

ISE 2.1 Threat-Centric NAC (TC-NAC) configureren met Qualys

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Snel stroomschema op hoog niveau](#)

[Cloud- en scanner voor kwaliteit instellen](#)

[Stap 1. Quiet implementeren](#)

[Stap 2. Steeksleutel configureren](#)

[ISE configureren](#)

[Stap 1: Cloudinstellingen van de hoge dichtheid voor integratie met ISE](#)

[Stap 2. Schakel TC-NAC-services in](#)

[Stap 3. Het configureren van Qualys Adapter-connectiviteit op ISE VA-framework](#)

[Stap 4. Het machtigingsprofiel configureren om VA Scannen te activeren](#)

[Stap 5. Instellen van het vergunningsbeleid](#)

[Verifiëren](#)

[Identity Services Engine](#)

[Cloud](#)

[Problemen oplossen](#)

[Debugs op ISE](#)

[Typische problemen](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u Threat-Centric NAC kunt configureren met Qualys on Identity Services Engine (ISE) 2.1. De optie Threat Centric Network Access Control (TC-NAC) stelt u in staat een vergunningsbeleid te maken dat is gebaseerd op de dreigings- en kwetsbaarheidskenmerken die worden ontvangen van de bedreigings- en kwetsbaarheidsadapters.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco Identity Services Engine
- Qualys ScanGuard

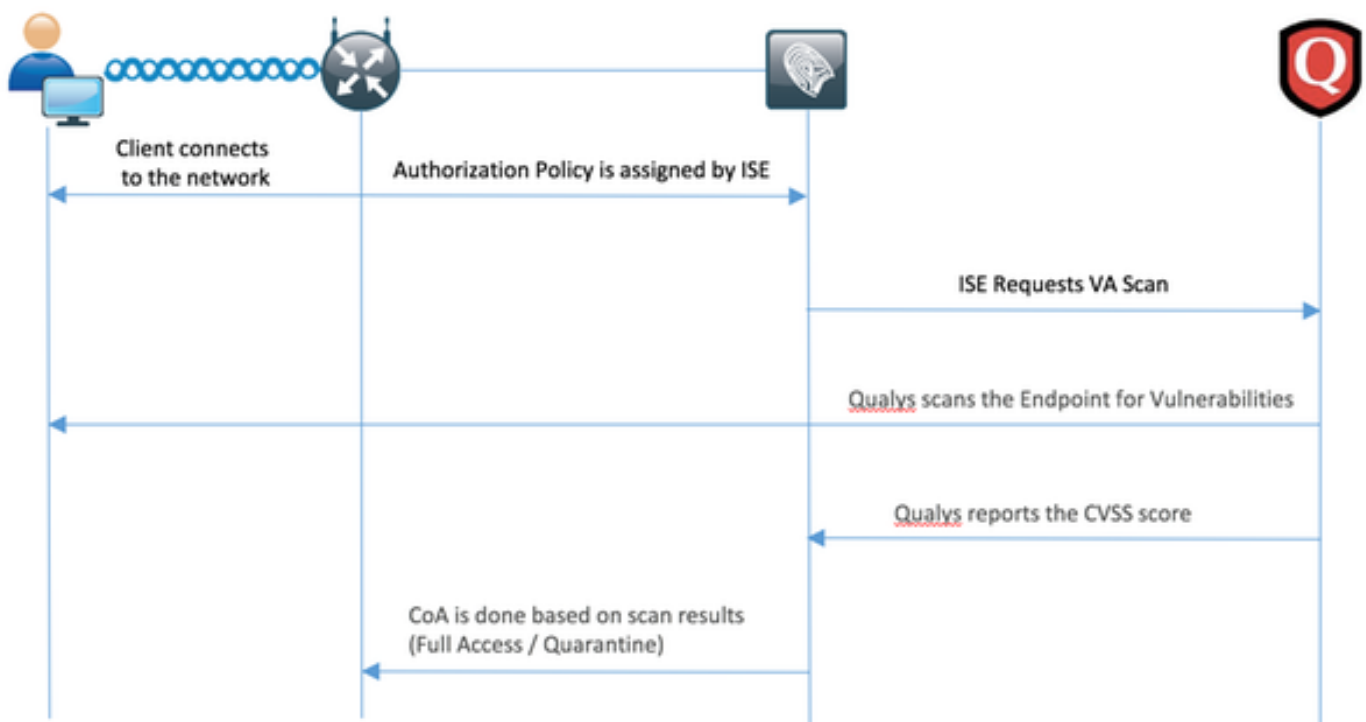
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 2.1
- Draadloze LAN-controller (WLC) 8.0.121.0
- Qualys Guard Scanner 8.3.36-1, handtekeningen 2.3.364-2
- Windows 7 Service Pack 1

Configureren

Snel stroomschema op hoog niveau



Dit is de stroom:

1. Clientverbindingen met het netwerk, beperkte toegang wordt verleend en profiel met selectieteken voor opties bij **beoordeling** is toegewezen
2. Het PSN-knooppunt verstuurt een systeemmeldingen naar het MNT-knooppunt, waarbij de authenticatie werd bevestigd en de VA Scan het resultaat was van het autorisatiebeleid
3. MNT-knooppunt vult SCAN met het TC-NAC-knooppunt (via Admin Webex) in met deze gegevens:
 - MAC-adres
 - IP-adres
 - Scaninterval
 - Periodieke scan ingeschakeld
 - van oorsprong PSN
4. Qualys TC-NAC (ingesloten in Docker-container) communiceert met Qualys Cloud (via REST API) om scan indien nodig te activeren

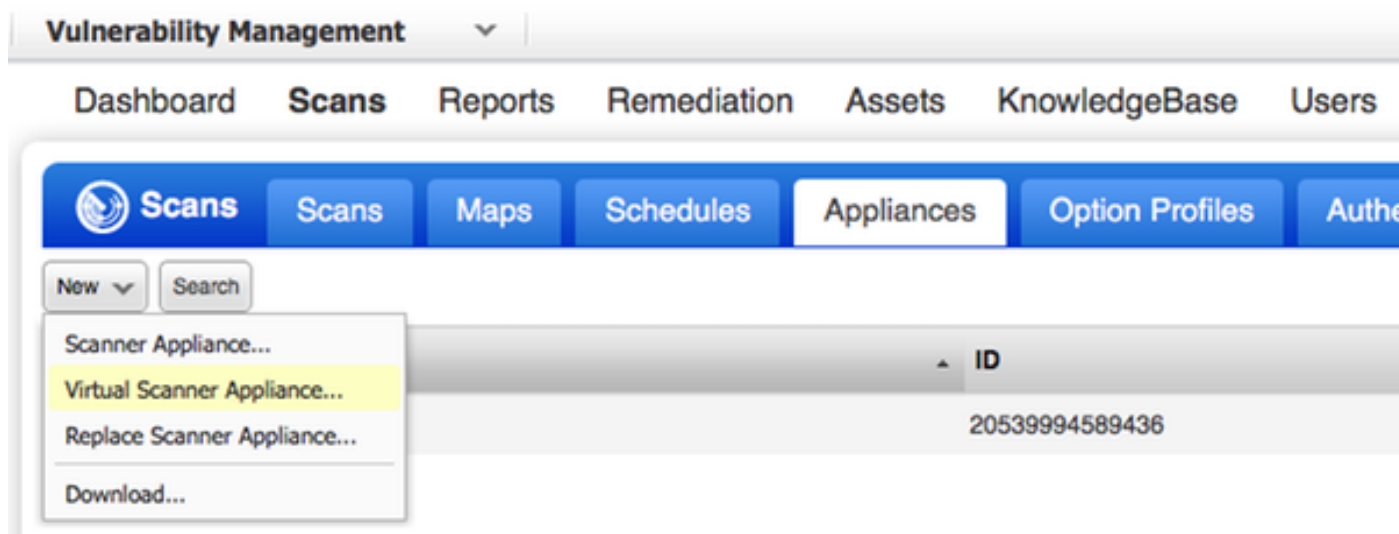
5. Qualys Cloud vertelt Qualys Scanner om het eindpunt te scannen
6. Qualys Scanner stuurt de resultaten van de scan naar de Qualys Cloud
7. Resultaten van de scan worden teruggestuurd naar TC-NAC:
 - MAC-adres
 - Alle CVSS-scores
 - Alle kwaliteiten (QID, titel, CVEID)
8. TC-NAC werkt PAN bij met alle gegevens uit stap 7.
9. CoA wordt indien nodig geactiveerd volgens een beleid voor autorisatie.

Cloud- en scanner voor kwaliteit instellen

Voorzichtig: De configuratie van de kwaliteit in dit document wordt uitgevoerd voor de laboratoriumdoeleinden. Neem voor ontwerpoverwegingen contact op met de Qualys-engineers

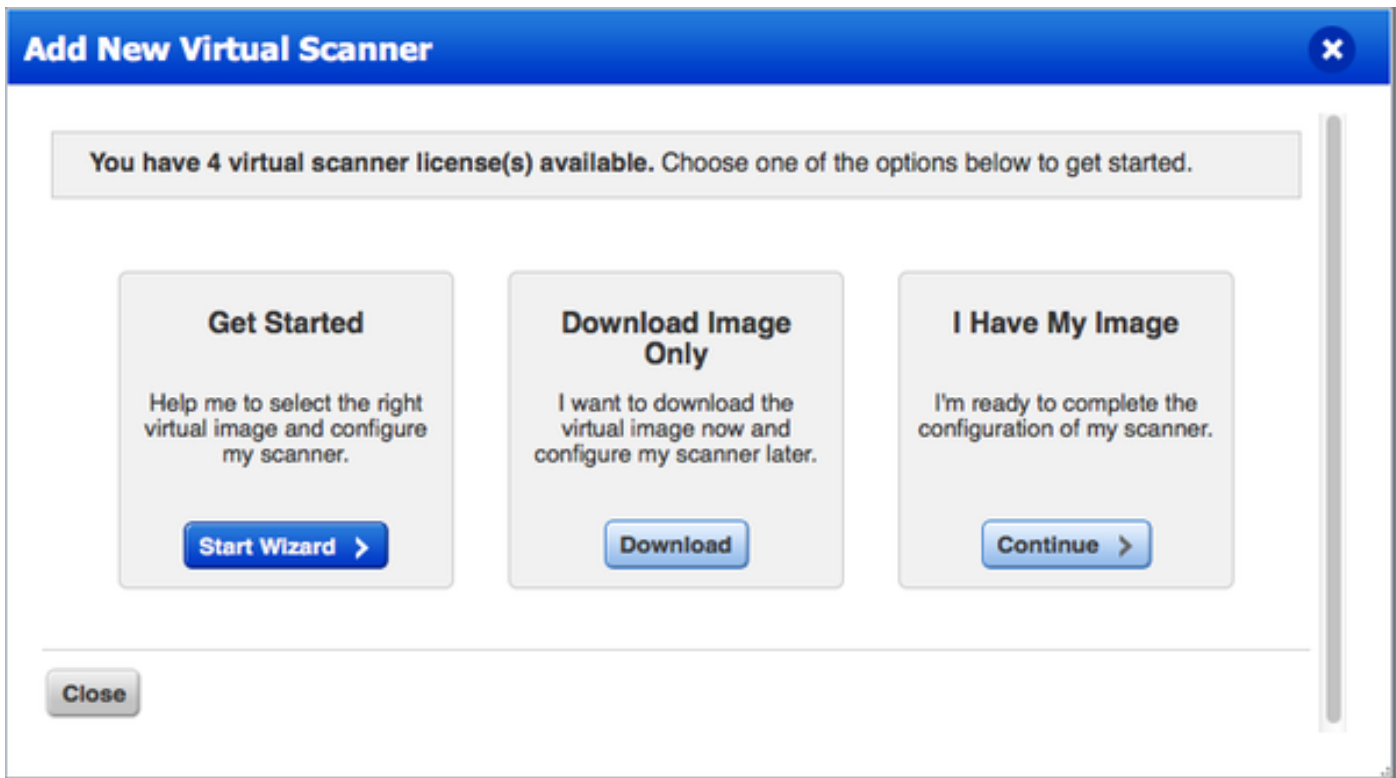
Stap 1. Quiet implementeren

U kunt de scanner van de Qualys vanuit het OVA-bestand gebruiken. Aanmelden bij Qualys wolk en navigeer naar Scans > Applicaties en selecteer Nieuw > Virtuele scanner applicatie

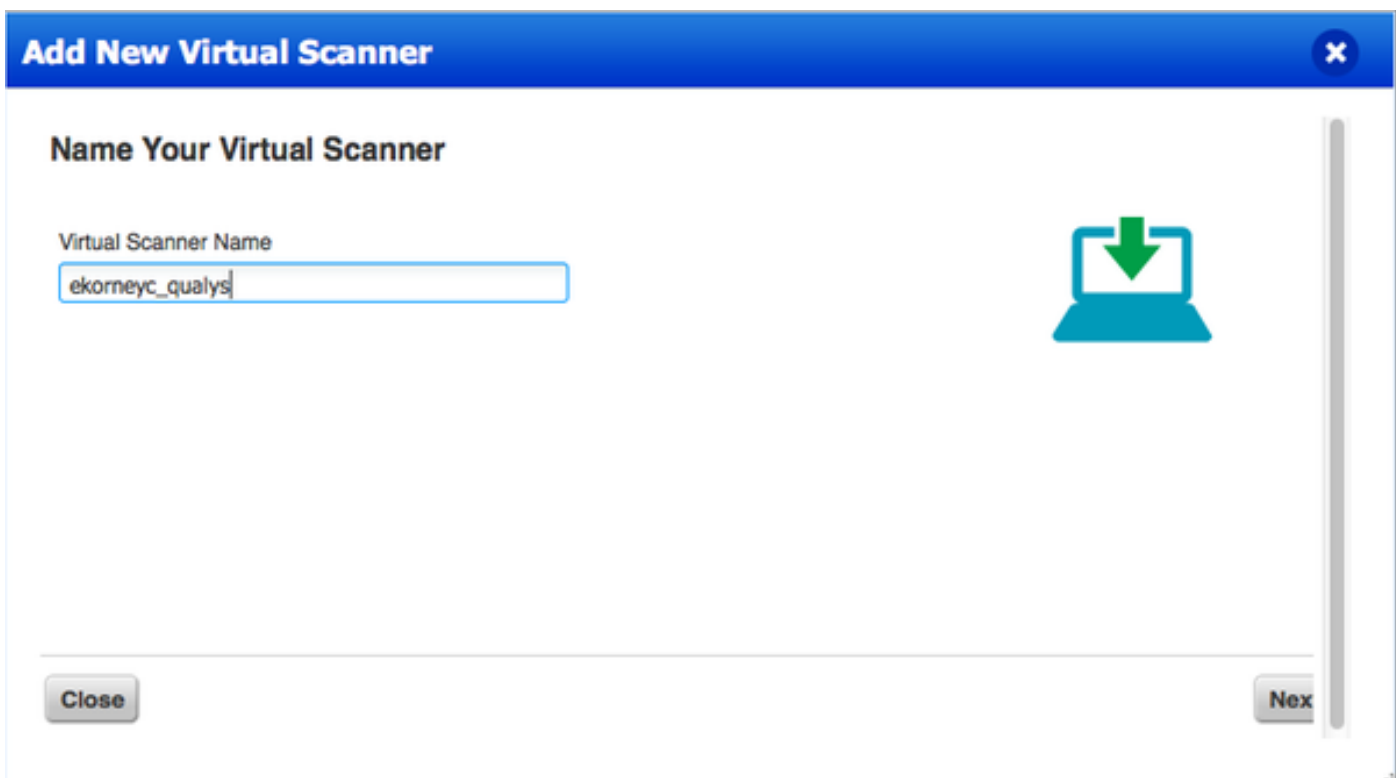


The screenshot shows the Qualys Vulnerability Management interface. At the top, there is a navigation bar with 'Vulnerability Management' and a dropdown arrow. Below this is a secondary navigation bar with tabs for 'Dashboard', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase', and 'Users'. The 'Scans' tab is active, and within it, the 'Appliances' sub-tab is selected. A 'New' dropdown menu is open, showing options: 'Scanner Appliance...', 'Virtual Scanner Appliance...' (highlighted in yellow), 'Replace Scanner Appliance...', and 'Download...'. Below the menu, a table is visible with a header 'ID' and a single row containing the value '20539994589436'.

Selecteer **Afbeelding alleen downloaden** en kies juiste distributie



U kunt activeringscode verkrijgen door naar SCANNEN > APPARATEN te gaan en Nieuw > Virtuele scanner-applicatie te selecteren en **door Mijn afbeelding te selecteren**



Nadat u de scannernaam hebt ingevoerd, krijgt u een autorisatie-code die u later gebruikt.

Stap 2. Steeksleutel configureren

Gebruik OVA op het virtualisatieplatform van uw keuze. Configureer de volgende instellingen:

- Netwerk instellen (LAN)

- WAN-interfacemodule (als u twee interfaces gebruikt)
- Instellingen proxy (als u proxy gebruikt)
- Deze scanner personaliseren



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)

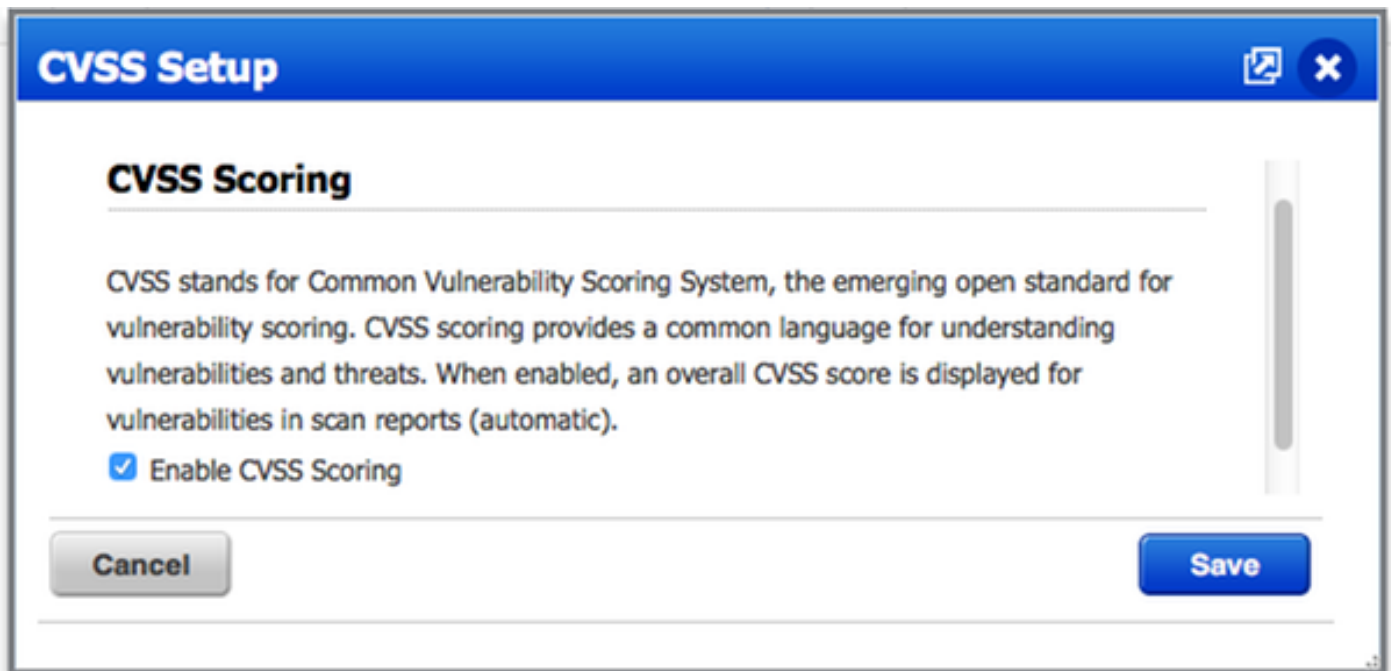
TIP:

This is the main (top-level) menu of the Virtual Scanner Console.

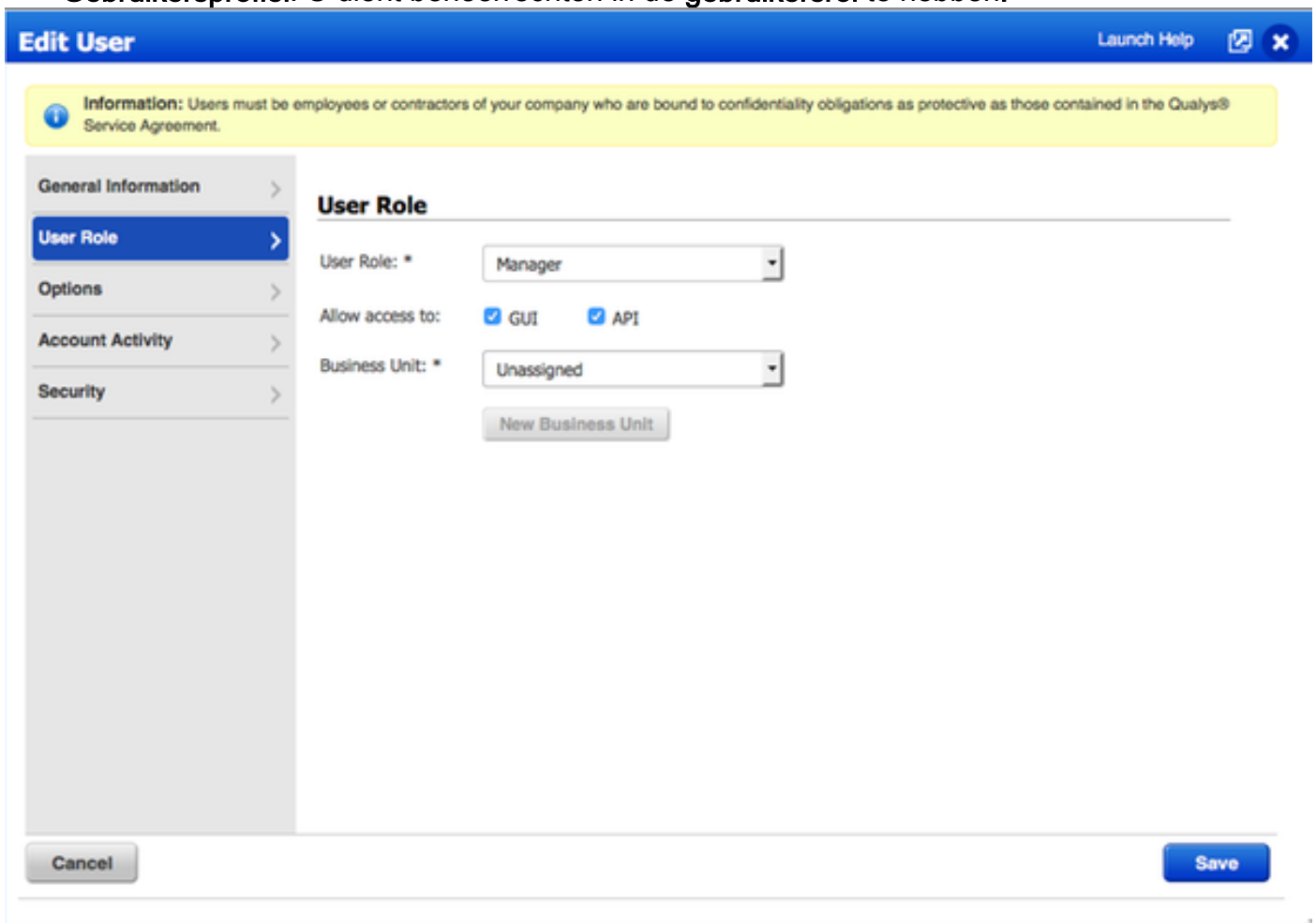
Press the UP and DOWN arrow keys to navigate the menu.

Press the RIGHT arrow or ENTER key to choose a menu item.

De scanner sluit zich vervolgens aan op Qualys en downloads van de laatste software en handtekeningen.



- Zorg ervoor dat de gebruikersreferenties die gebruikt worden in adapterconfiguratie beheerrechten hebben. Selecteer uw gebruiker in de linkerbovenhoek en klik op **Gebruikersprofiel**. U dient beheerrechten in de **gebruikersrol** te hebben.



- Zorg ervoor dat IP-adressen/subnetwerken van endpoints waarvoor een Kwaliteitsbeoordeling is vereist, aan Kwalingen worden toegevoegd bij Kwaliteitsbeheer > Activa > Host Asset > New > IP Tracking Hosts

Help for proper formatting.' Below this is a text input field labeled 'IPs: *' containing the IP range '10.62.148.1-10.62.148.128'. Underneath the input field is a checkbox labeled 'Add to Policy Compliance Module' which is currently unchecked. Below the checkbox is an example text '(ex: 192.168.0.200,192.168.0.87-192.168.0.92)'. At the bottom of the main area, it says 'Validate IPs through [Whois](#)'. At the very bottom of the window, there are two buttons: 'Cancel' on the left and 'Add' on the right."/>

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**

Stap 2. Schakel TC-NAC-services in

Schakel TC-NAC-services in onder Beheer > Implementatie > Knooppunt bewerken. controleren **Threat Centric NAC Service inschakelen** vakje.

Opmerking: Er kan slechts één TC-NAC knooppunt per implementatie zijn.

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

 AdministrationRole **STANDALONE**

Make Primary

 Monitoring

Role PRIMARY

Personas

Other Monitoring Node

 Policy Service Enable Session Services

Include Node in Node Group

None

 Enable Profiling Service Enable Threat Centric NAC Service

Stap 3. Het configureren van Qualys Adapter-connectiviteit op ISE VA-framework

Navigatie in naar Administratie > Bedreigingscentrifuge NAC > Verkopers van derden > Toevoegen. Klik op **Opslaan**.

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

Vendor * Qualys : VA

Instance Name * QUALYS_VA

Cancel Save

Wanneer Qualys Instance overschakelt naar **Ready om status te configureren** klikt u op **Ready om** optie in de Status **te configureren**.

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

De REST API-host moet degene zijn die u voor Qualys Cloud gebruikt, waar uw account zich bevindt. In dit voorbeeld: qualalaly.qg2.apps.qualys.com

Je account is degene met Manager rechten, klik op **Volgende**.

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.

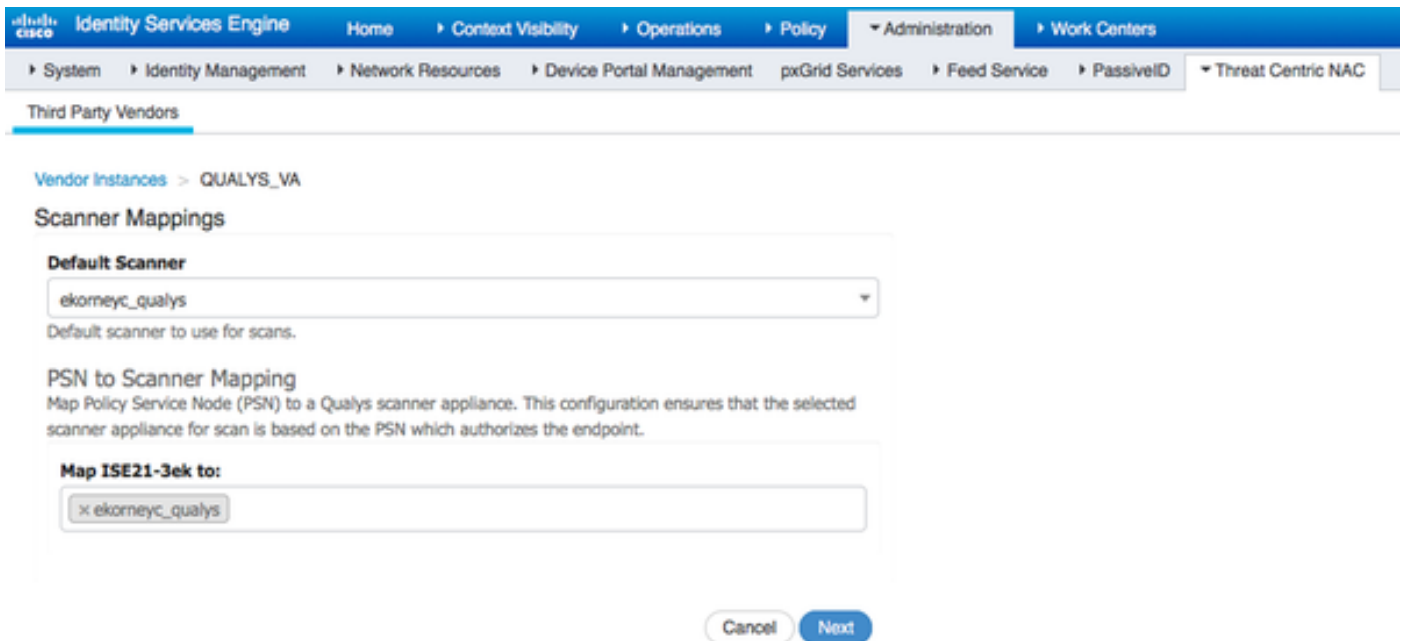
HTTP Proxy Host

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

HTTP Proxy Port

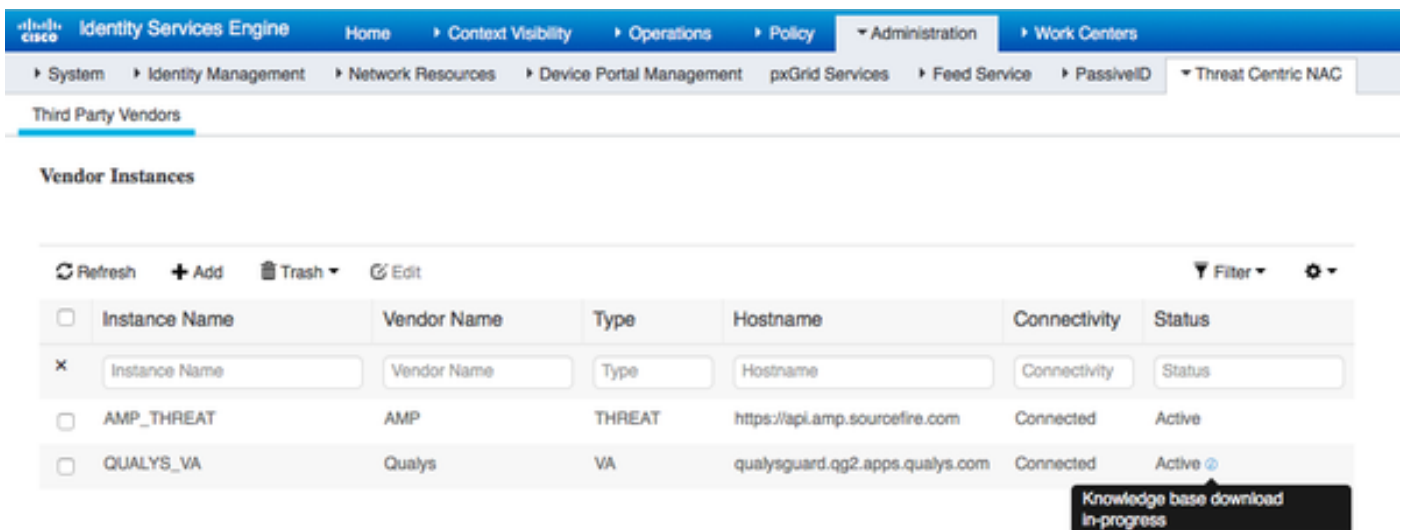
 Optional HTTP Proxy Port. Requires proxy host also to be set.

ISE downloads met informatie over scanners die zijn aangesloten op de Qualys Cloud, kunt u PSN configureren op scanner en deze pagina toewijzen. Hiermee wordt ervoor gezorgd dat de geselecteerde scanner is geselecteerd op basis van een PSN-document, waarbij het eindpunt wordt toegestaan.



Geavanceerde instellingen zijn duidelijk gedocumenteerd in ISE 2.1 Admin Guide, er is een link te vinden in het gedeelte Referenties van dit document. Klik op **Volgende** en op **Voltooien**. Qualys Instantie-overgangen naar **actieve** state en kennisbank download beginnen.

Opmerking: Er kan slechts één Qualys-instantie per implementatie zijn.



Stap 4. Het machtigingsprofiel configureren om VA Scannen te activeren

Navigeer in naar beleid > Gegevens van beleid > Resultaten > Vergunning > Auteur profielen van autorisatie. Nieuw profiel toevoegen. Selecteer onder **Common Tasks** de optie **Kwetsbaarheidsassessments**.

Het On-Demand scaninterval moet worden geselecteerd volgens uw netwerkontwerp.

autorisatieprofiel bevat die av-paren:

cisco-av-pair = on-demand-scan-interval=48

cisco-av-pair = periodiek-scan-enabled=0

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

Ze worden naar netwerkapparaten verzonden binnen een pakket voor toegangsaanvaarding, hoewel het echte doel ervan is om MNT Node te vertellen dat Scannen moet worden geactiveerd. MNT draagt TC-NAC-knooppunt op om met Qualys Cloud te communiceren.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a new Authorization Profile. The breadcrumb trail 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:

Below the main form is a section titled "Common Tasks" with a checked checkbox for "Assess Vulnerabilities".

Fields and options in the "Assess Vulnerabilities" section:

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

Stap 5. Instellen van het vergunningsbeleid

- Configureer beleid om het nieuwe autorisatieprofiel te gebruiken dat in stap 4 is geconfigureerd. Navigeer naar beleid > autorisatie > autorisatiebeleid, plaats **Basic_Authenticated_Access** regel en klik op **Bewerken**. Verander de toegangsrechten van **PermitAccess** naar de nieuwe **standaard VA_Scan**. Dit veroorzaakt een kwetsbaarheidsscan voor alle gebruikers. Klik op **Opslaan**.
- Maak een autorisatiebeleid voor geharde machines. Navigeren in op beleid > autorisatie > autorisatiebeleid > Exceptions en zorgen voor een **Exceptieregel**. Klik op Voorwaarden > Nieuwe conditionering maken (geavanceerde optie) > Eigenschappen selecteren, scrollen en **bedreigingen** selecteren. Vouw de **Threat** eigenschap uit en selecteer **Qualys-CVSS_Base_Score**. Verander de operator in **grotere mate** en voer een waarde in volgens uw beveiligingsbeleid. **Quarantaine** autorisatieprofiel dient beperkte toegang tot de kwetsbare machine te bieden.

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

Verifiëren

Identity Services Engine

De eerste verbinding voert een VA Scan in. Wanneer de scan is voltooid, wordt voor de toepassing van het nieuwe beleid van CoA een nieuwe echtheidscontrole op gang gebracht, indien het is afgestemd.

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

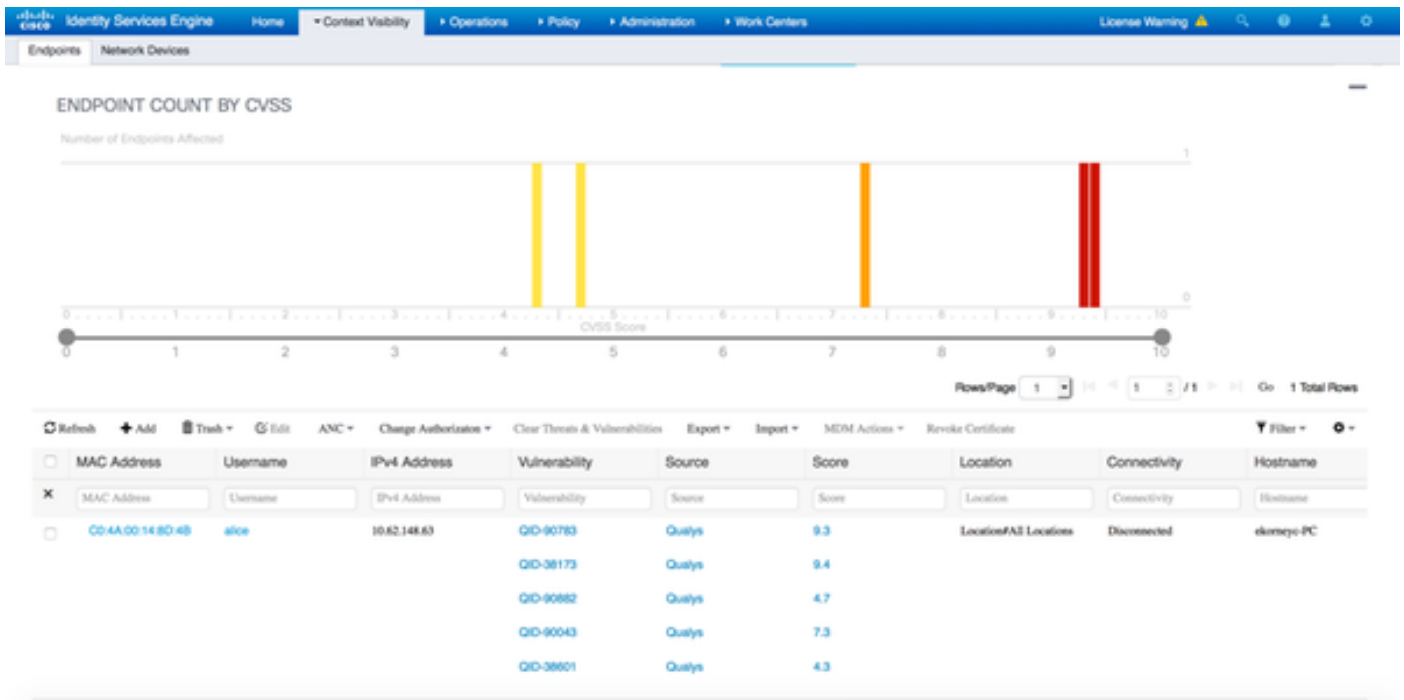
RADIUS TC-NAC Live Logs TACACS Reports Troubleshoot Adaptive Network Control

Live Logs Live Sessions

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

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

Om te verifiëren welke kwetsbaarheden werden gedetecteerd, navigeer naar Context Visibility > Endpoints. Controleer per eindpunt of de zwakheden voldoen aan de scores die Qualys geven.



Bij het selecteren van een specifiek eindpunt worden meer details over elke kwetsbaarheid weergegeven, waaronder Titel en EID.

The screenshot shows the detailed view of the endpoint C0:4A:00:14:8D:4B. The endpoint profile is Microsoft-Workstation, and the current IP address is 10.62.148.63. The 'Vulnerabilities' tab is selected, showing a list of vulnerabilities.

QID-90783

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

CVSS score: 9.3

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

Reported by: Qualys

Reported at:

QID-38173

Title: SSL Certificate - Signature Verification Failed Vulnerability

CVSS score: 9.4

CVEIDS:

Reported by: Qualys

Reported at:

Bij bewerkingen > TC-NAC Live Logs, ziet u oude vs nieuwe autorisatiebeleid toegepast en details over CVSS_Base_Score.

Opmerking: De vergunningsvoorwaarden worden uitgevoerd op basis van CVSS_Base_Score, die gelijk is aan de hoogste kwetsbaarheidsscore die op het eindpunt werd gedetecteerd.

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:...	02:4A:00:14:8D:4B	alice	vulnerability	Qualys	VA_Scan	Quarantine	Exception Rule	CVSS_Base_Score: 9.4 CVSS_Temporal_Score: 7.7

Cloud

Wanneer de VA Scan wordt geactiveerd door de TC-NAC Qualys wachtrijen voor het Scannen, kan dit worden bekeken op Scans > Scans

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

Daarna is de instelling naar actief, wat betekent dat de Qualys-wolk de Qualys Scanner heeft opgedragen het eigenlijke scannen uit te voeren

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

Tijdens het scannen ziet u "Scannen..." teken in de rechterbovenhoek van de Qualys Guard

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

Nadat het Scannen is uitgevoerd, verandert dit in de staat Klaar. U kunt resultaten bekijken op Scans > Scans, de gewenste scan selecteren en op **Summary** of **View Results** klikken.

QUALYS ENTERPRISE

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

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](#)

In het Rapport zelf kunt u **Gedetailleerde resultaten** zien, waar gedetecteerde zwakheden worden weergegeven.

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)

Problemen oplossen

Debugs op ISE

Om debugs op ISE in te schakelen navigeer naar Administratie > Systeem > Vastlegging > Loggen > Debug Log Configuration, selecteert u TC-NAC Node en wijzigt u het logniveau **va-run** en **va-service** component naar **DEBUG**

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

Aanmelden voor controle - varuntime.log. U kunt deze direct starten vanaf ISE CLI:

```
ISE21-3ek/admin# toont bloggingstoepassing varuntime.log tail
```

TC-NAC Docker heeft instructie ontvangen om scannen uit te voeren voor een specifiek eindpunt.

```
2016-06-28 19:06:30,823 DEBUG [Thread-70][] va.run.admin.mnt.endpointFileReader -::: VA: Lezen vanuit een script.  
[</"operationType":1,"macAddress":"C0:4A:00:14:8D:4B", "ondemandScanInterval":"48", "isPeriodicScanEnabled":vals, "PeriodicScanEnabledString":"0", "krasselaarInstance":"79644444 b7-09b5-4f3b-b611-199fb81a4b99", "psnHostName":"ISE21-3ek", "heartBeatTime":0, "lastScanTime":0]  
2016-06-28 19:06:30,824 DEBUG [Thread-70][] va.run.admin.vaservice.VaServiceRemoveHandler::: VA: ontvangen gegevens van Mnt:  
{ "operationType":1, "macAddress":"C0:4A:00:14:8D:4B", "ondemandScanInterval":"48", "isPeriodicScanEnabled":vals, "PeriodicScanStringString":"0", "krasthuis":"79640b7-09b5-4f3b-b611-
```

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

Zodra het resultaat ontvangen is slaat het alle Vulnerability gegevens in de Map van de Context op.

```
2016-06-28 19:25:02,020 DEBUG [pool-311-thread-8][  
va.run.admin.vaservice.VaServiceMessageLuistener::  
[<"macAddress": "C0:4A:00:14:8D:4B", "ipAddress": "10.62.148.63", "lastScanTime": 1467134394000, "kwet  
svermogens": [ "kwetsbaarheidID": "QID-90783", "cveIds": "CVE-2012-0002, CVE-2012-  
0152, ", "cvssBaseScore": "9.3",  
"cvssTemporalScore": "7.7", "kwetsbaarheidTitel": "Microsoft Windows Remote Desktop Protocol  
Afstandscode Uitvoerbaarheid code (MS12-  
020)", "kwetsbaarheidVendor": "Qualys"}], "kwetsbaarheid" ID: "QID-3  
", "cvssTemporalScore": "6.9", "kwetsbaarheidTitel": "SSL Certificaat - Signature  
Verificatie mislukt Kwetsbaarheid", "kwetsbaarheid Verkopers": "Qualys"},  
"cvssBaseScore": "QID-  
9082", "cvssIds": "4.7", "cvssTemporalScore": "4.7", "kwali"}],  
"kwetsbaarheidIDID": "QID90043", "cveIds": "KwID", "KwIDIDScore": "SKLV", "SIC  
Signing Disease Signing t. o. v. t.": "Kwaliteit", "kwetsbaarheidID": "KLEINE Ondertekening  
Niet vereist", "KwaliteitKwaliteit", "KwaliteitID": "QID-386", "cvss-2015-  
2808, "cvssBaseScore": "4.3", "cvssTemporalScore": "7", "kwetsabilityTitle": "SSL/TLS  
gebruik van zwak RC4 algoritme", "kwetsbaarheidVendor": "Qualys"}]
```

```
2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][  
va.run.admin.vaservice.VaServiceMessageLuistener::- VA: Op context db, laatste scantijd  
opslaan: 1467134394000, mac: C0:4A:00:14:8D:4B
```

```
2016-06-28 19:25:02,268 DEBUG [pool-311-thread-8][  
va.run.admin.vaservice.VaAdminServiceContext: het sturen van een elastische zoekfunctie naar  
pri-lan
```

```
2016-06-28 19:25:02,272 DEBUG [pool-311-thread-8][ va.run.admin.vaservice.VaPanRemoveHandler::-  
VA: Opslaan naar elastische zoekopdracht: {C0:4A:00:14:8D:4B=[<"kwetsabilityID": "QID-  
90783", "cveIds": "CVE-2012-0002, CVE-2012-0152, ", "cvss  
Score": "9.3", "cvssTemporalScore": "7.7", "kwetsbaarheidTitel": "Microsoft Windows Remote Desktop  
Protocol Afstandscode executie-kwetsbaarheid (MS12-020)", "kwetsbaarheidVendor": "Qualys"},  
{ "kwetsbaarheidID": "QID-3817  
3", "cveIds": "9.4", "cvssTemporalScore": "6.9", "kwetsabilityTitle": "SSL-  
certificaat - Signature Verification fail Vulnerability", "kwetsabilityVendor": "Qualys"},  
{ "kwetsbaarheidID": "QID  
9082", "cveIds": "4.7", "cvssTemporalScore": "4", "kwetsbaarheidTitel": "Windows  
Remote Desktop Protocol Weak Encryption Methode toegestaan", "kwetsbaarheidVendor": "Qualys"  
ID, "kwetsbaarheidTitel "QID-90043",  
"cveIds": "7.3", "cvssTemporalScore": "6.3", "kwetsbaarheidTitel": "Small Signing  
Disease of Small Small Business Signing Not ved", "kwetsbaarheidVendor": "Qualys",  
{ "kwetsbaarheidID": "QID-38601", "cveIds": "CVE-2013-2566, CVE-2015-  
2808, ", "cvssBaseScore": "4.3", "cvssTemporalScore "3.7", "kwetsabilityTitle": "SSL/TLS gebruik van  
een zwak RC4-algoritme", "kwetsbaarheidVendor": "Qualys"}]
```

Aantekeningen die moeten worden gecontroleerd - vaservice.log. U kunt deze direct staart vanaf ISE CLI:

```
ISE21-3ek/admin# toont logapplicatie vaservice.log tail
```

Aanvragen voor kwetsbaarheidsbeoordeling ingediend bij adapter

```
2016-06-28 17:07:13.200 DEBUG [END-OF-LIFEScheduler-3][] cpm.va.seervice.util.VaServiceUtil -  
::- VA SendSyslog systeemMsg : [<"systemMsg": "91019", "isAutoPlugSelfAcInstance": ware  
"attributes": ["TC-NAC.ServiceName", "Kwetsbaarheidsbeoordelingsservice", "TC-NAC.Status", "VA-  
verzoek ingediend bij adapter", "TC-NAC.Details", "VA-verzoek ingediend bij adapter voor
```

```
verwerking", "TC-NAC.MACAdjurk", "C0:4A:00:14:8D:4B", "TC-NAC.IpAddress", "10.62.148.63", "TC-NAC.AdapterInstanceUid", "79640b7-09S b5-4f3b-b611-199fb81a4b99", "TC-NAC.VendorName", "Qualys", "TC-NAC.AdapterInstanceName", "QUALYS_VA"]]
```

AdapterMessageList controleert elke 5 minuten de status van de scan, totdat deze is voltooid.

```
2016-06-28 17:09:43,459 DEBUG [SimpleAsyncTaskExecurement-2][]
cpm.va.seservice.processor.AdapterBerichtLuisteraar::: - Bericht van adapter:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a7031d6-6e3b-484a-adb0-627f30248ad0", "VendorName":"Qualys", "operationMessageText": "Aantal eindpunten dat in de wachtrij staat voor het controleren van scanresultaten: 1, Aantal eindpunten in de wachtrij voor scan: 0, Aantal eindpunten waarvoor de scan gaande is: 0"}
2016-06-28 17:14:43,760 DEBUG [SimpleAsyncTaskExecurement-2][]
cpm.va.seservice.processor.AdapterBerichtLuisteraar::: - Bericht van adapter:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a7031d6-6e3b-484a-adb0-627f30248ad0", "VendorName":"Qualys", "operationMessageText": "Aantal eindpunten dat in de wachtrij staat voor het controleren van scanresultaten: 0, Aantal eindpunten in de wachtrij voor scan: 0, Aantal eindpunten waarvoor de scan gaande is: 1"}
2016-06-28 17:19:43,837 DEBUG [SimpleAsyncTaskExecurement-2][]
cpm.va.seservice.processor.AdapterBerichtLuisteraar::: - Bericht van adapter:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a7031d6-6e3b-484a-adb0-627f30248ad0", "VendorName":"Qualys", "operationMessageText": "Aantal eindpunten dat in de wachtrij staat voor het controleren van scanresultaten: 0, Aantal eindpunten in de wachtrij voor scan: 0, Aantal eindpunten waarvoor de scan gaande is: 1"}
2016-06-28 17:24:43,867 DEBUG [SimpleAsyncTaskExecurement-2][]
cpm.va.seservice.processor.AdapterBerichtLuisteraar::: - Bericht van adapter:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a7031d6-6e3b-484a-adb0-627f30248ad0", "VendorName":"Qualys", "operationMessageText": "Aantal eindpunten dat in de wachtrij staat voor het controleren van scanresultaten: 0, Aantal eindpunten in de wachtrij voor scan: 0, Aantal eindpunten waarvoor de scan gaande is: 1"}
```

Adapter krijgt QID's, CVE's samen met CVSS-scores

```
2016-06-28 17:24:57,556 DEBUG [SimpleAsyncTaskExecurement-2][]
cpm.va.seservice.processor.AdapterBerichtLuisteraar::: - Bericht van adapter:
{"requestedMacAddress":"C0:4A:00:14:8D:4B", "ScanStatus":"ASSESSMENT_SUCCESS", "lastScanTimeLong": 146713439400, "ipAddress":"10.62.2 148.63", "kwetsbaarheden": [ </"kwetsabilityID": "QID-38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "kwetsabilityTitle": "SSL-certificaat - aard Verificatie mislukt kwetsbaarheid", "kwetsbaarheidVendor": "Qualys"}, {"kwetsbaarheidID": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "kwetsbaarheidTitle": "Small Signing Disease" of het niet-vereiste MKB-signalering", "kwetsabilityVendor": "Qualys"}, {"kwetsabilityID": "QID-90783", "cveIds": "CVE-2012-0002,CVE-2012-0152", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "kwetsbaarheidTitle": "Microsoft Windows Remote-desktopprotocol - mogelijkheden voor de uitvoering van de afstandsbediening (MS12-020)", "kwetsbaarheidVendor": "Qualys"}, {"kwetsbaarheidID": "QID -38601", "cveIds": "CVE-2013-2566,CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "kwetsbaarheidTitel": "SSL/TLS gebruik van een zwak RC4-algoritme", "kwetsabilityVendor": "Qualys"}, {"kwetsbaarheidID": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "kwetsbaarheidTitle": "Windows-methode voor onduidelijke encryptie van het desktopprotocol is toegestaan", "kwetsbaarheidleverancier": "kwaliteiten"}]
2016-06-28 17:25:01,282 INFO [SimpleAsyncTaskExecurement-2][]
cpm.va.seservice.processor.AdapterMessageLuisteraar::: - Endpoint Details die naar IRF worden gestuurd is {"C0:4A:00:14:8D:4B" 4: [ {"kwetsbaarheid": {"CVSS_Base_Score": 9.4, "CVSS_Temporal_Score": 7.7}, "time-stamp": 1467134394000, "title": "kwetsbaarheid", "kraan": "Qualys"}]
2016-06-28 17:25:01,853 DEBUG [END-OF-LIFEScheduler-2][] cpm.va.seervice.util.VaServiceUtil - ::: - VA SendSyslog systeemMsg :
[{"systemMsg": "91019", "isAutoPlugSelfAcInstance": True, "attributes": [{"TC-NAC.ServiceName", "Kwetsbaarheidsbeoordelingsdienst", "TC-NAC.Status", "VA met succes", "TC-NAC.Details", "VA met succes"; aantal geconstateerde kwetsbaarheden: 5}, {"TC-NAC.MACAdjurk", "C0:4A:00:14:8D:4B", "TC-NAC.IpAddress", "10.62.148.63", "TC-NAC.AdapterInstanceUid", "79640b7-7 09b5-4f3b-b611-199fb81a4b99", "TC-NAC.VendorName", "Qualys", "TC-NAC.AdapterInstanceName", "QUALYS_VA"}]
```

Typische problemen

Eenheid 1. ISE krijgt kwetsbaarheidsrapport met CVSS_Base_Score van 0.0 en CVSS_Temporal_Score van 0.0, terwijl het Clouddrapport van Qualys kwetsbaarheden bevat gedetecteerd.

Probleem:

Tijdens het controleren van het Rapport vanuit de Cloud van Qualys kunt u gedetecteerde zwakheden zien, maar op ISE ziet u deze niet.

Debugs in vaservice.log:

```
2016-06-02 08:30:10,323 INFO [SimpleAsyncTaskExectant-2][[]
cpm.va.seservice.processor.AdapterMessageLuistener::- Endpoint Details aan IRF worden verzonden
"C0:4A:00:15:75:C8 "kwetsbaarheid":<"CVSS_Base_Score":0.0, "CVSS_Temporal_Score":0.0}, "time-
stamp":1464855905000, "title": "kwetsbaarheid", "kraan": "Qualys"}}
```

Oplossing:

De reden dat de cvss score nul is is dat het geen kwetsbaarheden heeft of dat de cvss scoring niet in Qualys Cloud is ingeschakeld voordat u de adapter aanpast door UI. Nadat de adapter voor het eerst is ingesteld, wordt u gedownload met kennis die cvss-scoring bevat. U moet ervoor zorgen dat CVSS Scoring was ingeschakeld voordat de adapter instantie werd aangemaakt op ISE. Het kan worden uitgevoerd onder Kwetsbaarheidsbeheer > Rapporten > Instellingen > CVSS > CSS-scoring inschakelen

Onderdeel 2: ISE haalt geen resultaten terug uit de Qualys Cloud, ondanks dat er een juist machtigingsbeleid is gevoerd.

Probleem:

Er is een aangepast vergunningenbeleid gevoerd, waardoor VA Scan zou moeten worden geactiveerd. Desondanks wordt er geen scan gemaakt.

Debugs in vaservice.log:

```
2016-06-28 16:19:15.401 DEBUG [SimpleAsyncTaskExectant-2][[]
cpm.va.seservice.processor.AdapterBerichtLuisteraar:::: - Bericht van adapter:
(Tekst: '[B@6da5e620(byte[311])'MessageProperties [headers=<)], timestamp=ongeldige,
messageID=ongeldige, userID=ongeldige, appID=DN, appID=ongeldige, clusterID=DN, type=nul,
correlatieID=nul, antwoordtTo=nul, contentType=application/octet-stream,
contentEncoding=ongeldige, contentLength=0; Modus=PERSISTENT, expiration=zero, Priority=0,
herbezorgd=vals, ontvangenExchange=irf.topic.va-reports, ontvangenRoutingKey=, deliveryTag=9830,
messageCount=0])
```

```
2016-06-28 16:19:15.401 DEBUG [SimpleAsyncTaskExectant-2][[]
cpm.va.seservice.processor.AdapterBerichtLuisteraar:::: - Bericht van adapter:
{"requestedMacAddress": "24:77:03:3D:CF:20", "scanStatus": "SCAN_FOUT", "scanStatusMessage": "Error
trigNING-scan: Fout bij scancode en fout op aanvraag als volgt uit 1904: geen van de opgegeven
IP's komt in aanmerking voor scannen op kwetsbaarheidsbeheer.", "lastScanTimeLong": 0,
"ipAddress": "10.201.228.102"}
```

```
2016-06-28 16:19:15.771 DEBUG [SimpleAsyncTaskExec-2][[]
cpm.va.seService.processor.AdapterMessageLuistener::- scanresultaat adapter mislukt voor
Macadres:24:77:03:3D:CF:20, IP-adres (DB): 10.201.228.102, waarin de status werd vastgesteld op
het mislukken
```

```
2016-06-28 16:19:16.336 DEBUG [END-OF-LIFEScheduler-2][[] cpm.va.seervice.util.VaServiceUtil -
```

```
:::- VA SendSyslog systeemMsg :  
[<"systemMsg": "91008", "isAutoPlugSelfAcsInstance": True, "attributes": ["TC-  
NAC.ServiceName", "Kwetsbaarheid-beoordelingservice", "TC-NAC.Status", "VA-storing", "TC-  
NAC.Details", "Error-trigNING-scan: Fout bij scancode en fout op aanvraag als volgt uit 1904:  
geen van de gespecificeerde IP's komt in aanmerking voor Vulnerability Management scanning.",  
"TC-NAC.MACAdjurk", "24:77:03:3D:CF:20", "TC-NAC.IpAddress", "10.201.228.102", "TC-NAC.Adapter  
Instance UUID", "79640b7-09b5-4f3b-b611-199fb81a4b99", "TC-NAC.VendorName", "Qualys", "TC-  
NAC.AdapterInstanceName", "QUALYS_VA" ]]
```

Oplossing:

Qualys Cloud geeft aan dat IP-adres van het eindpunt niet in aanmerking komt voor Scannen. Zorg ervoor dat u IP-adres van het endpointbeheer > Activa > Host Asset > New > IP Tracked Hosts hebt toegevoegd

Referenties

- [Administrator-gids voor Cisco Identity Services Engine, release 2.1](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [Video: ISE 2.1 met wachtrijen](#)
- [Documentatie voor snelheden](#)