

Configurar o 2.1 NAC Ameaça-cêntrico ISE (TC-NAC) com Qualys

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de fluxo de nível elevado](#)

[Configurar a nuvem e o varredor de Qualys](#)

[Etapa 1. Distribua o varredor de Qualys](#)

[Etapa 2. Configurar o varredor de Qualys](#)

[Configurar o ISE](#)

[Etapa 1. Ajustes da nuvem de Qualys do acordo para a integração com ISE](#)

[Etapa 2. Permita serviços TC-NAC](#)

[Etapa 3. Configurar a Conectividade do adaptador de Qualys à estrutura ISE VA](#)

[Etapa 4. Configurar o perfil da autorização para provocar a varredura VA](#)

[Etapa 5. Configurar políticas da autorização](#)

[Verificar](#)

[Identity Services Engine](#)

[Nuvem de Qualys](#)

[Troubleshooting](#)

[Debuga no ISE](#)

[Edições típicas](#)

[Referências](#)

Introdução

Este original descreve como configurar o NAC Ameaça-cêntrico com o Qualys no 2.1 do Identity Services Engine (ISE). A característica cêntrica do controle de acesso de rede da ameaça (TC-NAC) permite-o de criar as políticas da autorização baseadas nos atributos da ameaça e da vulnerabilidade recebidos dos adaptadores da ameaça e da vulnerabilidade.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Motor do serviço da identidade de Cisco
- Qualys ScanGuard

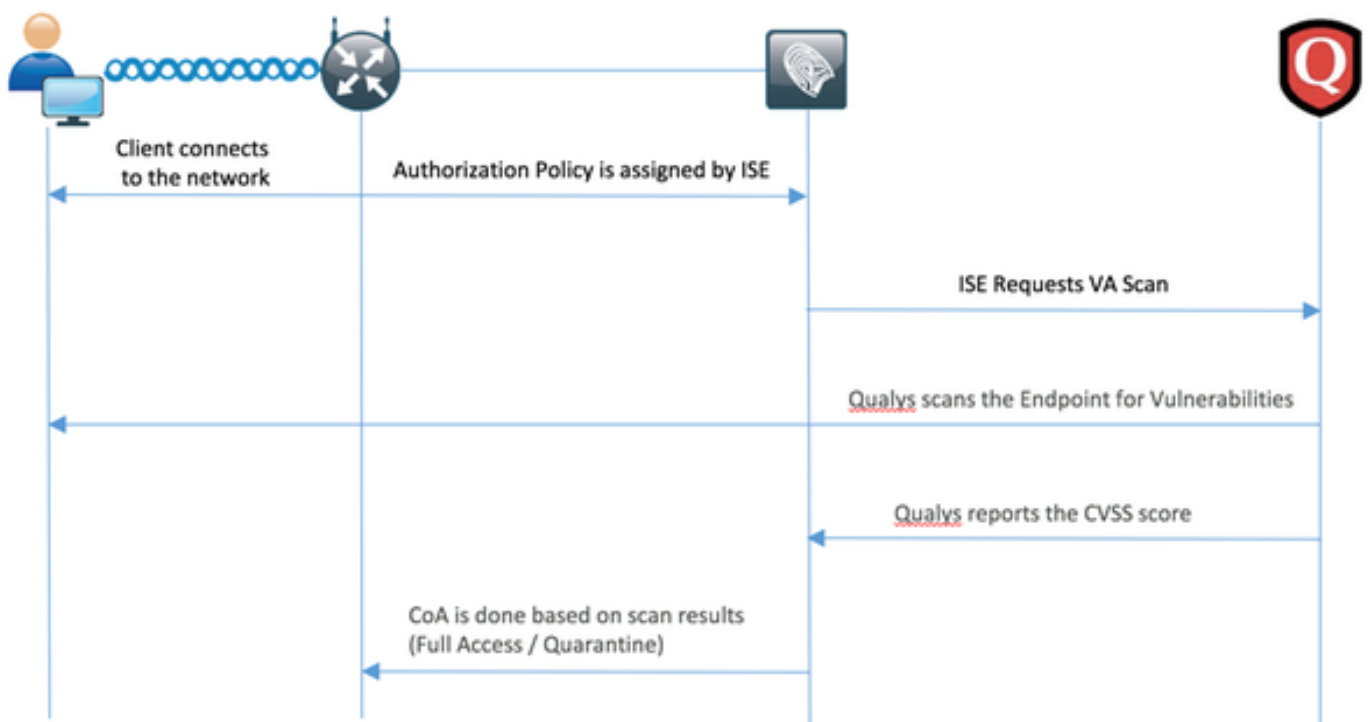
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2.1 do motor do serviço da identidade de Cisco
- Controlador do Wireless LAN (WLC) 8.0.121.0
- Varredor 8.3.36-1 do protetor de Qualys, assinaturas 2.3.364-2
- Pacote de serviços 1 de Windows 7

Configurar

Diagrama de fluxo de nível elevado



Este é o fluxo:

1. O cliente conecta à rede, o acesso limitado é dado e o perfil com **avalia vulnerabilidades que a caixa de seleção permitida é atribuída**
2. O nó PSN envia o mensagem do syslog à autenticação de confirmação do nó MNT ocorreu e a varredura VA era o resultado da política da autorização
3. O nó MNT submete a VARREDURA ao nó TC-NAC (que usa Admin WebApp) que usa estes dados:
 - MAC address
 - IP address
 - Intervalo da varredura
 - Varredura periódica permitida
 - Originando o PSN
4. Qualys TC-NAC (encapsulado no recipiente do estivador) comunica-se com a nuvem de Qualys (através do RESTO API) para provocar a varredura se necessário

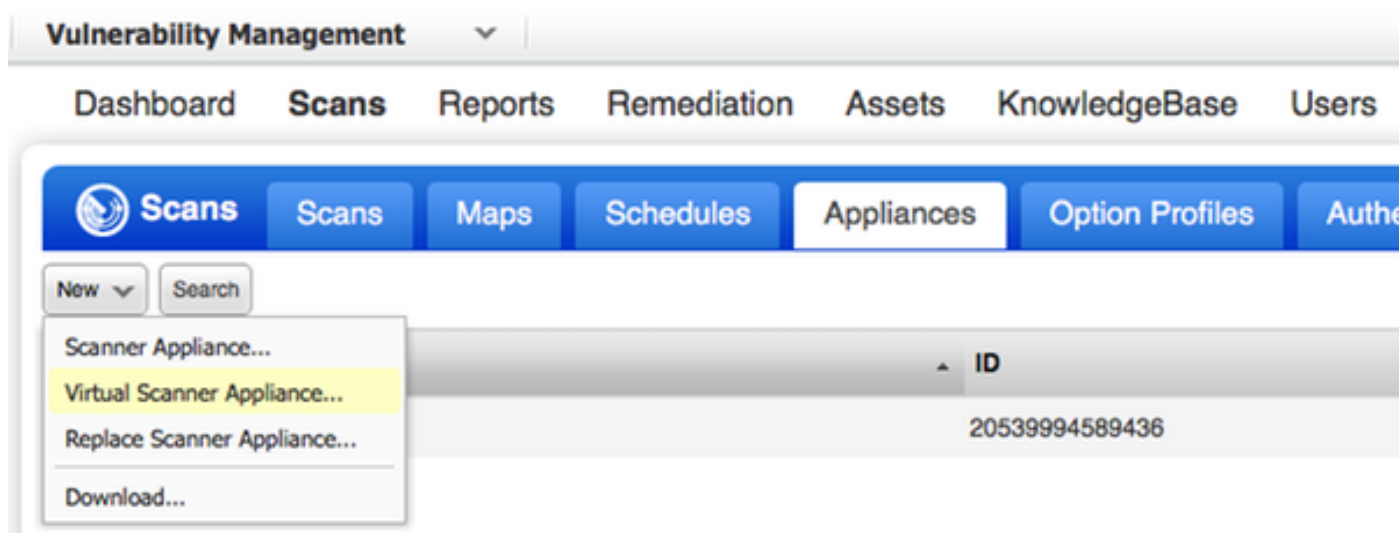
5. A nuvem de Qualys instrui o varredor de Qualys para fazer a varredura do valor-limite
6. O varredor de Qualys envia os resultados da varredura à nuvem de Qualys
7. Os resultados da varredura são enviados para trás a TC-NAC:
 - MAC address
 - Todas as contagens CVSS
 - Todas as vulnerabilidades (QID, título, CVEIDs)
8. TC-NAC atualiza a BANDEJA com todos os dados da etapa 7.
9. O CoA é provocado se necessário de acordo com a autorização a política configurada.

Configurar a nuvem e o varredor de Qualys

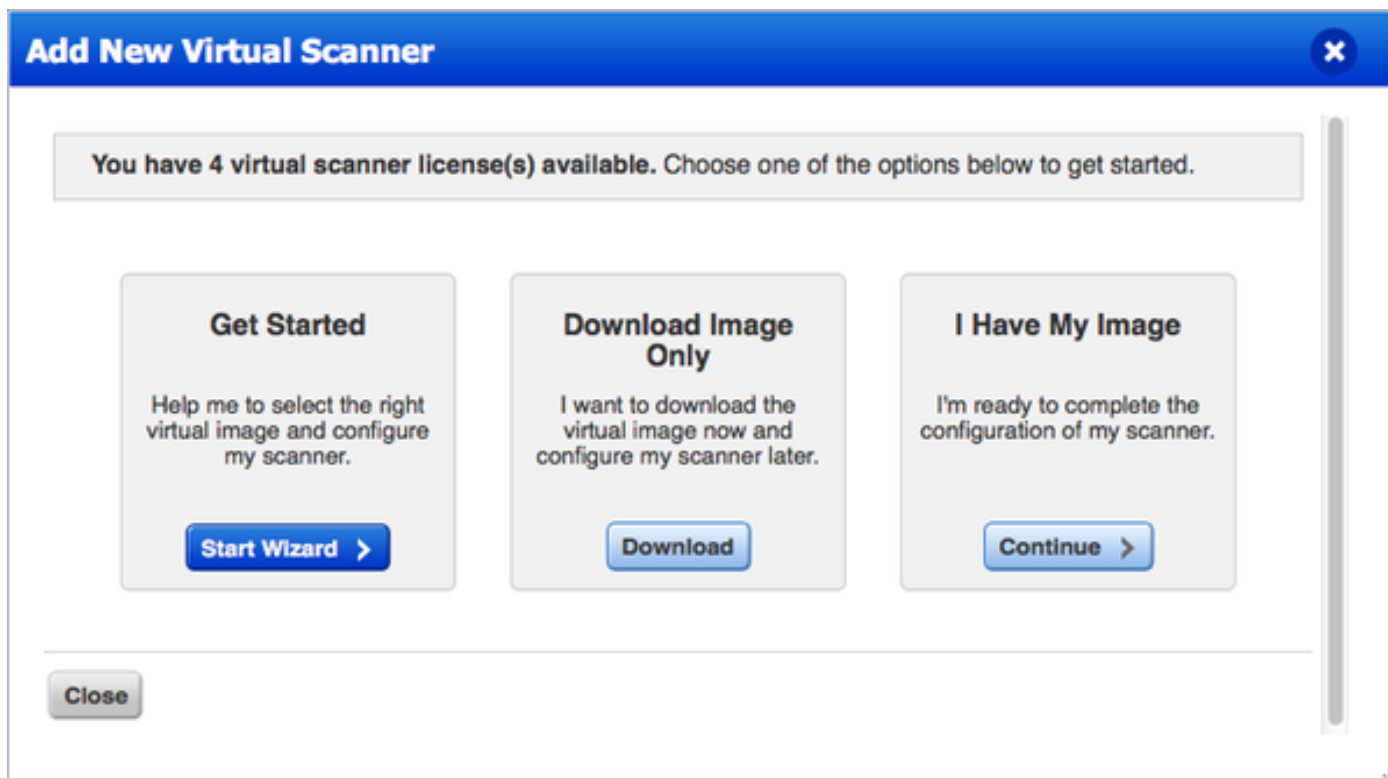
Cuidado: A configuração de Qualys neste original é feita para as finalidades do laboratório, consulta por favor com os coordenadores de Qualys para considerações de projeto

Etapa 1. Distribua o varredor de Qualys

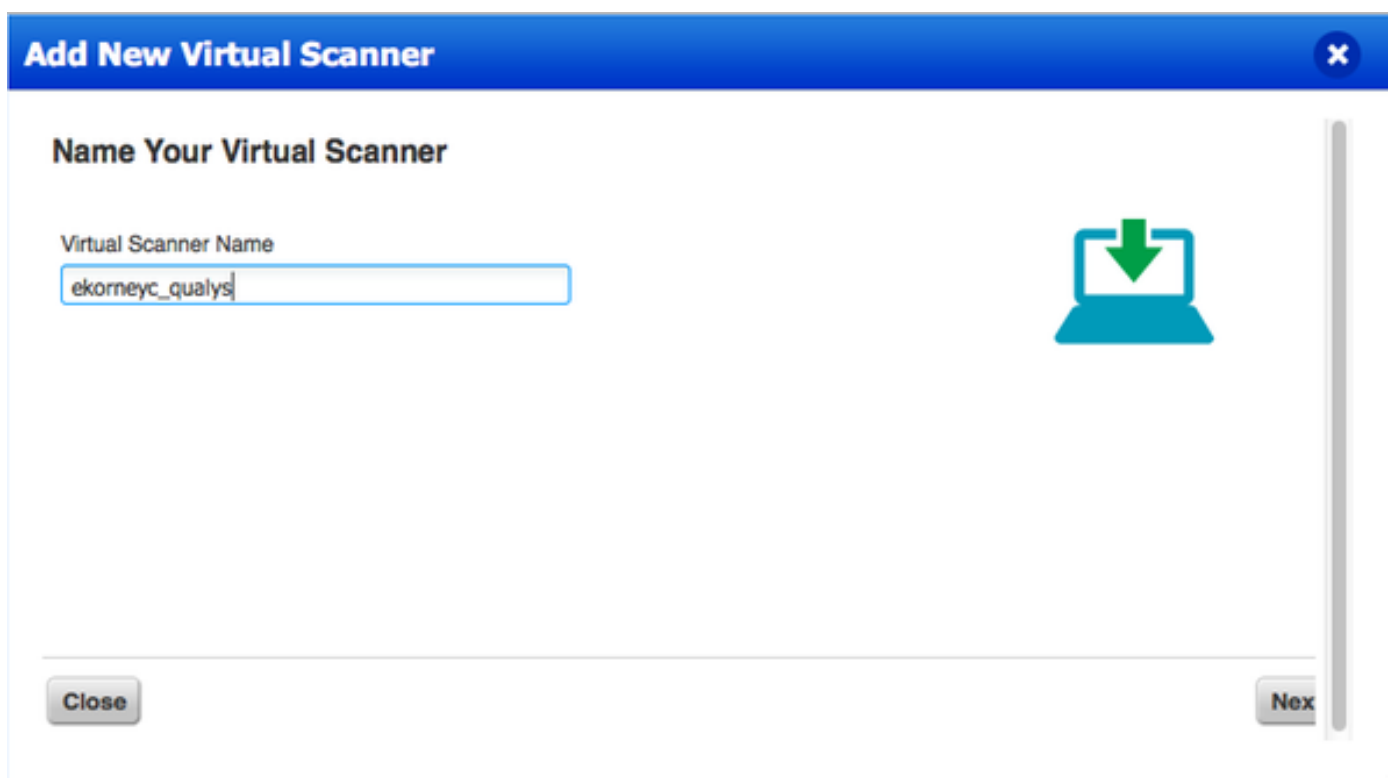
O varredor de Qualys pode ser distribuído do arquivo dos ÓVULOS. Entre à nuvem de Qualys e navegue às varreduras > aos dispositivos e selecione o dispositivo novo > virtual do varredor



Selecione a **imagem da transferência somente** e escolha a distribuição apropriada



Para obtê-lo a código de ativação pode ir às varreduras > aos dispositivos e dispositivo novo > virtual seletor do varredor e para selecionar **eu tenho minha imagem**



Depois que dando entrada com o nome do varredor você é dado o código de autorização que você usará mais tarde.

Etapa 2. Configurar o varredor de Qualys

Distribua ÓVULOS na plataforma da virtualização de sua escolha. Uma vez que feito, configurar aqueles ajustes:

- Estabelecer a rede (o LAN)
- Ajustes da interface WAN (se você está usando duas relações)
- Ajustes do proxy (se você está usando o proxy)
- Personalize este varredor



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.

Mais tarde o varredor conecta a Qualys e transfere o software mais recente e as assinaturas.

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 >

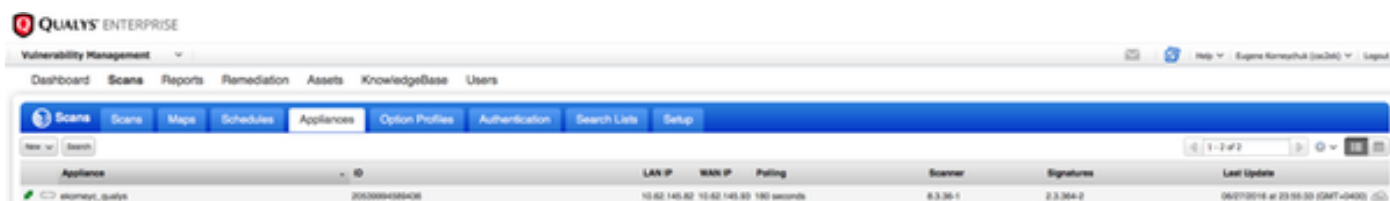
System reboot >

Version info: 3.9.7.5.11.0

Exit this menu? (Y/N)

Para verificar o varredor é-lhe conectada pode navegar às varreduras > aos dispositivos.

Esverdeie o sinal conectado à esquerda indica que o varredor está pronto, você pode igualmente ver o IP LAN, o IP de WAN, a versão do varredor e as assinaturas.

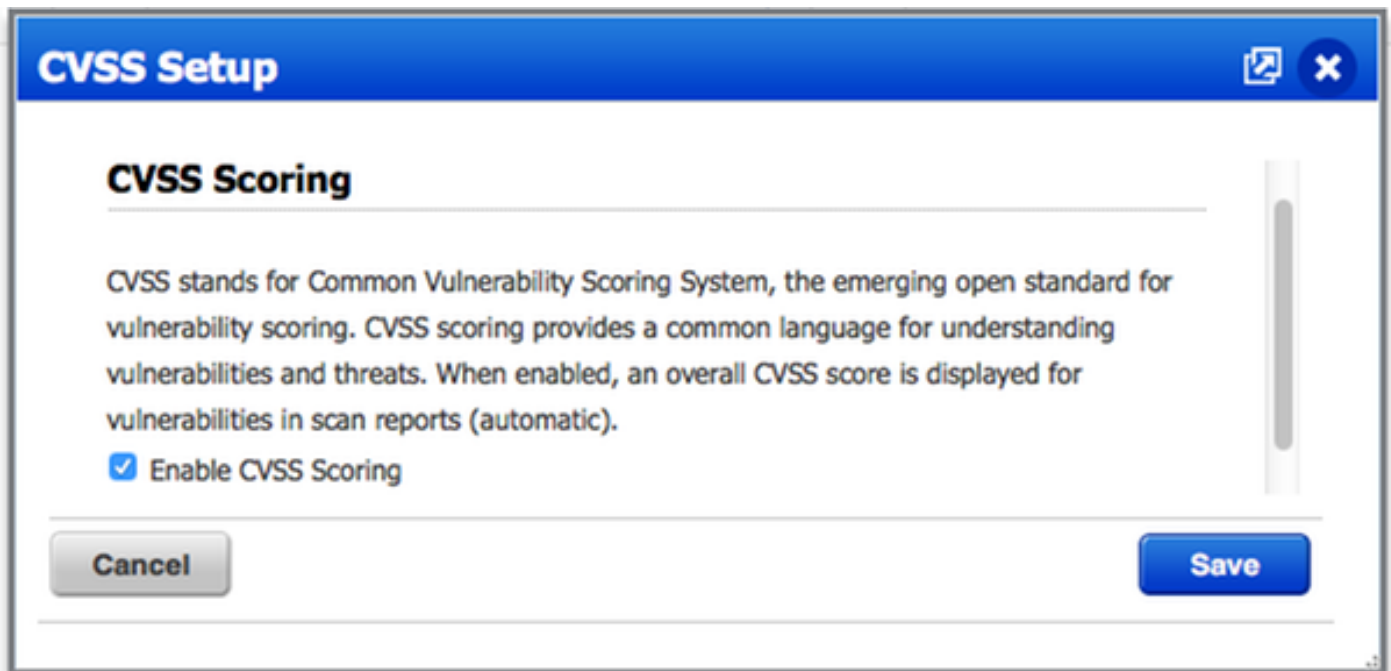


Configurar o ISE

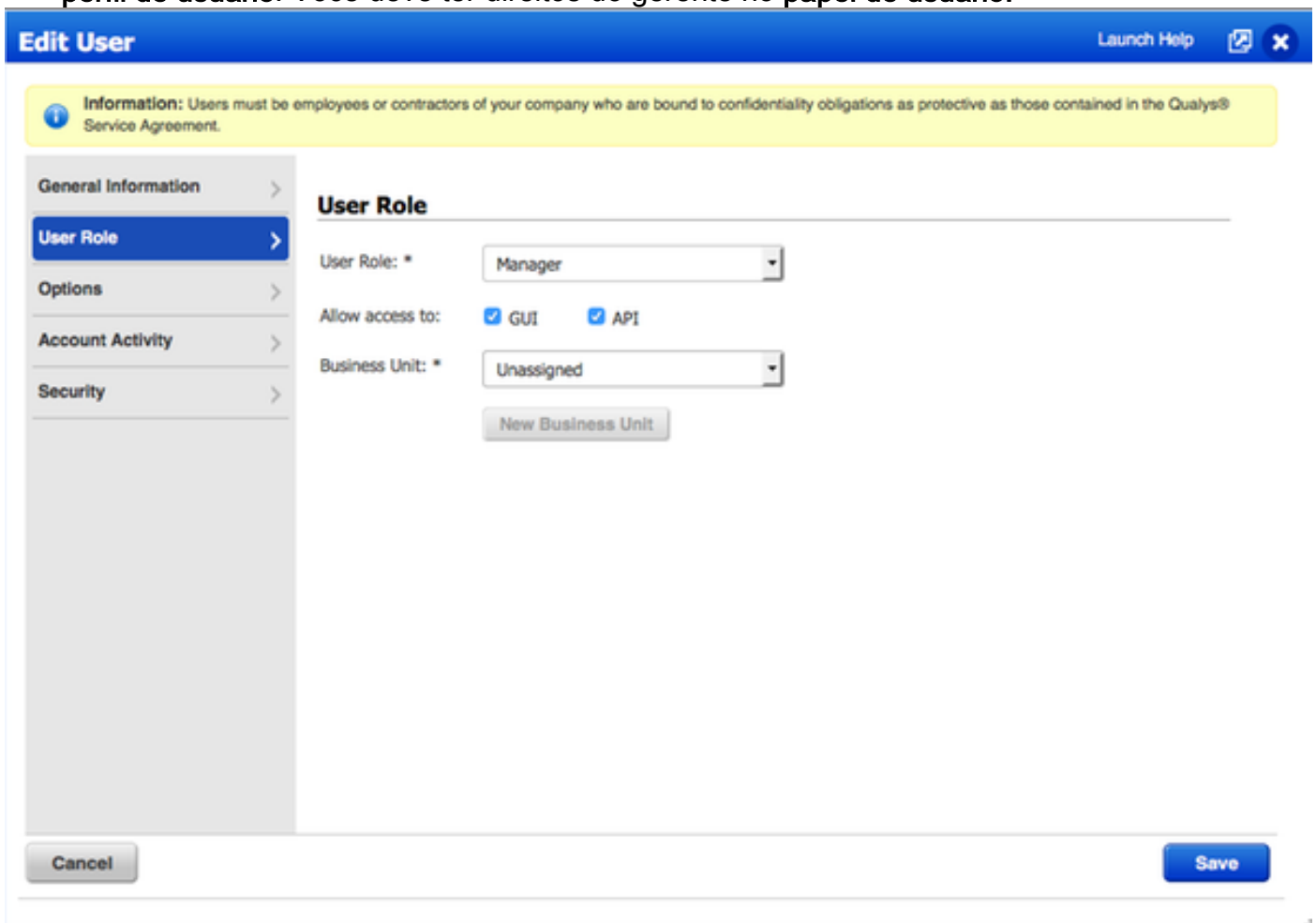
Embora você configurou o varredor e a nuvem de Qualys, você ainda tem que ajustar ajustes da nuvem para certificar-se muito bem da integração com trabalhos ISE. Note, ele deve ser feito antes que você configure o adaptador com o GUI, porque a base de conhecimentos que contém marcar CVSS está transferida depois que o adaptador é configurado pela primeira vez.

Etapa 1. Ajustes da nuvem de Qualys do acordo para a integração com ISE

- Permita CVSS que marca no Gerenciamento > nos relatórios da vulnerabilidade > Setup > CVSS > permitem marcar CVSS



- Assegure-se de que as credenciais do usuário usadas na configuração de adaptador tenham privilégios do gerente. Selecione seu usuário do canto superior esquerdo e clique sobre o **perfil de usuário**. Você deve ter direitos do gerente no **papel de usuário**.



- Assegure-se de que os IP address/sub-redes dos valores-limite que exigem a avaliação da vulnerabilidade estejam adicionados a Qualys no Gerenciamento da vulnerabilidade > nos ativos > nos ativos do host > novo > anfitriões 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: *

Add to Policy Compliance Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel Add

Etapa 2. Permita serviços TC-NAC

Permita serviços TC-NAC sob a administração > o desenvolvimento > editam o nó. A verificação permite a caixa de seleção céntrica do serviço da ameaça NAC.

Nota: Pode haver somente um nó TC-NAC pelo desenvolvimento.

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

Etapa 3. Configurar a Conectividade do adaptador de Qualys à estrutura ISE VA

Navegue à administração > à ameaça céntricas NAC > > Add dos fornecedores de terceira parte. Clique sobre a **salvaguarda**.

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 *

Quando as transições do exemplo de Qualys a se **aprontar para configurar** o estado, clicarem sobre **pronto para configurar** a opção no estado.

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

O host do RESTO API deve ser esse que você se usa para a nuvem de Qualys, onde sua conta é encontrada. Neste exemplo - qualysguard.qg2.apps.qualys.com

A conta deve ser essa com privilégios do gerente, clica sobre **em seguida**.

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.

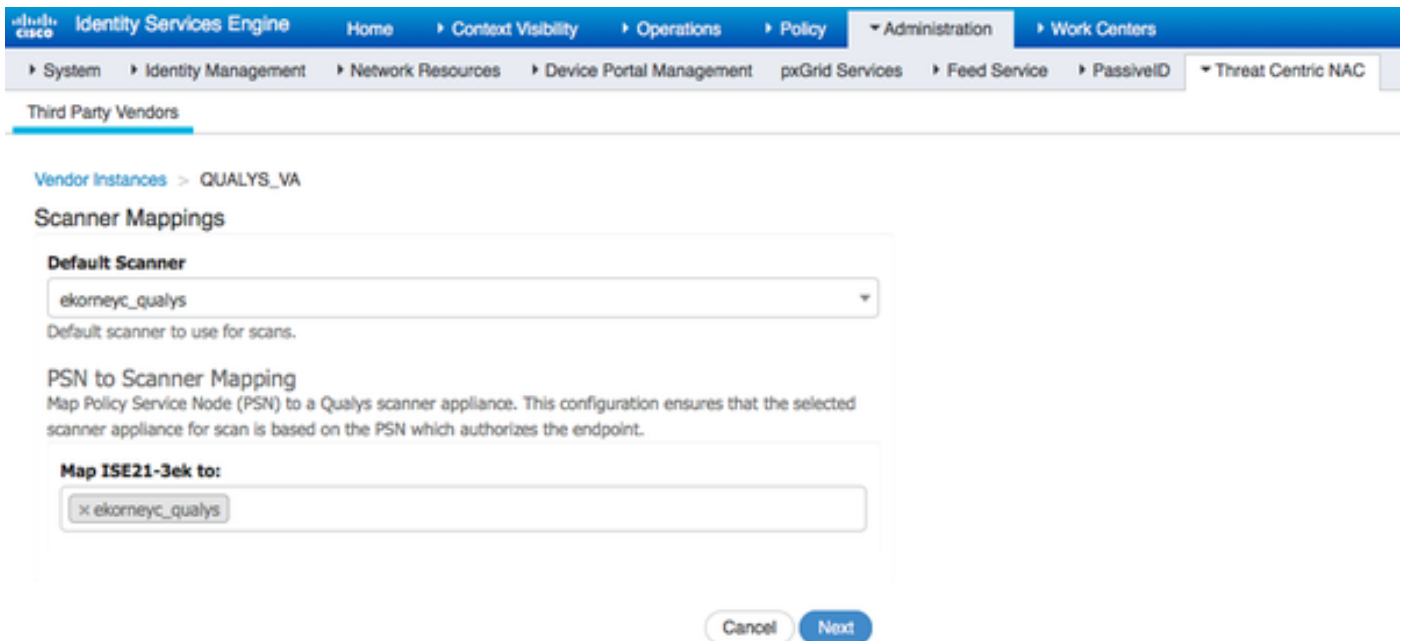
HTTP Proxy Host

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

HTTP Proxy Port

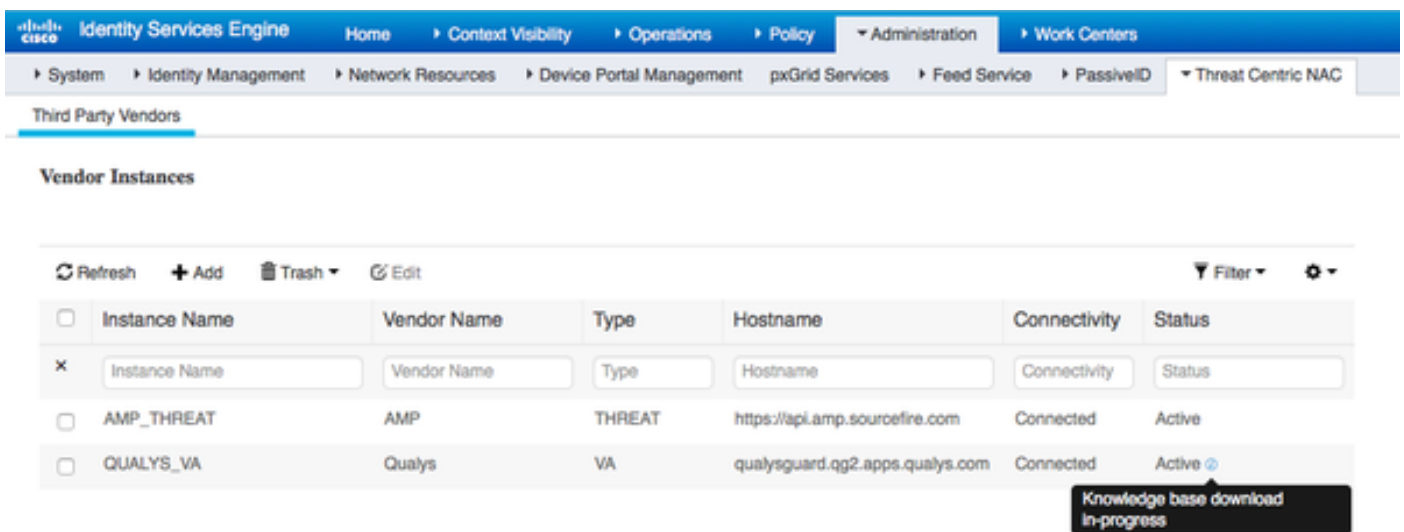
 Optional HTTP Proxy Port. Requires proxy host also to be set.

O ISE transfere a informação sobre os varredores que são conectados à nuvem de Qualys, você pode configurar o PSN ao mapeamento do varredor nesta página. Assegura-se de que o varredor selecionado esteja escolhido com base no PSN que autoriza o valor-limite.



Os ajustes avançados são bem documentados no guia Admin do 2.1 ISE, relação podem ser encontrados na seção de referências deste original. Clique sobre **em seguida e termine**. Transições do exemplo de Qualys aos começos da transferência do estado **ativo** e da base de conhecimento.

Nota: Pode haver somente um exemplo de Qualys pelo desenvolvimento.



Etapa 4. Configurar o perfil da autorização para provocar a varredura VA

Navegue à política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização. Adicionar o perfil novo. Sob **tarefas comuns** selecione a caixa de seleção da **avaliação da vulnerabilidade**.

O intervalo por encomenda da varredura deve ser selecionado de acordo com seu projeto de rede.

O perfil da autorização contém aqueles 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

São enviados aos dispositivos de rede dentro do pacote de aceitação acesso, embora o propósito real deles seja dizer o nó MNT que a varredura deve ser provocada. O MNT instrui o nó TC-NAC para comunicar-se com a nuvem de Qualys.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a new Authorization Profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with 'Authorization' expanded, containing 'Authorization Profiles', 'Downloadable ACLs', 'Profiling', 'Posture', and 'Client Provisioning'. The main content area is titled 'Authorization Profiles > New Authorization Profile' and 'Authorization Profile'. The form fields are: * Name: VA_Scan; Description: (empty); * Access Type: ACCESS_ACCEPT; Network Device Profile: Cisco; Service Template: (unchecked); Track Movement: (unchecked); Passive Identity Tracking: (unchecked). Below this is a 'Common Tasks' section with 'Assess Vulnerabilities' checked. Underneath, 'Adapter Instance' is set to QUALYS_VA and 'Trigger scan if the time since last scan is greater than' is set to 48 hours. A note says 'Enter value in hours (1-9999)'. There is also an unchecked checkbox for 'Assess periodically using above interval'.

Etapa 5. Configurar políticas da autorização

- Configurar a política da autorização para usar o perfil novo da autorização configurado em etapa 4. navegam à política > à autorização > à política da autorização, encontram a regra de **Basic_Authenticated_Access** e clicam sobre **Edit**. Mude as permissões de **PermitAccess** ao **VA_Scan padrão** recém-criado. Isto causa uma varredura da vulnerabilidade para todos os usuários. Clique sobre a **salv guarda**.
- Crie a política da autorização para máquinas Quarantined. Navegue à política > à autorização > à política > às exceções da autorização e crie uma **regra da exceção**. Clique sobre circunstâncias > criam a condição nova (opção avançada) > atributo seletor, enrolam para baixo e selecionam a **ameaça**. Expanda o atributo da **ameaça** e selecione **Qualys-CVSS_Base_Score**. Mude o operador a **maior do que** e incorpore um valor de acordo com sua política de segurança. O perfil da autorização da **quarentena** deve dar acesso limitado à máquina vulnerável.

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

Verificar

[Identity Services Engine](#)

A primeira varredura VA dos disparadores da conexão. Quando a varredura é terminada, o Reauthentication CoA está provocado para aplicar a política nova se é combinado.

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

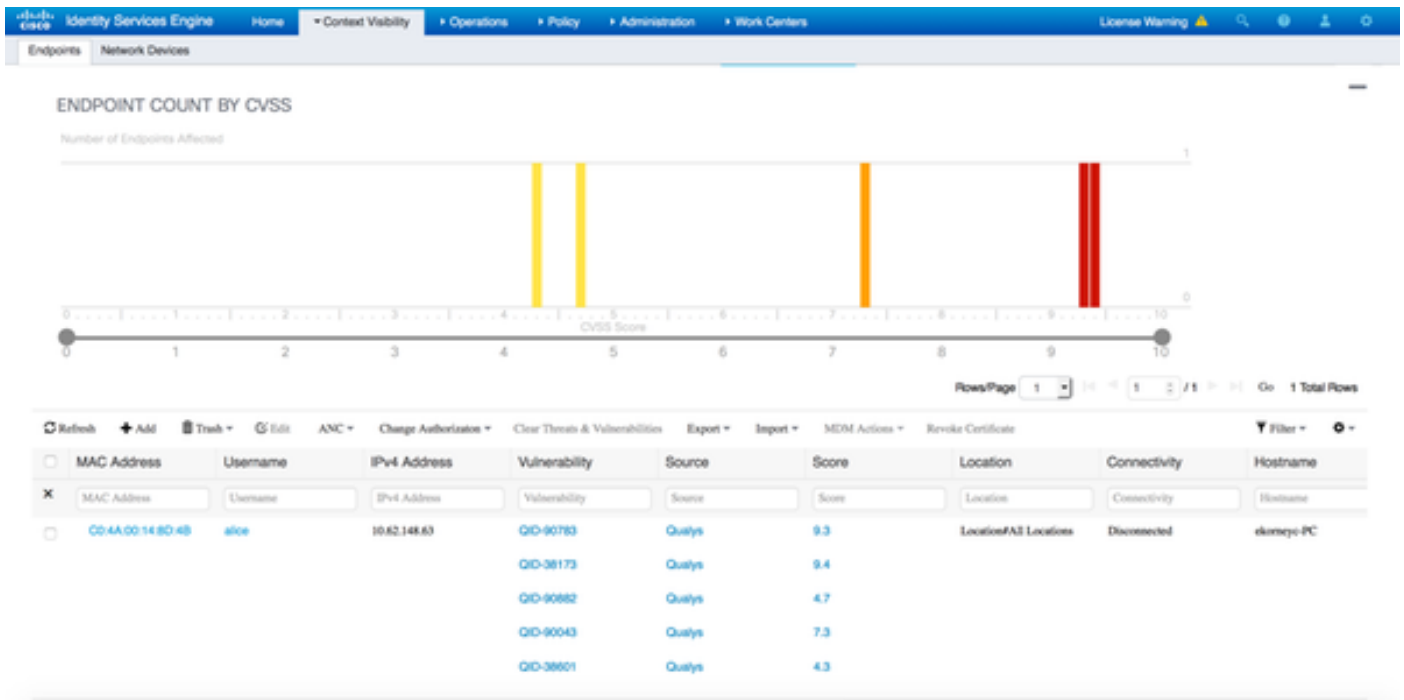
RADIUS TC-MAC Live Logs TACACS Reports Troubleshoot Adaptive Network Control

Live Logs Live Sessions

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

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
Jun 28, 2016 07:25:10:971 PM	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

A fim verificar que vulnerabilidades foram detectadas, navegue à visibilidade do contexto > aos valores-limite. Verifique por vulnerabilidades dos valores-limite com as contagens dadas a ele por Qualys.



Ao selecionar o ponto final particular, mais detalhes sobre cada vulnerabilidade aparecem, incluindo o título e os 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:

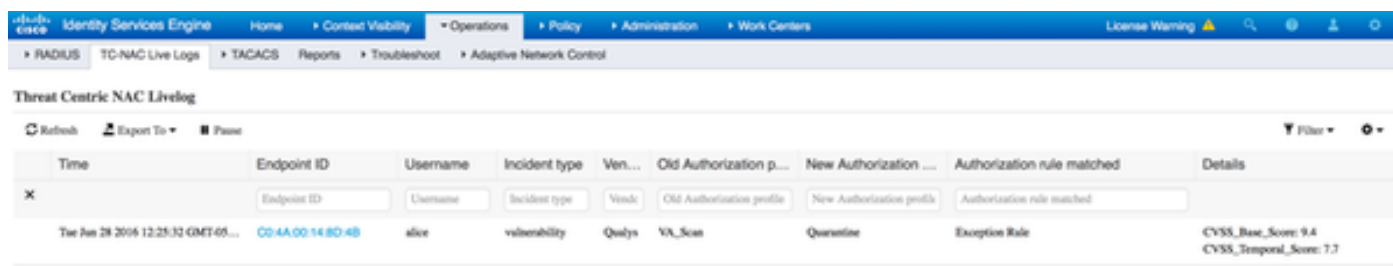
- Title:** Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- CVSS score:** 9.3
- CVEIDS:** CVE-2012-0002, CVE-2012-0152,
- Reported by:** Qualys
- Reported at:**

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:**

Nas operações > no TC-NAC vivem os logs, você pode ver velho contra as políticas novas da autorização aplicadas e os detalhes em CVSS_Base_Score.

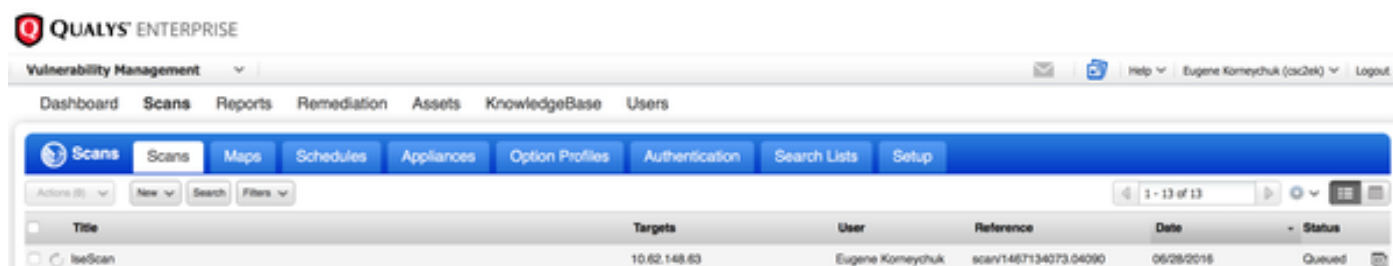
Nota: As condições da autorização são feitas com base em CVSS_Base_Score, que os iguais à contagem a mais alta da vulnerabilidade detectaram no valor-limite.



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 Rate	CVSS_Base_Score: 9.4 CVSS_Temporal_Score: 7.7

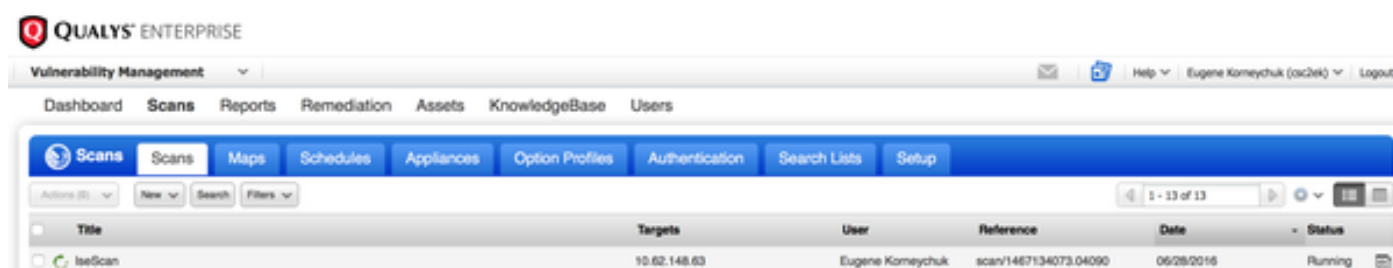
Nuvem de Qualys

Quando a varredura VA é provocada por TC-NAC Qualys enfileira a varredura, ele pode ser visto em varreduras > em varreduras



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

Mais tarde transições a ser executado, significando a nuvem de Qualys instruiu o varredor de Qualys para executar a exploração real



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

Quando o varredor executar a varredura, você deve ver a “exploração...” sinal no canto superior direito do protetor de Qualys

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

A varredura é-o feita uma vez transições ao estado terminado. Você pode ver resultados em varreduras > em varreduras, varredura exigida seleta e clicar sobre o **sumário da vista** ou os **resultados da vista**.

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 (sc2bk) | 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	

No relatório próprio você pode ver os **resultados detalhados**, onde as vulnerabilidades detectadas são mostradas.

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

Debuga no ISE

A fim permitir debuga no ISE navegam à administração > ao sistema > registrando > debugam a configuração do log, nó seletor TC-NAC e mudam o va-**Runtime do nível do log** e o componente do va-**serviço PARA DEBUGAR**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassivelD, Threat Centric NAC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The 'Logging' section is expanded, and the 'Debug Level Configuration' page is displayed for the 'va' component. The page shows a table with columns for Component Name, Log Level, and Description. The 'va' component is selected, and the log level is set to 'DEBUG'. The description for 'va' is 'Vulnerability Assessment Runtime messages'.

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

Logs a ser verificados - varuntime.log. Você pode atá-lo diretamente de ISE CLI:

Cauda de registro de varuntime.log do aplicativo da mostra ISE21-3ek/admin#

Instrução recebida estivador TC-NAC para executar a varredura para o ponto final particular.

```
2016-06-28 19:06:30,823 DEBUGAM [Thread-70][ ] va.runtime.admin.mnt.EndpointFileReader -::: :-
VA: Leia o tempo de execução 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 19:06:30,824 DEBUGAM [Thread-70][ ]
va.runtime.admin.vaservice.VaServiceRemotingHandler -::: :- VA: dados recebidos do 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}
```

Uma vez que o resultado é recebido armazena todos os dados da vulnerabilidade no diretório do contexto.

```
2016-06-28 19:25:02,020 DEBUGAM [pool-311-thread-8][  
va.runtime.admin.vaservice.VaServiceMessageListener -:::: :- mensagem recebida de VaService:  
Vulnerabilidade remota da execução de código do protocolo do Desktop remoto de Windows do  
[{"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 do MS12-020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveIds": "", "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityTitle": "SSL - assinatura falhada do Allowed", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB do método de criptografia fraca do protocolo do Desktop remoto de Vulnerability", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "vulnerabilityTitle": "Windows da verificação de assinatura desabilitada ou SMB que assina não o uso do Required", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566, CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS da cifra RC4 fraca", "vulnerabilityVendor": "Qualys"}]]
```

```
2016-06-28 19:25:02,127 DEBUGAM [pool-311-thread-8][  
va.runtime.admin.vaservice.VaServiceMessageListener -:::: :- VA: Salvar ao DB do contexto,  
lastscantime: 1467134394000, Mac: C0:4A:00:14:8D:4B  
2016-06-28 19:25:02,268 DEBUGAM [pool-311-thread-8][  
va.runtime.admin.vaservice.VaAdminServiceContext -:::: :- VA: enviando o json elástico da busca  
ao PRI-LAN
```

```
2016-06-28 19:25:02,272 DEBUGAM [pool-311-thread-8][  
va.runtime.admin.vaservice.VaPanRemotingHandler -:::: :- VA: Salvar à busca elástica:  
Vulnerabilidade remota da execução de código do protocolo do Desktop remoto de Windows do  
{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 - vulnerabilidade falhada da verificação de assinatura", "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 desabilitada ou SMB que assina não exigido", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566, CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporalScore": "3.7", "vulnerabilityTitle": "SSL/TLS da cifra RC4 fraca", "vulnerabilityVendor": "Qualys"}]]
```

Logs a ser verificados - vaservice.log. Você pode até-lo diretamente de ISE CLI:

```
Cauda de registro de vaservice.log do aplicativo da mostra ISE21-3ek/admin#
```

Pedido da avaliação da vulnerabilidade submetido ao adaptador

```
2016-06-28 17:07:13,200 DEBUGAM [endpointPollerScheduler-3][ cpm.va.service.util.VaServiceUtil  
-:::: :- systemMsg VA SendSyslog: Serviço da avaliação  
[{"systemMsg": "91019", "isAutoInsertSelfAcsInstance": true, "attributes": ["TC-NAC.ServiceName", "Vulnerability", "TC-NAC.Status", "pedido VA submetido ao adaptador", "TC-NAC.Details", "pedido VA submetido ao adaptador para o 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 verifica cada 5 cronometra o estado da varredura, até que esteja terminada.

```
2016-06-28 17:09:43,459 DEBUGAM [SimpleAsyncTaskExecutor-2][ ]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number dos valores-limite
enfileirados verificando resultados de varredura: 1, número de valores-limite enfileirados para
a varredura: 0, o número de valores-limite para que a varredura é em andamento: 0"}
2016-06-28 17:14:43,760 DEBUGAM [SimpleAsyncTaskExecutor-2][ ]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number dos valores-limite
enfileirados verificando resultados de varredura: 0, número de valores-limite enfileirados para
a varredura: 0, o número de valores-limite para que a varredura é em andamento: 1"}
2016-06-28 17:19:43,837 DEBUGAM [SimpleAsyncTaskExecutor-2][ ]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number dos valores-limite
enfileirados verificando resultados de varredura: 0, número de valores-limite enfileirados para
a varredura: 0, o número de valores-limite para que a varredura é em andamento: 1"}
2016-06-28 17:24:43,867 DEBUGAM [SimpleAsyncTaskExecutor-2][ ]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do adaptador:
{"AdapterInstanceName":"QUALYS_VA", "AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0", "VendorName":"Qualys", "OperationMessageText":"Number dos valores-limite
enfileirados verificando resultados de varredura: 0, número de valores-limite enfileirados para
a varredura: 0, o número de valores-limite para que a varredura é em andamento: 1"}
```

O adaptador é obtém QID, CVE junto com as contagens CVSS

```
2016-06-28 17:24:57,556 DEBUGAM [SimpleAsyncTaskExecutor-2][ ]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do adaptador: Certificado do
{"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 -
Assinatura falhada do Vulnerability", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90043", "cveIds":"","cvssBaseScore":"7.3", "cvssTemporalScore":"6.3", "vulnerabilityTitle":"SMB da
verificação de assinatura desabilitada ou SMB que assina não a vulnerabilidade remota da
execução de código do protocolo do Desktop remoto de Windows do
Required", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-90783", "cveIds":"CVE-2012-
0002,CVE-2012-
0152", "cvssBaseScore":"9.3", "cvssTemporalScore":"7.7", "vulnerabilityTitle":"Microsoft (uso do
MS12-020)", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-38601", "cveIds":"CVE-2013-
2566,CVE-2015-
2808", "cvssBaseScore":"4.3", "cvssTemporalScore":"3.7", "vulnerabilityTitle":"SSL/TLS do método
de criptografia fraca fraco do protocolo do Desktop remoto do
cipher", "vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90882", "cveIds":"","cvssBaseScore":"4.7", "cvssTemporalScore":"4", "vulnerabilityTitle":"Windows
RC4 permitido", "vulnerabilityVendor":"Qualys"}]}
2016-06-28 INFORMAÇÃO [SimpleAsyncTaskExecutor-
2][ ] cpm.va.service.processor.AdapterMessageListener de 17:25:01,282 -::: :- os detalhes do
valor-limite enviados ao IRF são
{"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 DEBUGAM [endpointPollerScheduler-2][ ] cpm.va.service.util.VaServiceUtil
-::: :- systemMsg VA SendSyslog: Serviço da avaliação
[{"systemMsg":"91019", "isAutoInsertSelfAcsInstance":true, "attributes":{"TC-
NAC.ServiceName", "Vulnerability", "TC-NAC.Status", "VA terminado com sucesso", "TC-NAC.Details",
```

```
"VA terminado; 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" ]}]
```

Edições típicas

A edição 1. ISE obtém o relatório da vulnerabilidade com o CVSS_Base_Score de 0.0 e o CVSS_Temporal_Score de 0.0, quando o relatório da nuvem de Qualys contiver as vulnerabilidades detectadas.

Problema:

Quando verificar o relatório da nuvem que de Qualys você pode ver detectou vulnerabilidades, porém no ISE você não as vê.

Debuga visto em vaservice.log:

```
2016-06-02 INFORMAÇÃO [SimpleAsyncTaskExecutor-
2][[] cpm.va.service.processor.AdapterMessageListener de 08:30:10,323 -::: :- os detalhes do
valor-limite enviados ao IRF são
{"C0:4A:00:15:75:C8": [{"vulnerability": {"CVSS_Base_Score": 0.0, "CVSS_Temporal_Score": 0.0}, "time-
stamp": 1464855905000, "title": "Vulnerability", "vendor": "Qualys"}]}
```

Solução:

A razão para cvss marca ser zero é qualquer uma que não tem nenhuma vulnerabilidade ou marcar dos cvss não esteve permitido na nuvem de Qualys antes que você configure o adaptador com o UI. A base de conhecimentos que contém os cvss que marcam a característica permitida é transferida depois que o adaptador é configurado primeira vez. Você tem que assegurar-se de que marcar CVSS esteja permitido antes, exemplo do adaptador foi criado no ISE. Pode ser feito sob o Gerenciamento > os relatórios da vulnerabilidade > Setup > CVSS > permite marcar CVSS

A edição 2. ISE não obtém resultados traseiros da nuvem de Qualys, mesmo que a política correta da autorização seja batida.

Problema:

A política corrigida da autorização foi combinada, que deve provocar a varredura VA. Apesar desse fato nenhuma varredura é feita.

Debuga visto em vaservice.log:

```
2016-06-28 16:19:15,401 DEBUGAM [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do 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 16:19:15,401 DEBUGAM [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.AdapterMessageListener -::: :- mensagem do adaptador:
{"requestedMacAddress": "24:77:03:3D:CF:20", "scanStatus": "SCAN_ERROR", "scanStatusMessage": "Error
que provoca a varredura: Erro quando código de exploração e erro da trigeringon-procura como
segue 1904: nenhuns do IPs especificado são elegíveis para o Gerenciamento
scanning.", "lastScanTimeLong": 0, "ipAddress": "10.201.228.102"} da vulnerabilidade
```

```
2016-06-28 16:19:15,771 DEBUGAM [SimpleAsyncTaskExecutor-2][  
cpm.va.service.processor.AdapterMessageListener -::: :- o resultado de varredura do adaptador  
falhou para Macaddress:24:77:03:3D:CF:20, IP Address(DB): 10.201.228.102, ajustando o estado ao  
falhado  
2016-06-28 16:19:16,336 DEBUGAM [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil  
-::: :- systemMsg VA SendSyslog: Serviço da avaliação  
[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-  
NAC.ServiceName","Vulnerability", "TC-NAC.Status", "falha VA", "TC-NAC.Details", "erro que  
provoca a varredura: Erro quando código de exploração e erro por encomenda trigering como segue  
1904: nenhuns do IPs especificado são elegíveis para o 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"]}]] do Gerenciamento da  
vulnerabilidade
```

Solução:

A nuvem de Qualys indica que o IP address do valor-limite não é elegível para a exploração, assegura-se de por favor que você adicione o IP address do valor-limite ao Gerenciamento da vulnerabilidade > aos ativos > aos ativos do host > novo > anfitriões seguidos IP

Referências

- [Guia do administrador do Cisco Identity Services Engine, 2.1 da liberação](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)
- [Vídeo: 2.1 ISE com Qualys](#)
- [Documentação de Qualys](#)