Korneychuk	scan/1467131435.03855	06/28/2016	Finished	1
IseScan					10.62.148.89	Eugene Korneychuk	scan/1464895232.91271	06/02/2016	Finished	1
IseScan					10.62.148.71	Eugene Korneychuk	scan/1464855593.86436	06/02/2016	Finished	1
IseScan					10.62.148.71	Eugene Korneychuk	scen/1464850315.85548	06/02/2016	Finished	
IseScan					10.62.148.71	Eugene Korneychuk	scan/1464847674.85321	06/02/2016	Finished	1
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	1
review									Actions 1	-
Autoerability Scan - arget: 1 IP(s)	IseScan									
Scan launched by Eugene I	(omeychuk (csc2ek)	Bart 06/28/2016 at 2	1.18.55 (OMT+0	400) I Ended: 06/28/2016 at	21.22.17 (GMT+0400) Sear	Finished (20.05.22)				
ummary ficannerial are fo	ahed. Results from th	is scan have been pro-	becaut.							

レポート自体では、[Detailed Results] に、検出された脆弱性が表示されます。

Detailed Results

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

 Vulnerabilities 	(6)	ΞΞ	
-------------------------------------	-----	----	--

- 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

トラブルシューティング

ISE でのデバッグ

ISE 上でデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration] で TC-NAC ノードを選択し、[Log Level va-runtime] と [va-service] コンポーネン トを [DEBUG] に変更します。

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	bebug teres configuration
Logging Categories	/ Edit kg Reset to Default
Message Catalog	Component Name Log Level Description
Debug Log Configuration	
Collection Filters	O va-runtime DEBUG Vulnerability Assessment Runtime messages
	O va-service DEBUG Vulnerability Assessment Service messages

チェック対象のログは varuntime.log です。 ISE CLI から直接次の tail コマンドを発行します。

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

TC-NAC Docker が、特定のエンドポイントに対するスキャン実行の指示を受け取ります。

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

結果を受信すると、すべての脆弱性データをコンテキスト ディレクトリに保存します。

```
2016-06-28 19:25:02,020 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -::::: -- Got message from VaService:
[{"[{"macAddress":"C0:4A:00:14:8D:4B","ipAddress":"10.62.148.63","lastScanTime":1467134394000,"v
ulnerabilities":["{\"vulnerabilityId\":\"QID-90783\",\"cveIds\":\"CVE-2012-0002,CVE-2012-
0152,\",\"cvssBaseScore\":\"9.3\",\"cvssTemporalScore\":\"7.7\",\"vulnerabilityTitle\":\"Microso
ft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
38173\",\"cveIds\":\"\",\"cvssBaseScore\":\"9.4\",\"cvssTemporalScore\":\"6.9\",\"vulnerabilityT
itle\":\"SSL Certificate - Signature Verification Failed
Vulnerability\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90882\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.7\",\"cvssTemporalScore\":\"4\",\"vulnerabilityTit
le\":\"Windows Remote Desktop Protocol Weak Encryption Method
Allowed\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"vulnerabilityT
itle\":\"SMB Signing Disabled or SMB Signing Not
Required\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
38601\",\"cveIds\":\"CVE-2013-2566,CVE-2015-
2808,\",\"cvssBaseScore\":\"4.3\",\"cvssTemporalScore\":\"3.7\",\"vulnerabilityTitle\":\"SSL/TLS
use of weak RC4 cipher\",\"vulnerabilityVendor\": \"\"Qualys\"}"]}]
2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -::::: -- VA: Save to context db,
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: sending elastic search json to
pri-lan
2016-06-28 19:25:02,272 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaPanRemotingHandler -::::: -- VA: Saved to elastic search:
{{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
Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
38173", "cveIds":"", "cvssBaseScore":"9.4", "cvssTemporalScore":"6.9", "vulnerabilityTitle":"SSL
Certificate - Signature Verification Failed Vulnerability", "vulnerabilityVendor": ""Qualys"},
{"vulnerabilityId":"QID-
90882", "cveIds":"", "cvssBaseScore":"4.7", "cvssTemporalScore":"4", "vulnerabilityTitle":"Windows
Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": ""Qualys"},
{ "vulnerabilityId": "QID-
90043", "cveIds":"", "cvssBaseScore":"7.3", "cvssTemporalScore":"6.3", "vulnerabilityTitle":"SMB
Signing Disabled or SMB Signing Not Required", "vulnerabilityVendor": ""Qualys"},
{"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-
2808, ", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS use of weak
RC4 cipher", "vulnerabilityVendor": ""Qualys"}]
```

チェック対象のログは vaservice.log です。 ISE CLI から直接次の tail コマンドを発行します。

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

次の脆弱性アセスメント要求がアダプタに送信されます。

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.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 が、スキャンが終了するまで5分ごとにスキャンの状態を確認します。

2016-06-28 17:09:43,459 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter : {"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0", "VendorName": "Qualys", "OperationMessageText": "Number of endpoints queued for checking scan results: 1, Number of endpoints queued for scan: 0, Number of endpoints for which the scan is in progress: 0"} 2016-06-28 17:14:43,760 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter : {"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0", "VendorName": "Qualys", "OperationMessageText": "Number of endpoints queued for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which the scan is in progress: 1"} 2016-06-28 17:19:43,837 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter : {"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0", "VendorName": "Qualys", "OperationMessageText": "Number of endpoints queued for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which the scan is in progress: 1"} 2016-06-28 17:24:43,867 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter : {"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0", "VendorName": "Qualys", "OperationMessageText": "Number of endpoints queued for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which the scan is in progress: 1"}

アダプタが QID、CVE、および CVSS スコアを取得します。

```
2016-06-28 17:24:57,556 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"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
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", "vulnerabilityVendor": "Qualys" }, { "vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-
0002,CVE-2012-
0152, ", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "vulnerabilityTitle": "Microsoft Windows
Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)", "vulnerabilityVendor": "Qualys" }, { "vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-
2566,CVE-2015-
2808, ", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS use of weak
RC4 cipher","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": ""Qualys"}]}
2016-06-28 17:25:01,282 INFO
                               [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Endpoint Details sent to IRF is
{"CO: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 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 successfully
completed", "TC-NAC.Details", "VA completed; number of vulnerabilities found: 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"]}]

よくある問題

問題点 1: ISE が取得したレポートでは CVSS_Base_Score は 0.0、CVSS_Temporal_Score は 0.0 だが、Qualys クラウドのレポートには検出された脆弱性が表示されている。

問題:

Qualys クラウドからのレポートには検出された脆弱性が表示されているが、ISE には脆弱性が表 示されない。

vaservice.log には次のデバッグが表示されている。

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

解決策:

CVSS スコアがゼロになるのは、脆弱性がないためか、または、Qualys クラウドでの CVSS ス コアの有効化が UI を使用してアダプタを設定する前に行われなかったためです。 CVSS スコア 機能の有効化が記載されたナレッジ ベースは、アダプタが初めて設定された後にダウンロードさ れます。 CVSS の有効化は、ISE にアダプタ インスタンスが作成される前に行う必要があります 。 これは、[Vulnerability Management] > [Reports] > [Setup] > [CVSS] > [Enable CVSS Scoring] で実行できます。

問題点 2:正しい許可ポリシーが一致するにもかかわらず、結果が Qualys クラウドから ISE に 返送されない。

問題:

修正された許可ポリシーが一致したため、VA スキャンがトリガーされるはずである。 にもかか わらず、スキャンが実行されない。

vaservice.log には次のデバッグが表示されている。

```
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
((Body:'[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=irf.topic.va-reports, receivedRoutingKey=, deliveryTag=9830, messageCount=0])
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"Erro
r triggering scan: Error while trigeringon-demand scan code and error as follows 1904: none of
the specified IPs are eligible for Vulnerability Management
scanning.","lastScanTimeLong":0,"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15,771 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Adapter scan result failed for
Macaddress:24:77:03:3D:CF:20, IP Address(DB): 10.201.228.102, setting status to failed
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", "Error triggering scan: Error while trigering on-demand scan code and error as follows 1904: none of the specified IPs are eligible for Vulnerability Management 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"]}]

解決策:

Qualys クラウドは、エンドポイントの IP アドレスがスキャンの対象ではないことを示していま す。[Vulnerability Management] > [Assets] > [Host Assets] > [New] > [IP Tracked Hosts] で、IP ア ドレスがエンドポイントに追加されていることを確認してください。

参考資料

- Cisco Identity Services Engine 管理者ガイド リリース 2.1
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>
- ・ビデオ: ISE 2.1 with Qualys
- Qualys に関するドキュメント