

Configurazione di ISE 2.1 Threat-Centric NAC (TC-NAC) con Qualys

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Diagramma di flusso ad alto livello](#)

[Configura Qualys Cloud e scanner](#)

[Passaggio 1. Distribuire uno scanner Qualys](#)

[Passaggio 2. Configurare lo scanner Qualys](#)

[Configurare ISE](#)

[Passaggio 1. Regolare le impostazioni di Qualys Cloud per l'integrazione con ISE](#)

[Passaggio 2. Abilitare i servizi TC-NAC](#)

[Passaggio 3. Configurare la connettività della scheda Qualys a ISE VA Framework](#)

[Passaggio 4. Configurare il profilo di autorizzazione per attivare la scansione VA](#)

[Passaggio 5. Configurare i criteri di autorizzazione](#)

[Verifica](#)

[Identity Services Engine](#)

[Qualys Cloud](#)

[Risoluzione dei problemi](#)

[Debug su ISE](#)

[Problemi tipici](#)

[Riferimenti](#)

Introduzione

Questo documento descrive come configurare un NAC incentrato sulle minacce con Qualys on Identity Services Engine (ISE) 2.1. La funzionalità TC-NAC (Threat Centric Network Access Control) consente di creare criteri di autorizzazione basati sugli attributi di minaccia e vulnerabilità ricevuti dagli adattatori minacce e vulnerabilità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco Identity Service Engine
- Qualys ScanGuard

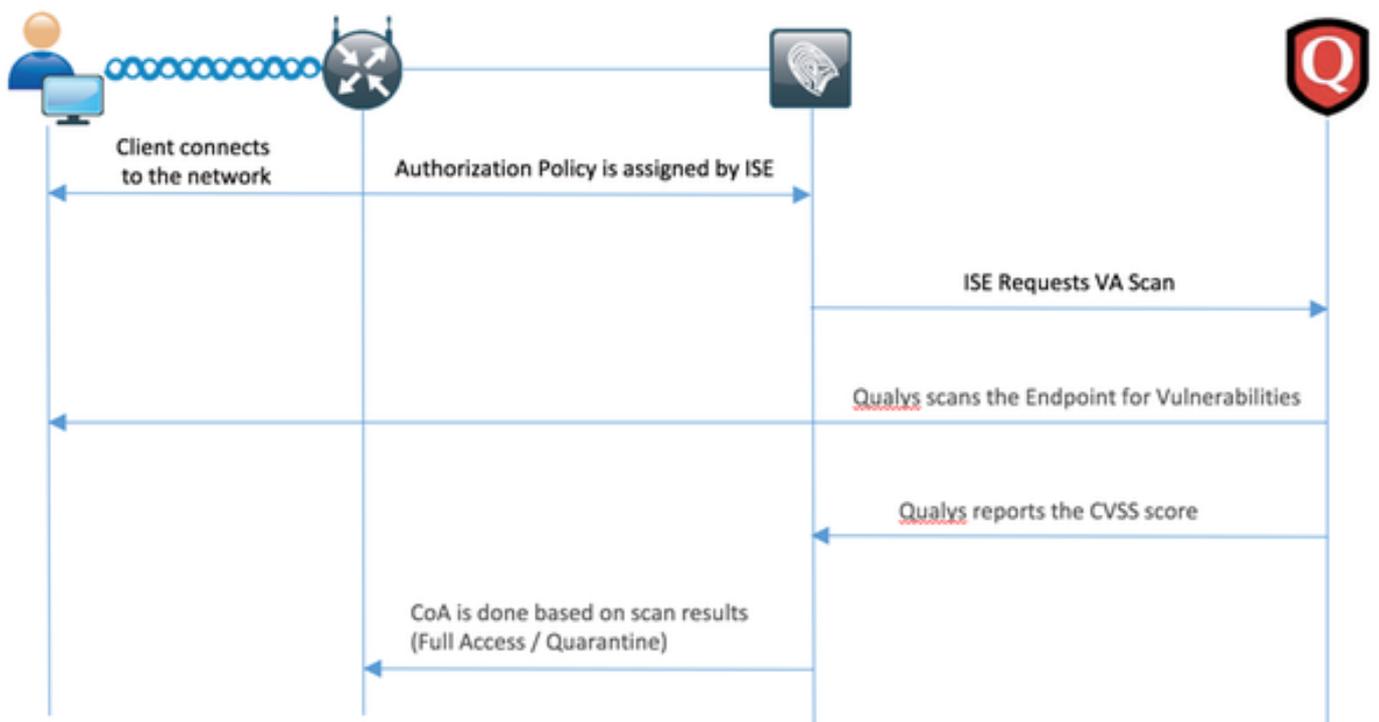
Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Service Engine versione 2.1
- Controller LAN wireless (WLC) 8.0.121.0
- Scanner Qualys Guard 8.3.36-1, Firme 2.3.364-2
- Windows 7 Service Pack 1

Configurazione

Diagramma di flusso ad alto livello



Questo è il flusso:

1. Il client si connette alla rete, viene concesso un accesso limitato e viene assegnato un profilo con la casella di controllo **Valuta vulnerabilità** abilitata
2. Il nodo PSN invia un messaggio Syslog al nodo MNT per confermare l'autenticazione e l'analisi VA è il risultato dei criteri di autorizzazione
3. Il nodo MNT invia SCAN al nodo TC-NAC (utilizzando Admin WebApp) utilizzando questi dati:
 - Indirizzo MAC
 - Indirizzo IP
 - Intervallo di scansione
 - Scansione periodica abilitata
 - PSN di origine
4. Qualys TC-NAC (incapsulato nel contenitore Docker) comunica con Qualys Cloud (tramite

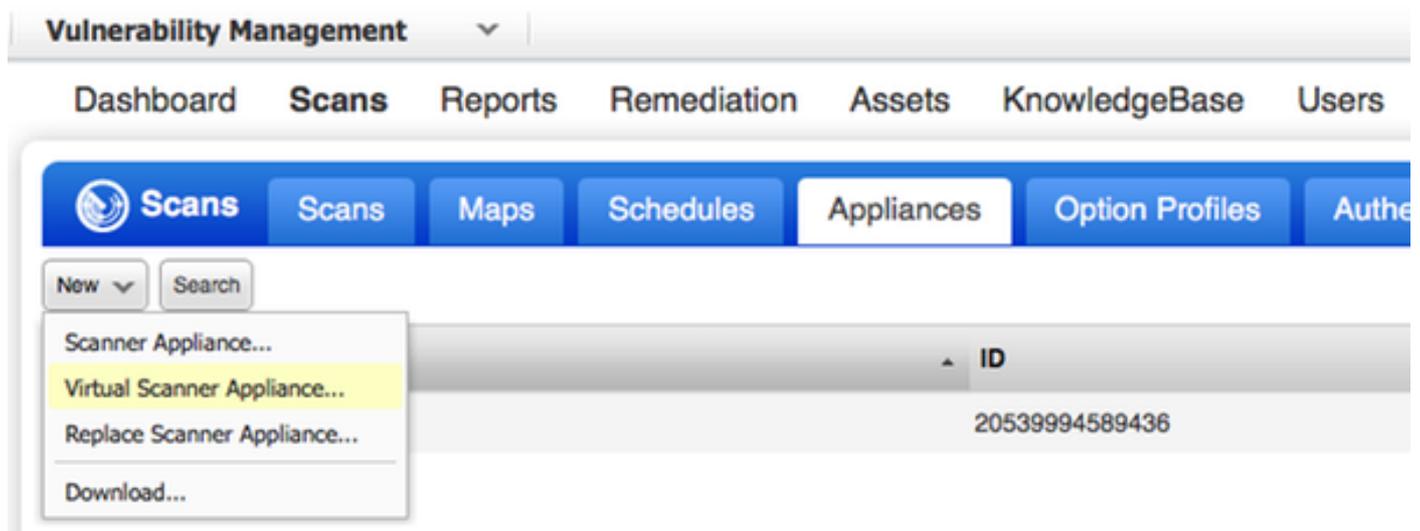
- l'API REST) per avviare la scansione se necessario
- Qualys Cloud indica allo scanner Qualys di analizzare l'endpoint
 - Lo scanner Qualys invia i risultati della scansione al cloud Qualys
 - I risultati della scansione vengono inviati al TC-NAC:
 - Indirizzo MAC
 - Tutti i punteggi CVSS
 - Tutte le vulnerabilità (QID, titolo, CVEID)
 - TC-NAC aggiorna la PAN con tutti i dati del passaggio 7.
 - Il CoA viene attivato se necessario in base ai criteri di autorizzazione configurati.

Configura Qualys Cloud e scanner

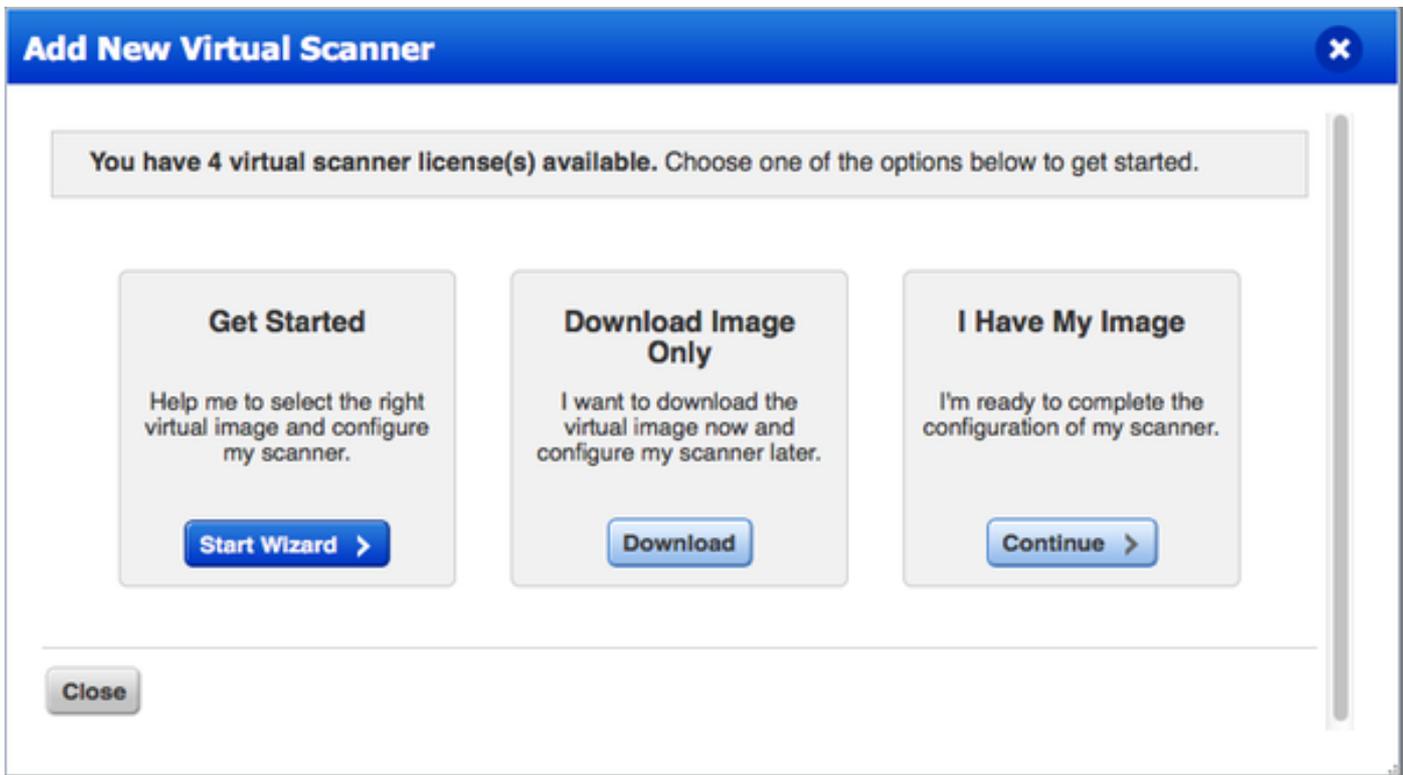
Attenzione: La configurazione Qualys descritta in questo documento è stata realizzata per scopi di laboratorio. Consultare i tecnici Qualys per le considerazioni sulla progettazione

Passaggio 1. Distribuire uno scanner Qualys

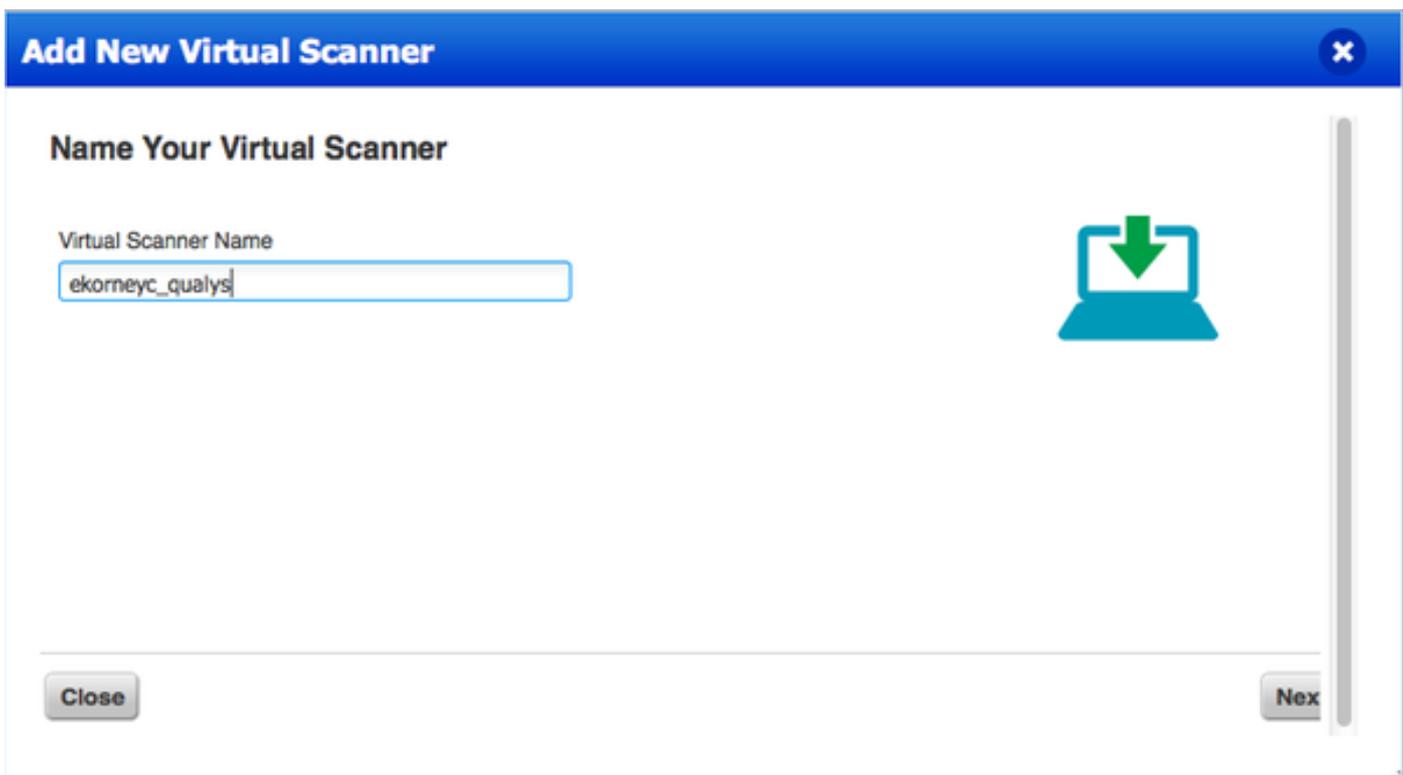
Lo scanner Qualys può essere distribuito da file OVA. Accedere al cloud Qualys e selezionare Scans > Appliance, quindi selezionare New > Virtual Scanner Appliance



Selezionare **Scarica solo immagine** e scegliere la distribuzione appropriata



Per ottenere il codice di attivazione, andare a Scans > Appliance e selezionare New > Virtual Scanner Appliance, quindi selezionare **I Have My Image (Ho la mia immagine)**.



Dopo aver immesso il nome dello scanner, si riceve il codice di autorizzazione che verrà utilizzato in seguito.

Passaggio 2. Configurare lo scanner Qualys

Distribuire OAV sulla piattaforma di virtualizzazione desiderata. Al termine, configurare le seguenti impostazioni:

- Configurazione della rete (LAN)
- Impostazioni dell'interfaccia WAN (se si utilizzano due interfacce)
- Impostazioni proxy (se si utilizza il proxy)
- Personalizza questo 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.

Successivamente lo scanner si collega a Qualys e scarica il software e le firme più recenti.

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)

Per verificare che lo scanner sia collegato, selezionare Scansioni > Accessori.

Il segno verde connesso a sinistra indica che lo scanner è pronto, è possibile vedere anche IP LAN, IP WAN, versione dello scanner e firme.

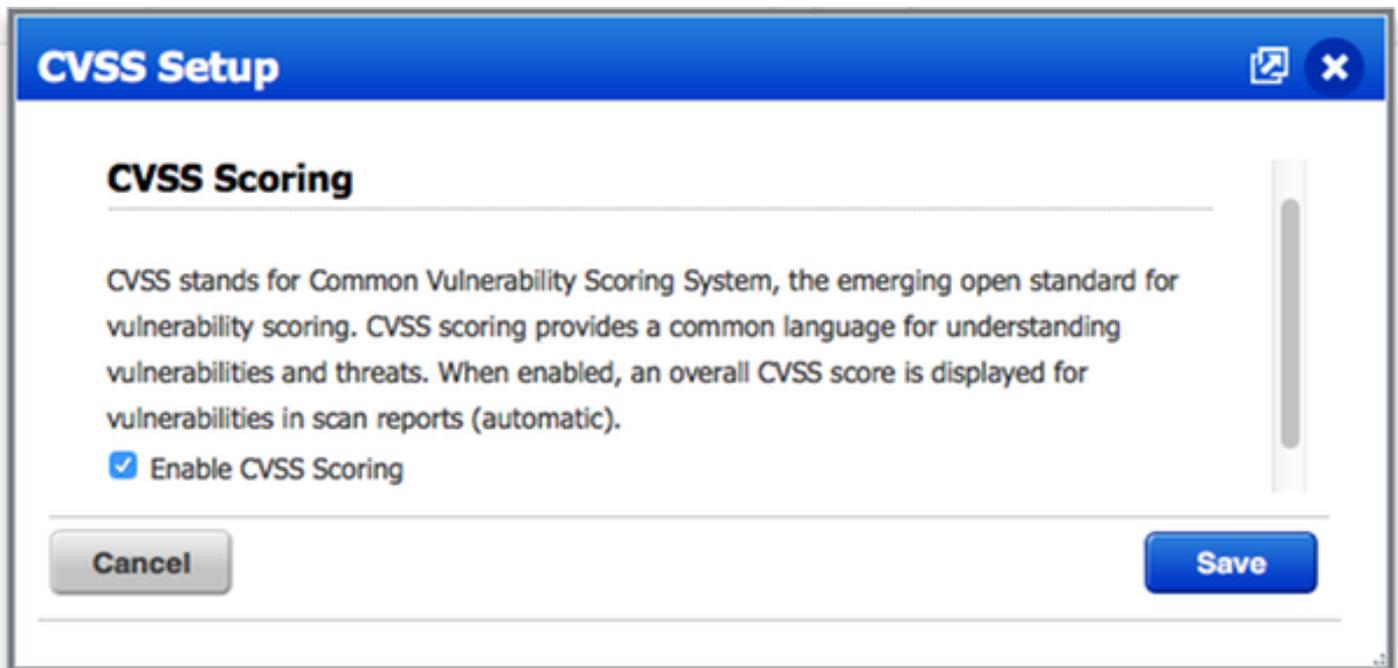


Configurare ISE

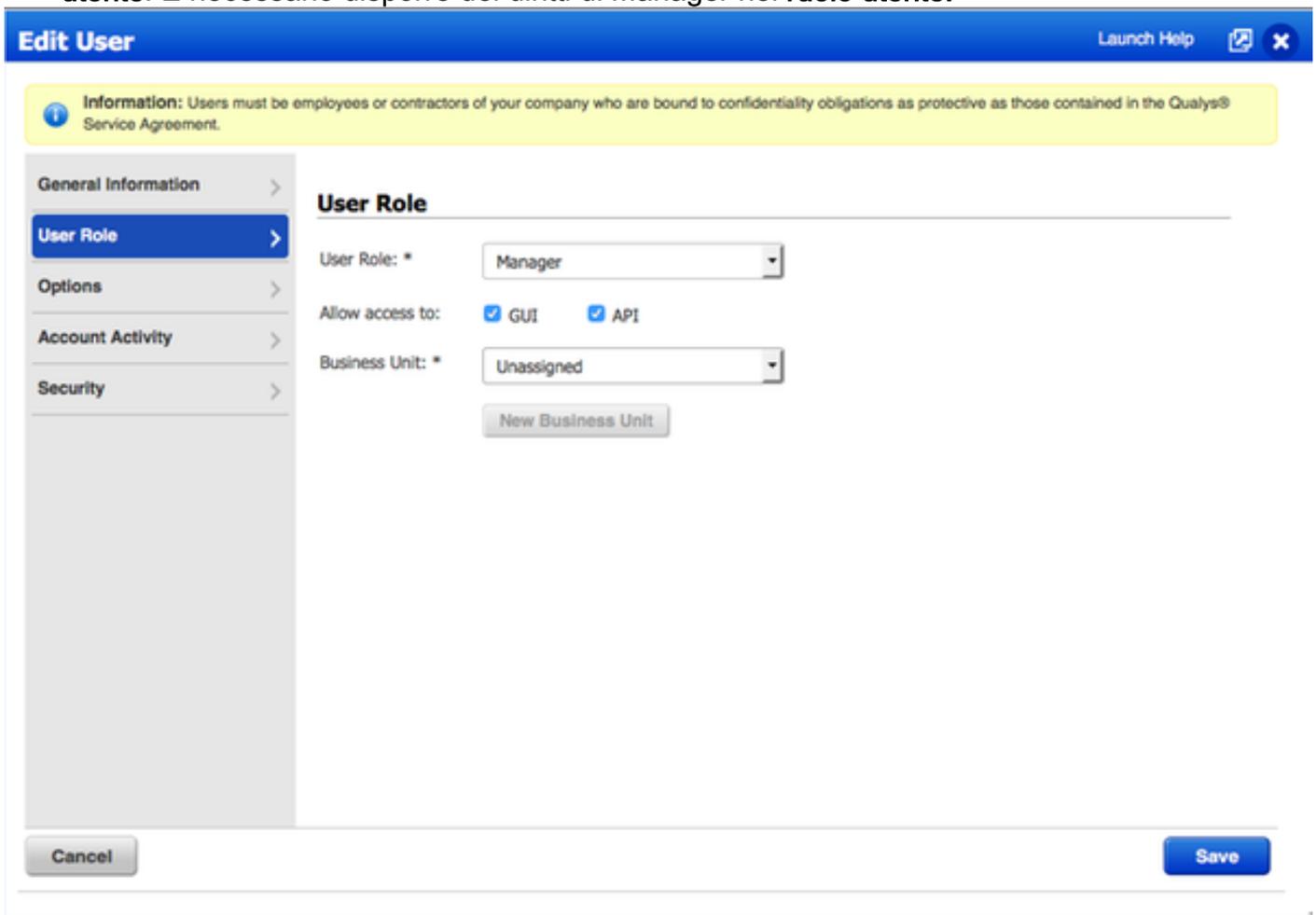
Anche se hai configurato Qualys Scanner e Cloud, devi comunque regolare le impostazioni del cloud per assicurarti che l'integrazione con ISE funzioni correttamente. Nota: questa operazione deve essere eseguita prima di configurare la scheda tramite GUI, poiché la knowledge base contenente il punteggio CVSS viene scaricata dopo la prima configurazione della scheda.

Passaggio 1. Regolare le impostazioni di Qualys Cloud per l'integrazione con ISE

- Abilita assegnazione punteggio CVSS in Gestione vulnerabilità > Report > Impostazione > CVSS > Abilita assegnazione punteggio CVSS



- Verificare che le credenziali utente utilizzate nella configurazione dell'adattatore dispongano dei privilegi di gestione. Selezionare l'utente dall'angolo superiore sinistro e fare clic su **Profilo utente**. È necessario disporre dei diritti di Manager nel **ruolo utente**.



- Verificare che gli indirizzi IP e le subnet di endpoint che richiedono la valutazione delle vulnerabilità vengano aggiunti a Qualys at Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts

New Hosts Launch Help

General Information: >

Host IPs >

Host Attributes >

Host IPs

Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

IPs: *

Add to Policy Compliance Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel **Add**

Passaggio 2. Abilitare i servizi TC-NAC

Abilitare TC-NAC Services in Amministrazione > Distribuzione > Modifica nodo. Verifica **Abilitazione del servizio NAC incentrato sulle minacce** casella di controllo.

Nota: Può esistere un solo nodo TC-NAC per distribuzione.

Edit Node

General Settings

Profiling Configuration

Hostname **ISE21-3ek**
FQDN **ISE21-3ek.example.com**
IP Address **10.62.145.25**
Node Type **Identity Services Engine (ISE)**

Personas

<input checked="" type="checkbox"/> Administration	Role STANDALONE Make Primary
<input checked="" type="checkbox"/> Monitoring	Role PRIMARY Personas <input type="text" value="Other Monitoring Node"/>
<input checked="" type="checkbox"/> Policy Service	Include Node in Node Group None i
<input checked="" type="checkbox"/> Enable Session Services i	
<input checked="" type="checkbox"/> Enable Profiling Service	
<input checked="" type="checkbox"/> Enable Threat Centric NAC Service i	

Passaggio 3. Configurare la connettività della scheda Qualys a ISE VA Framework

Passare a Amministrazione > NAC incentrato sulle minacce > Fornitori terzi > Aggiungi. Fare clic su **Save** (Salva).

Identity 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

Third Party Vendors

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

Vendor *

Instance Name *

Cancel Save

Quando l'istanza di Qualys passa allo stato **Pronta per la configurazione**, fare clic sull'opzione **Pronta per la configurazione** nella casella Stato.

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

L'host dell'API REST deve essere quello utilizzato per Qualys Cloud, dove si trova l'account. In questo esempio - qualysguard.qg2.apps.qualys.com

L'account deve essere quello con i privilegi di Manager, fare clic su **Avanti**.

Vendor Instances > QUALYS_VA

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

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

REST API Port

 The port used by the REST API host.

Username

 User account with Manager privileges to the Qualys platform.

Password

 Password of the user.

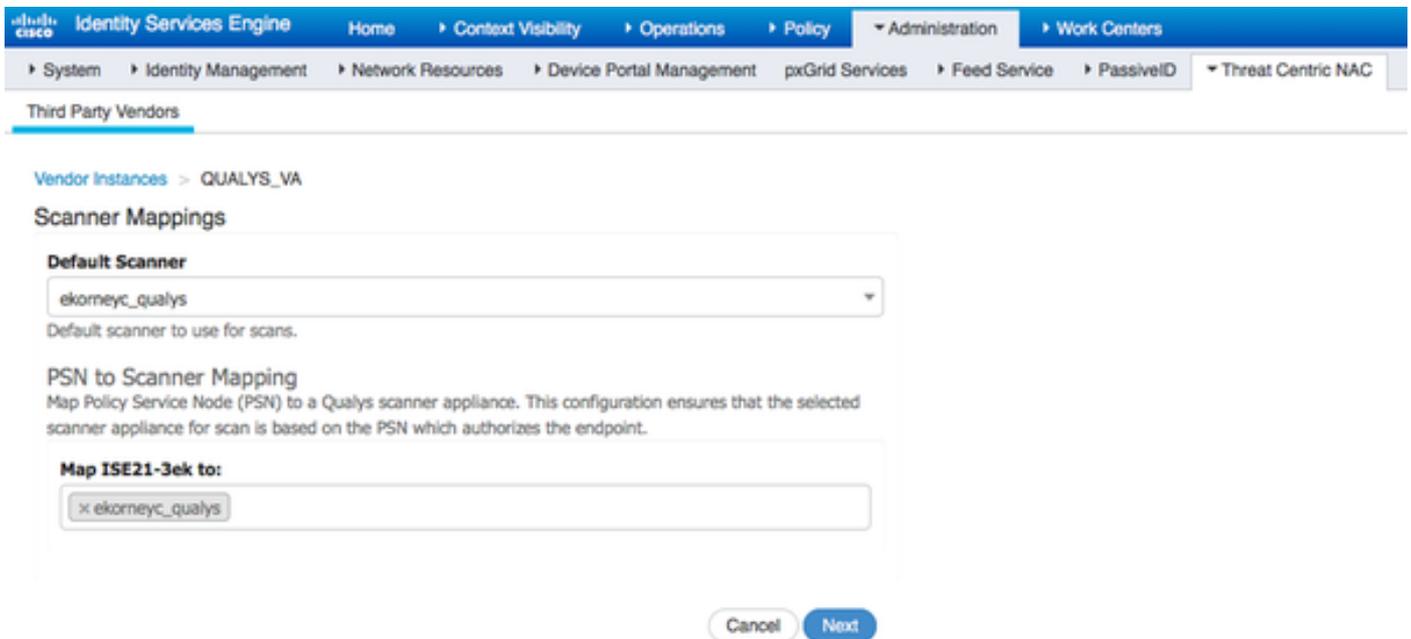
HTTP Proxy Host

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

HTTP Proxy Port

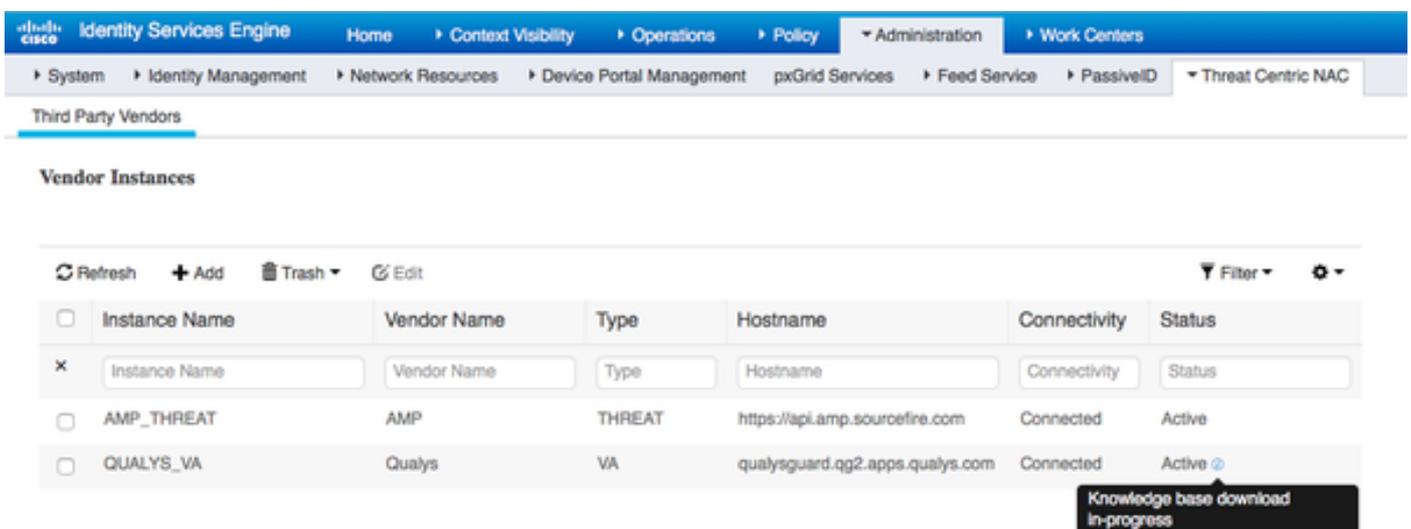
 Optional HTTP Proxy Port. Requires proxy host also to be set.

ISE scarica informazioni sugli scanner connessi a Qualys Cloud. In questa pagina è possibile configurare PSN su Mapping scanner. Assicura che lo scanner selezionato venga scelto in base al PSN che autorizza l'endpoint.



Le impostazioni avanzate sono ben documentate nella guida per l'amministratore di ISE 2.1, il collegamento è disponibile nella sezione Riferimenti di questo documento. Fare clic su **Next** (Avanti) e **Finish** (Fine). Le transizioni dell'istanza Qualys allo stato **Attivo** e il download della Knowledge Base vengono avviati.

Nota: Può esistere una sola istanza di Qualys per distribuzione.



Passaggio 4. Configurare il profilo di autorizzazione per attivare la scansione VA

Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili autorizzazione. Aggiungere un nuovo profilo. In **Operazioni comuni** selezionare la casella di controllo **Valutazione vulnerabilità**. L'intervallo di scansione su richiesta deve essere selezionato in base alla progettazione della rete.

Il profilo di autorizzazione contiene le seguenti coppie av:

cisco-av-pair = intervallo di scansione su richiesta=48

cisco-av-pair = analisi periodica abilitata=0

cisco-av-pair = va-adapter-instance=796440b7-09b5-4f3b-b611-199fb81a4b99

Vengono inviati ai dispositivi di rete all'interno di un pacchetto di accettazione dell'accesso, anche se il loro vero scopo è quello di dire al nodo MNT che l'analisi deve essere attivata. MNT indica al nodo TC-NAC di comunicare con Qualys Cloud.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a new Authorization Profile. The breadcrumb navigation is "Authorization Profiles > New Authorization Profile". The page title is "Authorization Profile".

Fields and options visible:

- * Name:
- Description:
- * Access Type:
- Network Device Profile:
- Service Template:
- Track Movement:
- Passive Identity Tracking:

Common Tasks section:

- Assess Vulnerabilities
- Adapter Instance:
- Trigger scan if the time since last scan is greater than:
Enter value in hours (1-9999)
- Assess periodically using above interval

Passaggio 5. Configurare i criteri di autorizzazione

- Configurare il criterio di autorizzazione per utilizzare il nuovo profilo di autorizzazione configurato nel passaggio 4. Passare a Criterio > Autorizzazione > Criterio di autorizzazione, individuare la regola **Basic_Authenticated_Access** e fare clic su **Modifica**. Modificare il campo Autorizzazioni da **PermitAccess** al nuovo **standard VA_Scan** creato. In questo modo, tutti gli utenti possono eseguire una scansione delle vulnerabilità. Fare clic su **Save** (Salva).
- Crea criteri di autorizzazione per computer in quarantena. Passare a Criterio > Autorizzazione > Criterio di autorizzazione > Eccezioni e creare una **regola di eccezione**. Fare clic su Condizioni > Crea nuova condizione (opzione avanzata) > Seleziona attributo, scorrere verso il basso e selezionare **Minaccia**. Espandere l'attributo **Threat** e selezionare **Qualys-CVSS_Base_Score**. Modificare l'operatore in **Maggiore di** e immettere un valore in base ai criteri di sicurezza. Il profilo di autorizzazione della **quarantena** deve consentire un accesso limitato alla macchina vulnerabile.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

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 ThreatQualys-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

Verifica

Identity Services Engine

La prima connessione attiva VA Scan. Al termine dell'analisi, la riautenticazione CoA viene attivata per applicare nuovi criteri, se corrispondenti.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

RADIUS TC-MAC Live Logs TACACS Reports Troubleshoot Adaptive Network Control

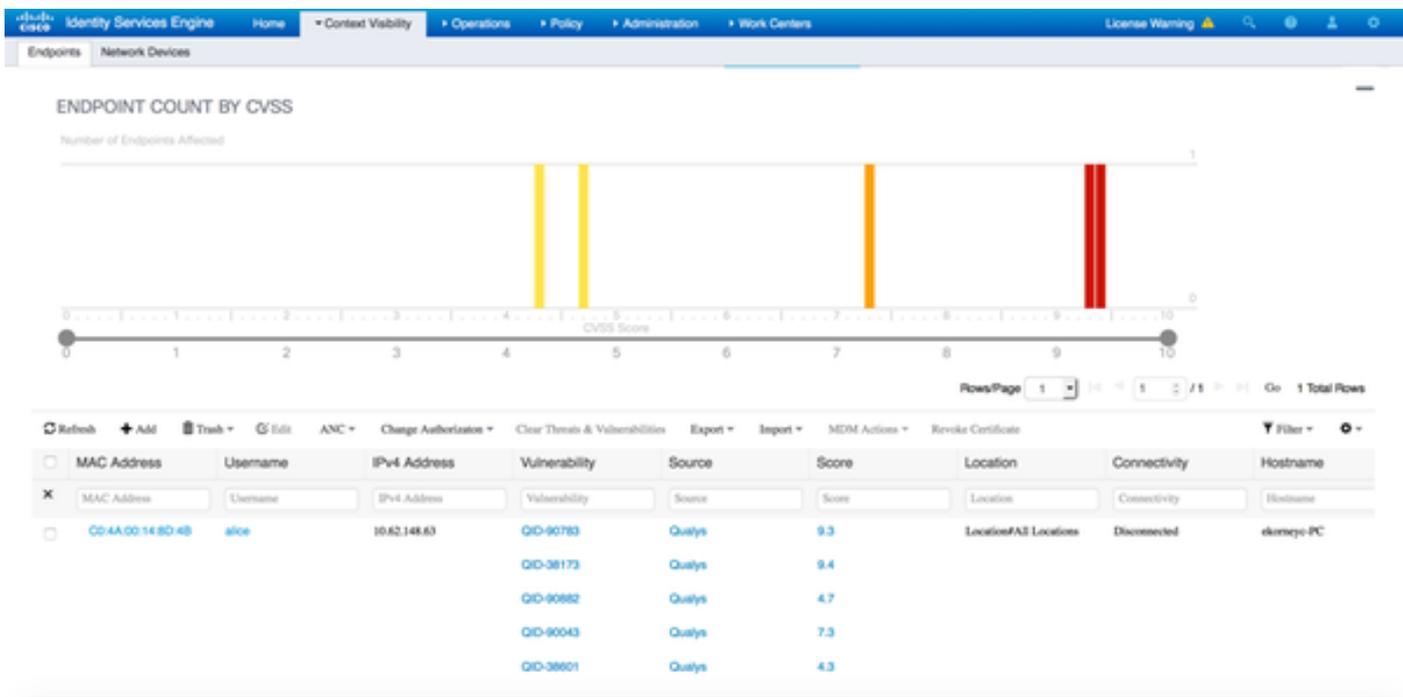
Live Logs Live Sessions

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

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
Jun 28, 2016 07:25:10:971 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	Endpoint Profi	Authentication Policy	Authorization Policy	Authorization
Jun 28, 2016 07:25:07:065 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	Microsoft-Wo...	Default >> Dot1X >> Default	Default >> Exception Rule	Quarantine
Jun 28, 2016 07:06:23:437 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	TP-LINK De...	Default >> Dot1X >> Default	Default >> Basic_Authenticated_Access	VA_Scan

Per verificare quali vulnerabilità sono state rilevate, selezionare Context Visibility > Endpoints. Verificare le vulnerabilità per endpoint con i punteggi assegnati da Qualys.



Quando si seleziona un particolare endpoint, vengono visualizzati ulteriori dettagli su ciascuna Vulnerabilità, inclusi Titolo e CVEID.

The screenshot shows the detailed view of the endpoint **C0:4A:00:14:8D:4B**. The endpoint profile is **Microsoft-Workstation** with a current IP address of **10.62.148.63**. The **Vulnerabilities** tab is selected, showing the following details for **QID-90783**:

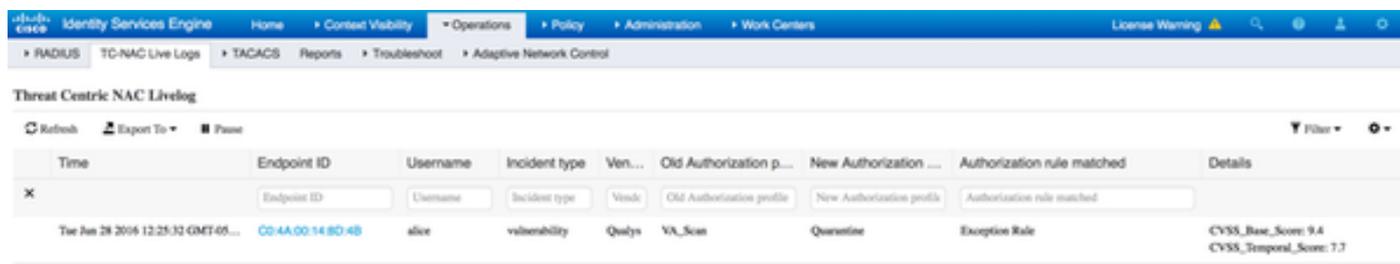
- Title:** Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- CVSS score:** 9.3
- CVEIDS:** CVE-2012-0002, CVE-2012-0152,
- Reported by:** Qualys
- Reported at:**

The next vulnerability, **QID-38173**, is also visible:

- Title:** SSL Certificate - Signature Verification Failed Vulnerability
- CVSS score:** 9.4
- CVEIDS:**
- Reported by:** Qualys
- Reported at:**

In Operazioni > TC-NAC Live Logs, è possibile visualizzare i criteri di autorizzazione vecchi e nuovi applicati e i dettagli su CVSS_Base_Score.

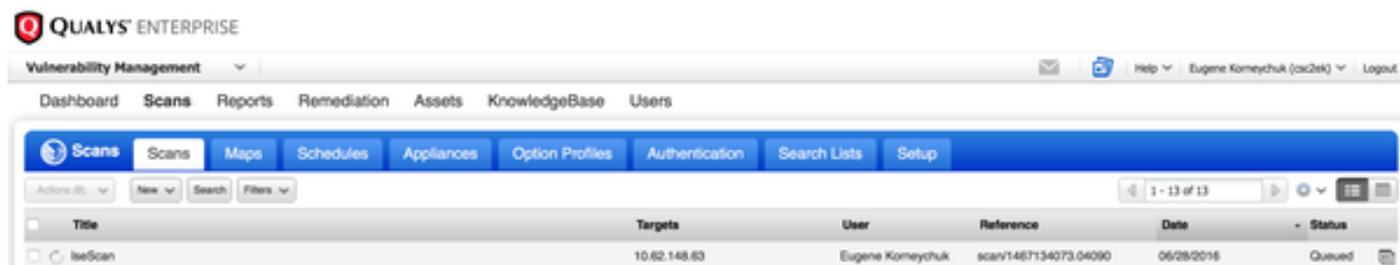
Nota: Le condizioni di autorizzazione vengono eseguite in base a CVSS_Base_Score, che equivale al punteggio di vulnerabilità più alto rilevato sull'endpoint.



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

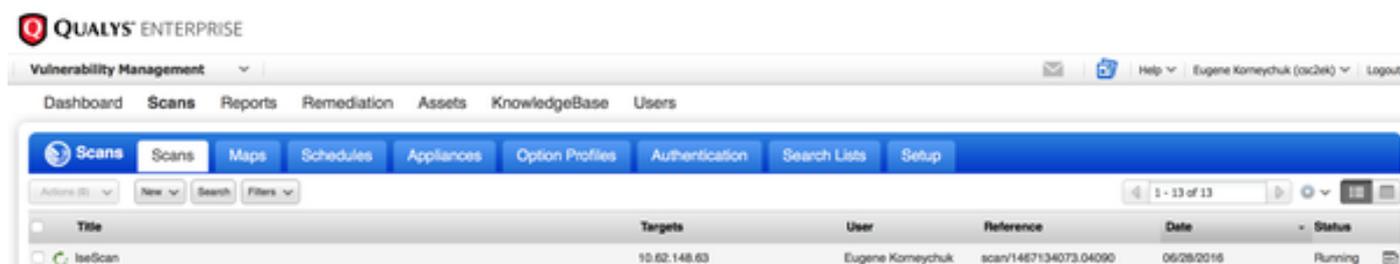
Qualys Cloud

Quando la scansione VA viene attivata da TC-NAC Qualys accoda la scansione, può essere visualizzata in Scans > Scans



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

Successivamente passa alla modalità In esecuzione, ovvero Qualys cloud ha istruito lo scanner Qualys per eseguire la scansione effettiva



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

Mentre lo scanner esegue la scansione, dovrebbe essere visualizzato "Scanning..." (Scansione in corso...) firma nell'angolo superiore destro di Qualys Guard

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

Al termine dell'analisi, il sistema passa allo stato Finito. È possibile visualizzare i risultati in Scans > Scans, selezionare la scansione richiesta e fare clic su **View Summary** o **View Results**.

The screenshot shows the Qualys Enterprise interface. At the top, there's a navigation bar with 'Dashboard', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase', and 'Users'. Below this is a sub-navigation bar with 'Scans', 'Maps', 'Schedules', 'Appliances', 'Option Profiles', 'Authentication', 'Search Lists', and 'Setup'. A table lists several 'IseScan' entries with columns for Title, Targets, User, Reference, Date, and Status. The first entry is highlighted in yellow. Below the table is a 'Preview' section for a 'Vulnerability Scan - IseScan' on target 1 IP(s). It shows scan details and summary statistics: Total Hosts Alive: 1, Total appliances used: 1, Aggregate Vulnerabilities: 7. Two buttons, 'View Summary' and 'View Results', are highlighted with a red box.

Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.83	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Finished
IseScan	10.201.228.107	Eugene Korneychuk	scan/1467132757.03967	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

Preview

Vulnerability Scan - IseScan
Target: 1 IP(s)

Scan launched by Eugene Korneychuk (sc2ek) | Start: 06/28/2016 at 21:18:55 (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

[View Summary](#) | [View Results](#)

Nel report stesso è possibile visualizzare **Risultati dettagliati**, in cui sono visualizzate le vulnerabilità rilevate.

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)

Risoluzione dei problemi

Debug su ISE

Per abilitare i debug su ISE, selezionare Amministrazione > Sistema > Registrazione > Configurazione log di debug, selezionare TC-NAC Node e modificare il componente **Log Level** **via-runtime** e **va-service** in **DEBUG**

Component Name	Log Level	Description
va		
<input type="radio"/> va-runtime	DEBUG	Vulnerability Assessment Runtime messages
<input type="radio"/> va-service	DEBUG	Vulnerability Assessment Service messages

Registri da controllare - varuntime.log. È possibile archiviarlo direttamente dalla CLI di ISE:

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

TC-NAC Docker ha ricevuto istruzioni per eseguire la ricerca di un endpoint specifico.

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

```
199fb81a4b99", snHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}
```

Una volta ricevuto il risultato, tutti i dati di Vulnerabilità vengono memorizzati nella directory di contesto.

```
2016-06-28 19:25:02,020 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaServiceMessageListener -::: - Ricevuto messaggio da VaService:  
[{"macAddress":"C0:4A:00:14:8D:4B","ipAddress":"10.62.148.63","lastScanTime":1467134394000,"vulnerability":[{"\vulnerabilityId\":"QID-90783","\cveIds\":"CVE-2012-002,CVE-2012-0152","\cvssBaseScore\":"9.3","\cvssTemporalScore\":"7.7","\vulnerabilityTitle\":"Vulnerabilità dell'esecuzione di codice remoto del protocollo Desktop remoto Microsoft Windows (MS12-020)","\vulnerabilityVendor\":"Qualys"}],{"\vulnerabilityId\":"QID-8173","\cveIds\":"","\cvssBaseScore\":"9.4","\cvssTemporalScore\":"6.9","\vulnerabilityTitle\":"Certificato SSL - Verifica firma non riuscita Vulnerabilità","\vulnerabilityVendor\":"Qualys"}],{"\vulnerabilityId\":"QID-90882","\cveIds\":"","\cvssBaseScore\":"4.7","\cvssTemporalScore\":"4","\vulnerabilityTitle\":"Metodo di crittografia vulnerabile protocollo Desktop remoto consentito","\vulnerabilityVendor\":"Qualys"}],{"\vulnerabilityId\":"QID-90043","\cveIds\":"","\cvssBaseScore\":"7.3","\cvssTemporalScore\":"6.3","\vulnerabilityTitle\":"Firma SMB disabilitata o firma SMB non richiesta","\vulnerabilityVendor\":"Qualys"}],{"\vulnerabilityId\":"QID-38601","\cveIds\":"CVE-2013-2566,CVE-2015-2808","\cvssBaseScore\":"4.3","\cvssTemporalScore\":"3.7","\vulnerabilityTitle\":"Uso SSL/TLS di cifratura RC4 debole","\vulnerabilityVendor\":"Qualys"}]  
2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaServiceMessageListener -::: - VA: Salva nel database di contesto, 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: invio di elastic search json a pri-lan  
2016-06-28 19:25:02,272 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaPanRemotingHandler -::: - VA: Salvato in ricerca elastica:  
{C0:4A:00:14:8D:4B=[{"vulnerabilityId":"QID-90783","cveIds":"CVE-2012-0002,CVE-2012-0152","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Vulnerabilità di esecuzione codice remoto del protocollo Desktop remoto Microsoft Windows ability (MS12-020)","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"Certificato SSL - Verifica firma non riuscita Vulnerabilità","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Metodo di crittografia vulnerabile del protocollo Windows Remote Desktop","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore Score":"6.3","vulnerabilityTitle":"Firma SMB disabilitata o firma SMB non richiesta","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-2808","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"Uso SSL/TLS di cifratura RC4 debole","vulnerabilityVendor":"Qualys"}]}
```

Registri da controllare - vaservice.log. È possibile archivarlo direttamente dalla CLI di ISE:

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

Richiesta di valutazione della vulnerabilità inviata alla scheda

```
2016-06-28 17:07:13,200 DEBUG [endpointPollerScheduler-3][ cpm.va.seservice.util.VaServiceUtil  
-:::- VA SendSyslog systemMsg :  
[{"systemMsg":"91019","isAutoInsertSelfAcInstance":true,"attributes":["TC-NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","Richiesta VA inviata alla scheda","TC-NAC.Details","Richiesta VA inviata alla scheda per l'elaborazione","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"]}]}
```

AdapterManagerListener controlla ogni 5 minuti lo stato dell'analisi fino al completamento.

```
2016-06-28 17:09:43,459 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.seservice.processor.AdapterMessageListener -::: - Messaggio dalla scheda:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUuid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Numero di endpoint in coda per il
controllo dei risultati dell'analisi: 1, Numero di endpoint in coda per l'analisi: 0, Numero di
endpoint per cui è in corso l'analisi: 0"}
2016-06-28 17:14:43,760 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.seservice.processor.AdapterMessageListener -::: - Messaggio dalla scheda:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUuid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Numero di endpoint in coda per il
controllo dei risultati dell'analisi: 0, Numero di endpoint in coda per l'analisi: 0, Numero di
endpoint per cui è in corso l'analisi: 1"}
2016-06-28 17:19:43,837 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.seservice.processor.AdapterMessageListener -::: - Messaggio dalla scheda:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUuid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Numero di endpoint in coda per il
controllo dei risultati dell'analisi: 0, Numero di endpoint in coda per l'analisi: 0, Numero di
endpoint per cui è in corso l'analisi: 1"}
2016-06-28 17:24:43,867 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.seservice.processor.AdapterMessageListener -::: - Messaggio dalla scheda:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUuid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Numero di endpoint in coda per il
controllo dei risultati dell'analisi: 0, Numero di endpoint in coda per l'analisi: 0, Numero di
endpoint per cui è in corso l'analisi: 1"}
```

L'adattatore ottiene i QID, i CVE e i punteggi CVSS

```
2016-06-28 17:24:57,556 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.seservice.processor.AdapterMessageListener -::: - Messaggio dalla scheda:
{"requestedMacAddress":"C0:4A:00:14:8D:4B", "scanStatus":"ASSESSMENT_SUCCESS", "lastScanTimeLong":
1467134394000, "ipAddress":"10.62.148.63", "vulnerabilities":[{"vulnerabilityId":"QID-
38173", "cveIds":", "cvss
BaseScore":"9.4", "cvssTemporalScore":"6.9", "vulnerabilityTitle":"Certificato SSL - Verifica
della firma non riuscita Vulnerabilità", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90043", "cveIds":", "cvssBaseScore":"7.3", "cvssTemporalScore":"6.3", "vulnerabilityTitle":"SMB
Signer Disabilitato o firma SMB non
richiesta", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-90783", "cveIds":"CVE-2012-
0002,CVE-2012-
0152", "cvssBaseScore":"9.3", "cvssTemporalScore":"7.7", "vulnerabilityTitle":"Esecuzione codice
remoto del protocollo Microsoft Windows Remote Desktop Vulnerabilità (MS12-
020)", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-38601", "cveIds":"CVE-2013-
2566,CVE-2015-2808", "cvssBaseScore":"4.3", "cvssTemporalScore":"3.7", "vulnerabilityTitle": "/TLS
utilizzo di una cifratura RC4 debole", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90882", "cveIds":", "cvssBaseScore":"4.7", "cvssTemporalScore":"4", "vulnerabilityTitle":"Metodo di
crittografia debole di Windows Remote Desktop Protocol", "vulnerabilityVendor":"Qualys"}]}]
2016-06-28 17:25:01,282 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Endpoint Dettagli inviati a IRF è
{"C0:4A:00:14:8D:4B":[{"vulnerability":{"CVSS_Base_Score":9.4, "CVSS_Temporal_Score":7.7}, {"time-
stamp":1467134394000, "title":"Vulnerabilità", "vendor":"Qualys"}]}
2016-06-28 17:25:01,853 DEBUG [endpointPollerScheduler-2][] cpm.va.seservice.util.VaServiceUtil
-:::- VA SendSyslog systemMsg :
[{"systemMsg":"91019", "isAutoInsertSelfAcsInstance":true, "attributes":["TC-
NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA completato con
successo", "TC-NAC.Details", "VA completato; numero di vulnerabilità trovate: 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.Vendor", "Qualys", "TC-
NAC.AdapterInstanceName", "QUALYS_VA"]}]}
```

Problemi tipici

Problema 1. ISE ottiene il report sulle vulnerabilità con CVSS_Base_Score 0.0 e CVSS_Temporal_Score 0.0, mentre il report di Qualys Cloud contiene le vulnerabilità rilevate.

Problema:

Mentre si controlla il report da Qualys Cloud è possibile vedere le Vulnerabilità rilevate, ma su ISE non le si vede.

Debug rilevati in vaservice.log:

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

Soluzione:

Il motivo per cui il punteggio cvss è zero è che non presenta vulnerabilità o che il punteggio cvss non è stato abilitato in Qualys Cloud prima di configurare la scheda tramite l'interfaccia utente. La Knowledge Base contenente la funzionalità di punteggio CVSS attivata viene scaricata dopo la prima configurazione della scheda. È necessario verificare che il punteggio CVSS sia stato abilitato prima che l'istanza della scheda di rete fosse stata creata su ISE. È possibile eseguire questa operazione in Gestione vulnerabilità > Report > Impostazione > CVSS > Abilita punteggio CVSS

Problema 2. ISE non ottiene risultati da Qualys Cloud, anche se è stata trovata la corretta politica di autorizzazione.

Problema:

È stata trovata una corrispondenza con i criteri di autorizzazione corretti che dovrebbe attivare la scansione VA. Nonostante questo fatto non viene fatta alcuna scansione.

Debug rilevati in vaservice.log:

```
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][[]
cpm.va.seservice.processor.AdapterMessageListener -:::- Messaggio dalla scheda:
(Corpo:'[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, redelivery=false,
receivedExchange=irf.topic.va-reports, receivedRoutingKey=, deliveryTag=930, messageCount=0])
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][[]
cpm.va.seservice.processor.AdapterMessageListener -:::- Messaggio dalla scheda:
{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"Errore
durante l'attivazione della scansione: Errore durante l'attivazione del codice di analisi su
richiesta. Errore 1904: nessuno degli IP specificati è idoneo per la scansione di Vulnerability
Management.","lastScanTimeLong":0,"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15,771 DEBUG [SimpleAsyncTaskExecutor-2][[]
cpm.va.seservice.processor.AdapterMessageListener -:::- Risultato della scansione
dell'adattatore non riuscito per Macaddress:24:77:03:3D:CF:20, IP Address(DB): 10.201.228.102,
impostazione dello stato su non riuscito
2016-06-28 16:19:16,336 DEBUG [endpointPollerScheduler-2][[] cpm.va.seservice.util.VaServiceUtil
-:::- VA SendSyslog systemMsg :
```

```
[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","Errore VA","TC-NAC.Details","Errore durante l'attivazione dell'analisi: Errore durante l'attivazione del codice di analisi su richiesta. Errore 1904: nessuno degli IP specificati è idoneo per la scansione di Vulnerability Management.","TC-NAC.MACAddress","24:77:03:3D:CF:20","TC-NAC.IpAddress","10.201.228.102","TC-NAC.AdapterInstanceUuid","79640b7-09b5-4f3b-b611-199fb81a4b99","TC-NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

Soluzione:

Qualys Cloud indica che l'indirizzo IP dell'endpoint non è idoneo per la scansione. Accertarsi di aver aggiunto l'indirizzo IP dell'endpoint a Gestione vulnerabilità > Risorse > Risorse host > Nuovo > Host con rilevamento IP

Riferimenti

- [Guida dell'amministratore di Cisco Identity Services Engine, versione 2.1](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)
- [VIDEO: ISE 2.1 con Qualys](#)
- [Documentazione di Qualys](#)