

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[High Level Flow Diagram](#)

[Configure Qualys Cloud and Scanner](#)

[Step 1. Deploy Qualys Scanner](#)

[Step 2. Configure Qualys Scanner](#)

[Configure ISE](#)

[Step 1. Tune Qualys Cloud Settings for Integration with ISE](#)

[Step 2. Enable TC-NAC Services](#)

[Step 3. Configure Qualys Adapter Connectivity to ISE VA Framework](#)

[Step 4. Configure Authorization Profile to trigger VA Scan](#)

[Step 5. Configure Authorization Policies](#)

[Verify](#)

[Identity Services Engine](#)

[Qualys Cloud](#)

[Troubleshoot](#)

[Debugs on ISE](#)

[Typical Issues](#)

[References](#)

Introduction

This document describes how to configure Threat-Centric NAC with Qualys on Identity Services Engine (ISE) 2.1. Threat Centric Network Access Control (TC-NAC) feature enables you to create authorization policies based on the threat and vulnerability attributes received from the threat and vulnerability adapters.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- Cisco Identity Service Engine
- Qualys ScanGuard

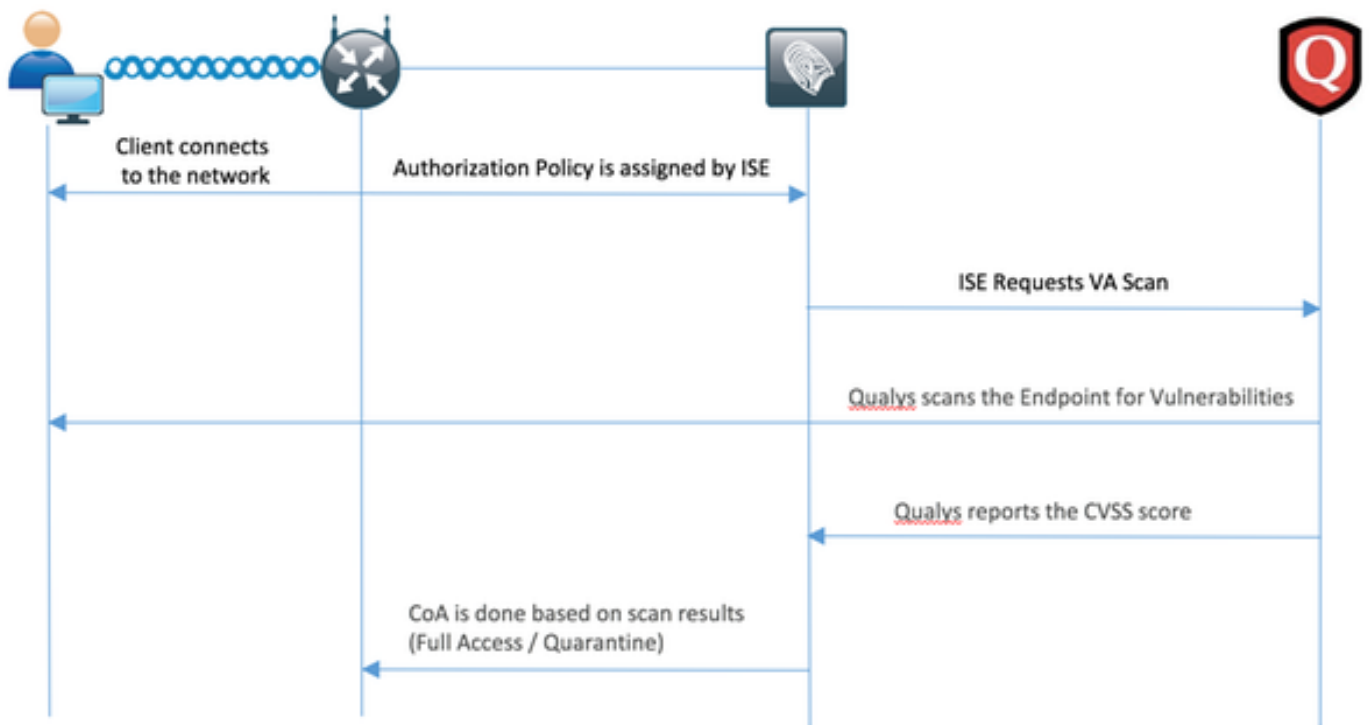
Components Used

The information in this document is based on these software and hardware versions:

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

Configure

High Level Flow Diagram



This is the flow:

1. Client connects to the network, limited access is given and profile with **Assess Vulnerabilities** checkbox enabled is assigned
2. PSN node sends Syslog message to MNT node confirming authentication took place and VA Scan was the result of Authorization Policy
3. MNT node submits SCAN to TC-NAC node (using Admin WebApp) using this data:
 - MAC Address
 - IP Address
 - Scan Interval
 - Periodic Scan Enabled
 - Originating PSN
4. Qualys TC-NAC (encapsulated in Docker Container) communicates with Qualys Cloud (via REST API) to trigger scan if needed
5. Qualys Cloud instructs Qualys Scanner to scan the endpoint
6. Qualys Scanner sends the results of the scan to the Qualys Cloud
7. Results of the scan are sent back to TC-NAC:
 - MAC Address
 - All CVSS Scores

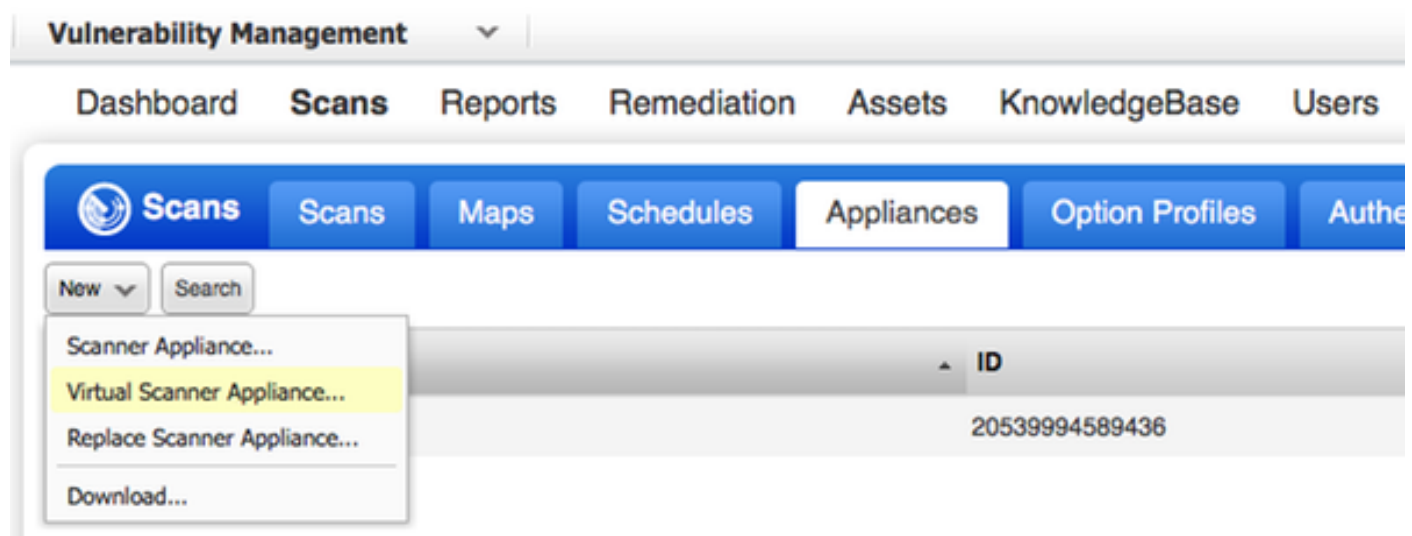
- All Vulnerabilities (QID, title, CVEIDs)
8. TC-NAC updates PAN with all the data from the step 7.
 9. CoA is triggered if needed according to Authorization Policy configured.

Configure Qualys Cloud and Scanner

Caution: Qualys configuration in this document is done for the lab purposes, please consult with Qualys engineers for design considerations

Step 1. Deploy Qualys Scanner

Qualys scanner can be deployed from OVA file. Login to Qualys cloud and navigate to Scans > Appliances and select New > Virtual Scanner Appliance



Select **Download Image Only** and pick appropriate distribution

Add New Virtual Scanner

You have 4 virtual scanner license(s) available. Choose one of the options below to get started.

Get Started

Help me to select the right virtual image and configure my scanner.

Start Wizard >

Download Image Only

I want to download the virtual image now and configure my scanner later.

Download

I Have My Image

I'm ready to complete the configuration of my scanner.

Continue >

Close


To get Activation Code you can go to Scans > Appliances and select New > Virtual Scanner Appliance and select **I Have My Image**

Add New Virtual Scanner

Name Your Virtual Scanner

Virtual Scanner Name

ekorneyc_qualys



Close

Next

After entering scanner name you are given Authorization Code which you will use later.

Step 2. Configure Qualys Scanner

Deploy OVA on the virtualization platform of your choice. Once done, configure those settings:

- Set up network (LAN)

- WAN interface settings (if you are using two interfaces)
- Proxy settings (if you are using proxy)
- Personalize this 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.

Afterwards scanner connects to Qualys and downloads the latest software and signatures.

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 >

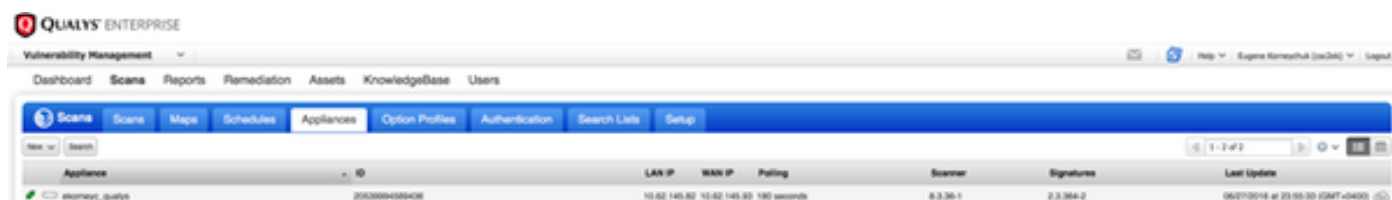
System reboot >

Version info: 3.9.7.5.11.0


Exit this menu? (Y/N)

To verify the scanner is connected you can navigate to Scans > Appliances.

Green connected sign on the left indicates that scanner is ready, you can also see LAN IP, WAN IP, version of Scanner and Signatures.



The screenshot shows the Qualys Enterprise Vulnerability Management interface. The 'Appliances' tab is selected, displaying a table with the following data:

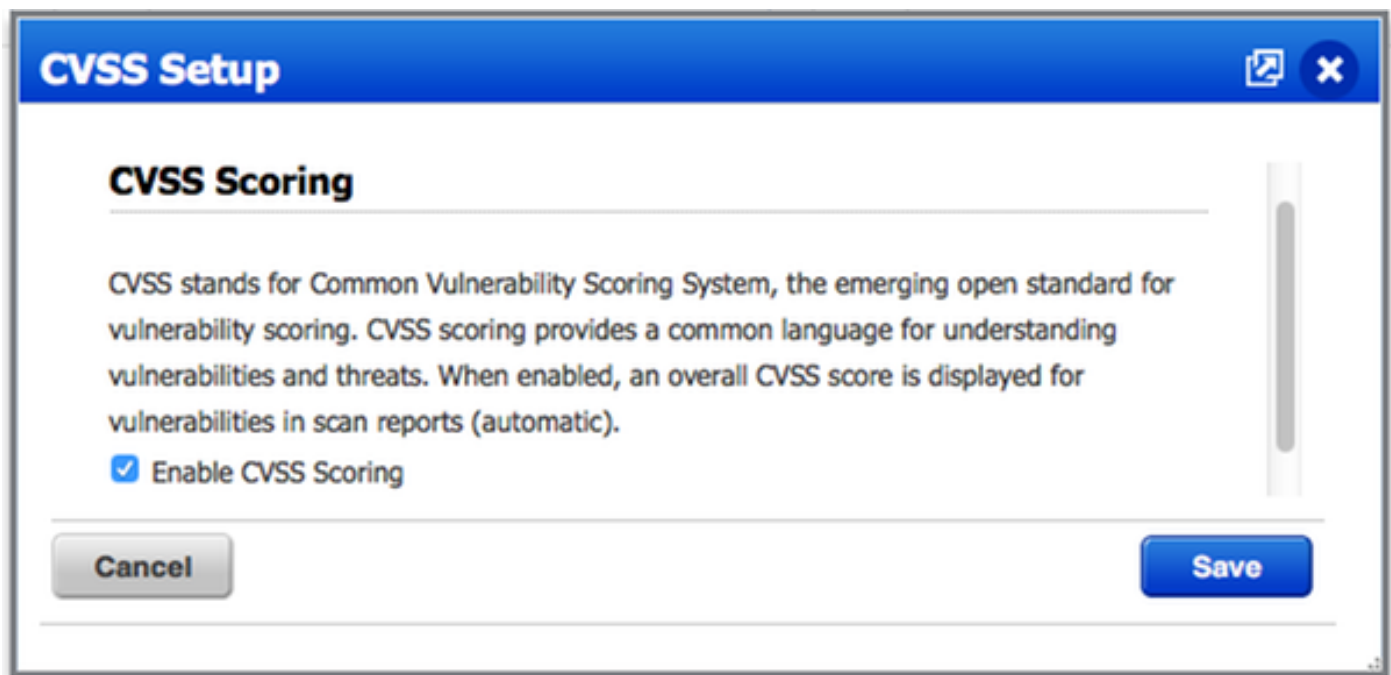
Appliance	ID	LAN IP	WAN IP	Poling	Scanner	Signatures	Last Update
 economy_suite	2000004000000	10.62.145.82	10.62.145.82	180 seconds	3.3.36-1	2.3.364-2	06/27/2016 at 23:58:30 (GMT+0400)

Configure ISE

Though you have configured Qualys Scanner and Cloud, you still have to tune Cloud settings to make sure integration with ISE works fine. Note, it should be done before you configure adapter through GUI, as the knowledgebase containing CVSS scoring is downloaded after the adapter is configured for the first time.

Step 1. Tune Qualys Cloud Settings for Integration with ISE

- Enable CVSS Scoring at Vulnerability Management > Reports > Setup > CVSS > Enable CVSS Scoring



CVSS Setup

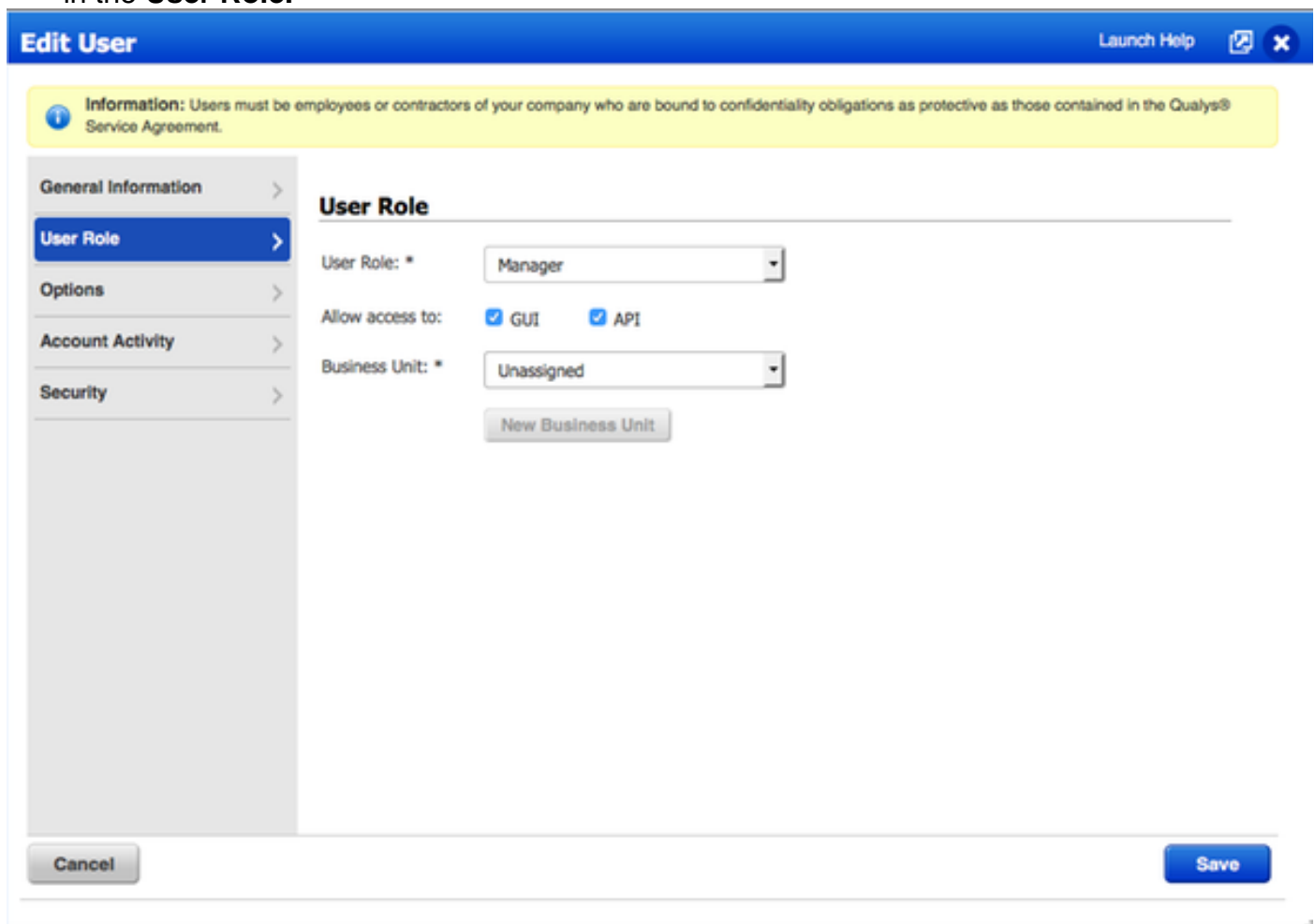
CVSS Scoring

CVSS stands for Common Vulnerability Scoring System, the emerging open standard for vulnerability scoring. CVSS scoring provides a common language for understanding vulnerabilities and threats. When enabled, an overall CVSS score is displayed for vulnerabilities in scan reports (automatic).

☒ Enable CVSS Scoring

Cancel **Save**

- Ensure that user credentials used in adapter configuration have manager privileges. Select your user from the left top corner and click on **User Profile**. You should have Manager rights in the **User Role**.



Edit User Launch Help

Information: Users must be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Qualys® Service Agreement.

General Information **User Role** **Options** **Account Activity** **Security**

User Role

User Role: * Manager

Allow access to: ☒ GUI ☒ API

Business Unit: * Unassigned

New Business Unit

Cancel **Save**

- Ensure that IP addresses/subnets of endpoints that require Vulnerability Assessment are added to 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: *

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

Step 2. Enable TC-NAC Services

Enable TC-NAC Services under Administration > Deployment > Edit Node. Check **Enable Threat Centric NAC Service** checkbox.

Note: There can be only one TC-NAC Node per Deployment.

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

☒ Administration

Role 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

Step 3. Configure Qualys Adapter Connectivity to ISE VA Framework

Navigate to Administration > Threat Centric NAC > Third Party Vendors > Add. Click on **Save**.

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 * Qualys : VA

Instance Name * QUALYS_VA

Cancel Save

When Qualys Instance transitions to **Ready to configure** state, click on **Ready to configure** option in the Status.

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

Refresh Add Trash Edit Filter

	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
<input type="checkbox"/>	QUALYS_VA	Qualys	VA		Disconnected	Ready to configure

REST API host should be the one you use for Qualys Cloud, where your account is located. In this example - qualysguard.qg2.apps.qualys.com

Account should be the one with Manager privileges, click on **Next**.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', 'PassiveID', and 'Threat Centric NAC'. The 'Third Party Vendors' section is selected, leading to 'Vendor instances > QUALYS_VA'. The main heading is 'Enter Qualys Configuration Details', with instructions to enable CVSS Scoring in Qualys and add the IP address of the endpoints. The configuration form includes fields for 'REST API Host' (qualysguard.qg2.apps.qualys.com), 'REST API Port' (443), 'Username' (csc2ek), 'Password' (masked), 'HTTP Proxy Host' (optional), and 'HTTP Proxy Port' (optional). The 'Next' button is highlighted in blue.

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
qualysguard.qg2.apps.qualys.com
The hostname of the Qualys platform where your account is located.

REST API Port
443
The port used by the REST API host.

Username
csc2ek
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.

Cancel Next

ISE downloads information about Scanners which are connected to Qualys Cloud, you can configure PSN to Scanner Mapping on this page. It ensures that selected scanner is picked based on PSN which authorizes the endpoint.

Third Party Vendors

Vendor Instances > QUALYS_VA

Scanner Mappings

Default Scanner

ekorneyc_qualys

Default scanner to use for scans.

PSN to Scanner Mapping

Map Policy Service Node (PSN) to a Qualys scanner appliance. This configuration ensures that the selected scanner appliance for scan is based on the PSN which authorizes the endpoint.

Map ISE21-3ek to:

ekorneyc_qualys

Cancel Next

Advanced settings are well documented in ISE 2.1 Admin Guide, link can be found in the References section of this document. Click on **Next** and **Finish**. Qualys Instance transitions to **Active** state and knowledge base download starts.

Note: There can be only one Qualys instance per deployment.

Third Party Vendors

Vendor Instances

Refresh Add Trash Edit Filter

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active Knowledge base downloaded in-progress

Step 4. Configure Authorization Profile to trigger VA Scan

Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles. Add new profile. Under **Common Tasks** select **Vulnerability Assessment** checkbox. On-Demand scan interval should be selected according to your network design.

Authorization Profile contains those av-pairs:

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

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

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

They are sent to network devices within Access-Accept packet, although the real purpose of them is to tell MNT Node that Scan should be triggered. MNT instructs TC-NAC node to communicate with Qualys Cloud.

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a new Authorization Profile. The breadcrumb trail indicates the path: Authorization Profiles > New Authorization Profile. The main form is titled 'Authorization Profile' and contains the following fields and options:

- Name:** A text input field containing 'VA_Scan'.
- Description:** An empty text input field.
- Access Type:** A dropdown menu set to 'ACCESS_ACCEPT'.
- Network Device Profile:** A dropdown menu set to 'Cisco'.
- Service Template:** An unchecked checkbox.
- Track Movement:** An unchecked checkbox with an information icon.
- Passive Identity Tracking:** An unchecked checkbox with an information icon.

Below the main form is a section titled 'Common Tasks' with a checked checkbox for 'Assess Vulnerabilities'. This section includes:

- Adapter Instance:** A dropdown menu set to 'QUALYS_VA'.
- Trigger scan if the time since last scan is greater than:** A text input field containing '48', with a note below it: 'Enter value in hours (1-9999)'.
- Assess periodically using above interval:** An unchecked checkbox.

Step 5. Configure Authorization Policies

- Configure Authorization Policy to use the new Authorization Profile configured in step 4. Navigate to Policy > Authorization > Authorization Policy, locate **Basic_Authenticated_Access** rule and click on **Edit**. Change the Permissions from **PermitAccess** to the newly created **Standard VA_Scan**. This causes a Vulnerability Scan for all users. Click on **Save**.
- Create Authorization Policy for Quarantined machines. Navigate to Policy > Authorization > Authorization Policy > Exceptions and create an **Exception Rule**. Click on Conditions > Create New Condition (Advanced Option) > Select Attribute, scroll down and select **Threat**. Expand the **Threat** attribute and select **Qualys-CVSS_Base_Score**. Change the operator to **Greater Than** and enter a value according to your Security Policy. **Quarantine** authorization profile should give limited access to the vulnerable machine.

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_Profiling_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

Verify

Identity Services Engine

The first connection triggers VA Scan. When the scan is finished, CoA Reauthentication is triggered to apply new policy if it is matched.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

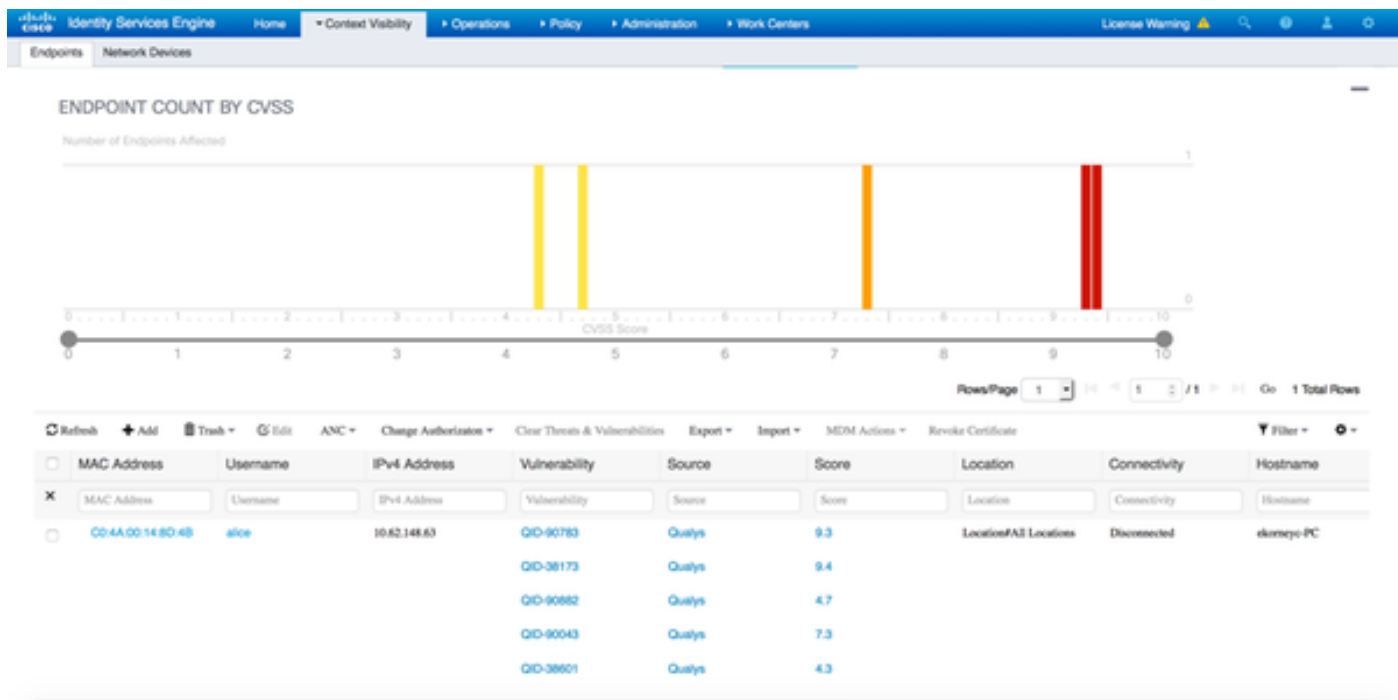
Live Logs Live Sessions

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

Refresh Reset Repeat Counts Export To Filter

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

In order to verify which vulnerabilities were detected, navigate to Context Visibility > Endpoints. Check per endpoints Vulnerabilities with the Scores given to it by Qualys.



When selecting particular endpoint, more details about each Vulnerability appears, including **Title** and **CVEID's**.

The screenshot displays the Cisco Identity Services Engine (ISE) interface, showing detailed information for the endpoint C0:4A:00:14:8D:4B. The 'Vulnerabilities' tab is selected, showing a list of vulnerabilities. The first vulnerability is QID-90783, titled 'Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)'. The CVSS score is 9.3, and the CVEIDs are CVE-2012-0002 and CVE-2012-0152. The vulnerability was reported by Qualys. The second vulnerability is QID-38173, titled 'SSL Certificate - Signature Verification Failed Vulnerability'. The CVSS score is 9.4, and the CVEIDs are not listed. The vulnerability was reported by Qualys.

Endpoint Details:

- MAC Address: C0:4A:00:14:8D:4B
- Username: alice
- Endpoint Profile: Microsoft-Workstation
- Current IP Address: 10.62.148.63
- Location:

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

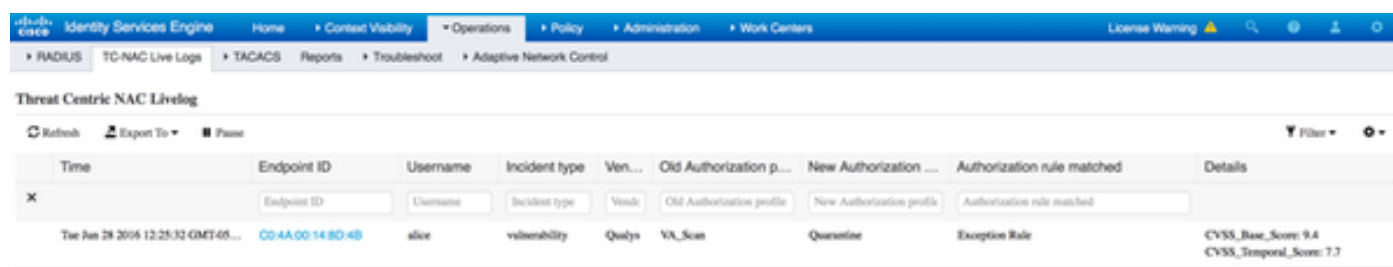
CVEIDS:

Reported by: Qualys

Reported at:

In Operations > TC-NAC Live Logs, you can see Old vs New authorization policies applied and details on CVSS_Base_Score.

Note: Authorization conditions are done based on CVSS_Base_Score, which equals to the highest Vulnerability Score detected on the endpoint.

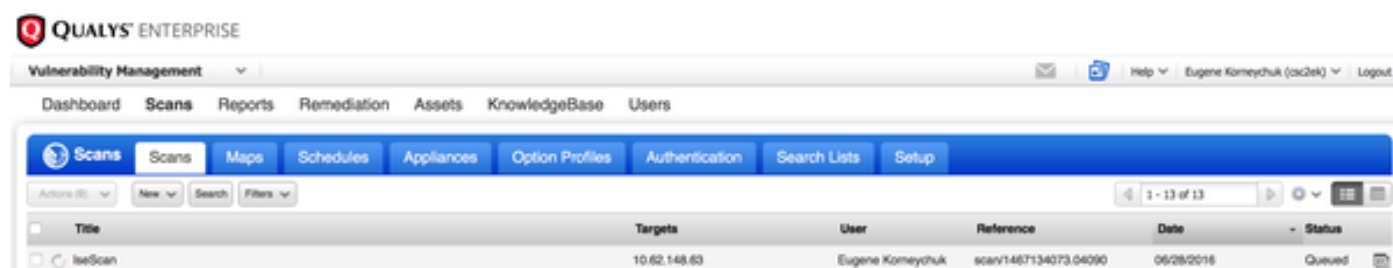


The screenshot shows the 'Threat Centric NAC LiveLog' interface. It features a table with columns: Time, Endpoint ID, Username, Incident type, Ven..., Old Authorization p..., New Authorization ..., Authorization rule matched, and Details. A single entry is visible for 'Tue Jan 28 2016 12:25:32 GMT+05:00' with endpoint 'CO-4A:00:14:8D:4B', username 'alice', incident type 'vulnerability', and source 'Qualys VA_Scan'. The details show 'CVSS_Base_Score: 9.4' and 'CVSS_Temporal_Score: 7.7'.

Time	Endpoint ID	Username	Incident type	Ven...	Old Authorization p...	New Authorization ...	Authorization rule matched	Details
Tue Jan 28 2016 12:25:32 GMT+05:00	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

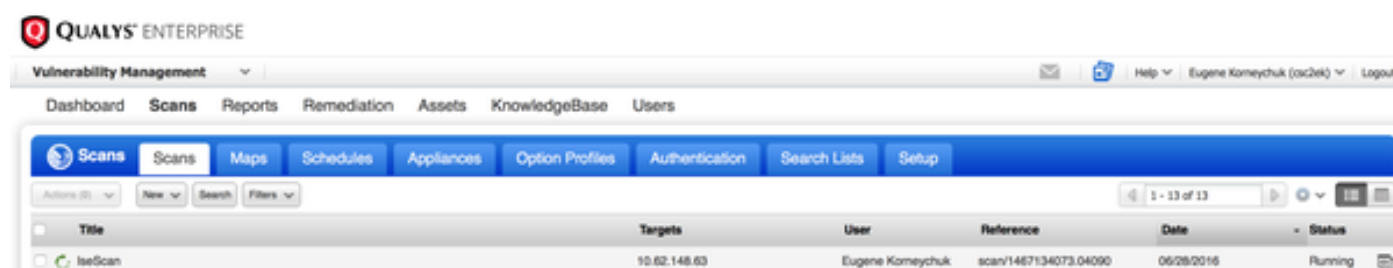
When the VA Scan is triggered by TC-NAC Qualys queues the Scan, it can be viewed at Scans > Scans



The screenshot shows the 'Qualys Enterprise' 'Vulnerability Management' interface. The 'Scans' tab is active, displaying a table with columns: Title, Targets, User, Reference, Date, and Status. A single scan titled 'IseScan' is shown with target '10.62.148.63', user 'Eugene Komeychuk', reference 'scan/1467134073.04090', date '06/28/2016', and status 'Queued'.

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

Afterwards it transitions to Running, meaning Qualys cloud has instructed the Qualys Scanner to perform actual scanning



The screenshot shows the 'Qualys Enterprise' 'Vulnerability Management' interface. The 'Scans' tab is active, displaying a table with columns: Title, Targets, User, Reference, Date, and Status. A single scan titled 'IseScan' is shown with target '10.62.148.63', user 'Eugene Komeychuk', reference 'scan/1467134073.04090', date '06/28/2016', and status 'Running'.

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

While the Scanner performs the Scan, you should see "Scanning..." sign in the top right corner of the Qualys Guard

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:

Press ENTER to access the menu.

Once the Scan is done it transitions to Finished state. You can view results at Scans > Scans, select required scan and click on **View Summary** or **View Results**.

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (7) New Search Filters 1 - 13 of 13

Title	Targets	User	Reference	Date	Status
<input checked="" type="checkbox"/> IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Finished
<input type="checkbox"/> IseScan	10.201.228.107	Eugene Komeychuk	scan/1467132757.03967	06/28/2016	Finished
<input type="checkbox"/> IseScan	10.201.228.102	Eugene Komeychuk	scan/1467131435.03855	06/28/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.89	Eugene Komeychuk	scan/1464895232.91271	06/02/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464855593.86436	06/02/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464850315.85548	06/02/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464847674.85321	06/02/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464841736.84337	06/02/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464836454.83651	06/02/2016	Finished

Preview

Vulnerability Scan - IseScan
Target: 1 IP(s)

Scan launched by Eugene Komeychuk (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	View Summary View Results
1	1	7	

In the Report itself you can see **Detailed Results**, where detected Vulnerabilities are shown.

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)

Troubleshoot

Debugs on ISE

In order to enable debugs on ISE navigate to Administration > System > Logging > Debug Log Configuration, select TC-NAC Node and change the **Log Level va-runtime** and **va-service** component to **DEBUG**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left includes options like Local Log Settings, Remote Logging Targets, Logging Categories, Message Catalog, Debug Log Configuration, and Collection Filters. The main content area is titled 'Node List > ISE21-3ek.example.com Debug Level Configuration'. It features a table with the following data:

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

Logs to be checked - varuntime.log. You can tail it directly from ISE CLI:

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

TC-NAC Docker received instruction to perform Scan for particular endpoint.

```
2016-06-28 19:06:30,823 DEBUG [Thread-70][] va.runtime.admin.mnt.EndpointFileReader -:::- VA:
Read va runtime.
[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","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: received data from Mnt:
{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScanE
nabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
```

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

Once the result is received it stores all Vulnerability data in the Context Directory.

```
2016-06-28 19:25:02,020 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaServiceMessageListener -:::- Got message from VaService:  
[{"macAddress": "C0:4A:00:14:8D:4B", "ipAddress": "10.62.148.63", "lastScanTime": 1467134394000, "vulnerabilities": [{"vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-0002, CVE-2012-0152", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "vulnerabilityTitle": "Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityTitle": "SSL Certificate - Signature Verification Failed Vulnerability", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "vulnerabilityTitle": "Windows Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB Signing Disabled or SMB Signing Not Required", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566, CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS use of weak RC4 cipher", "vulnerabilityVendor": "Qualys"}]]  
2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaServiceMessageListener -:::- VA: Save to context db,  
lastscantime: 1467134394000, mac: C0:4A:00:14:8D:4B  
2016-06-28 19:25:02,268 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaAdminServiceContext -:::- VA: sending elastic search json to pri-  
lan  
2016-06-28 19:25:02,272 DEBUG [pool-311-thread-8][  
va.runtime.admin.vaservice.VaPanRemotingHandler -:::- VA: Saved to elastic search:  
{C0:4A:00:14:8D:4B=[{"vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-0002, CVE-2012-0152", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "vulnerabilityTitle": "Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityTitle": "SSL Certificate - Signature Verification Failed Vulnerability", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "vulnerabilityTitle": "Windows Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB Signing Disabled or SMB Signing Not Required", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566, CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS use of weak RC4 cipher", "vulnerabilityVendor": "Qualys"}]]}
```

Logs to be checked - vaservice.log. You can tail it directly from ISE CLI:

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

Vulnerability Assessment Request Submitted to Adapter

```
2016-06-28 17:07:13,200 DEBUG [endpointPollerScheduler-3][ cpm.va.service.util.VaServiceUtil -  
:::- VA SendSyslog systemMsg :  
[{"systemMsg": "91019", "isAutoInsertSelfAcsInstance": true, "attributes": ["TC-NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA request submitted to adapter", "TC-NAC.Details", "VA request submitted to adapter for processing", "TC-
```

```
NAC.MACAddress", "C0:4A:00:14:8D:4B", "TC-NAC.IpAddress", "10.62.148.63", "TC-  
NAC.AdapterInstanceUuid", "796440b7-09b5-4f3b-b611-199fb81a4b99", "TC-  
NAC.VendorName", "Qualys", "TC-NAC.AdapterInstanceName", "QUALYS_VA"]}]}
```

AdapterManagerListener checks each 5 minutes the status of the scan, until it is finished.

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

Adapter is gets QID's, CVE's along with the CVSS Scores

```
2016-06-28 17:24:57,556 DEBUG [SimpleAsyncTaskExecutor-2][  
cpm.va.service.processor.AdapterMessageListener -:::- Message from adapter :  
{ "requestedMacAddress": "C0:4A:00:14:8D:4B", "scanStatus": "ASSESSMENT_SUCCESS", "lastScanTimeLong":  
1467134394000, "ipAddress": "10.62.148.63", "vulnerabilities": [{"vulnerabilityId": "QID-  
38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityTitle": "SSL  
Certificate - Signature Verification Failed  
Vulnerability", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-  
90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB  
Signing Disabled or SMB Signing Not  
Required", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-  
0002,CVE-2012-  
0152", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "vulnerabilityTitle": "Microsoft Windows  
Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-  
020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-  
2566,CVE-2015-  
2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS use of weak  
RC4 cipher", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-  
90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "vulnerabilityTitle": "Windows  
Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": "Qualys"}]}  
2016-06-28 17:25:01,282 INFO [SimpleAsyncTaskExecutor-2][  
cpm.va.service.processor.AdapterMessageListener -:::- Endpoint Details sent to IRF is  
{ "C0:4A:00:14:8D:4B": [{"vulnerability": {"CVSS_Base_Score": 9.4, "CVSS_Temporal_Score": 7.7}, "time-  
stamp": 1467134394000, "title": "Vulnerability", "vendor": "Qualys"}]}  
2016-06-28 17:25:01,853 DEBUG [endpointPollerScheduler-2][ cpm.va.service.util.VaServiceUtil -  
:::- VA SendSyslog systemMsg :  
[{"systemMsg": "91019", "isAutoInsertSelfAcsInstance": true, "attributes": ["TC-  
NAC.ServiceName", "Vulnerability Assessment Service", "TC-NAC.Status", "VA successfully  
completed", "TC-NAC.Details", "VA completed; number of vulnerabilities found: 5", "TC-  
NAC.MACAddress", "C0:4A:00:14:8D:4B", "TC-NAC.IpAddress", "10.62.148.63", "TC-  
NAC.AdapterInstanceUuid", "796440b7-09b5-4f3b-b611-199fb81a4b99", "TC-
```

```
NAC.VendorName", "Qualys", "TC-NAC.AdapterInstanceName", "QUALYS_VA"]}]}
```

Typical Issues

Issue 1. ISE gets Vulnerability Report with CVSS_Base_Score of 0.0 and CVSS_Temporal_Score of 0.0, while Qualys Cloud report contains Vulnerabilities detected.

Problem:

While checking the Report from Qualys Cloud you can see detected Vulnerabilities, however on ISE you do not see them.

Debugs seen 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": [{ "vulnerability": { "CVSS_Base_Score": 0.0, "CVSS_Temporal_Score": 0.0 }, "time-  
stamp": 1464855905000, "title": "Vulnerability", "vendor": "Qualys" } ] }
```

Solution:

The reason for cvss score being zero is either that it has no vulnerabilities or the cvss scoring was not enabled in Qualys Cloud before you configure the adapter through UI. Knowledgebase containing cvss scoring feature enabled is downloaded after the adapter is configured first time. You have to ensure that CVSS Scoring was enabled before, adapter instance was created on ISE. It can be done under Vulnerability Management > Reports > Setup > CVSS > Enable CVSS Scoring

Issue 2. ISE does not get results back from the Qualys Cloud, even though correct Authorization Policy was hit.

Problem:

Corrected Authorization Policy was matched, which should trigger VA Scan. Despite that fact no scan is done.

Debugs seen in vaservice.log:

```
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][  
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :  
(Body: '[B@6da5e620(byte[311])' MessageProperties [headers={}, timestamp=null, messageId=null,  
userId=null, appId=null, clusterId=null, type=null, correlationId=null, replyTo=null,  
contentType=application/octet-stream, contentEncoding=null, contentLength=0,  
deliveryMode=PERSISTENT, expiration=null, priority=0, redelivered=false,  
receivedExchange=irf.topic.va-reports, receivedRoutingKey=, deliveryTag=9830, messageCount=0])  
2016-06-28 16:19:15,401 DEBUG [SimpleAsyncTaskExecutor-2][  
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :  
{ "requestedMacAddress": "24:77:03:3D:CF:20", "scanStatus": "SCAN_ERROR", "scanStatusMessage": "Error  
triggering scan: Error while triggering on-demand scan code and error as follows 1904: none of  
the specified IPs are eligible for Vulnerability Management  
scanning.", "lastScanTimeLong": 0, "ipAddress": "10.201.228.102" }  
2016-06-28 16:19:15,771 DEBUG [SimpleAsyncTaskExecutor-2][  
cpm.va.service.processor.AdapterMessageListener -:::::- Adapter scan result failed for  
Macaddress:24:77:03:3D:CF:20, IP Address(DB): 10.201.228.102, setting status to failed  
2016-06-28 16:19:16,336 DEBUG [endpointPollerScheduler-2][ cpm.va.service.util.VaServiceUtil -  
:::::- VA SendSyslog systemMsg :  
[{"systemMsg": "91008", "isAutoInsertSelfAcsInstance": true, "attributes": [{"TC-
```

```
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA Failure","TC-  
NAC.Details","Error triggering scan: Error while triggering on-demand scan code and error as  
follows 1904: none of the specified IPs are eligible for Vulnerability Management  
scanning.", "TC-NAC.MACAddress", "24:77:03:3D:CF:20", "TC-NAC.IpAddress", "10.201.228.102", "TC-  
NAC.AdapterInstanceUuid", "796440b7-09b5-4f3b-b611-199fb81a4b99", "TC-  
NAC.VendorName", "Qualys", "TC-NAC.AdapterInstanceName", "QUALYS_VA"]}]
```

Solution:

Qualys Cloud indicates that ip address of the endpoint is not eligible for the Scanning, please ensure you have added ip address of the endpoint to Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts

References

- [Cisco Identity Services Engine Administrator Guide, Release 2.1](#)
- [Technical Support & Documentation - Cisco Systems](#)
- [Video: ISE 2.1 with Qualys](#)
- [Qualys Documentation](#)