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

Contenido

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

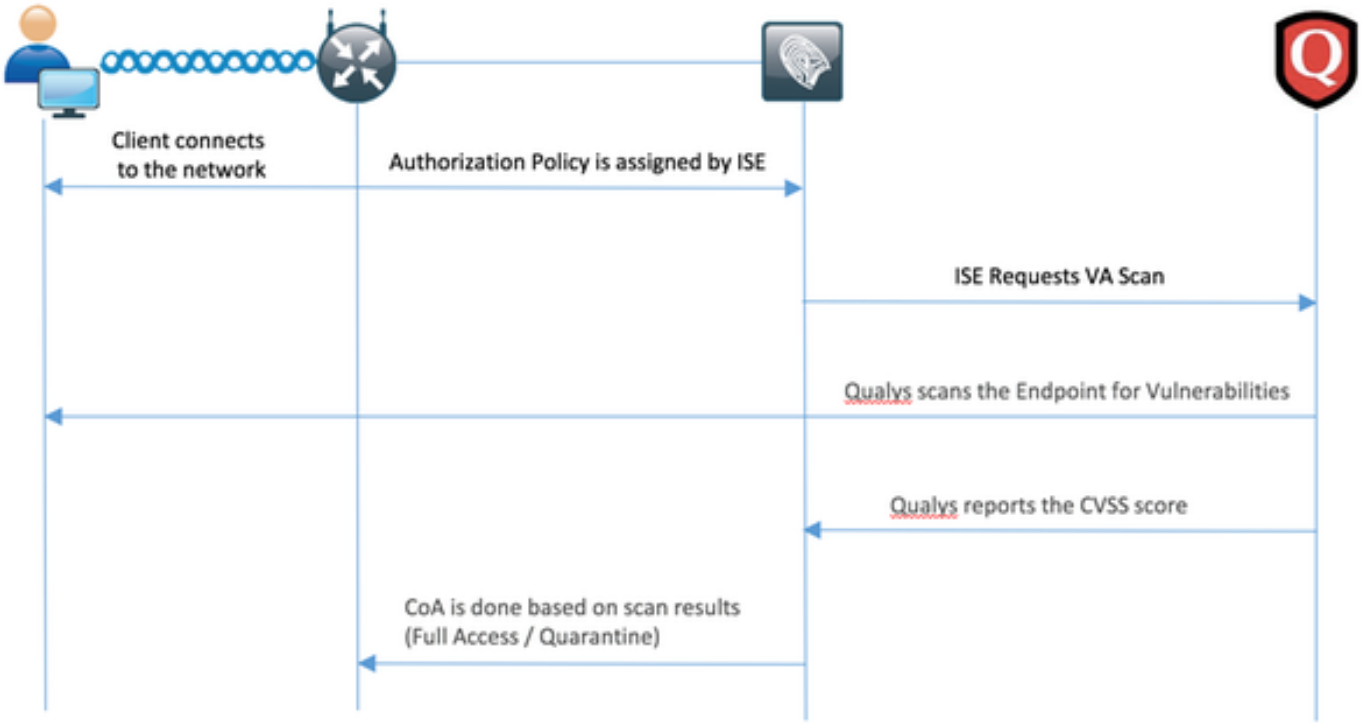
Componentes Utilizados

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

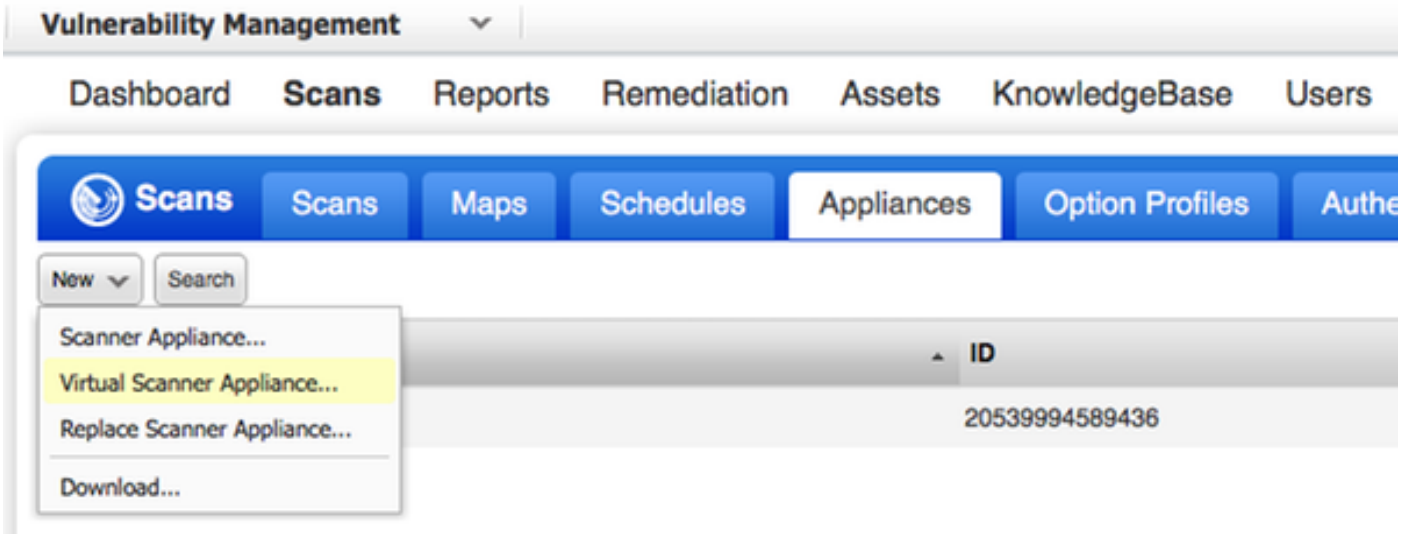
(vía el RESTO API) para accionar la exploración si es necesario
5. La nube de Qualys da instrucciones el escáner de Qualys para analizar el punto final
6. El escáner de Qualys envía los resultados de la exploración a la nube de Qualys
7. Los resultados de la exploración se devuelven a TC-NAC:
   - Dirección 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

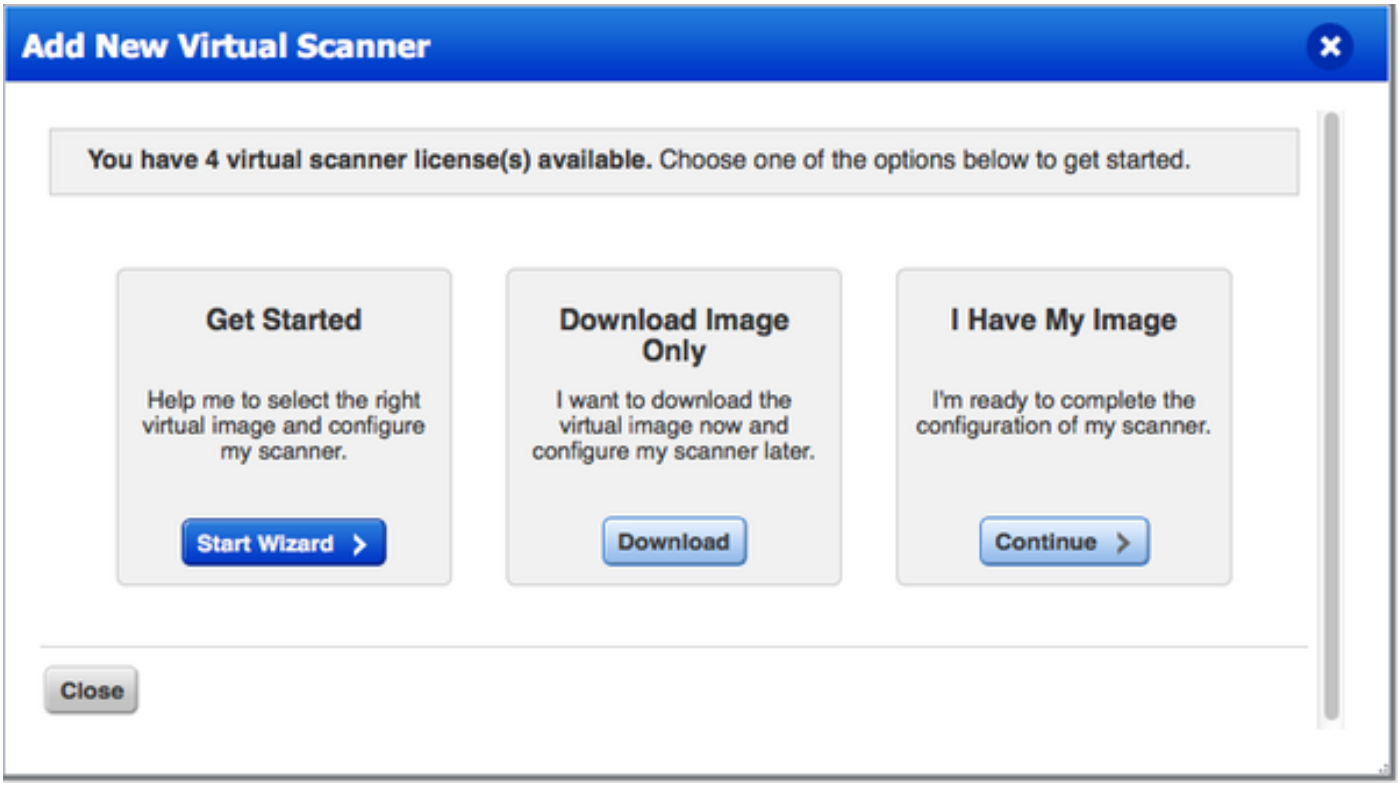
> **Caution**: La configuración de Qualys en este documento se hace para los propósitos del laboratorio, consulta por favor con los ingenieros de Qualys para los aspectos del diseño

Paso 1. Despliegue el escáner de Qualys

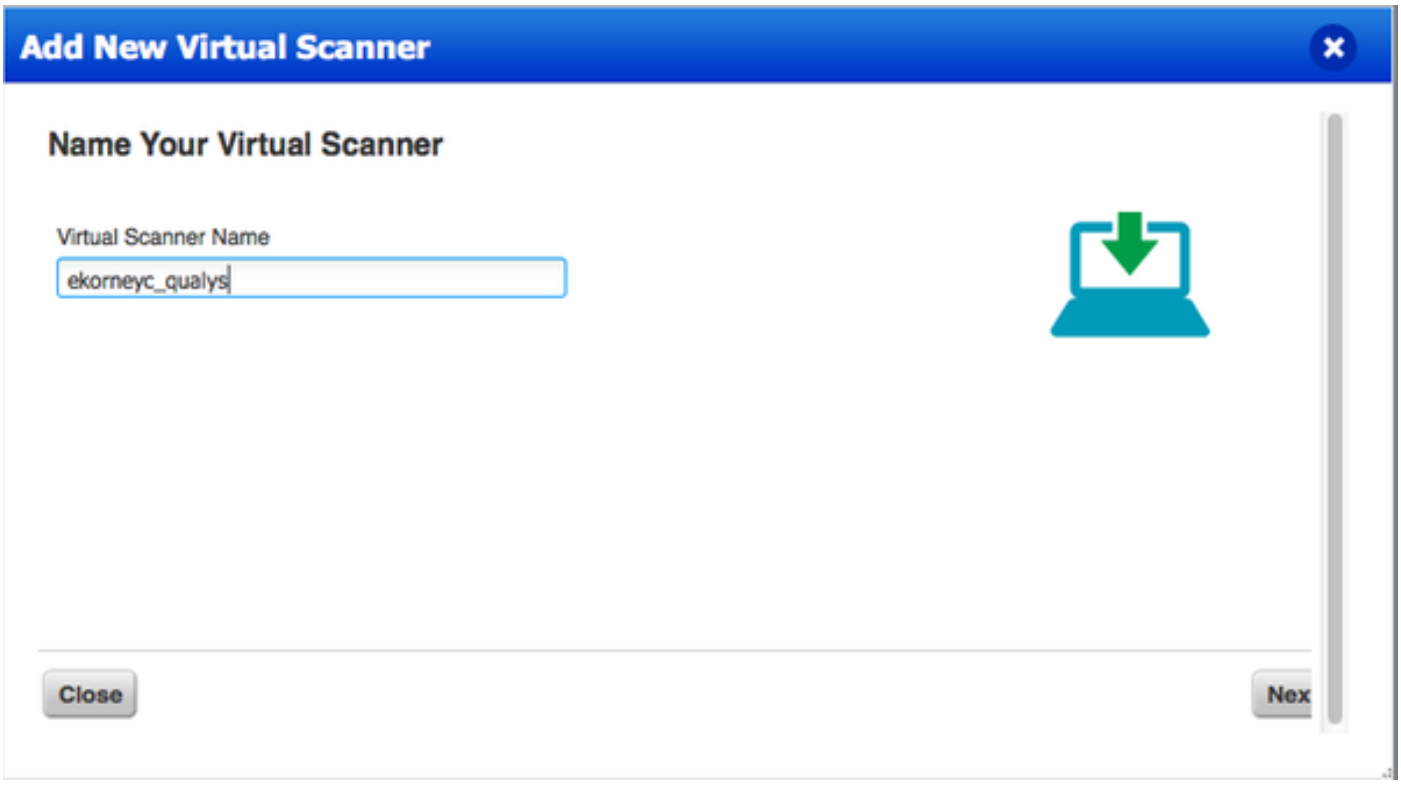
El escáner de Qualys se puede desplegar del archivo de los HUEVOS. Inicie sesión a la nube de Qualys y navegue a las exploraciones > a los dispositivos y seleccione el dispositivo nuevo > virtual del escáner



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**



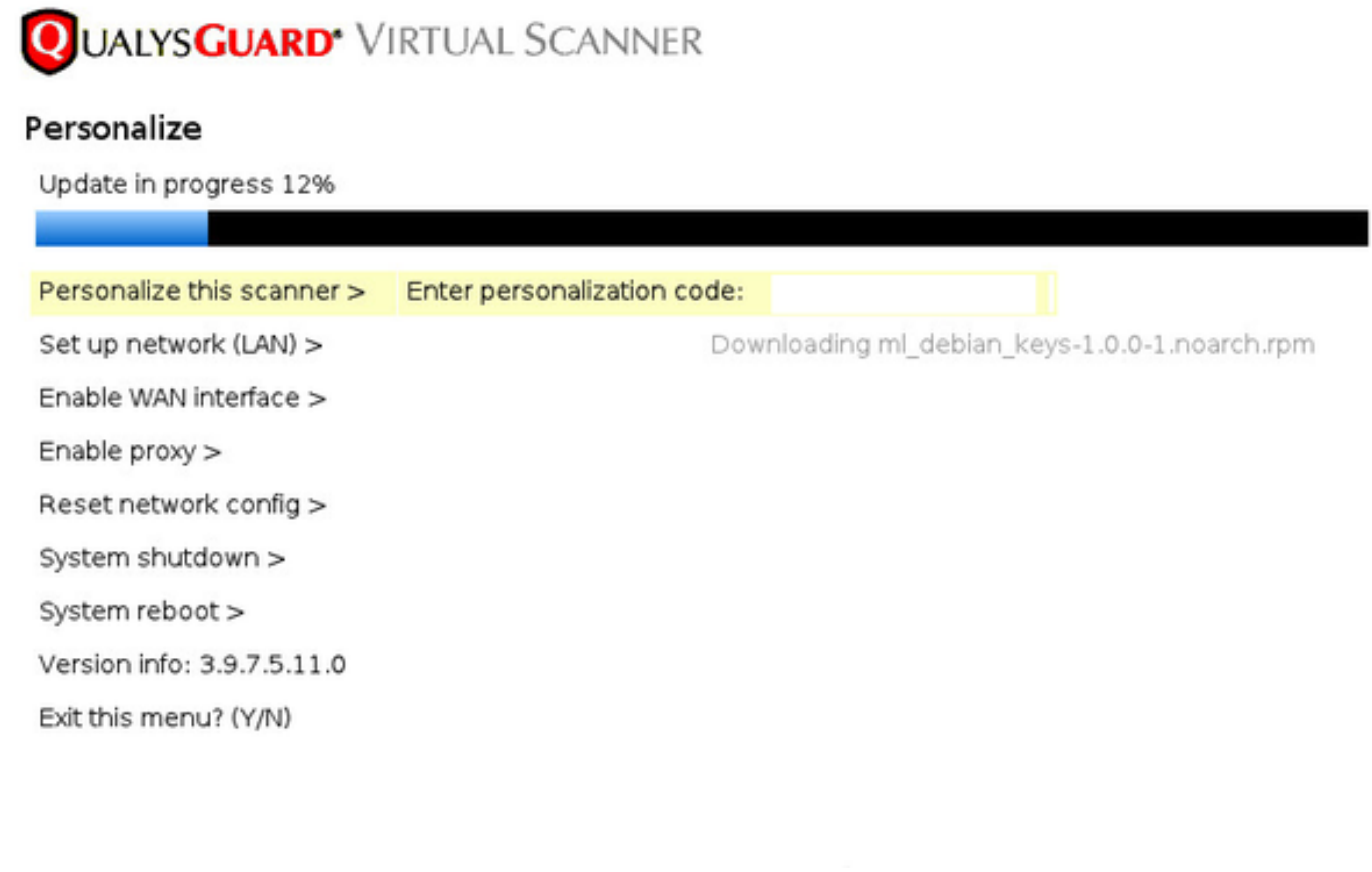
Después de ingresar el nombre del escáner le dan el código de autorización que usted utilizará más adelante.

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

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



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

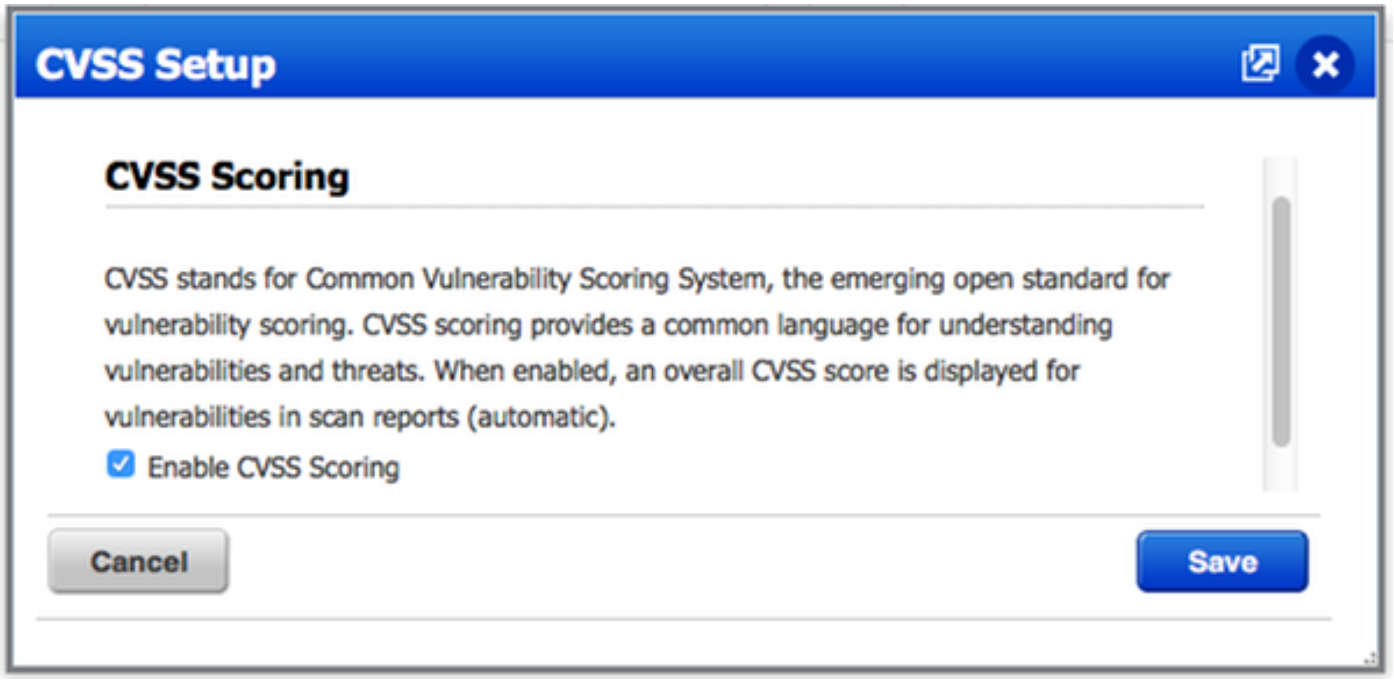
Ponga verde la muestra conectada a la izquierda indica que el escáner está listo, usted puede también ver el IP LAN, el IP de WAN, la versión del escáner y las firmas.

Configure el ISE

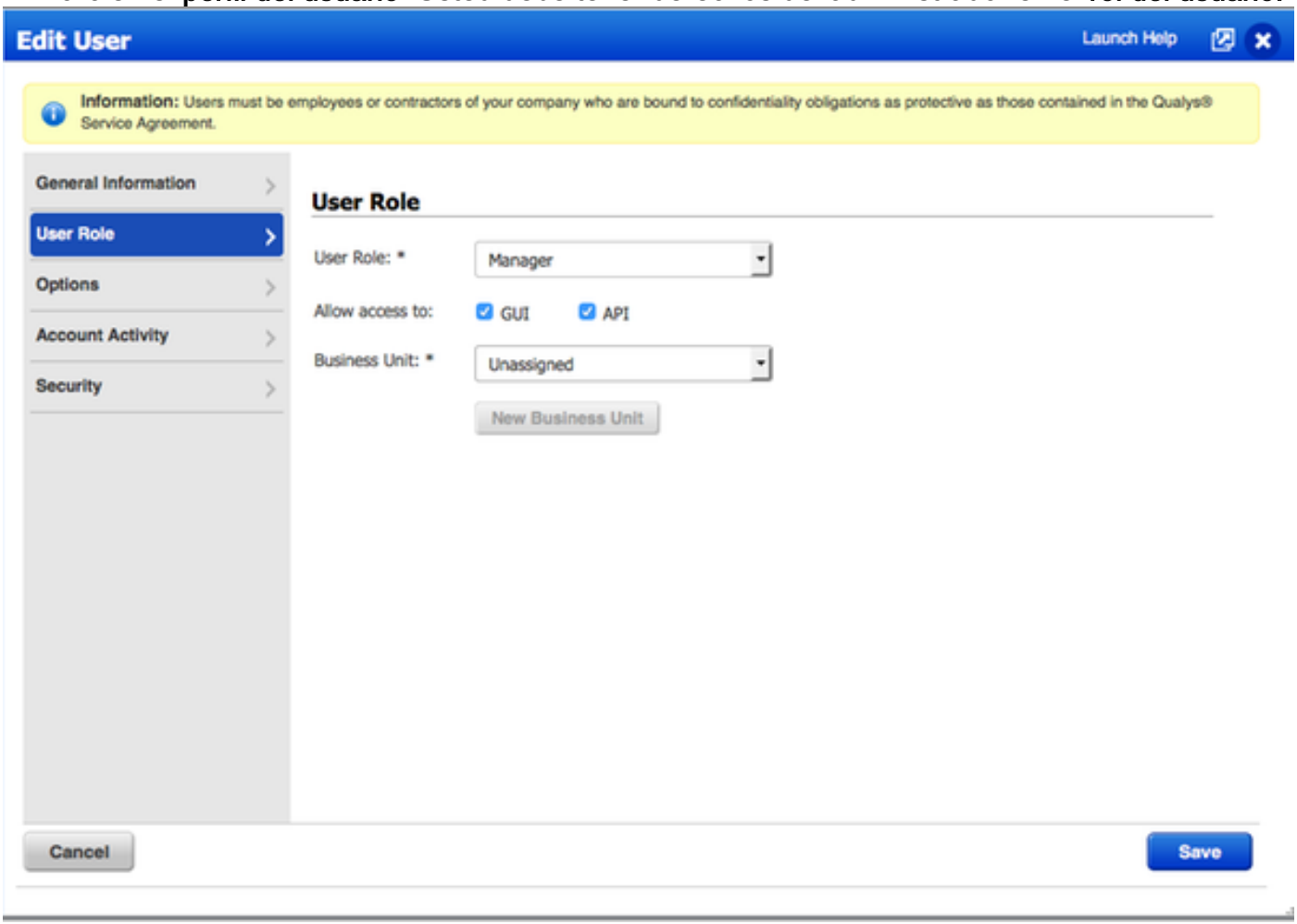
Aunque usted ha configurado el escáner y la nube de Qualys, usted todavía tiene que ajustar las configuraciones de la nube para aseegurarse la integración con los trabajos ISE muy bien. Observe, él debe ser hecho antes de que usted configure el adaptador con el GUI, pues la base de conocimiento que contiene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

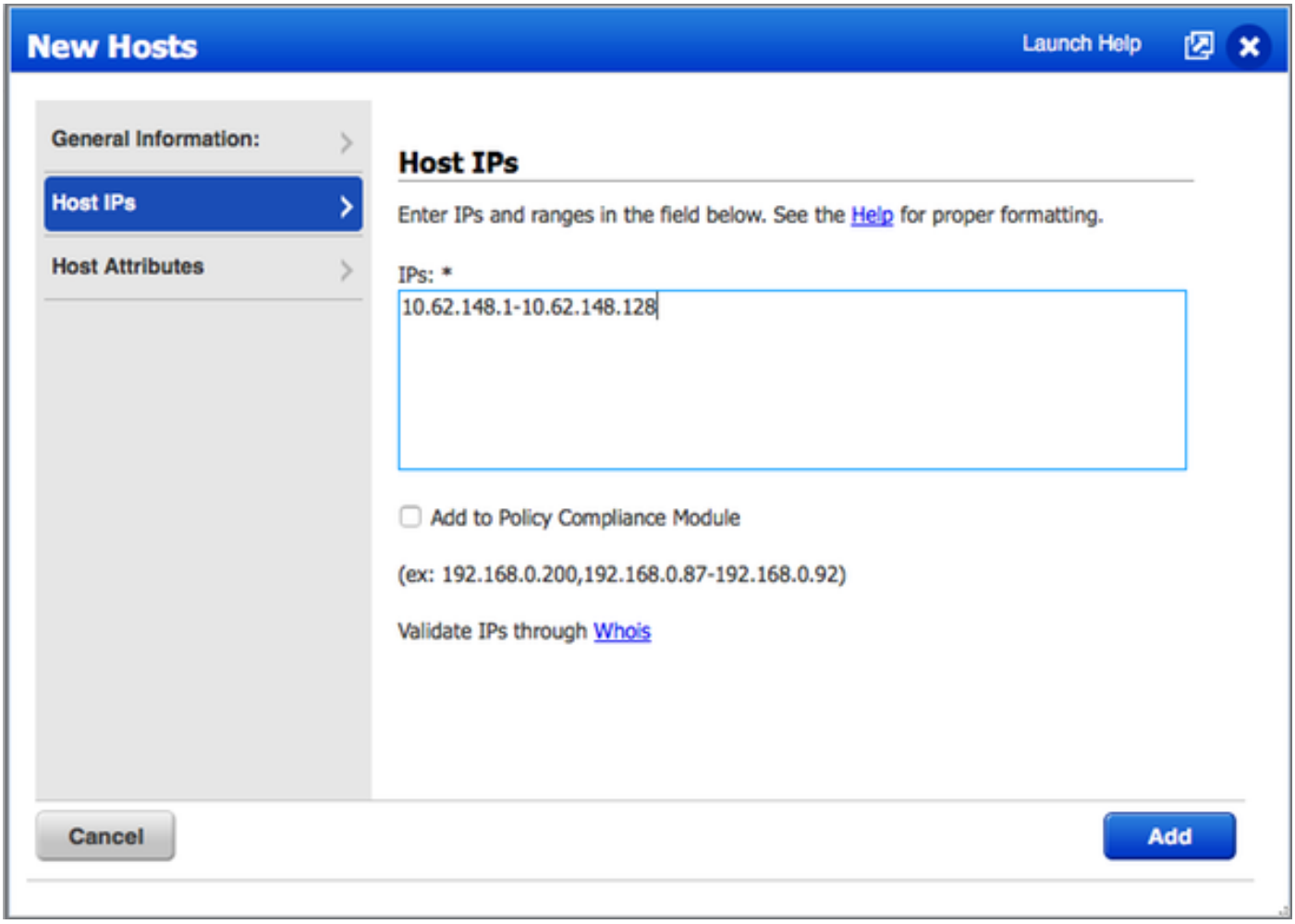
- El permiso CVSS que anota en la administración de vulnerabilidades > señala > puesto > el anotar CVSS > del permiso CVSS



- 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.**



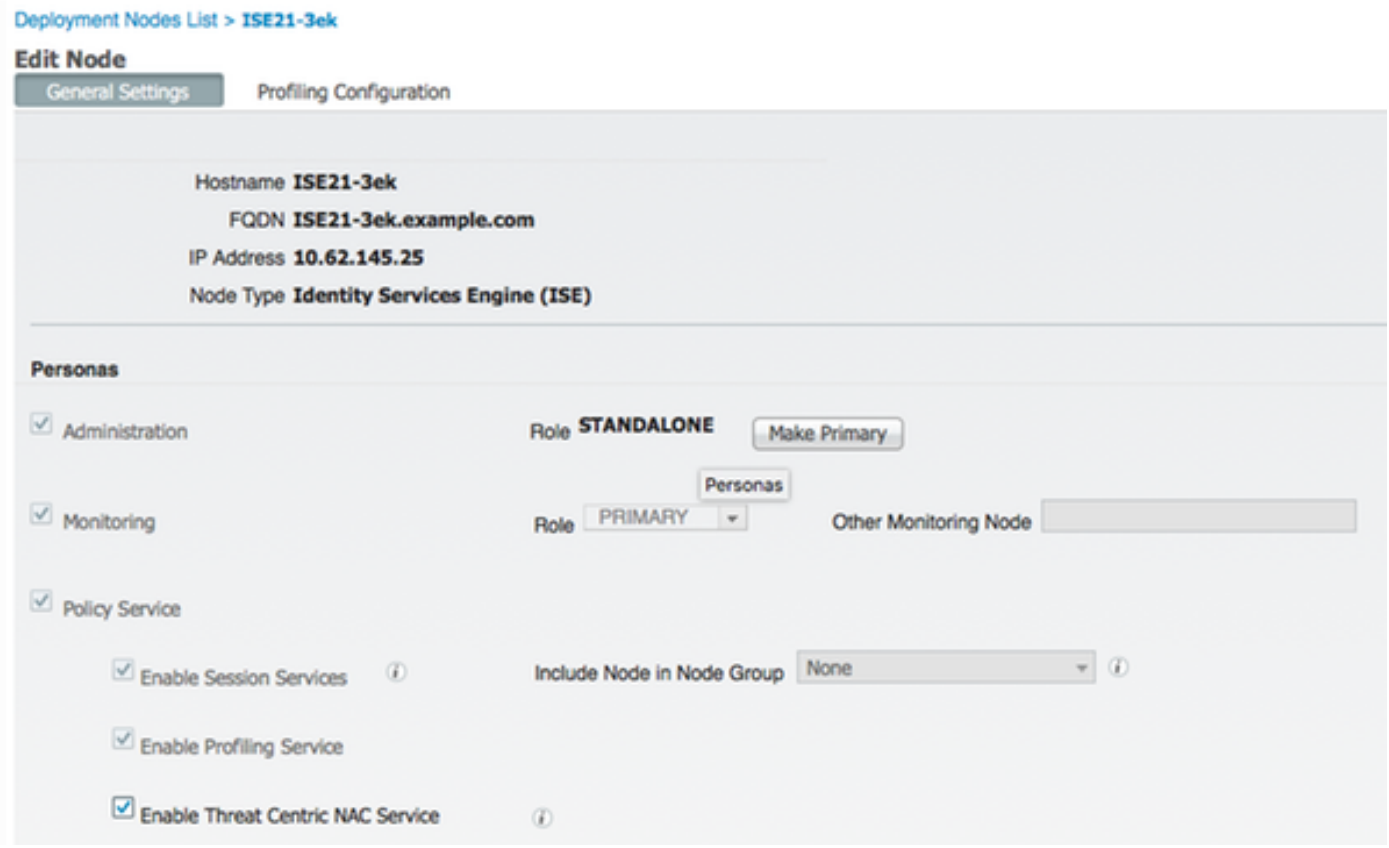
- Asegúrese que esos IP Addresses/las subredes de los puntos finales que requieren la evaluación de vulnerabilidades estén agregados a Qualys en la administración de vulnerabilidades > los activos > los activos del host > nuevo > los host seguidos IP



Paso 2. Servicios del permiso TC-NAC

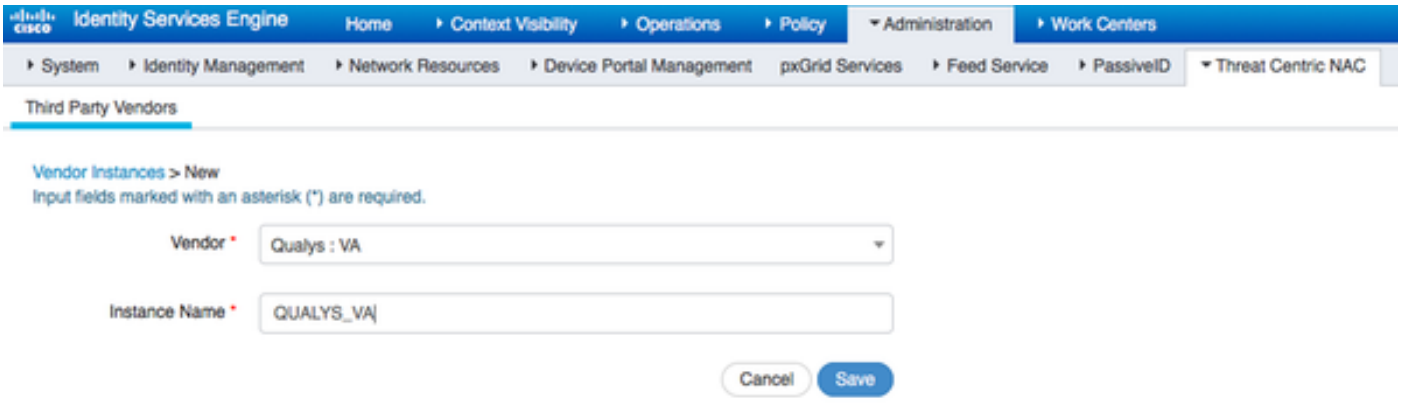
Los servicios del permiso TC-NAC bajo la administración > despliegue > editan el nodo. Checkbox **céntrico del servicio del NAC de la amenaza del permiso** del control.

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

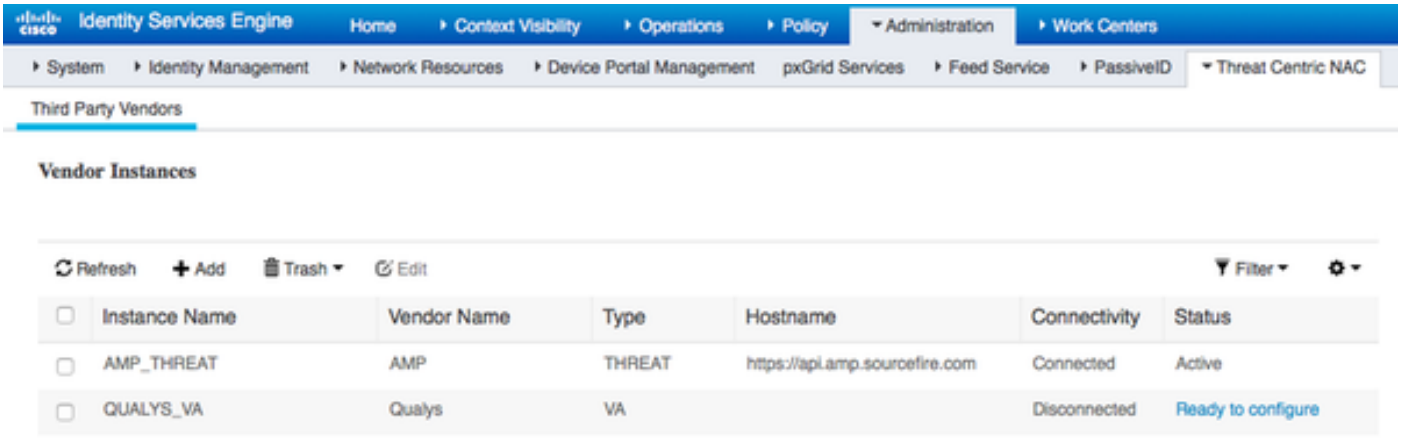


Paso 3. Conectividad del adaptador de Qualys de la configuración al marco ISE VA

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

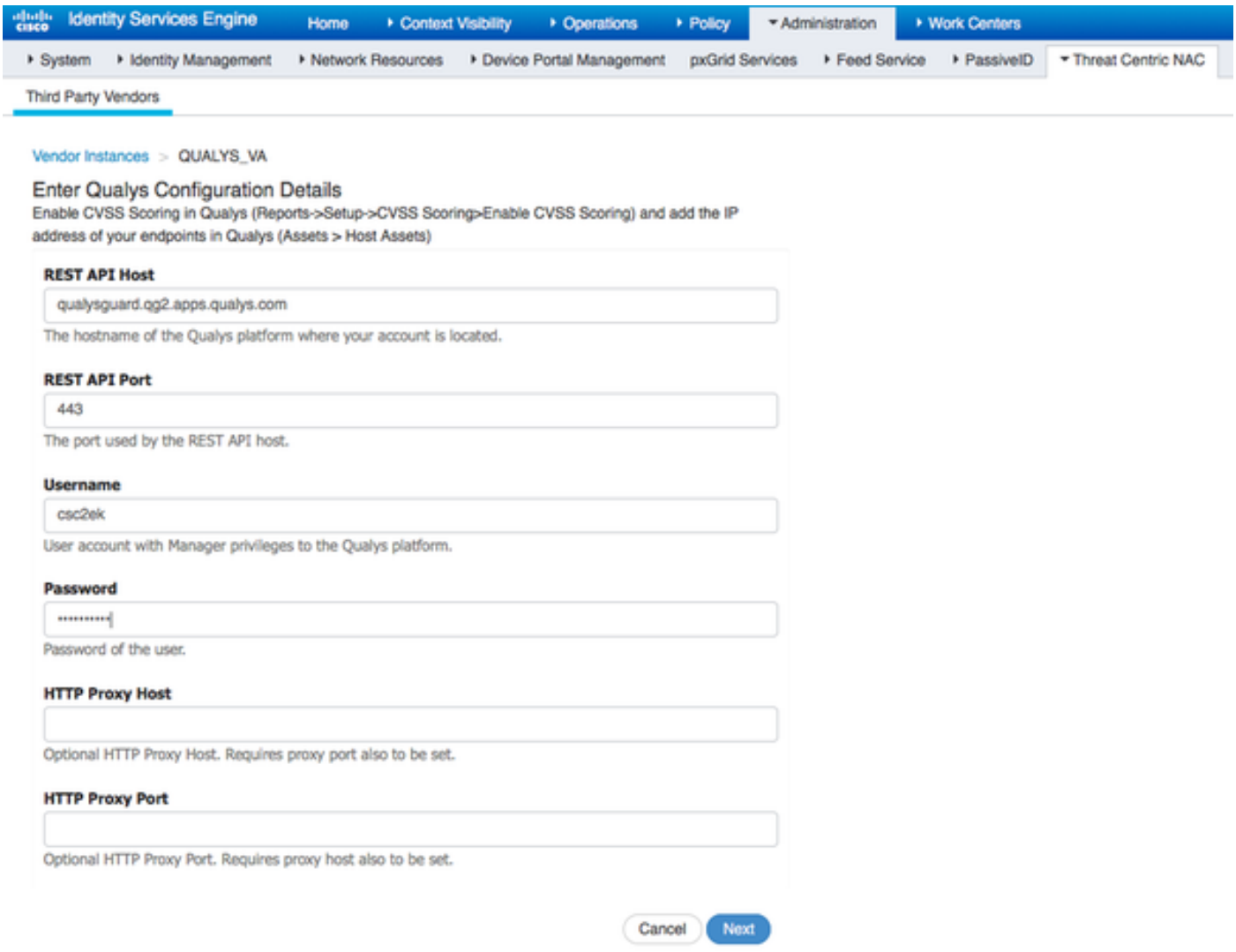


Cuando las transiciones del caso de Qualys **a alistar para configurar el** estado, hacen clic en **listo para configurar la** opción en el estatus.

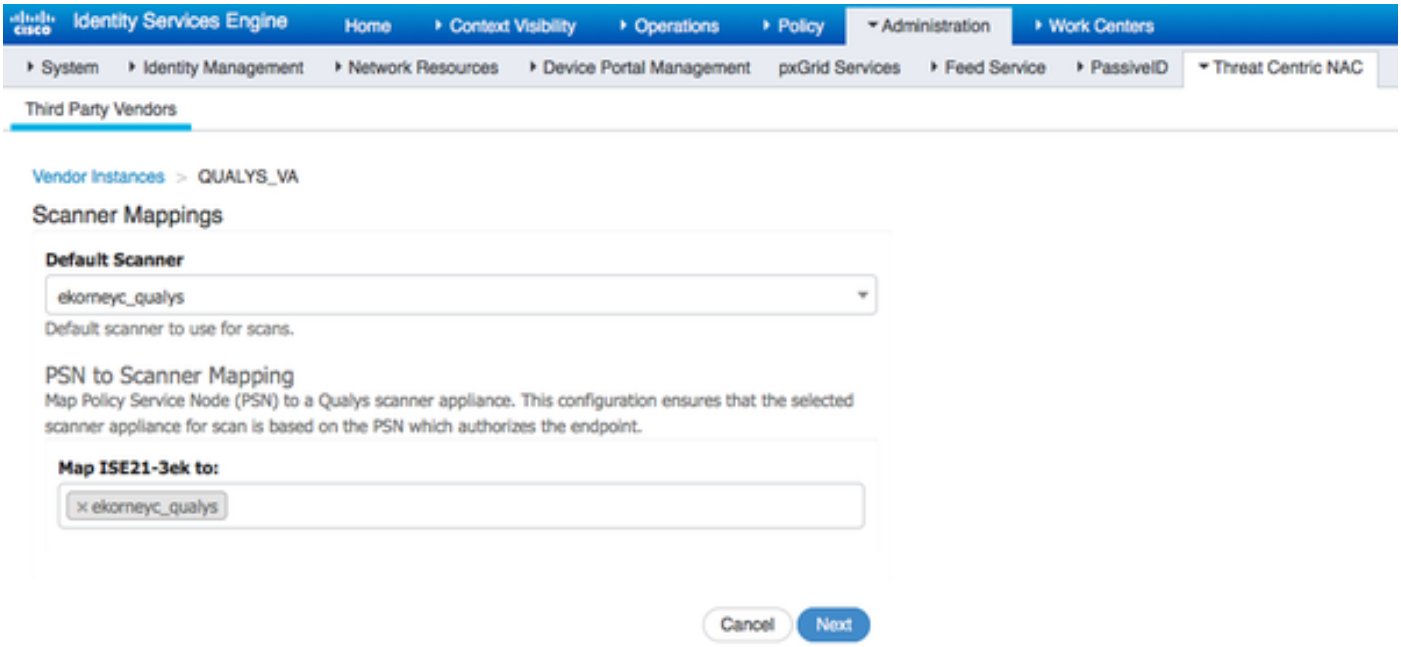


El host del RESTO API debe ser el que usted utiliza para la nube de Qualys, donde se localiza su cuenta. En este ejemplo - qualysguard.qg2.apps.qualys.com

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

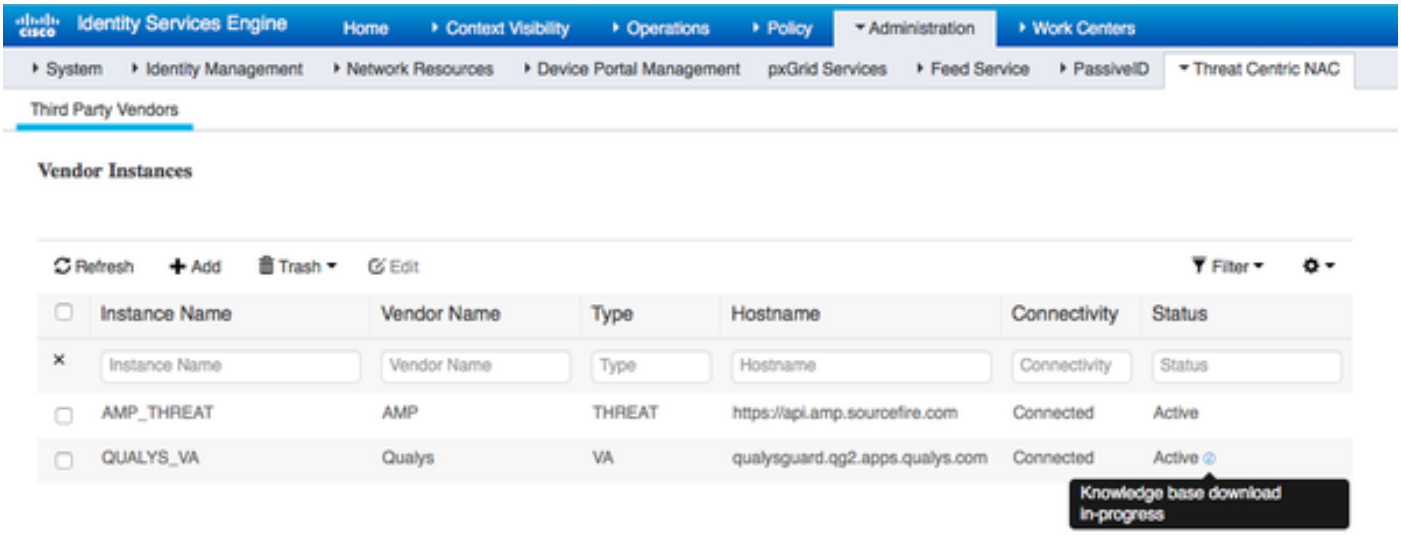


El ISE descarga la información sobre los escáneres que están conectados con la nube de Qualys, usted puede configurar el PSN a la asignación del escáner en esta página. Se asegura de que el escáner seleccionado esté escogido sobre la base del PSN que autoriza el punto final.



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

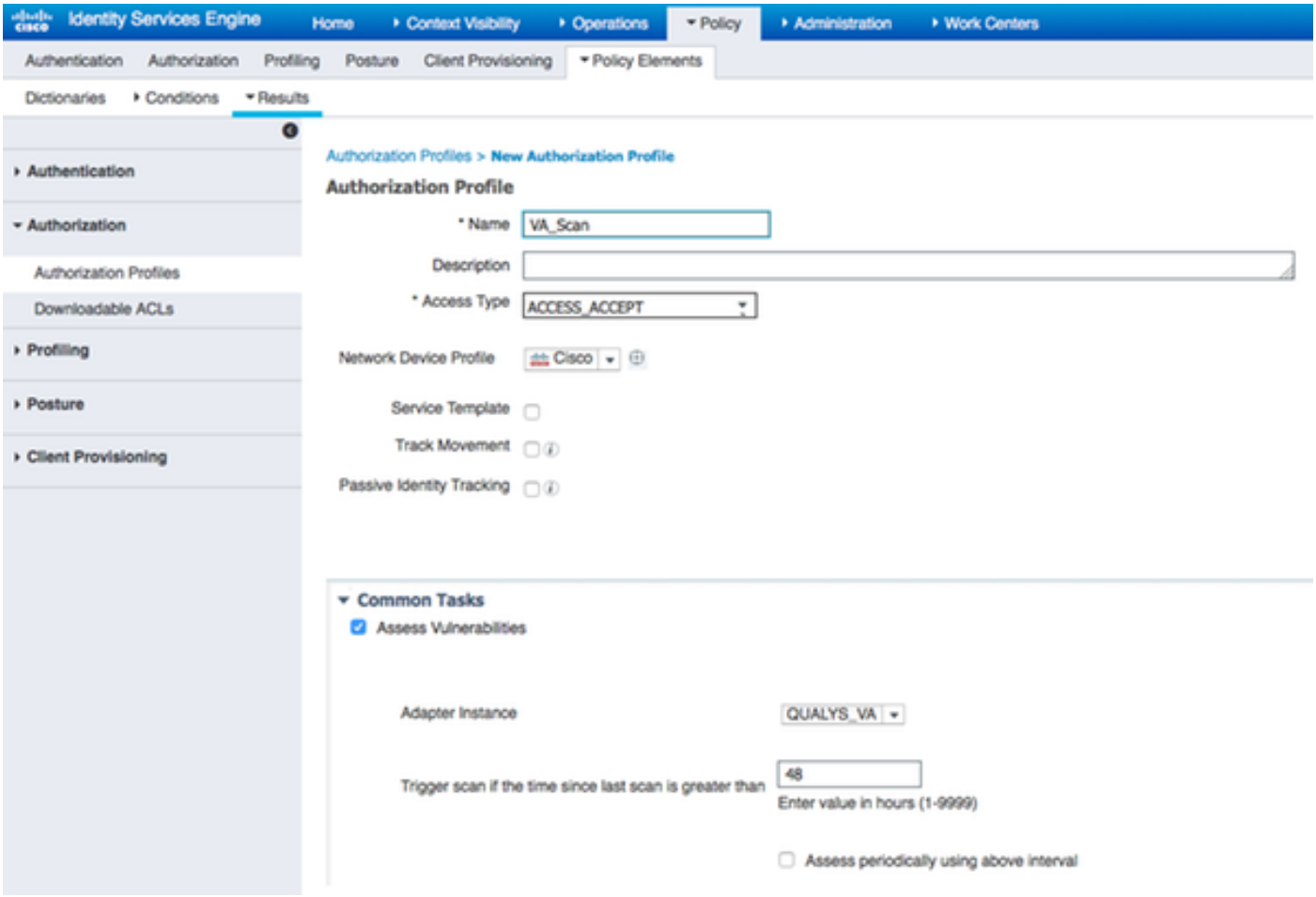
Navegue a la directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización. Agregue el nuevo perfil. Bajo **tareas comunes** seleccione el checkbox de la **evaluación de vulnerabilidades**.
El intervalo a pedido de la exploración se debe seleccionar 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

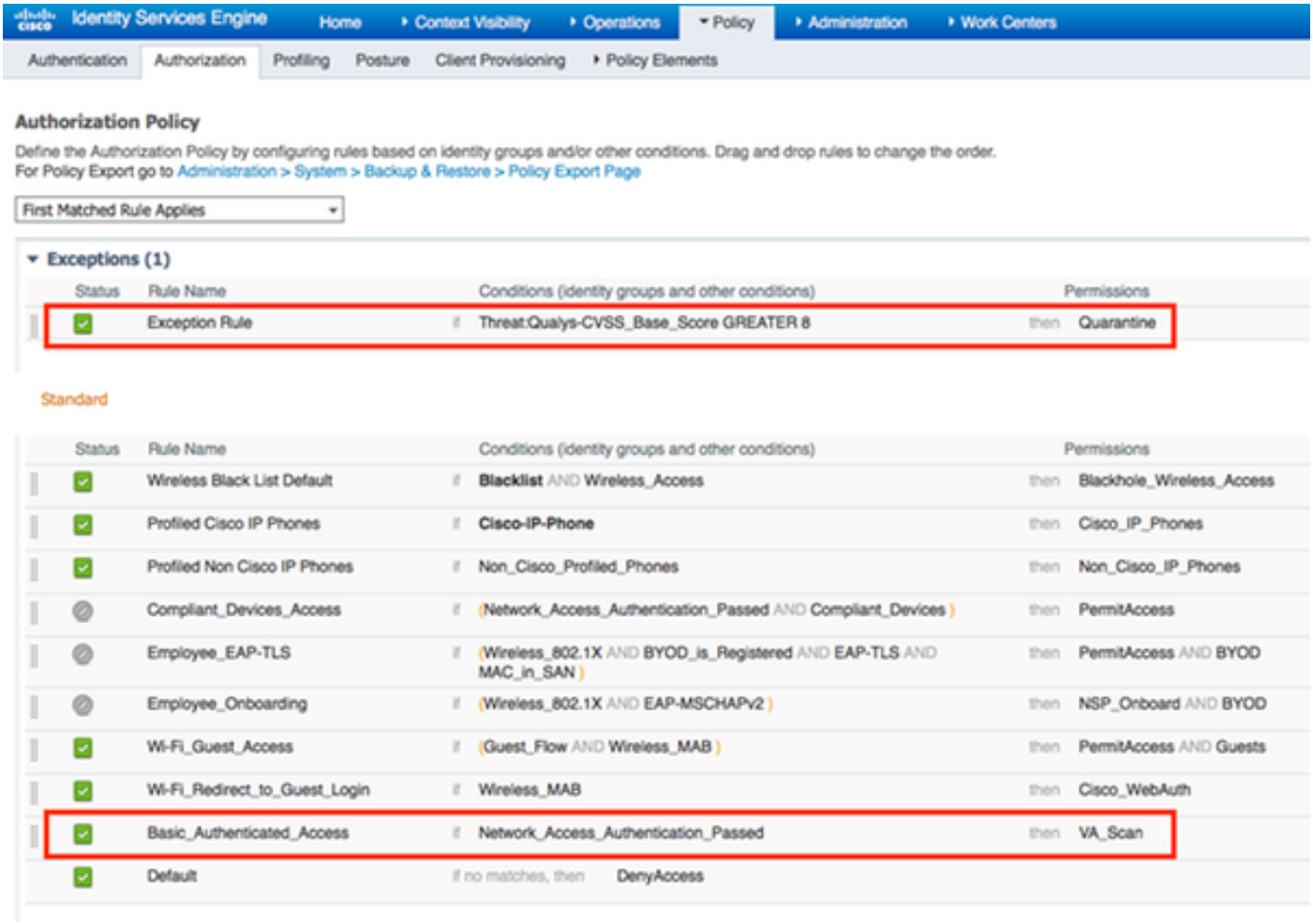
Se envían a los dispositivos de red dentro del paquete access-accept, aunque el propósito real de ellos sea decir el nodo MNT que la exploración debe ser accionada. El MNT da instrucciones el nodo TC-NAC para comunicar con la nube de Qualys.



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**.

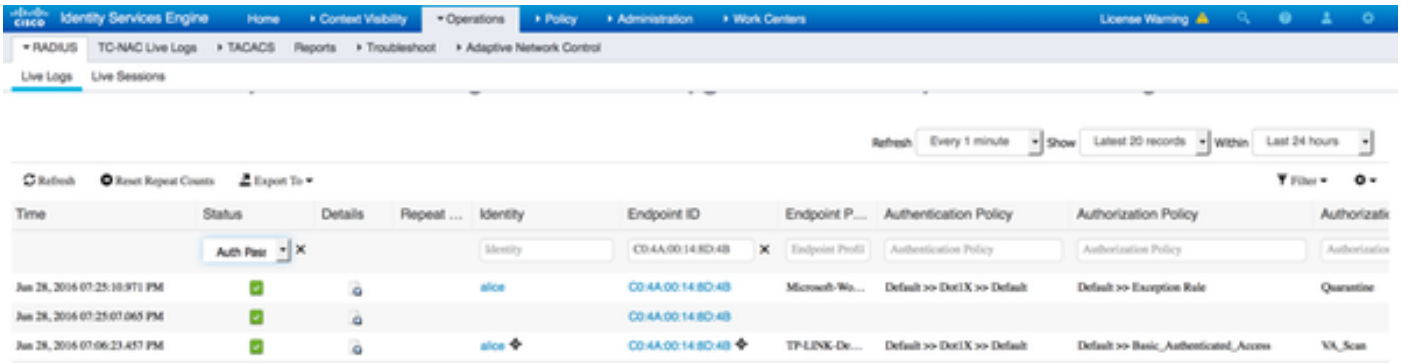
- Cree la directiva de la autorización para las máquinas Quarantined. Navegue a la directiva > a la autorización > a la directiva > a las excepciones de la autorización y cree una **regla de excepciones**. Haga clic en las condiciones > crean la nueva condición (opción avanzada) > atributo selecto, navegan 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.



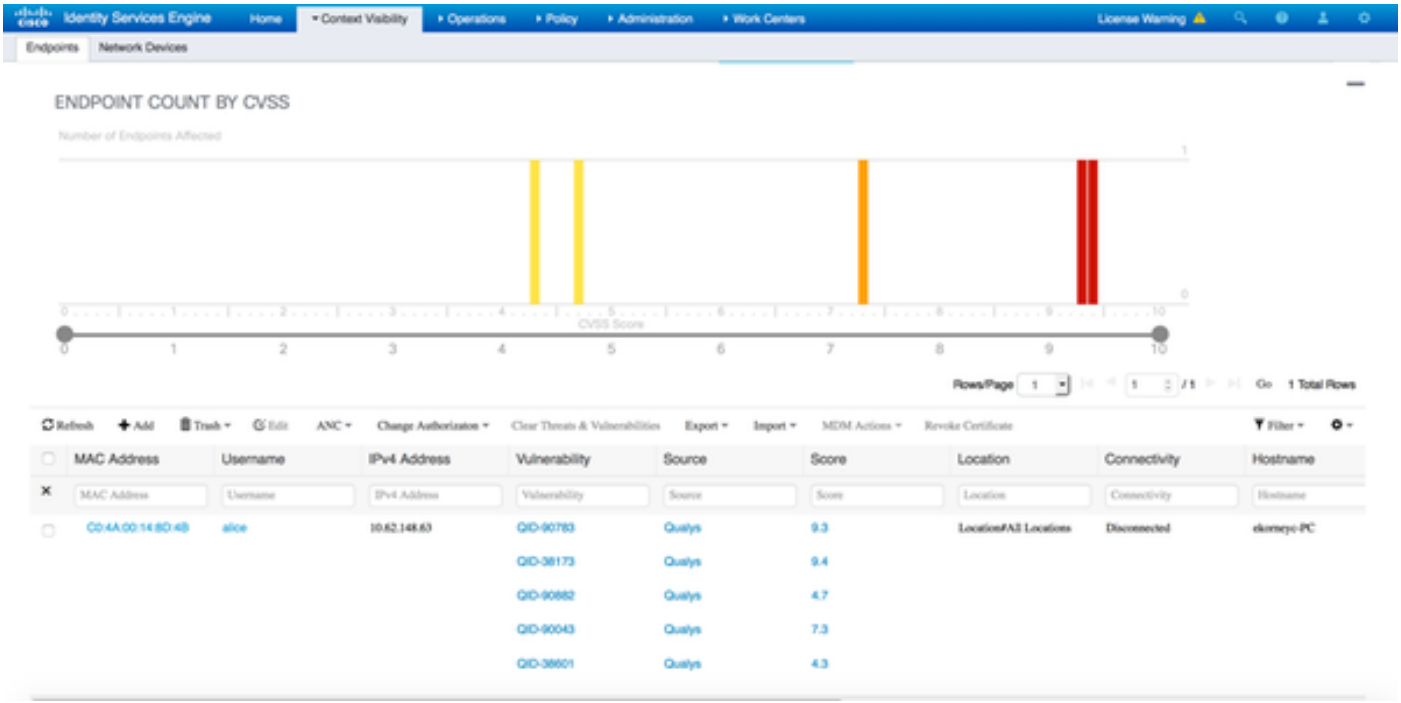
Verificación

Identity Services Engine

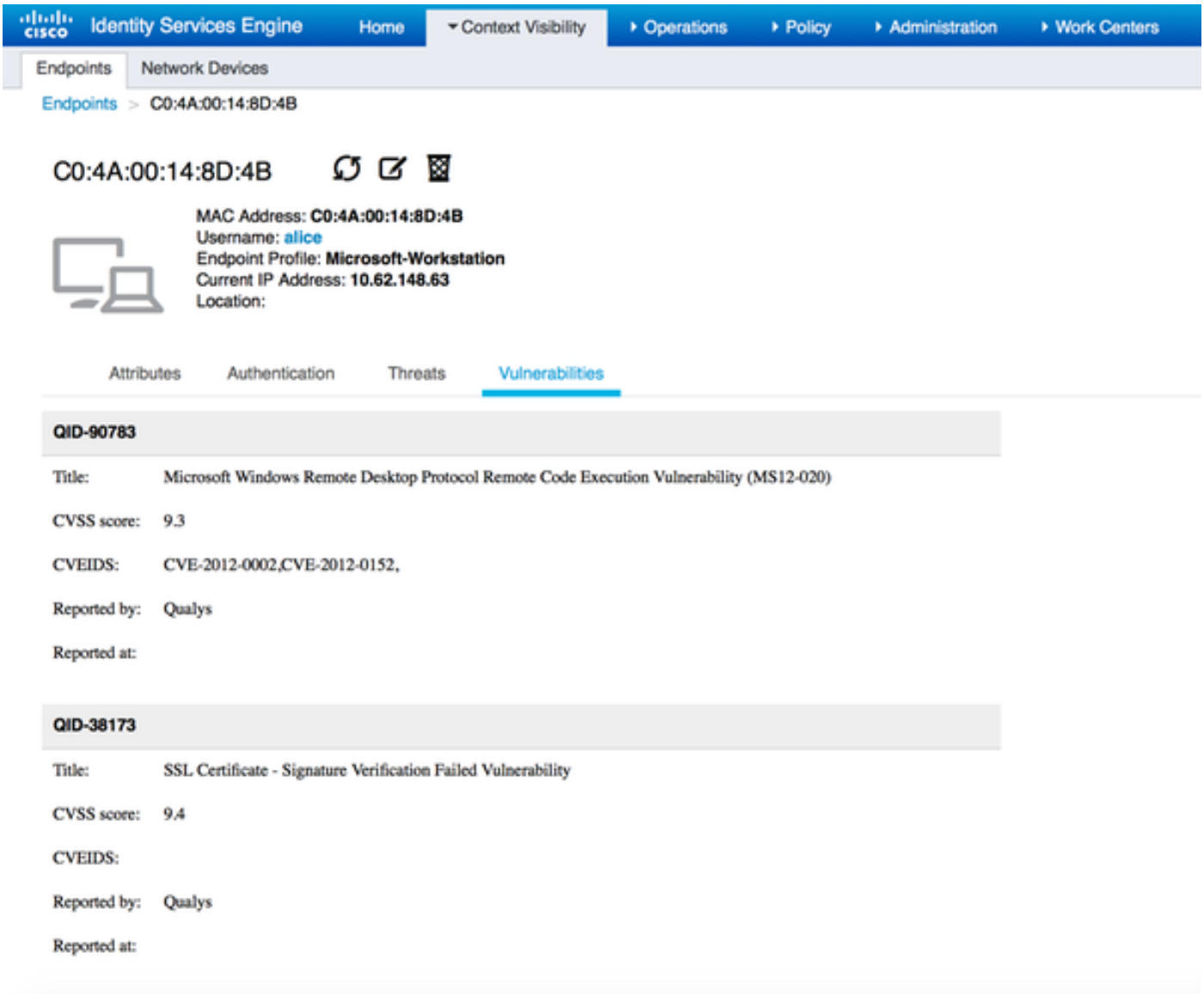
La primera exploración VA de los activadores de la conexión. Cuando se acaba la exploración, el Reauthentication CoA se acciona para aplicar la nueva directiva si se corresponde con.



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.

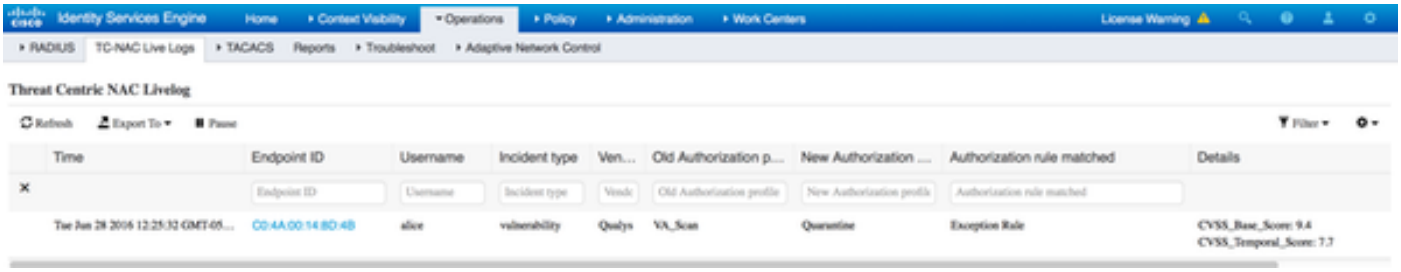


Al seleccionar el punto final específico, más detalles sobre cada vulnerabilidad aparecen, incluyendo el **título** y **CVEID**.



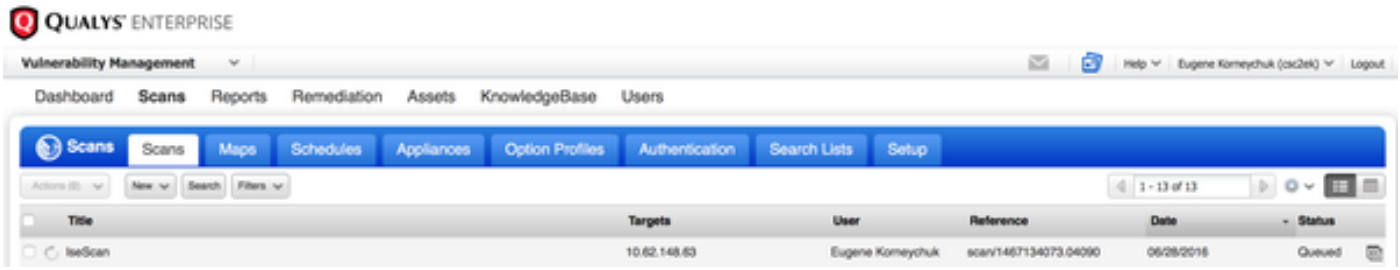
En las operaciones > TC-NAC viven los registros, usted puede ver viejo contra las nuevas directivas de la autorización aplicadas y los detalles en CVSS_Base_Score.

> **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.

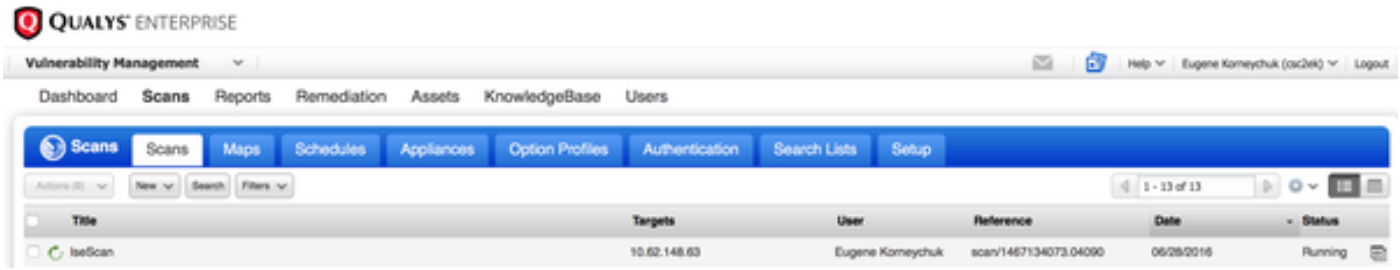


Nube de Qualys

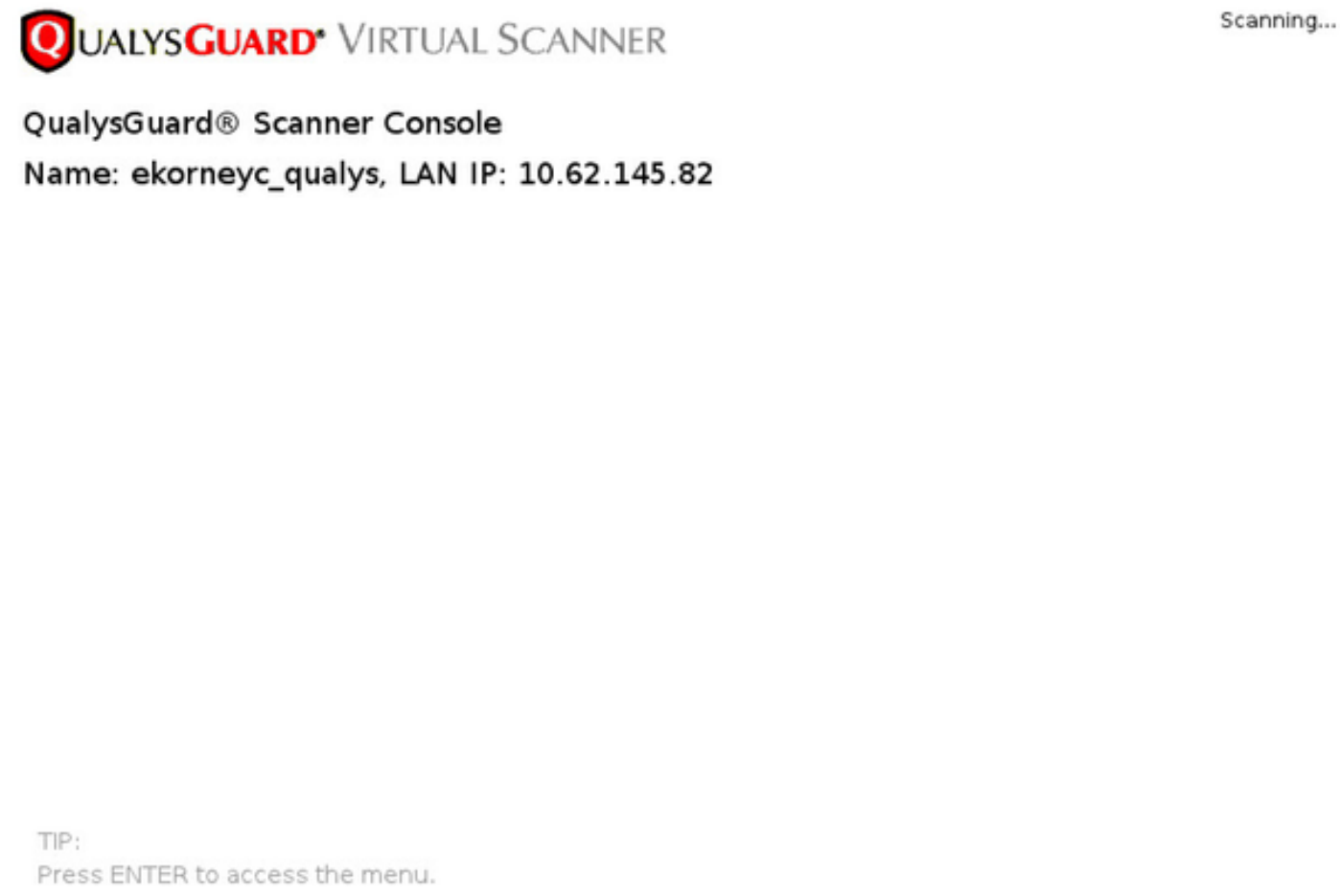
Cuando la exploración VA es accionada por TC-NAC Qualys hace cola la exploración, él puede ser visto en las exploraciones > las exploraciones



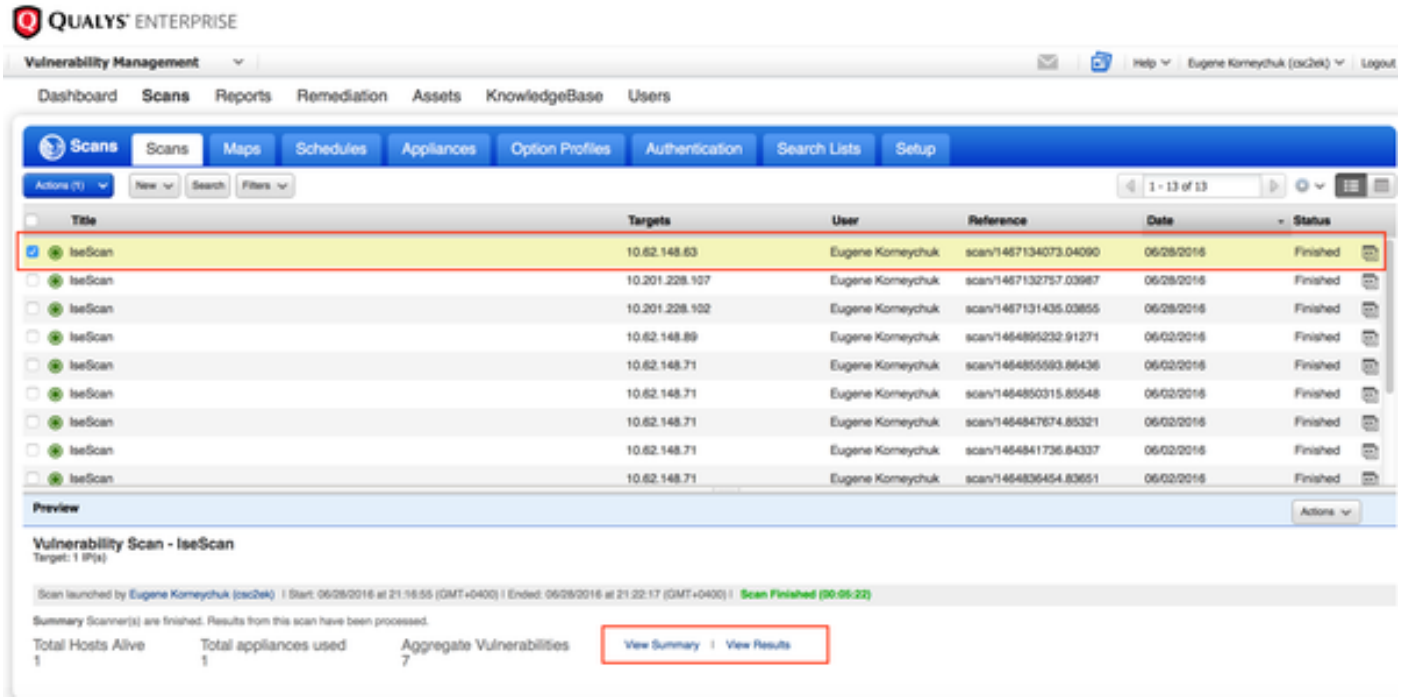
Luego las transiciones a ejecutarse, significando la nube de Qualys ha dado instrucciones el escáner de Qualys para realizar la exploración real



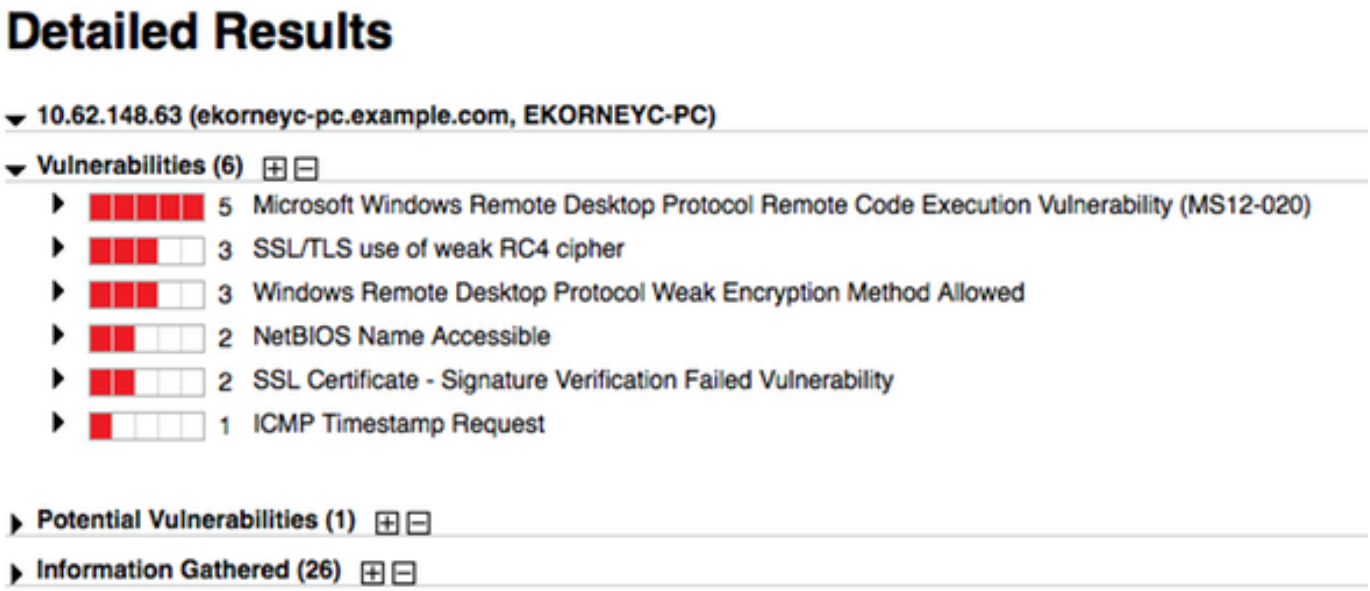
Mientras que el escáner realiza la exploración, usted debe ver la “exploración…” muestra en la esquina superior derecha del guardia de Qualys



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**.



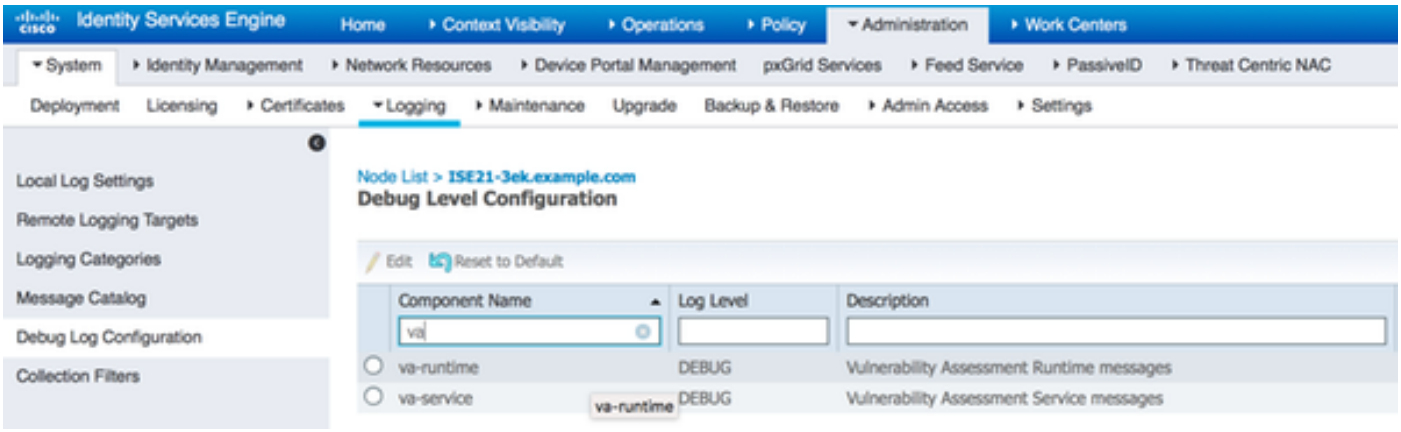
En el informe sí mismo usted puede ver los **resultados detallados**, donde se muestran las vulnerabilidades detectadas.



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,"vuln
erabilities":["{\"vulnerabilityId\":\"QID-90783\",\"cveIds\":\"CVE-2012-0002,CVE-2012-
0152,\",\"cvssBaseScore\":\"9.3\",\"cvssTemporalScore\":\"7.7\",\"vulnerabilityTitle\":\"Microso
ft (certificado del MS12-
020)\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
38173\",\"cveIds\":\"\",\"cvssBaseScore\":\"9.4\",\"cvssTemporalScore\":\"6.9\",\"vulnerabilityT
itle\":\"SSL - firma fallada del
Allowed\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"vulnerabilityT
itle\":\"SMB del método de encripción vulnerable del protocolo del Escritorio Remoto del
Vulnerability\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90882\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.7\",\"cvssTemporalScore\":\"4\",\"vulnerabilityTit
le\":\"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"}, certificado {"vulnerabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL -
vulnerabilidad fallada de la verificación de firma”, “vulnerabilityVendor”: “Qualys”}, método de
encripción vulnerable del protocolo del Escritorio Remoto {"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
permitido”, “vulnerabilityVendor”: “Qualys”}, firma {"vulnerabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
inhabilitada o SMB que firma no requerido”, “vulnerabilityVendor”: “Qualys”}, uso del
{"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 encripción 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 trigeringon-
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 trigering 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