

Konfiguration von ISE 2.1 Threat-Centric NAC (TC-NAC) mit Qualys

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Übergeordnetes Flussdiagramm](#)

[Konfiguration von Qualys Cloud und Scanner](#)

[Schritt 1: Qualys-Scanner bereitstellen](#)

[Schritt 2: Qualys-Scanner konfigurieren](#)

[ISE konfigurieren](#)

[Schritt 1: Abstimmung der Qualys-Cloud-Einstellungen für die Integration mit der ISE](#)

[Schritt 2: Aktivieren von TC-NAC-Services](#)

[Schritt 3: Konfiguration der Qualyst Adapter-Verbindung mit ISE VA Framework](#)

[Schritt 4: Konfigurieren des Autorisierungsprofils zum Auslösen der VA-Prüfung](#)

[Schritt 5: Autorisierungsrichtlinien konfigurieren](#)

[Überprüfen](#)

[Identity Services Engine](#)

[Qualys-Cloud](#)

[Fehlerbehebung](#)

[Debugger auf der ISE](#)

[Typische Probleme](#)

[Referenzen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration von Threat-Centric NAC mit Qualys auf Identity Services Engine (ISE) 2.1. Mit der Threat Centric Network Access Control (TC-NAC)-Funktion können Sie Autorisierungsrichtlinien erstellen, die auf den Bedrohungs- und Schwachstellenattributen basieren, die von den Adaptern für Bedrohungen und Schwachstellen empfangen wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Identity Service Engine
- Qualys ScanGuard

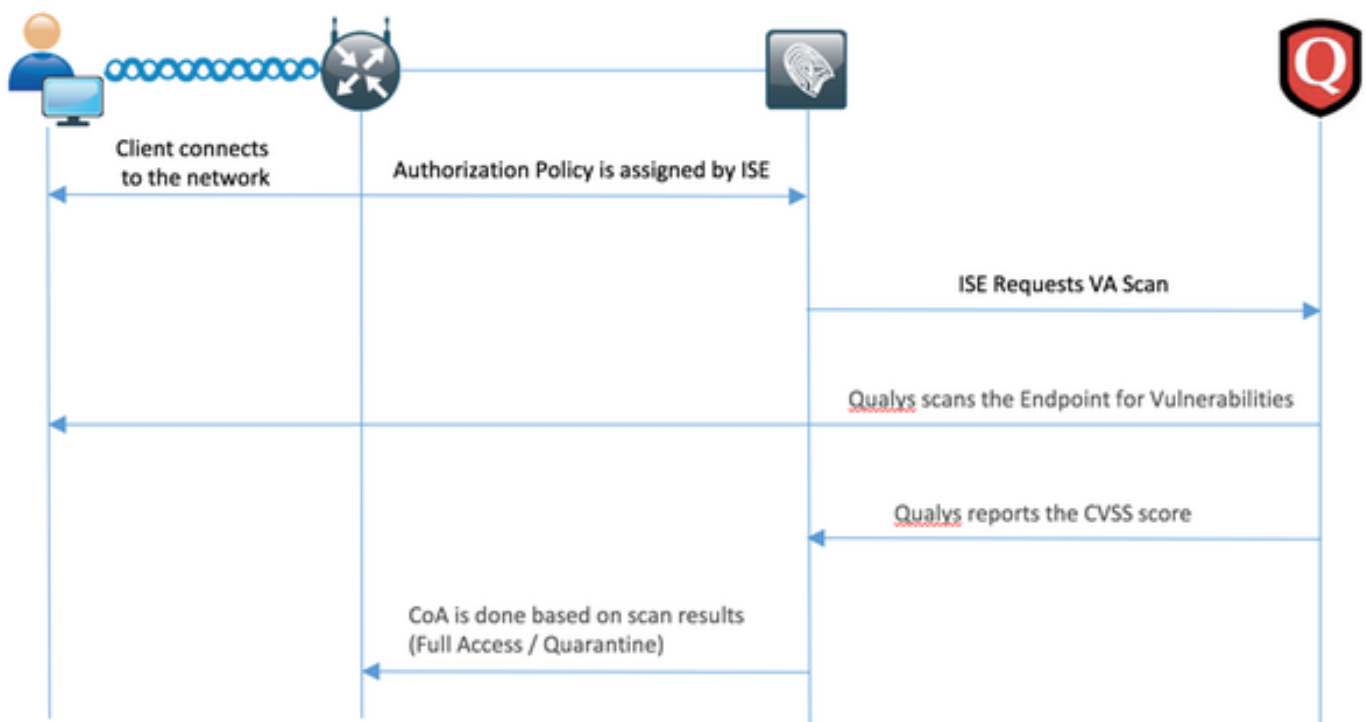
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Service Engine Version 2.1
- Wireless LAN Controller (WLC) 8.0.121.0
- Qualys Guard Scanner 8.3.36-1, Signaturen 2.3.364-2
- Windows 7 Service Pack 1

Konfigurieren

Übergeordnetes Flussdiagramm



Dies ist der Fluss:

1. Der Client stellt eine Verbindung zum Netzwerk her, der Zugriff ist beschränkt, und das Kontrollkästchen **Schwachstellen bewerten** ist aktiviert.
2. PSN-Knoten sendet Syslog-Meldung an MNT-Knoten, die bestätigt, dass die Authentifizierung erfolgt ist, und VA Scan war das Ergebnis der Autorisierungsrichtlinie
3. Der MNT-Knoten sendet SCAN mithilfe der folgenden Daten an den TC-NAC-Knoten (unter Verwendung von Admin WebApp):
 - MAC-Adresse
 - IP-Adresse
 - Scan-Intervall
 - Periodischer Scan aktiviert
 - Ursprungs-PSN
4. Qualys TC-NAC (in Docker-Container eingebettet) kommuniziert mit Qualys Cloud (über

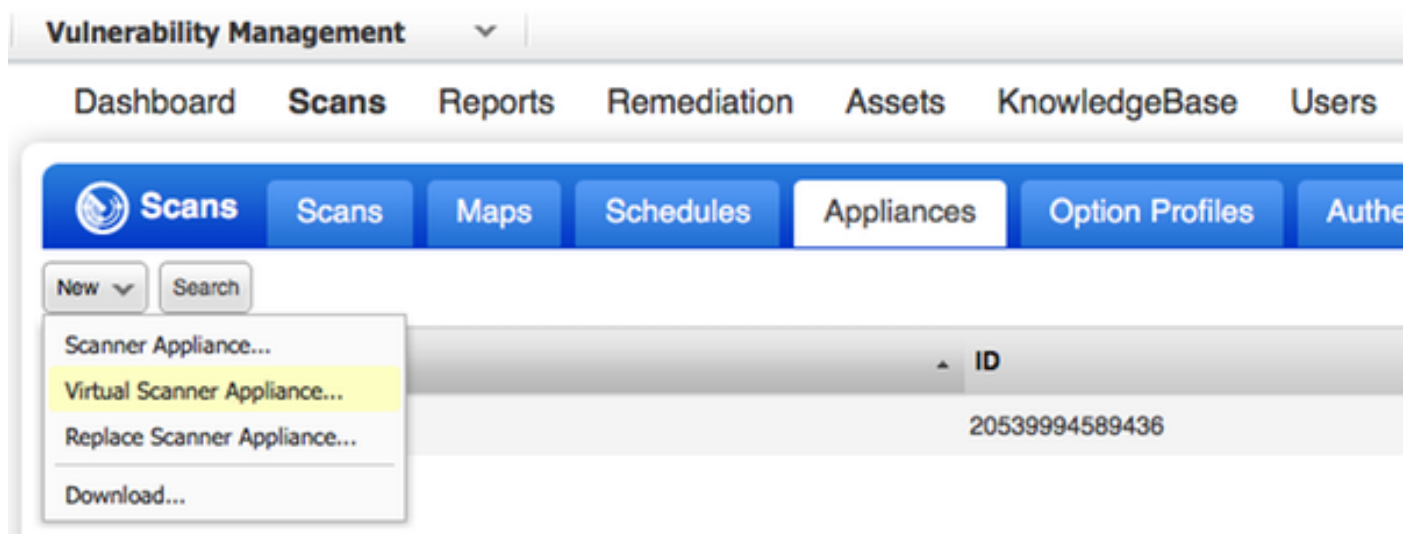
- REST-API), um bei Bedarf einen Scan auszulösen
5. Qualys Cloud weist Qualys Scanner an, das Endgerät zu prüfen
 6. Qualys Scanner sendet die Ergebnisse des Scans an die Qualys Cloud
 7. Die Ergebnisse der Prüfung werden an TC-NAC zurückgesendet:
 - MAC-Adresse
 - Alle CVSS-Bewertungen
 - Alle Sicherheitslücken (QID, Titel, CVEIDs)
 8. TC-NAC aktualisiert PAN mit allen Daten aus Schritt 7.
 9. CoA wird bei Bedarf gemäß konfigurierter Autorisierungsrichtlinie ausgelöst.

Konfiguration von Qualys Cloud und Scanner

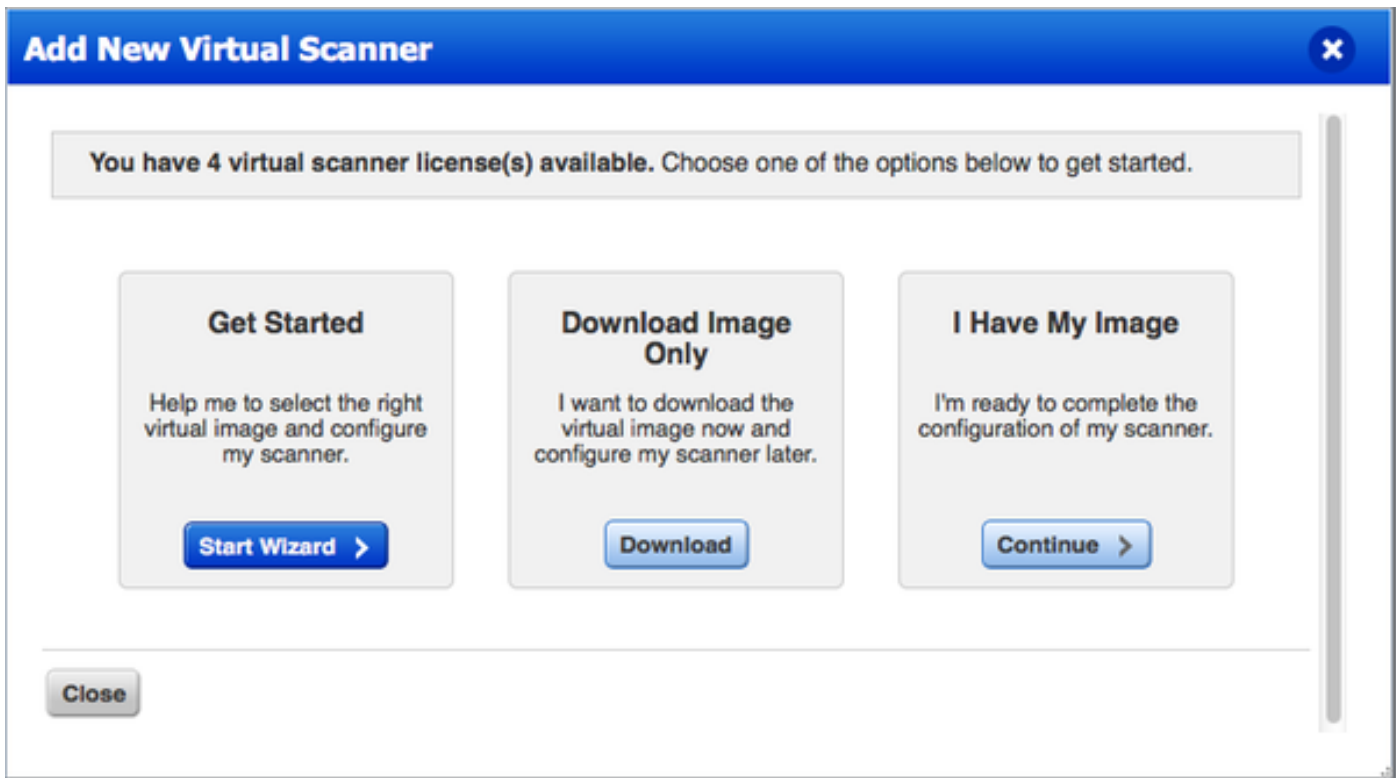
Vorsicht: Fragen Sie die Qualys-Konfiguration in diesem Dokument zu Lab-Zwecken. Wenden Sie sich an die Qualys-Techniker, wenn Sie Fragen zum Design haben.

Schritt 1: Qualys-Scanner bereitstellen

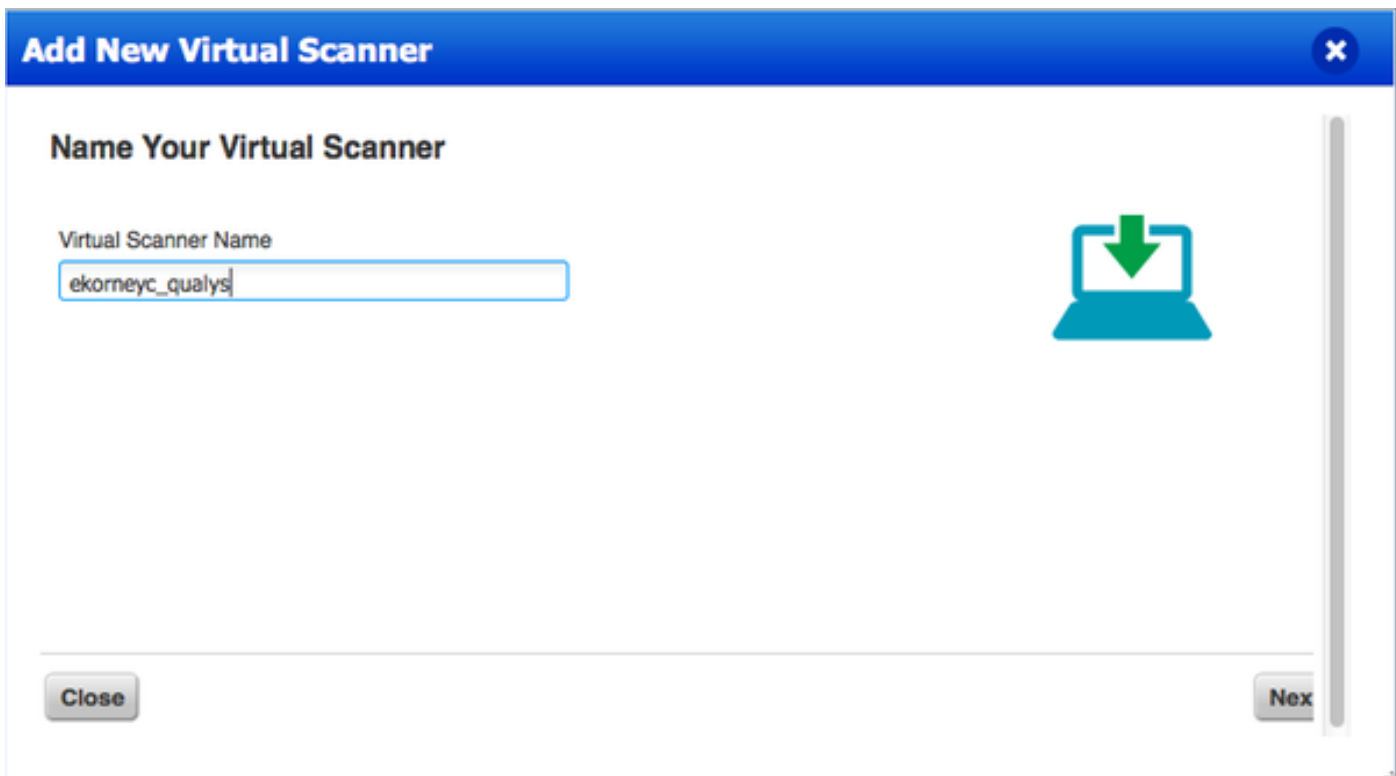
Der Qualys-Scanner kann aus der OVA-Datei bereitgestellt werden. Melden Sie sich bei Qualys Cloud an, navigieren Sie zu Scans > Appliances, und wählen Sie Neu > Virtuelle Scanner-Appliance aus.



Wählen Sie **Image Only (Nur Bild herunterladen)** und anschließend die entsprechende Distribution aus.



Um den Aktivierungscode abzurufen, gehen Sie zu Scans > Appliances, wählen Sie Neu > Virtuelle Scanner-Appliance, und wählen **I Have My Image (Eigenes Bild haben)** aus.



Nach der Eingabe des Scannernamens erhalten Sie einen Autorisierungscode, den Sie später verwenden werden.

Schritt 2: Qualys-Scanner konfigurieren

Stellen Sie OVA auf der Virtualisierungsplattform Ihrer Wahl bereit. Konfigurieren Sie anschließend die folgenden Einstellungen:

- Netzwerk einrichten
- WAN-Schnittstelleneinstellungen (wenn Sie zwei Schnittstellen verwenden)
- Proxy-Einstellungen (wenn Sie Proxy verwenden)
- Scanner anpassen



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)

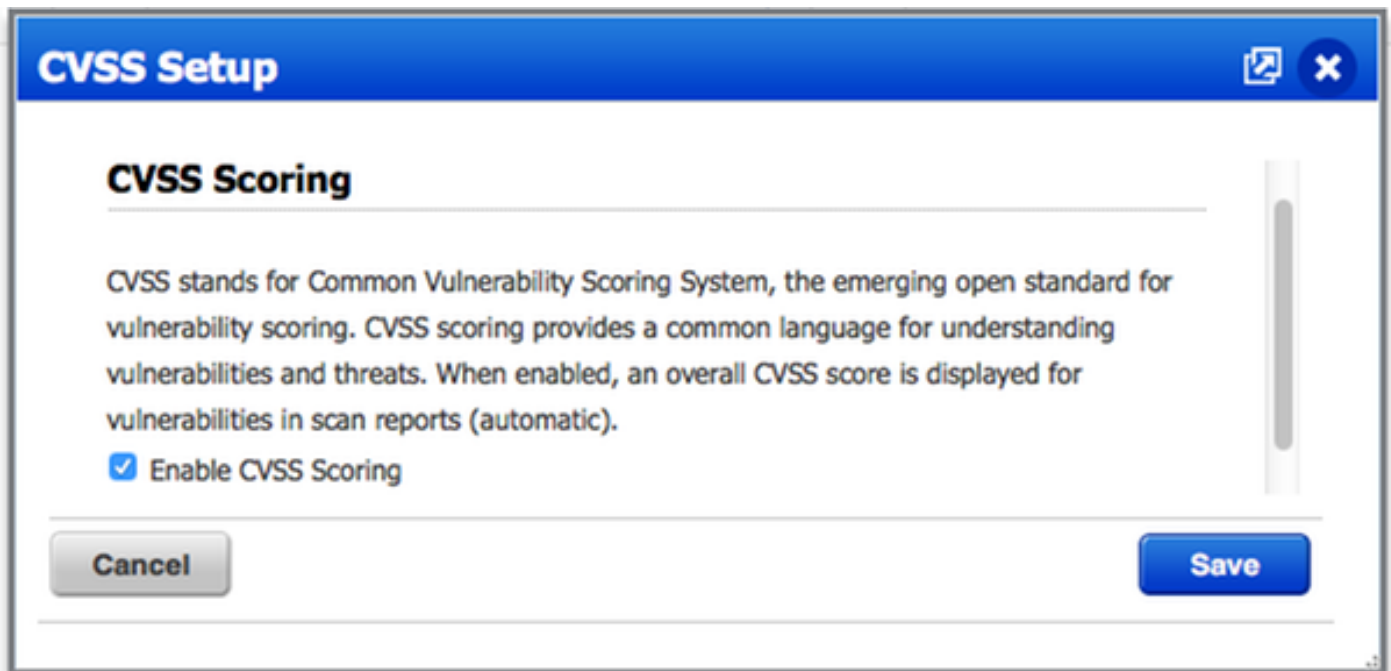
TIP:

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

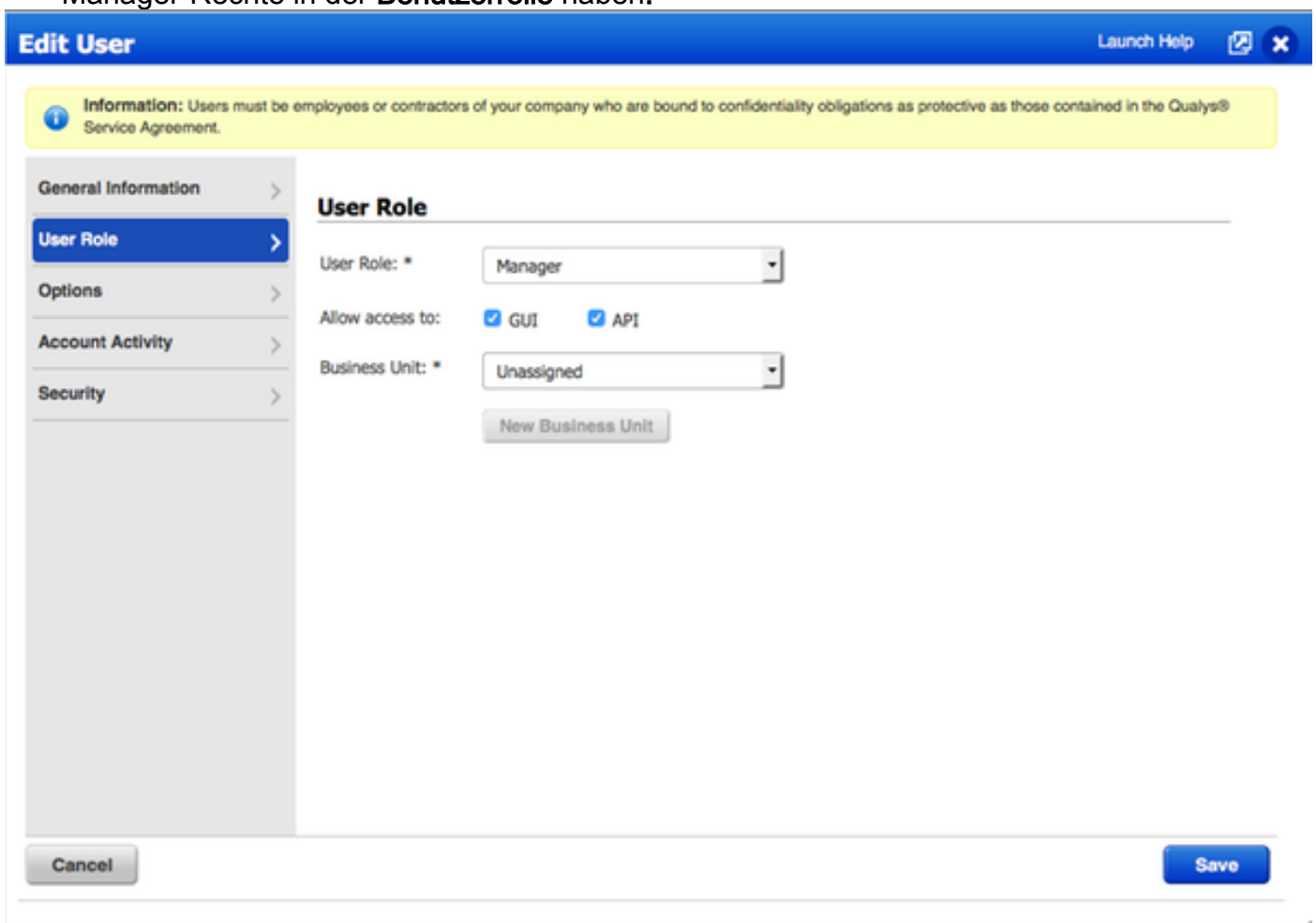
Press the UP and DOWN arrow keys to navigate the menu.

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



Anschließend stellt der Scanner eine Verbindung zu Qualys her und lädt die aktuelle Software und Signaturen herunter.



- Stellen Sie sicher, dass die in der Adapterkonfiguration verwendeten Benutzeranmeldeinformationen über Manager-Berechtigungen verfügen. Wählen Sie Ihren Benutzer in der linken oberen Ecke aus, und klicken Sie auf **Benutzerprofil**. Sie sollten Manager-Rechte in der **Benutzerrolle** haben.



- Stellen Sie sicher, dass IP-Adressen/Subnetze von Endpunkten, die eine Schwachstellenbewertung erfordern, zu Qualysat Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts hinzugefügt werden.

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: *

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 **Add**

Schritt 2: Aktivieren von TC-NAC-Services

Aktivieren Sie TC-NAC Services unter Administration > Deployment > Edit Node. Überprüfen **Threat Centric NAC Service aktivieren** aktivieren.

Hinweis: Pro Bereitstellung kann nur ein TC-NAC-Knoten vorhanden sein.

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 Other Monitoring Node
<input checked="" type="checkbox"/> Policy Service	Include Node in Node Group None
<input checked="" type="checkbox"/> Enable Session Services	
<input checked="" type="checkbox"/> Enable Profiling Service	
<input checked="" type="checkbox"/> Enable Threat Centric NAC Service	

Schritt 3: Konfiguration der Qualyst Adapter-Verbindung mit ISE VA Framework

Navigieren Sie zu Administration > Threat Centric NAC > Third Party Vendors > Add. Klicken Sie auf **Speichern**.

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

Wenn die Qualys-Instanz in den Status **Ready to configure (Bereit zur Konfiguration)** wechselt, klicken Sie auf **Ready to configure (Bereit zur Konfiguration)** in der Status-Option.

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

Der REST-API-Host sollte derjenige sein, den Sie für Qualys Cloud verwenden, wo sich Ihr Konto befindet. In diesem Beispiel: qualysguard.qg2.apps.qualys.com

Account sollte derjenige sein, der über Manager-Berechtigungen verfügt. Klicken Sie auf **Weiter**.

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.

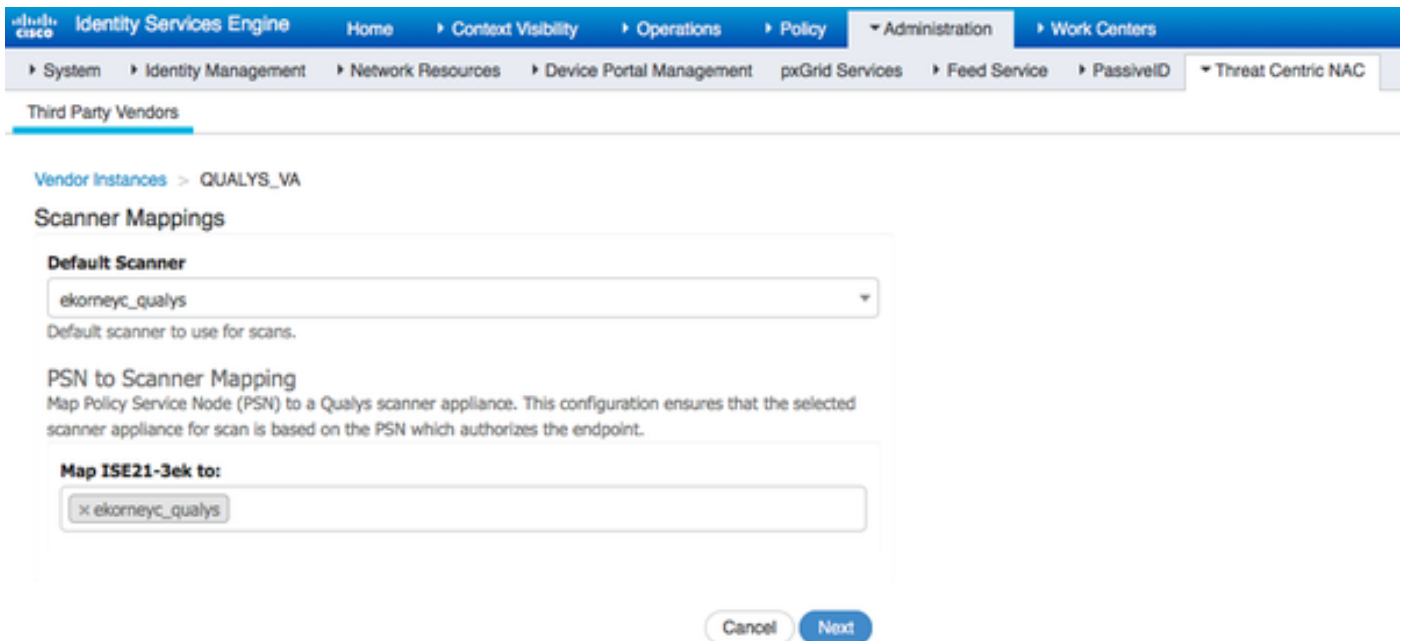
HTTP Proxy Host

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

HTTP Proxy Port

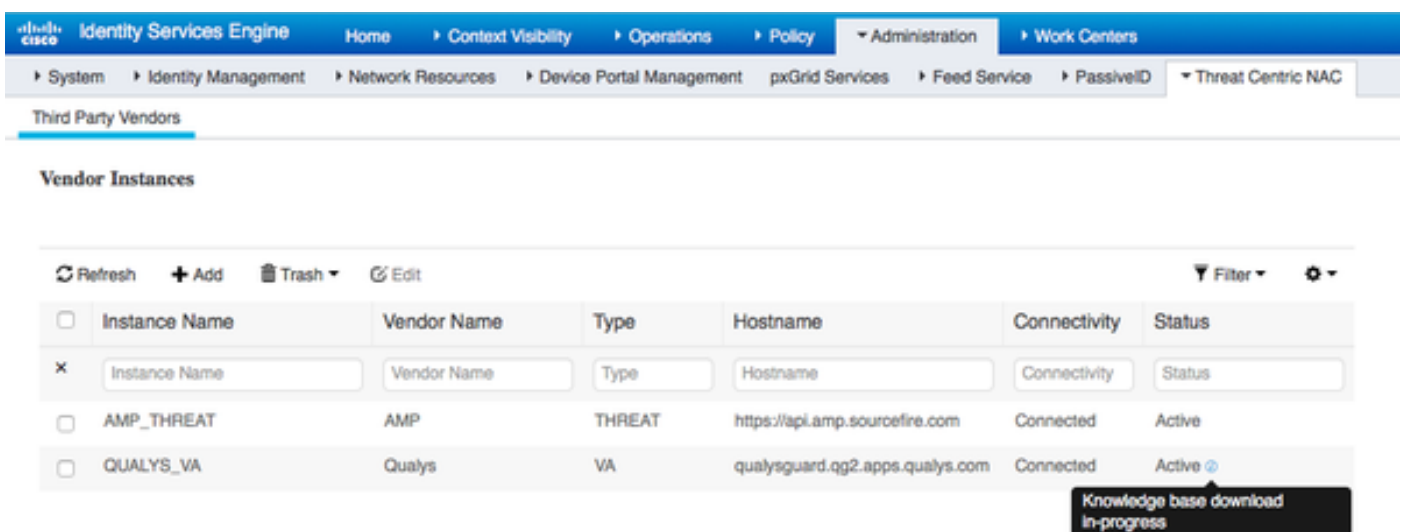
 Optional HTTP Proxy Port. Requires proxy host also to be set.

Die ISE lädt Informationen zu Scannern herunter, die mit der Qualys Cloud verbunden sind. Sie können auf dieser Seite PSN-Scanner-Zuordnung konfigurieren. Sie stellt sicher, dass der ausgewählte Scanner auf Basis von PSN ausgewählt wird, wodurch der Endpunkt autorisiert wird.



Erweiterte Einstellungen sind im ISE 2.1-Administratorhandbuch gut dokumentiert. Der Link ist im Abschnitt Referenzen dieses Dokuments zu finden. Klicken Sie auf **Weiter** und **Beenden**. Qualys Instance wird in den **aktiven** Status überführt und der Download der Knowledge Base wird gestartet.

Hinweis: Pro Bereitstellung kann nur eine Qualys-Instanz vorhanden sein.



Schritt 4: Konfigurieren des Autorisierungsprofils zum Auslösen der VA-Prüfung

Navigieren Sie zu Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile. Neues Profil hinzufügen Aktivieren Sie unter **Häufige Aufgaben** das Kontrollkästchen **Schwachstellenbewertung**. Das On-Demand-Scan-Intervall sollte entsprechend Ihrem Netzwerkdesign ausgewählt werden.

Das Autorisierungsprofil enthält diese av-pair-Kräfte:

cisco-av-pair = On-Demand-Scan-interval=48
 cisco-av-pair = periodisch scannen-enabled=0

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

Sie werden innerhalb des Access-Accept-Pakets an Netzwerkgeräte gesendet, obwohl der eigentliche Zweck dieser Geräte darin besteht, dem MNT-Knoten mitzuteilen, dass der Scan ausgelöst werden soll. MNT weist den TC-NAC-Knoten an, mit der Qualys Cloud zu kommunizieren.

The screenshot displays the 'New Authorization Profile' configuration in Cisco ISE. The breadcrumb trail is 'Authorization Profiles > New Authorization Profile'. The main form includes the following fields and options:

- Name:** VA_Scan
- Description:** (empty text field)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**
- Passive Identity Tracking:**

The 'Common Tasks' section is expanded, showing:

- Assess Vulnerabilities**
- Adapter Instance:** QUALYS_VA
- Trigger scan if the time since last scan is greater than:** 48 (with a note: 'Enter value in hours (1-9999)')
- Assess periodically using above interval

Schritt 5: Autorisierungsrichtlinien konfigurieren

- Konfigurieren Sie die Autorisierungsrichtlinie, um das in Schritt 4 konfigurierte neue Autorisierungsprofil zu verwenden. Navigieren Sie zu Richtlinien > Autorisierung > Autorisierungsrichtlinie, suchen Sie die Regel **Basic_Authenticated_Access**, und klicken Sie auf **Bearbeiten**. Ändern Sie die Berechtigungen von **PermitAccess** in den neu erstellten **Standard VA_Scan**. Dies führt zu einer Schwachstellenüberprüfung für alle Benutzer. Klicken Sie auf **Speichern**.
- Erstellen einer Autorisierungsrichtlinie für isolierte Computer. Navigieren Sie zu Richtlinien > Autorisierung > Autorisierungsrichtlinie > Ausnahmen, und erstellen Sie eine **Ausnahmeregel**. Klicken Sie auf Bedingungen > Neue Bedingung erstellen (Erweiterte Option) > Attribute auswählen, scrollen Sie nach unten, und wählen Sie **Bedrohung aus**. Erweitern Sie das **Threat**-Attribut, und wählen Sie **Qualys-CVSS_Base_Score aus**. Ändern Sie den Operator in **Greater Than**, und geben Sie einen Wert gemäß Ihrer Sicherheitsrichtlinie ein. Das **Quarantäne**-Autorisierungsprofil sollte eingeschränkten Zugriff auf das anfällige System ermöglichen.

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

Überprüfen

Identity Services Engine

Die erste Verbindung löst VA Scan aus. Wenn die Prüfung abgeschlossen ist, wird die CoA-Neuauthentifizierung ausgelöst, um neue Richtlinien anzuwenden, wenn sie abgeglichen werden.

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

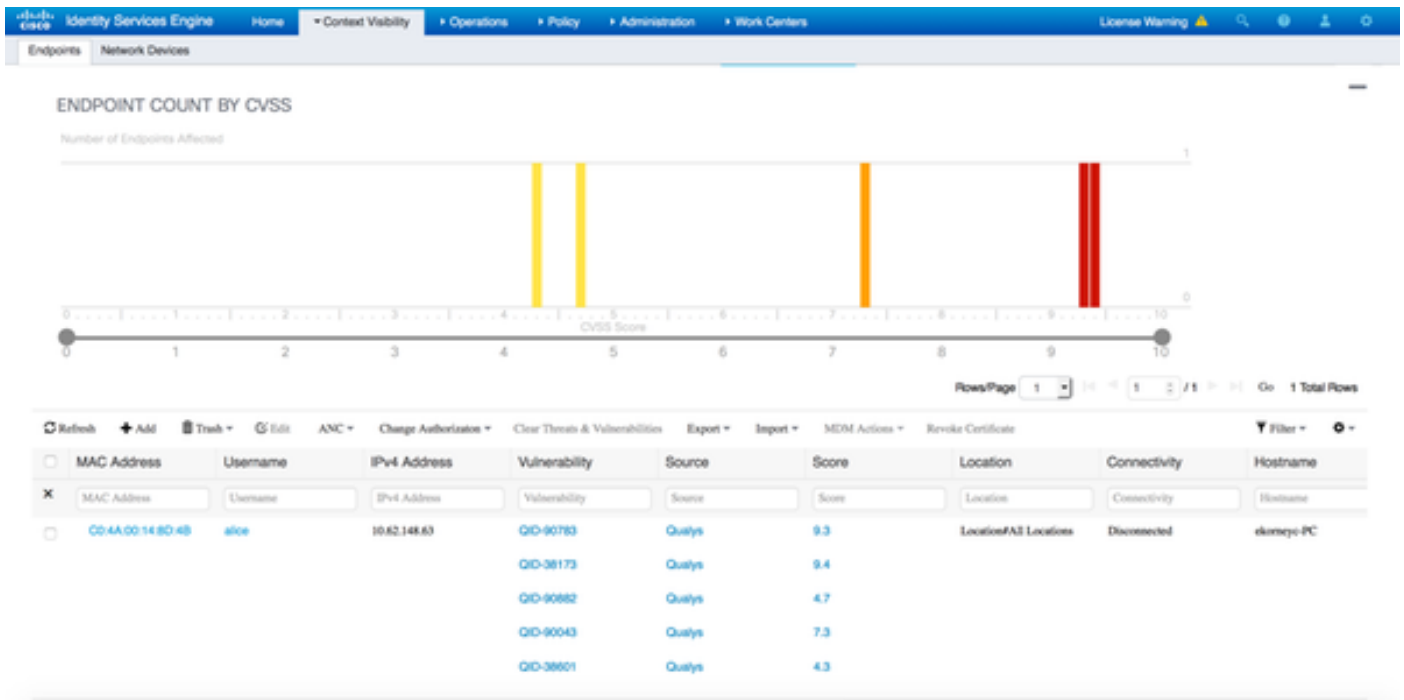
RADIUS TC-MAC Live Logs TACACS Reports Troubleshoot Adaptive Network Control

Live Logs Live Sessions

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

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	Microsoft-Wo...	Default >> Dot1X >> Default	Default >> Exception Rule	Quarantine
Jun 28, 2016 07:25:07:065 PM	✓			alice	CO-4A:00:14:8D:4B				
Jun 28, 2016 07:06:23:437 PM	✓			alice	CO-4A:00:14:8D:4B	TP-LINK De...	Default >> Dot1X >> Default	Default >> Basic_Authenticated_Access	VA_Scan

Um zu überprüfen, welche Sicherheitslücken erkannt wurden, navigieren Sie zu Context Visibility > Endpoints. Überprüfen Sie die Schwachstellen der einzelnen Endpunkte mithilfe der von Qualys angegebenen Punktzahlen.



Wenn Sie einen bestimmten Endpunkt auswählen, werden weitere Details zu jeder Schwachstelle angezeigt, darunter **Titel** und **CVEIDs**.

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:

In Operations > TC-NAC Live Logs (Vorgänge > TC-NAC Live-Protokolle) werden alte und neue Autorisierungsrichtlinien angewendet, sowie Details zu CVSS_Base_Score.

Hinweis: Die Autorisierungsbedingungen basieren auf CVSS_Base_Score. Dies entspricht dem höchsten auf dem Endpunkt erkannten Schwachstellenwert.

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

Qualys-Cloud

Wenn der VA Scan von den Warteschlangen der TC-NAC Qualys ausgelöst wird, kann der Scan unter Scans > Scans angezeigt werden.

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

Nach der Umstellung auf Running (Ausführen), d. h. die Qualys-Cloud hat den Qualys-Scanner angewiesen, die eigentlichen Scanvorgänge auszuführen.

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

Während der Scanner den Scan durchführt, sollte "Scanning.." angezeigt werden. in der rechten oberen Ecke des Qualys Guard

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

Sobald der Scan abgeschlossen ist, wechselt der Status "Fertig gestellt". Sie können die Ergebnisse unter Scans > Scans (Scans > Scans) anzeigen, die gewünschte Prüfung auswählen und auf **Übersicht anzeigen** oder **Ergebnisse anzeigen** klicken.

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	10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Finished
IseScan	10.201.228.107	Eugene Korneychuk	scan/1467132757.03987	06/28/2016	Finished
IseScan	10.201.228.102	Eugene Korneychuk	scan/1467131435.03855	06/28/2016	Finished
IseScan	10.62.148.89	Eugene Korneychuk	scan/1464895232.91271	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464855593.86436	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464850315.85548	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464847674.85321	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464841736.84337	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464836454.83651	06/02/2016	Finished

Preview

Vulnerability Scan - IseScan
Target: 1 IP(s)

Scan launched by Eugene Korneychuk (ek2bk) | 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	View Summary View Results
1	1	7	

Im Bericht selbst sehen Sie **detaillierte Ergebnisse**, in denen die erkannten Schwachstellen angezeigt werden.

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)

Fehlerbehebung

Debugger auf der ISE

Um das Debuggen auf der ISE zu aktivieren, navigieren Sie zu Administration > System > Logging > Debug Log Configuration, wählen Sie TC-NAC Node aus, und ändern Sie die **Protokollstufe va-runtime** und **va-service**-Komponente 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

Protokolle, die überprüft werden sollen - varuntime.log. Sie können sie direkt über die ISE-CLI entfernen:

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

TC-NAC Docker erhielt Anweisungen zur Durchführung der Prüfung auf einen bestimmten Endpunkt.

```
2016-06-28 19:06:30,823 DEBUG [Thread-70][ ] va.runtime.admin.mnt.EndpointFileReader -:::- VA:
Lesen Sie über die Laufzeit.
[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScan
Enabled":false,"periodischerScanEnabledString":"0","vendorInstance":"7964 40b7-09b5-4f3b-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: Von Mnt empfangene Daten:

```
{ "operationType": 1, "macAddress": "C0:4A:00:14:8D:4B", "ondemandScanInterval": "48", "isPeriodicScanEnabled": false, "periodischesScanEnabledString": "0", "vendorInstance": "79644 0b7-09b5-4f3b-b611-199fb81a4b99", "psnHostName": "ISE21-3ek", "heartBeatTime": 0, "lastScanTime": 0 }
```

Sobald das Ergebnis empfangen wurde, werden alle Schwachstellendaten im Kontextverzeichnis gespeichert.

2016-06-28 19:25:02,020 DEBUG [pool-311-thread-8][

```
va.runtime.admin.vaservice.VaServiceMessageListener -:::-- Nachricht von VaService erhalten:
[{"macAddress": "C0:4A:00:14:8D:4B", "ipAddress": "10.62.148.63", "lastScanTime": 1467134394000, "Schwachstellen": [{"\ "Verwundbarkeits-ID\ ": "QID-90783", "\ "cveIds\ ": "CVE-2012-0002,CVE-2012-0152, "\ , "\ "cvssBaseScore\ ": "9.3", "\ "cvssTemporalScore\ ": "7.7", "\ "SchwachstelleTitel\ ": "Ausführungsschwachstelle des Microsoft Windows Remote Desktop Protocol (MS12-020)", "\ "SchwachstelleAnbieter\ ": "Qualys"}, {"\ "SchwachstelleId\ ": "QID-318173", "\ "cveIds\ ": "\ , "\ "cvssBaseScore\ ": "9.4", "\ "cvssTemporalScore\ ": "6.9", "\ "SchwachstelleTitel\ ": "SSL-Zertifikat - Signaturbestätigung fehlgeschlagene Schwachstelle", "\ "SchwachstelleAnbieter\ ": "Qualys"}, {"\ "SchwachstelleId\ ": "QID-90882", "\ "cveIds\ ": "\ , "\ "cvssBaseScore\ ": "4.7", "\ "cvssTemporalScore\ ": "4", "\ "SchwachstelleTitel\ ": "Windows Remote Desktop Protocol Weak Encryption Method Allowed", "\ "VulabilityVendor\ ": "Qualys"}, {"\ "Schwachstellenkennung\ ": "QID-90043", "\ "cveIds\ ": "\ , "\ "cvssBaseScore\ ": "7.3", "\ "cvssTemporalScore\ ": "6.3", "\ "SchwachstelleTitel\ ": "SMB-Signierung deaktiviert oder SMB-Signierung nicht erforderlich", "\ "SchwachstelleAnbieter\ ": "Qualys"}, {"\ "Schwachstellenkennung\ ": "QID-38601", "\ "cveIds\ ": "CVE-2013-2566,CVE-2015-2808, "\ , "\ "cvssBaseScore\ ": "4.3", "\ "cvssTemporalScore\ ": "3.7", "\ "SchwachstelleTitel\ ": "SSL/TLS-Verwendung schwacher RC4-Chiffre", "\ "SchwachstelleAnbieter\ ": "Qualys"}]}]
```

2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][

```
va.runtime.admin.vaservice.VaServiceMessageListener -:::-- VA: Speichern in 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: Elastic Search Json an pri-lan
senden
```

2016-06-28 19:25:02,272 DEBUG [pool-311-thread-8][

```
va.runtime.admin.vaservice.VaPanRemotingHandler -:::-- VA: In elastische Suche gespeichert:
{C0:4A:00:14:8D:4B=[{"VulabilityId": "QID-90783", "cveID": "CVE-2012-0002,CVE-2012-0152, ", "cvssBaseBewertung": "9.3", "cvssTemporalScore": "7.7", "VulnerabilityTitle": "Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)", "VulabilityVendor": "Qualys"}, {"VulabilityId": "QID-38173", "cveIds": ", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "VulabilityTitle": "SSL-Zertifikat - Signature-Verification-Fehlgeschlagene Schwachstelle", "VulabilityVendor": "Qualys"}, {"VulabilityId": "QID-90882", "cveIds": ", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "VulabilityTitle": "Windows Remote Desktop Protocol Weak Encryption Method Allowed", "VulabilityVendor": "Qualys" ID, {"Schwachstelle": "QID-90043", "cveIds": ", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "SchwachstelleTitel": "SMB Signing Disabled oder SMB Signing Not Required", "SchwachstelleVendor": "Qualys" {"VulabilityId": "QID-38601", "cveIds": "CVE-2013-2566,CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "VulabilityTitle": "SSL/TLS-Verwendung schwacher RC4-Chiffre", "VulabilityVendor": "Qualys"}]}
```

Protokolle zu überprüfen - vaservice.log. Sie können sie direkt über die ISE-CLI entfernen:

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

Anfrage zur Schwachstellenbewertung an Adapter gesendet

```
2016-06-28 17:07:13,200 DEBUG [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg:
[{"systemMsg":"91019","isAutoInsertSelfAcInstance":true,"attribute":["TC-
NAC.ServiceName","Schwachstellenanalyseservice","TC-NAC.Status","VA-Anfrage an Adapter
gesendet","TC-NAC.Details","VA-Anfrage zur Verarbeitung an Adapter gesendet", TC-
NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IPAddress","10.62.148.63","TC-
NAC.AdapterInstanceUUUID","79640b7-09A b5-4f3b-b611-199fb81a4b99","TC-
NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

AdapterMessageListener überprüft alle 5 Minuten den Status der Prüfung, bis sie abgeschlossen ist.

```
2016-06-28 17:09:43,459 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Nachricht vom Adapter:
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText": "Anzahl der Endpunkte, die zur
Überprüfung der Scanergebnisse in die Warteschlange gestellt werden: 1, Anzahl der zum Scannen
in die Warteschlange gestellten Endpunkte: 0, Anzahl der Endpunkte, für die die Prüfung
ausgeführt wird: 0"}
```

```
2016-06-28 17:14:43,760 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Nachricht vom Adapter:
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText": "Anzahl der Endpunkte, die zur
Überprüfung der Scanergebnisse in die Warteschlange gestellt werden: 0, Anzahl der zum Scannen
in die Warteschlange gestellten Endpunkte: 0, Anzahl der Endpunkte, für die die Prüfung
ausgeführt wird: 1"}
```

```
2016-06-28 17:19:43.837 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Nachricht vom Adapter:
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText": "Anzahl der Endpunkte, die zur
Überprüfung der Scanergebnisse in die Warteschlange gestellt werden: 0, Anzahl der zum Scannen
in die Warteschlange gestellten Endpunkte: 0, Anzahl der Endpunkte, für die die Prüfung
ausgeführt wird: 1"}
```

```
2016-06-28 17:24:43,867 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Nachricht vom Adapter:
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText": "Anzahl der Endpunkte, die zur
Überprüfung der Scanergebnisse in die Warteschlange gestellt werden: 0, Anzahl der zum Scannen
in die Warteschlange gestellten Endpunkte: 0, Anzahl der Endpunkte, für die die Prüfung
ausgeführt wird: 1"}
```

Der Adapter erhält QIDs, CVEs zusammen mit den CVSS-Bewertungen.

```
2016-06-28 17:24:57,556 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Nachricht vom Adapter:
{"AngeforderteMacAddress":"C0:4A:00:14:8D:4B","scanStatus":"ASSESSMENT_SUCCESS","lastScanTimeLon
g":1467134394000,"ipAddress":"10.62. 148.63", "Schwachstellen":[{"VulabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","SchwachstelleTitle":"SSL-
Zertifikat - Signatur Verification Failed
Vulnerability","VulabilityVendor":"Qualys"}, {"VulabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","Title":"SMB Signing Disabled
or SMB Signing Not Required","VulabilityVendor":"Qualys"}, {"VulabilityId":"QID-
90783","cveIds":"CVE-2012-0002,CVE-2012-
0152","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","VulnerabilityTitle":"Ausführungsschwachst
elle des Microsoft Windows Remote Desktop Protocol-Codes (MS12-
020)","VulabilityVendor":"Qualys"}, {"QverwundabilityId":"ID-38601","cveIds":"CVE-2013-2566,CVE-
2015-2808","cvssBaseScore":"4.3","cvssTemporalScore":"3.7", abilityTitle":"SSL/TLS-Verwendung
schwacher RC4-Chiffre","VulabilityVendor":"Qualys"}, {"VulabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore": "4","VulabilityTitle":"Windows
Remote Desktop Protocol Weak Encryption Method Allowed","VulabilityVendor":"Qualys"}]}
2016-06-28 17:25:01,282 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Endpoint Details sent to IRF is
```

```
{ "C0:4A:00:14:8D:4B": [{"Schwachstelle": {"CVSS_Base_Score": 9.4, "CVSS_Temporal_Score": 7.7}, "Zeitstempel": 1467134394000, "Titel": "Schwachstelle", "Anbieter": "Qualys"}]}
2016-06-28 17:25:01,853 DEBUG [endpointPollerScheduler-2] [] cpm.va.service.util.VaServiceUtil -
::::- VA SendSyslog systemMsg:
[{"systemMsg": "91019", "isAutoInsertSelfAcInstance": true, "attribute": [{"TC-
NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA successfully", "TC-
NAC.Details", "VA completed; Anzahl der gefundenen Schwachstellen: 5", "TC-
NAC.MACAddress", "C0:4A:00:14:8D:4B", "TC-NAC.IPAddress", "10.62.148.63", "TC-
NAC.AdapterInstanceUuid", "79640b7-09b5-4f3b-b611-199fb81a4b99", "TC-NAC.VendorName", "Qualys", "TC-
NAC.AdapterInstanceName", "QUALYS_VA"}]}
```

Typische Probleme

Ausgabe 1 Die ISE erhält den Schwachstellenbericht mit CVSS_Base_Score von 0.0 und CVSS_Temporal_Score von 0.0, während der Qualys Cloud-Bericht Schwachstellen enthält.

Problem:

Beim Überprüfen des Berichts von der Qualys Cloud können Sie erkannte Schwachstellen sehen, auf der ISE werden diese jedoch nicht angezeigt.

Debuggen in vaservice.log:

```
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": [{"Schwachstelle": {"CVSS_Base_Score": 0.0, "CVSS_Temporal_Score": 0.0}, "Zeitstempel": 1464855905000, "Titel": "Schwachstelle", "Anbieter": "Qualys"}]}
```

Lösung:

Der Grund dafür, dass der CSS-Wert 0 ist, ist entweder, dass er keine Schwachstellen aufweist, oder die CVSS-Bewertung wurde in der Qualys Cloud nicht aktiviert, bevor Sie den Adapter über die Benutzeroberfläche konfigurieren. Die Knowledgebase, die die aktivierte CVSS-Bewertungsfunktion enthält, wird nach der erstmaligen Konfiguration des Adapters heruntergeladen. Sie müssen sicherstellen, dass CVSS Scoring zuvor aktiviert wurde. Die Adapterinstanz wurde auf der ISE erstellt. Sie kann unter Vulnerability Management > Reports > Setup > CVSS > Enable CVSS Scoring ausgeführt werden.

Ausgabe 2: Die ISE erhält keine Ergebnisse aus der Qualys Cloud, obwohl die richtige Autorisierungsrichtlinie erreicht wurde.

Problem:

Die korrigierte Autorisierungsrichtlinie wurde zugeordnet, was einen VA-Scan auslösen sollte. Dennoch wird kein Scan durchgeführt.

Debuggen in vaservice.log:

```
2016-06-28 16:19:15.401 DEBUG [SimpleAsyncTaskExecutor-2] []
cpm.va.service.processor.AdapterMessageListener -:::::- Nachricht vom Adapter:
(Text: '[B@6da5e620(byte[311])'MessageProperties [headers={}, timestamp=null, messageId=null,
userId=null, appId=null, clusterId=null, type=null, relationId=null, replyTo=null,
contentType=application/octet-stream, contentEncoding=null, contentLength=0, Delivery
Mode=PERSISTENT, expiration=null, priority=0, redelivery=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 -:::::- Nachricht vom Adapter:
{"AngeforderteMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"Error Triggering scan: Fehler beim Auslösen des Scan-Codes und -Fehlers bei Bedarf wie folgt 1904: Keine der angegebenen IPs ist für den Schwachstellenmanagement-Scan zulässig.","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 ist nicht in
Macaddress:24:77:03:3D:CF:20, IP-Adresse(DB): 10.201.228.102, Festlegen des Status auf
fehlgeschlagen
2016-06-28 16:19:16.336 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
::::- VA SendSyslog systemMsg:
[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attribute":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA Failure","TC-
NAC.Details","Error Triggering scan: Fehler beim Auslösen des Scan-Codes und -Fehlers bei Bedarf
wie folgt 1904: keines der angegebenen IPs ist für die Prüfung der Schwachstellenverwaltung
zulässig.,"TC-NAC.MACAddress","24:77:03:3D:CF:20","TC-NAC.IpAddress","10.201.228.102","TC-
NAC.AdapterInstance UUID","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-
NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]]
```

Lösung:

Qualys Cloud gibt an, dass die IP-Adresse des Endpunkts nicht für das Scannen zugelassen ist. Stellen Sie sicher, dass Sie die IP-Adresse des Endpunkts zu Schwachstellenmanagement > Ressourcen > Hostressourcen > Neu > IP Tracked Hosts hinzugefügt haben.

Referenzen

- [Administratoranleitung für Cisco Identity Services Engine, Version 2.1](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)
- [Video: ISE 2.1 mit Qualys](#)
- [Qualys-Dokumentation](#)