

Configure el NAC Amenaza-céntrico del 2.1 ISE (TC-NAC) con Qualys

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de flujo de alto nivel](#)

[Nube y escáner de Qualys de la configuración](#)

[Paso 1. Despliegue el escáner de Qualys](#)

[Paso 2. Escáner de Qualys de la configuración](#)

[Configuración ISE](#)

[Paso 1. Configuraciones de la nube de Qualys del ajuste para la integración con el ISE](#)

[Paso 2. Servicios del permiso TC-NAC](#)

[Paso 3. Conectividad del adaptador de Qualys de la configuración al marco ISE VA](#)

[Paso 4. Perfil de la autorización de la configuración para accionar la exploración VA](#)

[Paso 5. Directivas de la autorización de la configuración](#)

[Verificación](#)

[Identity Services Engine](#)

[Nube de Qualys](#)

[Troubleshooting](#)

[Debugs en el ISE](#)

[Problemas típicos](#)

[Referencias](#)

Introducción

Este documento describe cómo configurar el NAC Amenaza-céntrico con Qualys en el 2.1 del Identity Services Engine (ISE). La característica céntrica del Control de acceso a la red de la amenaza (TC-NAC) le permite para crear las directivas de la autorización basadas en los atributos de la amenaza y de la vulnerabilidad recibidos de los adaptadores de la amenaza y de la vulnerabilidad.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Motor del servicio de la identidad de Cisco
- Qualys ScanGuard

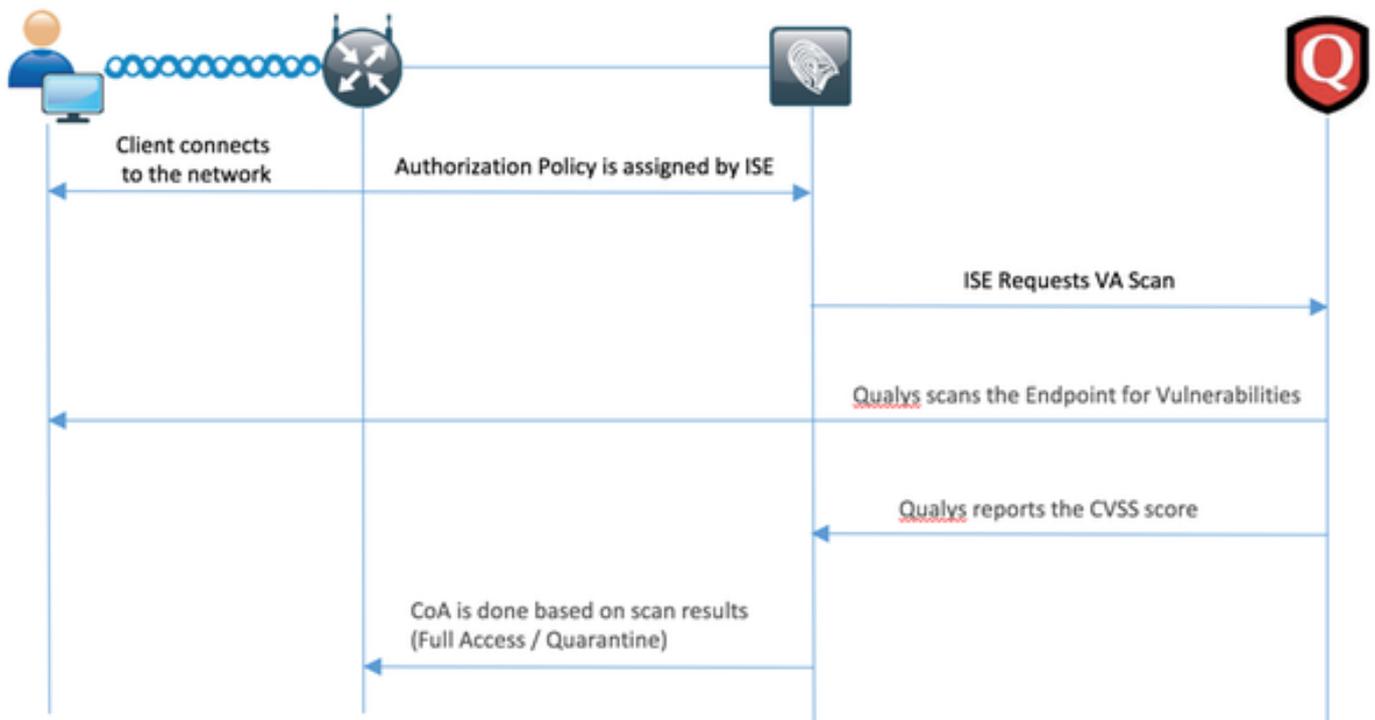
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.1 del motor del servicio de la identidad de Cisco
- Regulador del Wireless LAN (WLC) 8.0.121.0
- Escáner 8.3.36-1 del guardia de Qualys, firmas 2.3.364-2
- Service Pack 1 de Windows 7

Configurar

Diagrama de flujo de alto nivel



Éste es el flujo:

1. El cliente conecta con la red, se da el acceso limitado y el perfil con **evalúa las vulnerabilidades que el checkbox habilitado se asigna**
2. El nodo PSN envía el mensaje de Syslog a la autenticación que confirma del nodo MNT ocurrió y la exploración VA era el resultado de la directiva de la autorización
3. El nodo MNT somete la EXPLORACIÓN al nodo TC-NAC (usando Admin WebApp) usando estos datos:
 - Dirección MAC
 - Dirección IP
 - Intervalo de la exploración
 - Exploración periódica habilitada
 - Originar el PSN
4. Qualys TC-NAC (encapsulado en el envase del estibador) comunica con la nube de Qualys

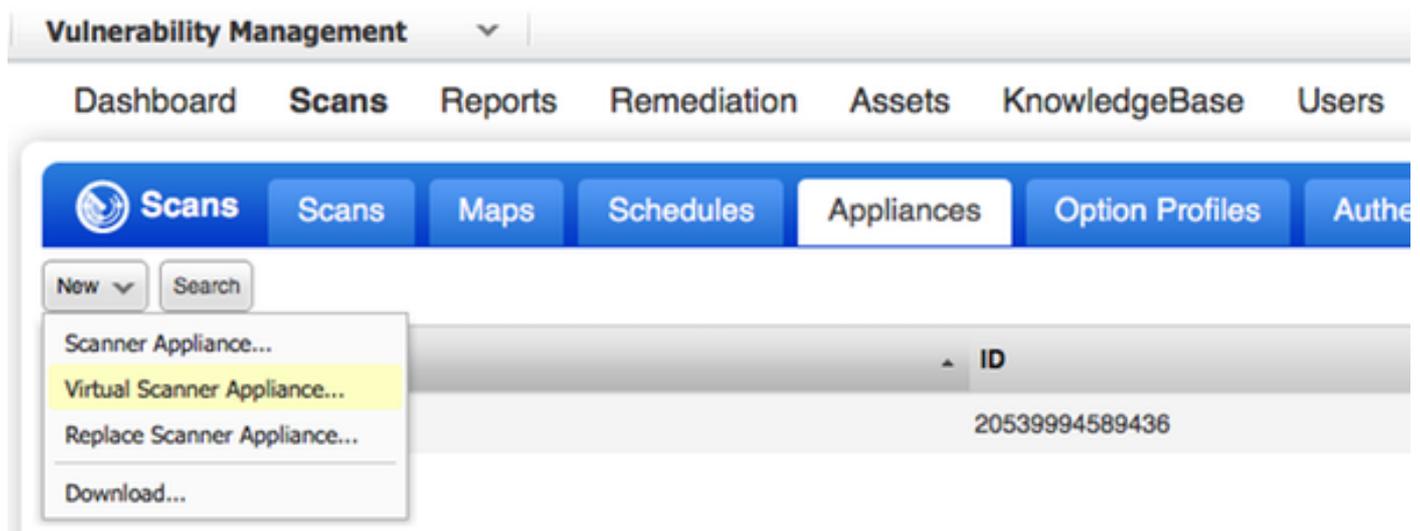
- (vía el RESTO API) para accionar la exploración si es necesario
5. La nube de Qualys da instrucciones al escáner de Qualys para analizar el punto final
 6. El escáner de Qualys envía los resultados de la exploración a la nube de Qualys
 7. Los resultados de la exploración se devuelven a TC-NAC:
 - Dirección MAC
 - Todas las calificaciones CVSS
 - Todas las vulnerabilidades (QID, título, CVEIDs)
 8. TC-NAC pone al día la CACEROLA con todos los datos del paso 7.
 9. El CoA se acciona si es necesario según la directiva de la autorización configurada.

Nube y escáner de Qualys de la configuración

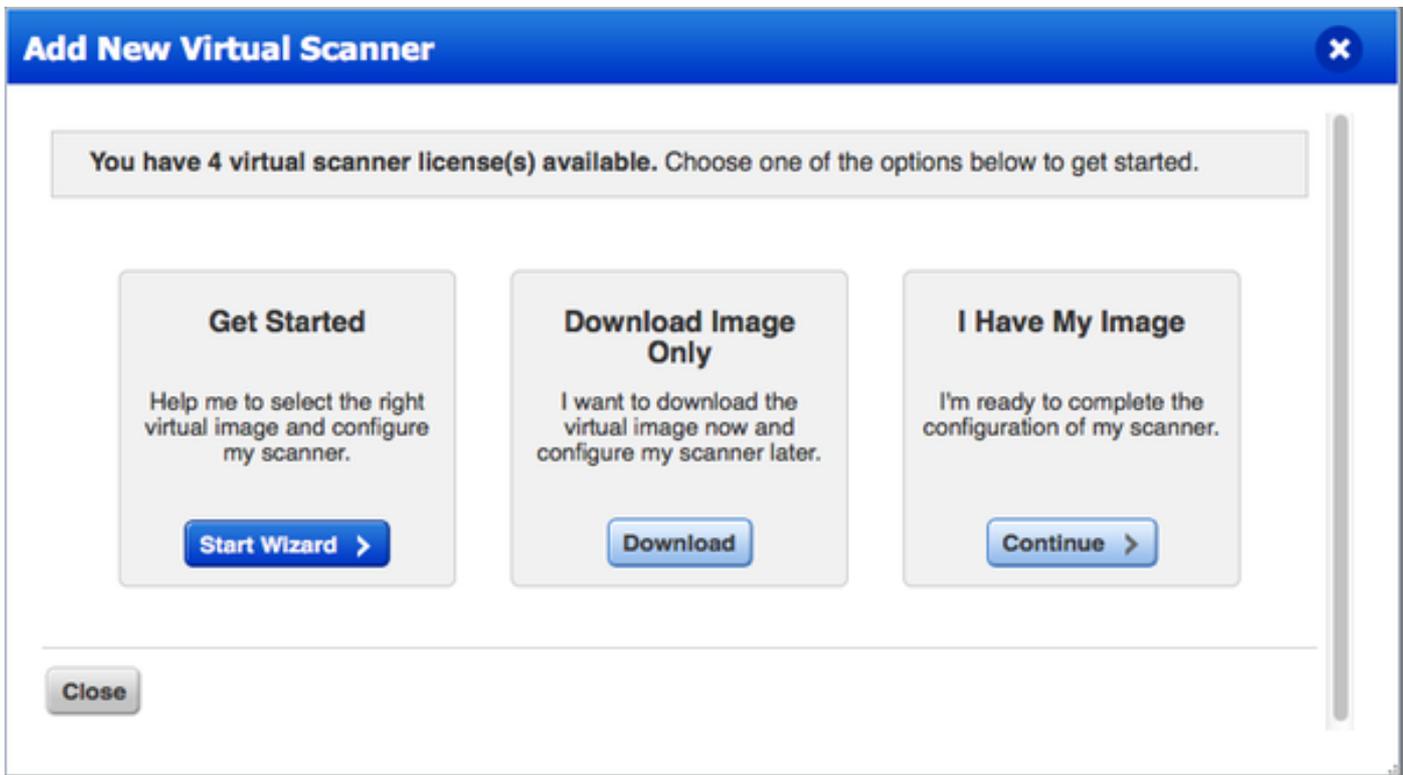
Caution: La configuración de Qualys en este documento se hace para los propósitos del laboratorio, consulta por favor con los ingenieros de Qualys para los aspectos del diseño

Paso 1. Despliegue el escáner de Qualys

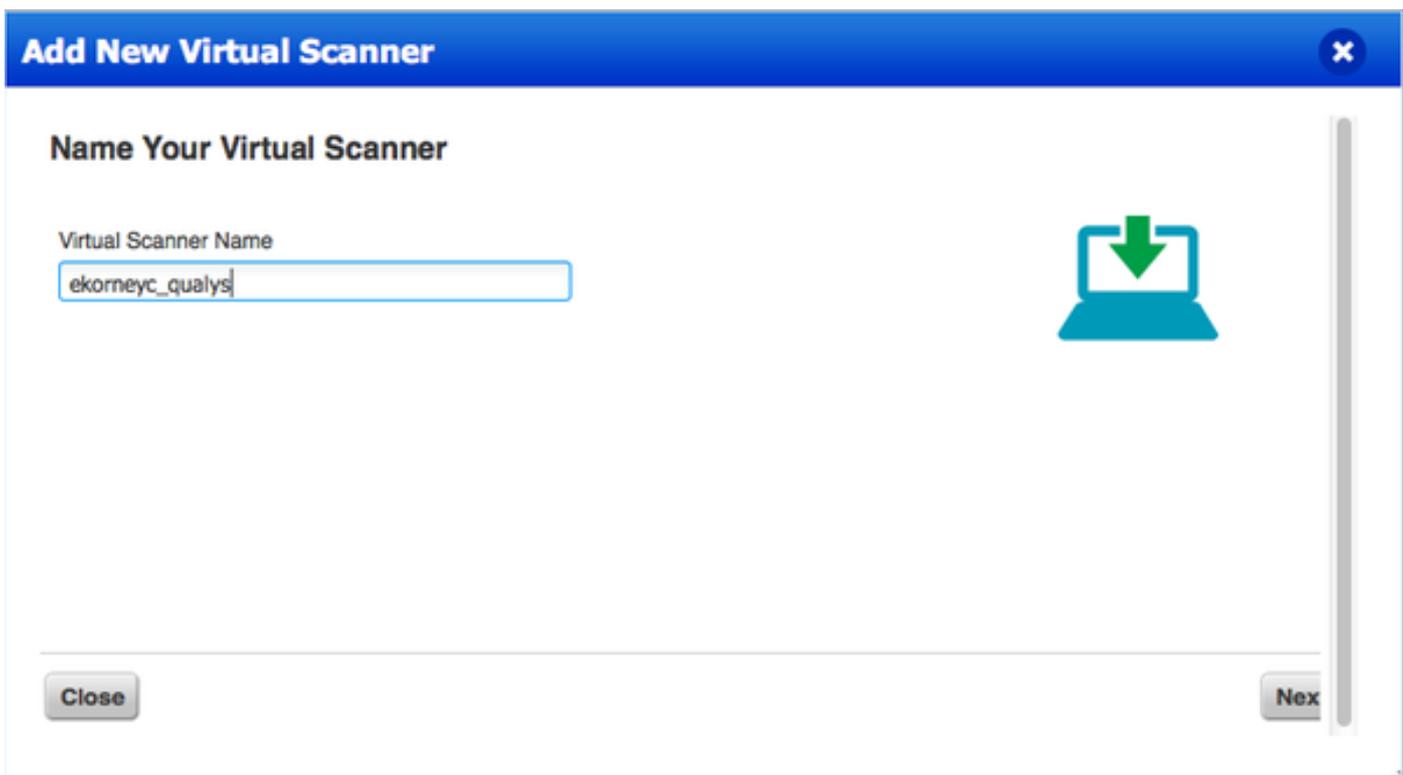
El escáner de Qualys se puede desplegar del archivo de los HUEVOS. Inicie sesión a la nube de Qualys y navegue a las exploraciones > a los dispositivos y seleccione el dispositivo nuevo > virtual del escáner



Seleccione la **imagen de la descarga solamente** y escoja la distribución apropiada



Para conseguirle a código de activación puede ir a las exploraciones > a los dispositivos y dispositivo nuevo > virtual selecto del escáner y seleccionar **me tengo mi imagen**



Después de ingresar el nombre del escáner le dan el código de autorización que usted utilizará más adelante.

Paso 2. Escáner de Qualys de la configuración

Despliegue los HUEVOS en la plataforma de la virtualización de su opción. Una vez que está hecho, configure esas configuraciones:

- Configure la red (el LAN)
- Configuraciones de la interfaz de WAN (si usted está utilizando dos interfaces)
- Configuraciones de representación (si usted está utilizando el proxy)
- Personalice este escáner



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.

El escáner conecta con Qualys y descarga luego el último software y las firmas.

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)

Para verificar el escáner le está conectado puede navegar a las exploraciones > a los dispositivos.

Ponga verde la muestra conectada a la izquierda indica que el escáner está listo, usted puede también ver el IP LAN, el IP de WAN, la versión del escáner y las firmas.



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

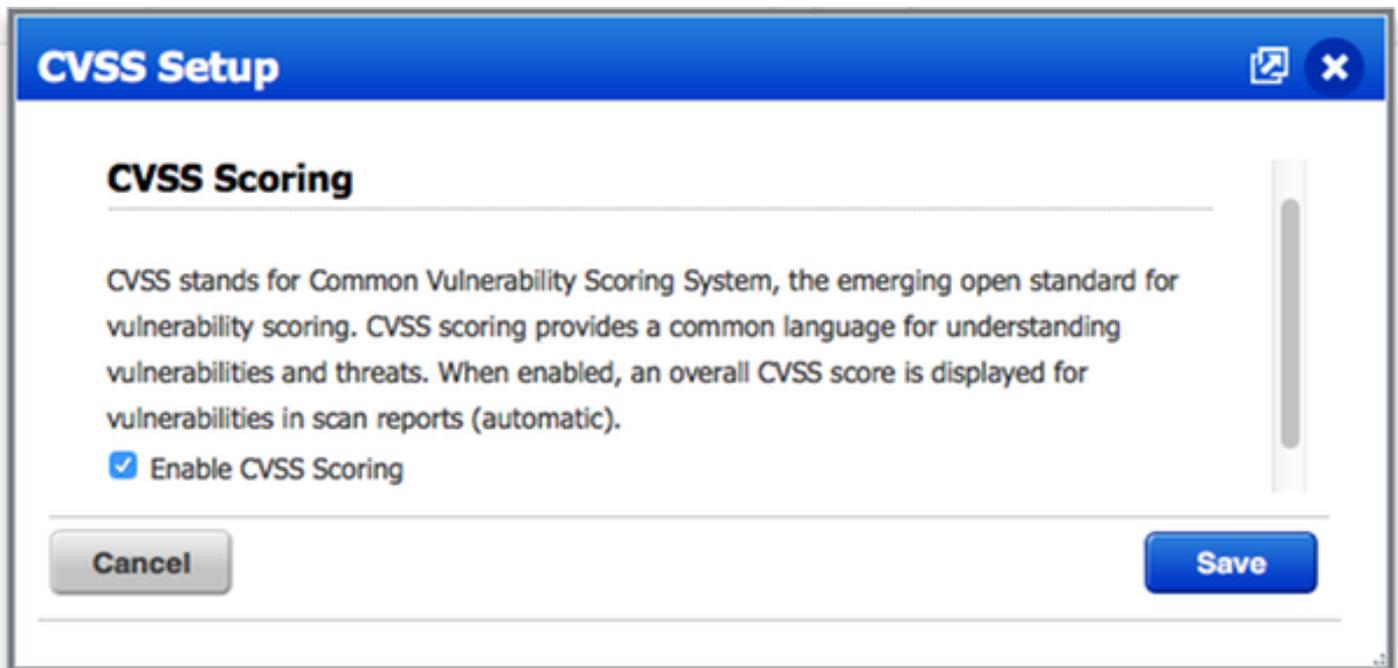
Appliance	ID	LAN IP	WAN IP	Polling	Scanner	Signatures	Last Update
 stoney_qualys	200000402008	10.62.145.82	10.62.145.82	180 seconds	8.3.36-1	2.3.384-2	06/11/2016 at 23:55:30 (GMT+0400)

Configure el ISE

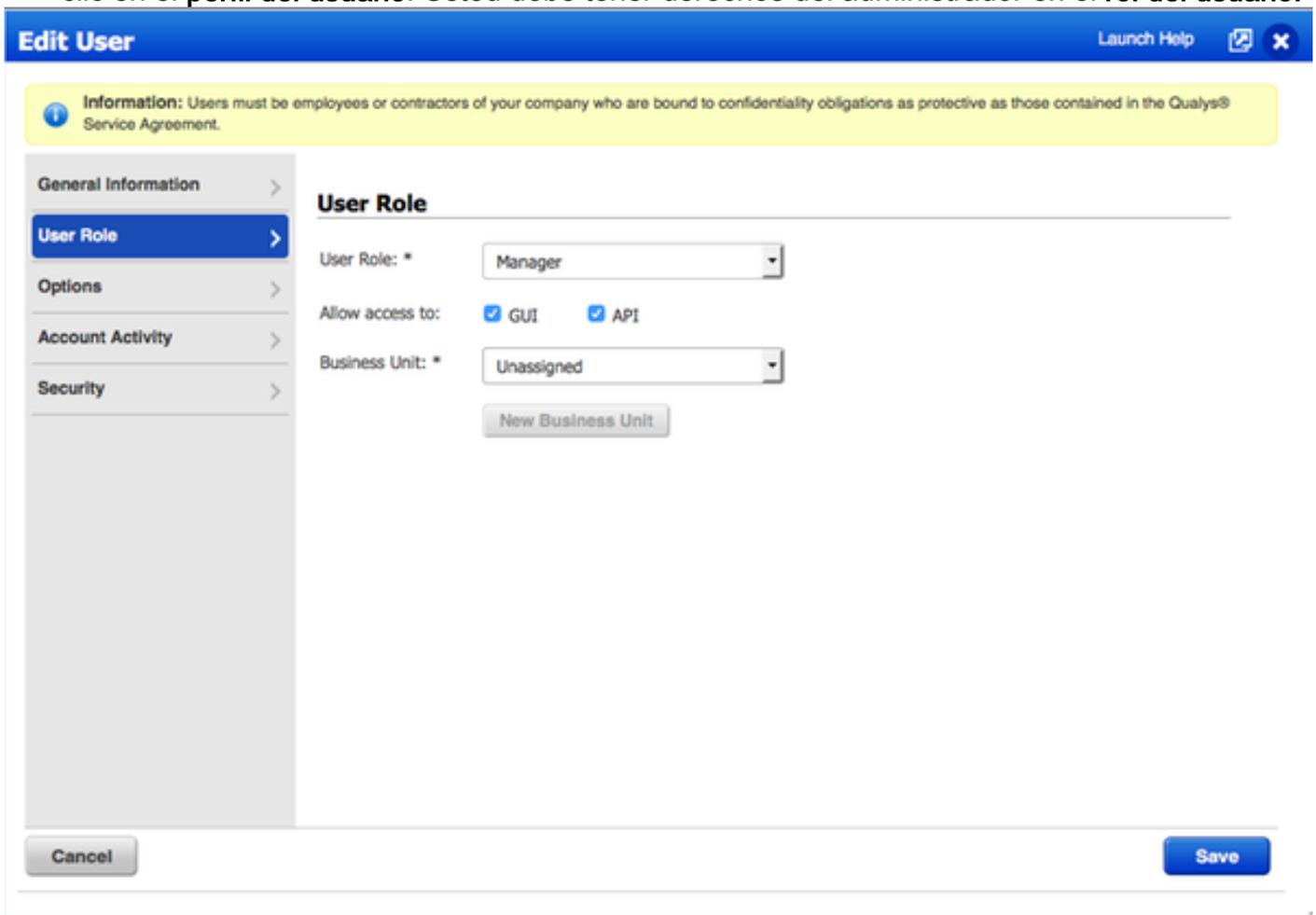
Aunque usted ha configurado el escáner y la nube de Qualys, usted todavía tiene que ajustar las configuraciones de la nube para asegurarse la integración con los trabajos ISE muy bien. Observe, él debe ser hecho antes de que usted configure el adaptador con el GUI, pues la base de conocimiento que contiene anotar CVSS se descarga después de que el adaptador se configure por primera vez.

Paso 1. Configuraciones de la nube de Qualys del ajuste para la integración con el ISE

- El permiso CVSS que anota en la administración de vulnerabilidades > señala > puesto > el anotar CVSS > del permiso CVSS



- Asegúrese de que los credenciales de usuario usados en configuración del adaptador tengan privilegios del administrador. Seleccione a su usuario de la esquina superior izquierda y haga clic en el **perfil del usuario**. Usted debe tener derechos del administrador en el **rol del usuario**.



- Asegúrese que esos IP Addresses/las subredes de los puntos finales que requieren la evaluación de vulnerabilidades estén agregados a Qualys en la administración de vulnerabilidades > los activos > los activos del host > nuevo > los host seguidos IP

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**

Paso 2. Servicios del permiso TC-NAC

Los servicios del permiso TC-NAC bajo la administración > despliegue > editan el nodo. Checkbox **céntrico del servicio del NAC de la amenaza del permiso** del control.

Note: Puede haber solamente un nodo TC-NAC por el despliegue.

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**

Monitoring Role **PRIMARY** Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group **None**

Enable Profiling Service

Enable Threat Centric NAC Service

Paso 3. Conectividad del adaptador de Qualys de la configuración al marco ISE VA

Navegue a la administración > al NAC > a los terceros proveedores céntricos de la amenaza > Add. Haga clic en la **salvaguardia**.

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 *

Cuando las transiciones del caso de Qualys a **alistar para configurar el estado**, hacen clic en **listo para configurar la** opción en el estatus.

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

El host del RESTO API debe ser el que usted utiliza para la nube de Qualys, donde se localiza su cuenta. En este ejemplo - qualysguard.qg2.apps.qualys.com

La cuenta debe ser la que está con los privilegios del administrador, hace clic en **después**.

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.

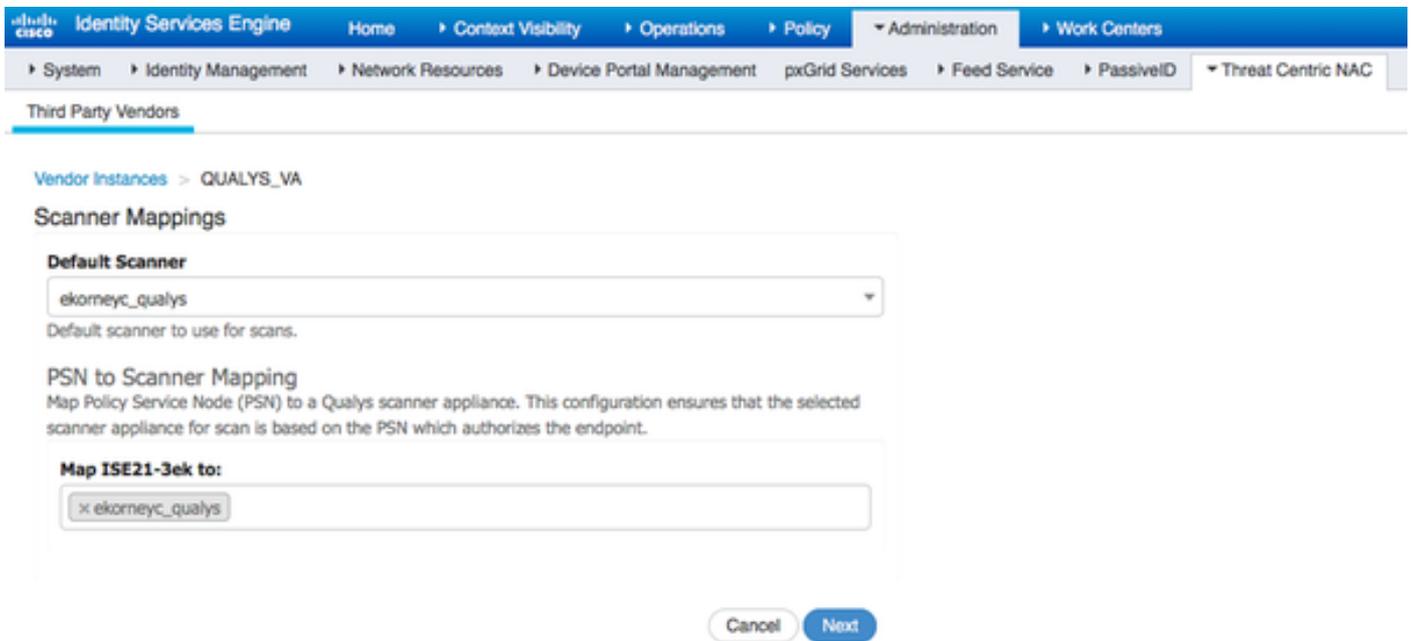
HTTP Proxy Host

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

HTTP Proxy Port

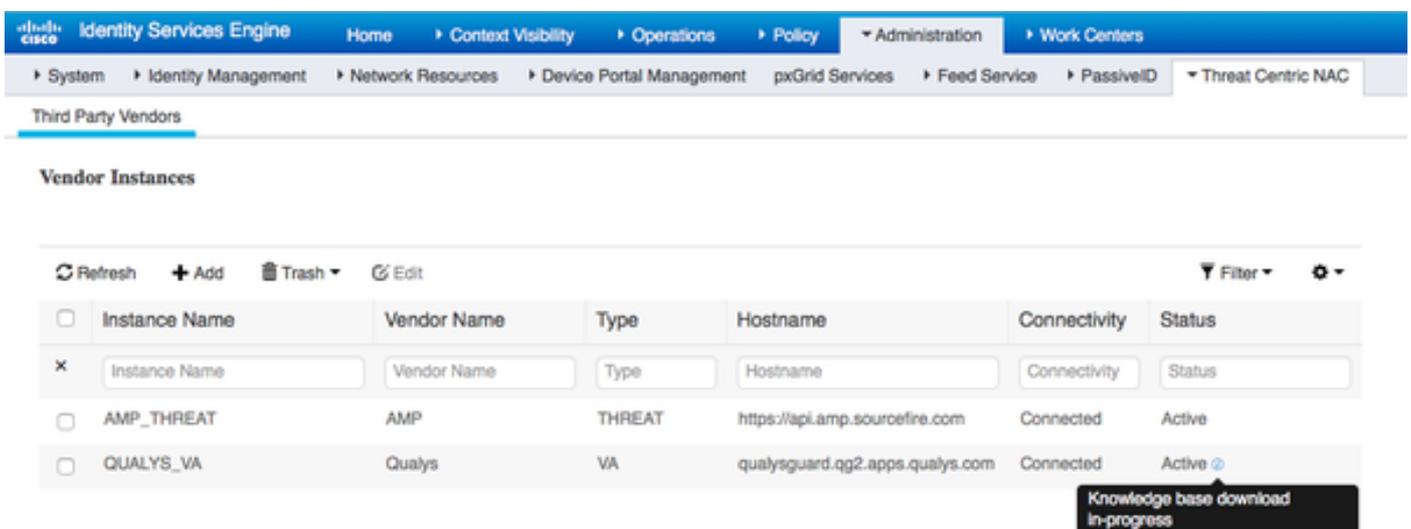
 Optional HTTP Proxy Port. Requires proxy host also to be set.

El ISE descarga la información sobre los escáneres que están conectados con la nube de Qualys, usted puede configurar el PSN a la asignación del escáner en esta página. Se asegura de que el escáner seleccionado esté escogido sobre la base del PSN que autoriza el punto final.



Las configuraciones avanzadas están bien documentadas en la guía Admin del 2.1 ISE, link se pueden encontrar en la sección de referencias de este documento. Haga clic en **después** y **acabe**. Transiciones del caso de Qualys al comienzo de la descarga del estado **activo** y del Knowledge Base.

Note: Puede haber solamente un caso de Qualys por el despliegue.



Paso 4. Perfil de la autorización de la configuración para accionar la exploración VA

Navigate a la directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización. Agregue el nuevo perfil. Bajo **tareas comunes** seleccione el checkbox de la **evaluación de vulnerabilidades**.

El intervalo a pedido de la exploración se debe seleccionar según su diseño de red.

El perfil de la autorización contiene esos AV-pares:

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

Se envían a los dispositivos de red dentro del paquete access-accept, aunque el propósito real de ellos sea decir el nodo MNT que la exploración debe ser accionada. El MNT da instrucciones el nodo TC-NAC para comunicar con la nube de Qualys.

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 left sidebar shows a tree view with 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The main content area is titled 'Authorization Profiles > New Authorization Profile'. The 'Authorization Profile' section includes the following fields: 'Name' (VA_Scan), 'Description' (empty), 'Access Type' (ACCESS_ACCEPT), 'Network Device Profile' (Cisco), 'Service Template' (unchecked), 'Track Movement' (unchecked), and 'Passive Identity Tracking' (unchecked). Below this is the 'Common Tasks' section, which is expanded to show 'Assess Vulnerabilities' (checked). Under 'Assess Vulnerabilities', there is an 'Adapter Instance' dropdown set to 'QUALYS_VA', a 'Trigger scan if the time since last scan is greater than' input field set to '48' (with a note 'Enter value in hours (1-9999)'), and an unchecked checkbox for 'Assess periodically using above interval'.

Paso 5. Directivas de la autorización de la configuración

- Configure la directiva de la autorización para utilizar el nuevo perfil de la autorización configurado en el paso 4. navegan a la directiva > a la autorización > a la directiva de la autorización, localizan la regla de **Basic_Authenticated_Access** y hacen clic en **editan**. Cambie los permisos de **PermitAccess** al **VA_Scan estándar** creado recientemente. Esto causa una exploración de la vulnerabilidad para todos los usuarios. Haga clic en la **salvaguardia**.
- Cree la directiva de la autorización para las máquinas Quarantined. Navegue a la directiva > a la autorización > a la directiva > a las excepciones de la autorización y cree una **regla de excepciones**. Haga clic en las condiciones > crean la nueva condición (opción avanzada) > atributo selecto, navegan hacia abajo y seleccionan la **amenaza**. Amplíe el atributo de la **amenaza** y seleccione **Qualys-CVSS_Base_Score**. Cambie al operador a **mayor que** y ingrese un valor según su política de seguridad. El perfil de la autorización de la **cuarentena** debe dar el acceso limitado a la máquina vulnerable.

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

Verificación

Identity Services Engine

La primera exploración VA de los activadores de la conexión. Cuando se acaba la exploración, el Reauthentication CoA se acciona para aplicar la nueva directiva si se corresponde con.

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

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

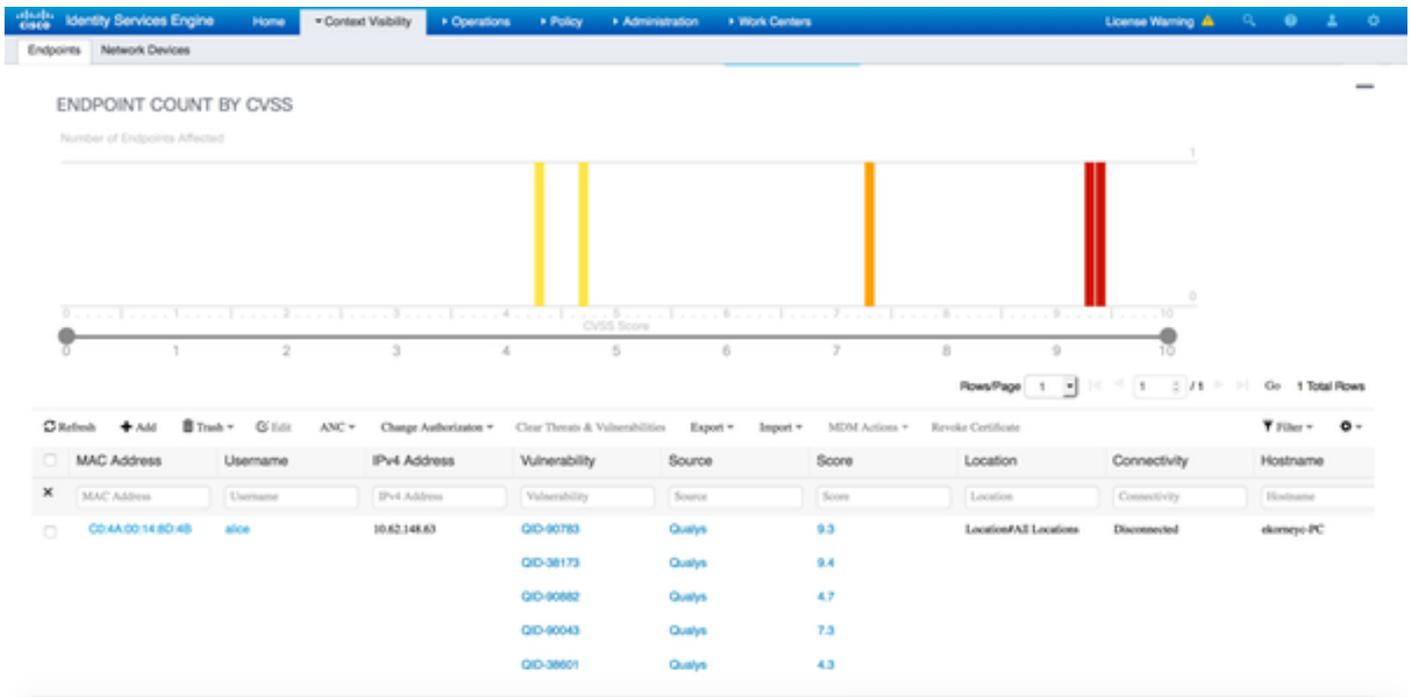
Live Logs Live Sessions

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

Refresh Reset Repeat Counts Export To Filter

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

Para verificar qué vulnerabilidades fueron detectadas, navegue a la visibilidad del contexto > a los puntos finales. Marque por las vulnerabilidades de los puntos finales con las calificaciones dadas a él por Qualys.



Al seleccionar el punto final específico, más detalles sobre cada vulnerabilidad aparecen, incluyendo el título y CVEID.

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 the following details for QID-90783:

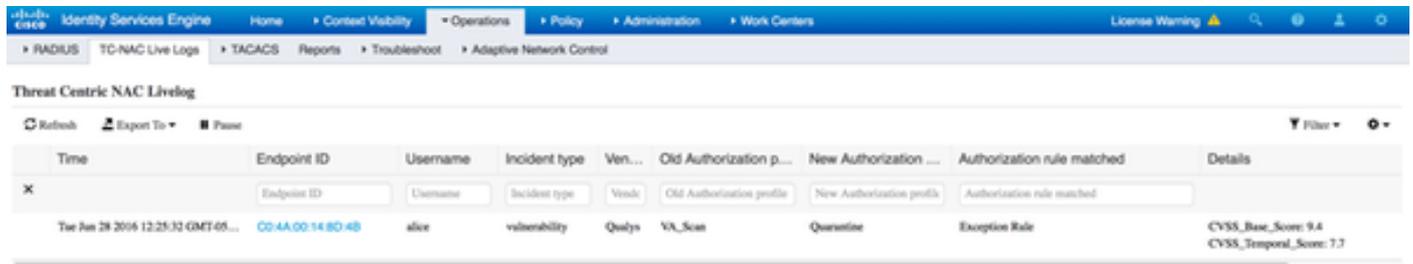
- Title:** Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- CVSS score:** 9.3
- CVEIDS:** CVE-2012-0002, CVE-2012-0152,
- Reported by:** Qualys
- Reported at:**

The following details are shown for QID-38173:

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

En las operaciones > TC-NAC viven los registros, usted puede ver viejo contra las nuevas directivas de la autorización aplicadas y los detalles en CVSS_Base_Score.

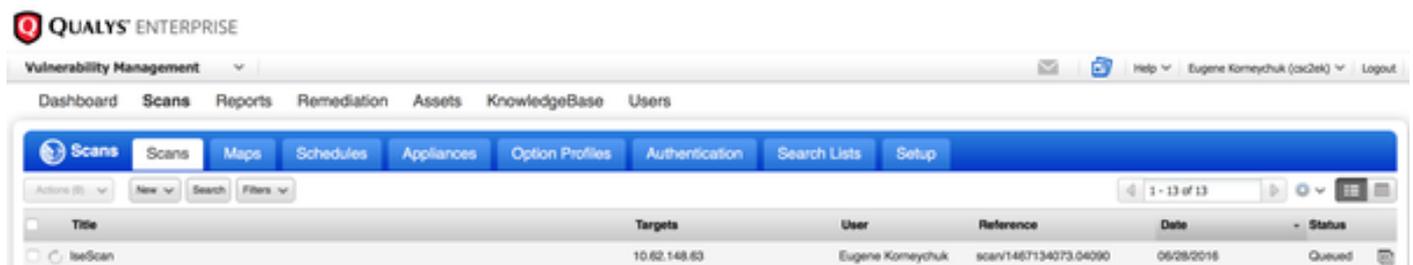
Note: Las condiciones de la autorización se hacen sobre la base de CVSS_Base_Score, que los iguales a la calificación más alta de la vulnerabilidad detectaron en el punto final.



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

Nube de Qualys

Cuando la exploración VA es accionada por TC-NAC Qualys hace cola la exploración, él puede ser visto en las exploraciones > las exploraciones



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

Luego las transiciones a ejecutarse, significando la nube de Qualys ha dado instrucciones el escáner de Qualys para realizar la exploración real



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

Mientras que el escáner realiza la exploración, usted debe ver la “exploración...” muestra en la esquina superior derecha del guardia de Qualys

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

La exploración se hace una vez la las transiciones al estado acabado. Usted puede ver los resultados en las exploraciones > las exploraciones, exploración requerida selecta y hacer clic en el **resumen de la visión** o los **resultados de la visión**.

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/1464855583.86436	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 (ec2ek) | 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: 1 Total appliances used: 1 Aggregate Vulnerabilities: 7

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

En el informe sí mismo usted puede ver los **resultados detallados**, donde se muestran las vulnerabilidades detectadas.

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

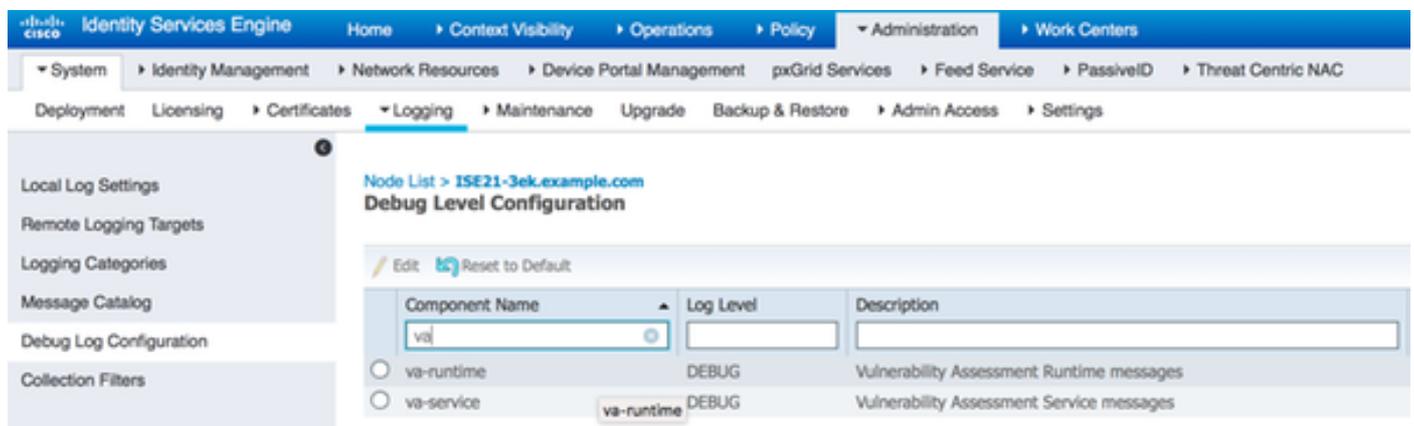
Potential Vulnerabilities (1)

Information Gathered (26)

Troubleshooting

Debugs en el ISE

Para habilitar los debugs en el ISE navegue a la administración > al sistema > a la configuración del registro del registro > del debug, nodo selecto TC-NAC y cambie el va-**Runtime del nivel del registro** y el componente del va-**servicio PARA HACER EL DEBUG DE**



Registros que se marcarán - varuntime.log. Usted puede atarlo directamente de ISE CLI:

Cola de varuntime.log de la aplicación del registro de la demostración ISE21-3ek/admin#

Instrucción recibida estibador TC-NAC de realizar la exploración para el punto final específico.

```
2016-06-28 DEBUG [Thread-70][ ] va.runtime.admin.mnt.EndpointFileReader de 19:06:30,823 -::: :-
VA: Lea el tiempo de ejecución va.
[{"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 DEBUG [Thread-70][ ] va.runtime.admin.vaservice.VaServiceRemotingHandler de
19:06:30,824 -::: :- VA: datos recibidos del 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}
```

Una vez que se recibe el resultado salva todos los datos de la vulnerabilidad en el directorio del contexto.

```
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaServiceMessageListener de
19:25:02,020 -::: :- mensaje conseguido de VaService: Vulnerabilidad remota de la ejecución de
códigos del protocolo del Escritorio Remoto de Windows del
[{"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 (certificado del MS12-020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityTitle": "SSL - firma fallada del Allowed", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB del método de encriptación vulnerable del protocolo del Escritorio Remoto del Vulnerability", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "vulnerabilityTitle": "Windows de la verificación de firma inhabilitada o SMB que firma no el uso del Required", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566,CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS de la cifra débil RC4", "vulnerabilityVendor": "Qualys"}]]
```

```
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaServiceMessageListener de
19:25:02,127 -::: :- VA: Salve al DB del contexto, lastscantime: 1467134394000, mac:
C0:4A:00:14:8D:4B
```

```
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaAdminServiceContext de
19:25:02,268 -::: :- VA: envío del json elástico de la búsqueda al PRI-LAN
```

```
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaPanRemotingHandler de
19:25:02,272 -::: :- VA: Guardado a la búsqueda elástico: Vulnerabilidad remota de la ejecución
de códigos del protocolo del Escritorio Remoto de Windows del
{C0:4A:00:14:8D:4B=[{"vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-0002,CVE-2012-0152", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "vulnerabilityTitle": "Microsoft (MS12-020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityTitle": "SSL - vulnerabilidad fallada de la verificación de firma", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "vulnerabilityTitle": "Windows permitido", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB inhabilitada o SMB que firma no requerido", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566,CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS de la cifra débil RC4", "vulnerabilityVendor": "Qualys"}]]
```

Registros que se marcarán - vaservice.log. Usted puede atarlo directamente de ISE CLI:

Cola de vaservice.log de la aplicación del registro de la demostración ISE21-3ek/admin#

Petición de la evaluación de vulnerabilidades sometida al adaptador

```
2016-06-28 DEBUG [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil de 17:07:13,200
-::: :- systemMsg VA SendSyslog: Servicio de la evaluación
[{"systemMsg": "91019", "isAutoInsertSelfAcsInstance": true, "attributes": [{"TC-NAC.ServiceName", "Vulnerability", "TC-NAC.Status", "petición VA sometida al adaptador", "TC-NAC.Details", "petición VA sometida al adaptador para el processing", "TC-
```

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

AdapterMessageListener marca cada 5 anota el estatus de la exploración, hasta que se acabe.

```
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:09:43,459 -::: :- mensaje del adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number de los puntos finales hechos
cola para marcar los resultados de exploración: 1, número de puntos finales hechos cola para la
exploración: 0, el número de puntos finales para los cuales la exploración está en curso: 0"}
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:14:43,760 -::: :- mensaje del adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number de los puntos finales hechos
cola para marcar los resultados de exploración: 0, número de puntos finales hechos cola para la
exploración: 0, el número de puntos finales para los cuales la exploración está en curso: 1"}
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:19:43,837 -::: :- mensaje del adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number de los puntos finales hechos
cola para marcar los resultados de exploración: 0, número de puntos finales hechos cola para la
exploración: 0, el número de puntos finales para los cuales la exploración está en curso: 1"}
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:24:43,867 -::: :- mensaje del adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number de los puntos finales hechos
cola para marcar los resultados de exploración: 0, número de puntos finales hechos cola para la
exploración: 0, el número de puntos finales para los cuales la exploración está en curso: 1"}
```

El adaptador es consigue QID, los CVE junto con las calificaciones CVSS

```
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:24:57,556 -::: :- mensaje del adaptador: Certificado del
{"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 -
Firma fallada del Vulnerability", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90043", "cveIds":"","cvssBaseScore":"7.3", "cvssTemporalScore":"6.3", "vulnerabilityTitle":"SMB de
la verificación de firma inhabilitada o SMB que firma no la vulnerabilidad remota de la
ejecución de códigos del protocolo del Escritorio Remoto de Windows del
Required", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-90783", "cveIds":"CVE-2012-
0002,CVE-2012-
0152", "cvssBaseScore":"9.3", "cvssTemporalScore":"7.7", "vulnerabilityTitle":"Microsoft (uso del
MS12-020)", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-38601", "cveIds":"CVE-2013-
2566,CVE-2015-
2808", "cvssBaseScore":"4.3", "cvssTemporalScore":"3.7", "vulnerabilityTitle":"SSL/TLS del método
de encriptación vulnerable débil del protocolo del Escritorio Remoto del
cipher", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90882", "cveIds":"","cvssBaseScore":"4.7", "cvssTemporalScore":"4", "vulnerabilityTitle":"Windows
RC4 permitido", "vulnerabilityVendor":"Qualys"}]}
2016-06-28 INFORMACIÓN [SimpleAsyncTaskExecutor-
2][] cpm.va.service.processor.AdapterMessageListener de 17:25:01,282 -::: :- los detalles del
punto final enviados al IRF son
{"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 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil de 17:25:01,853
-::: :- systemMsg VA SendSyslog: Servicio de la evaluación
[{"systemMsg":"91019", "isAutoInsertSelfAcsInstance":true, "attributes":["TC-
NAC.ServiceName", "Vulnerability", "TC-NAC.Status", "VA completado con éxito", "TC-NAC.Details",
"VA completado; número de vulnerabilidades encontradas: 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" ]}]
```

Problemas típicos

El problema 1. ISE consigue el informe sobre vulnerabilidades con CVSS_Base_Score de 0.0 y CVSS_Temporal_Score de 0.0, mientras que el informe de la nube de Qualys contiene las vulnerabilidades detectadas.

Problema:

Mientras que marcar el informe de la nube de Qualys que usted puede ver detectó las vulnerabilidades, no obstante en el ISE usted no las ve.

Debugs vistos en vaservice.log:

```
2016-06-02 INFORMACIÓN [SimpleAsyncTaskExecutor-
2][[] cpm.va.service.processor.AdapterMessageListener de 08:30:10,323 -::: :- los detalles del
punto final enviados al IRF son
{"C0:4A:00:15:75:C8": [{"vulnerability": {"CVSS_Base_Score": 0.0, "CVSS_Temporal_Score": 0.0}, "time-
stamp": 1464855905000, "title": "Vulnerability", "vendor": "Qualys"}]}
```

Solución:

La razón de la calificación de los cvss que es cero es cualquiera que no tiene ninguna vulnerabilidad o el anotar de los cvss no fue habilitado en la nube de Qualys antes de que usted configure el adaptador con el UI. La base de conocimiento que contiene los cvss que anotan la característica habilitada se descarga después de que el adaptador se configure primera vez. Usted tiene que asegurarse de que el anotar CVSS fuera habilitado antes, caso del adaptador fue creado en el ISE. Puede ser hecho bajo la administración de vulnerabilidades > informes > puesto > el anotar CVSS > del permiso CVSS

El problema 2. ISE no consigue los resultados posteriores de la nube de Qualys, aunque la directiva correcta de la autorización fue golpeada.

Problema:

La directiva corregida de la autorización fue correspondida con, que debe accionar la exploración VA. A pesar de ese hecho no se hace ninguna exploración.

Debugs vistos en vaservice.log:

```
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][[] cpm.va.service.processor.AdapterMessageListener
de 16:19:15,401 -::: :- mensaje del adaptador: (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 DEBUG [SimpleAsyncTaskExecutor-2][[] cpm.va.service.processor.AdapterMessageListener
de 16:19:15,401 -::: :- mensaje del adaptador:
{"requestedMacAddress": "24:77:03:3D:CF:20", "scanStatus": "SCAN_ERROR", "scanStatusMessage": "Error
que acciona la exploración: Error mientras que código de exploración y error de la triggeringon-
demanda como sigue 1904: ningunos de los IP especificados son elegibles para la administración
de vulnerabilidades scanning.", "lastScanTimeLong": 0, "ipAddress": "10.201.228.102"}
```

```
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][[] cpm.va.service.processor.AdapterMessageListener
```

```
de 16:19:15,771 -::: :- el resultado de exploración del adaptador falló para
Macaddress:24:77:03:3D:CF:20, IP Address(DB): 10.201.228.102, fijando el estatus a fallado
2016-06-28 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil de 16:19:16,336
-::: :- systemMsg VA SendSyslog: Servicio de la evaluación
[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability", "TC-NAC.Status", "error VA", "TC-NAC.Details", "error que
acciona la exploración: Error mientras que código de exploración y error a pedido triggering como
sigue 1904: ningunos de los IP especificados son elegibles para el 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"]}]] de la administración de
vulnerabilidades
```

Solución:

La nube de Qualys indica que el IP Address del punto final no es elegible para la exploración, se asegura por favor que usted haya agregado el IP Address del punto final a la administración de vulnerabilidades > a los activos > a los activos del host > nuevo > los host seguidos IP

Referencias

- [Guía del administrador del Cisco Identity Services Engine, 2.1 de la versión](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Vídeo: 2.1 ISE con Qualys](#)
- [Documentación de Qualys](#)