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

Índice

Introdução

Este original descreve como configurar o NAC Ameaça-céntrico com o Qualys no 2.1 do Identity Services Engine (ISE). A característica céntrica 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

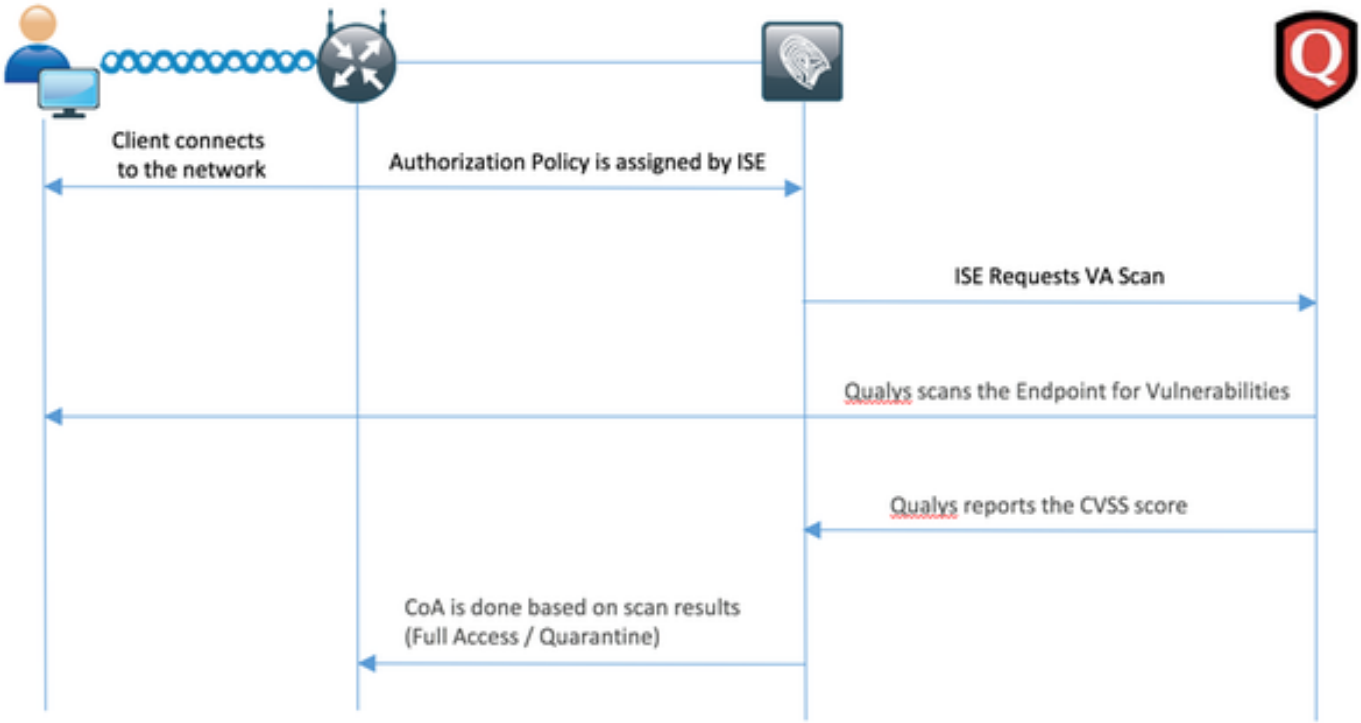
Componentes Utilizados

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

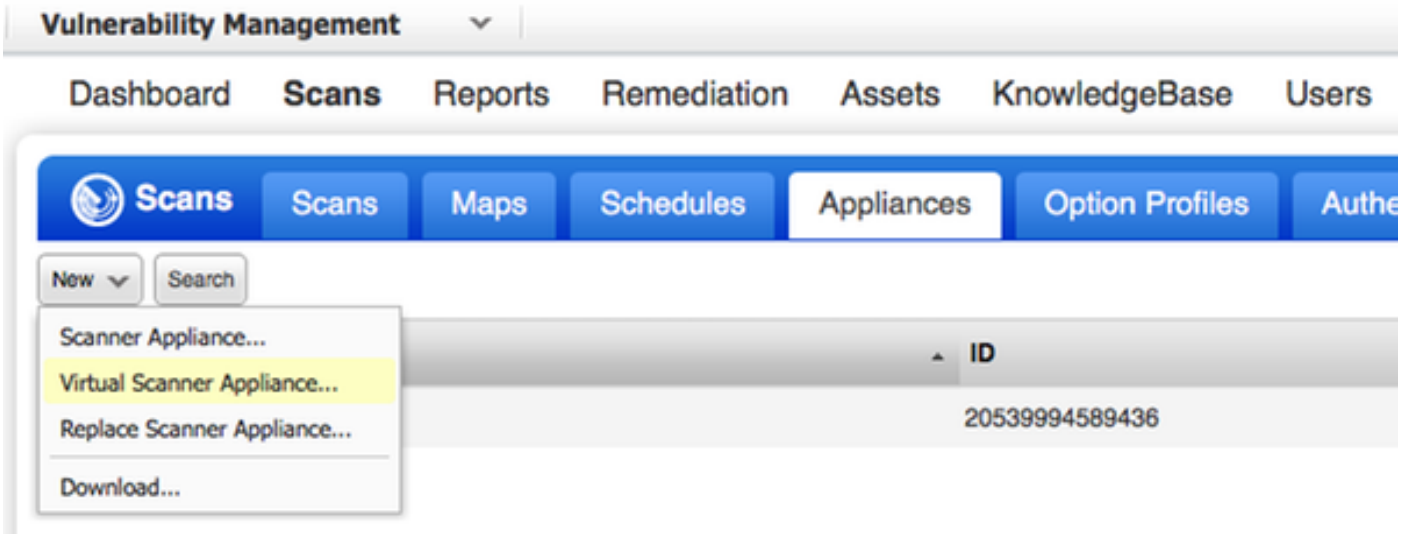
5. A nuvem de Qualys instrui o varredor de Qualys para fazer a varredura do valor-limite
6. O varredor de Qualys envia os resultados da varredura à nuvem de Qualys
7. Os resultados da varredura são enviados para trás a TC-NAC:
   - MAC address
   - Todas as contagens CVSS
   - Todas as vulnerabilidades (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

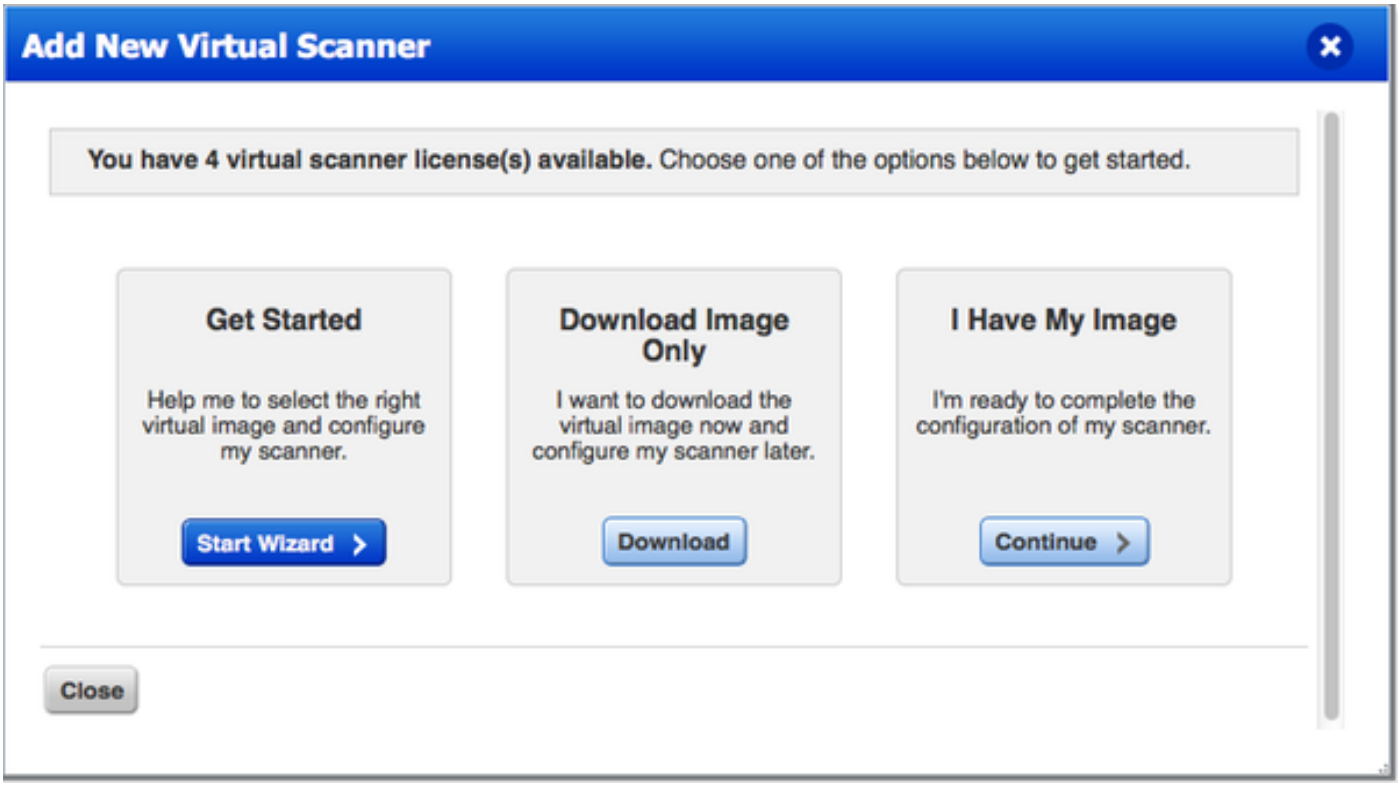
> Cuidado: A configuração de Qualys neste original é feita para as finalidades do laboratório, consulta por favor com os coordenadores de Qualys para considerações de projeto

Etapa 1. Distribua o varredor de Qualys

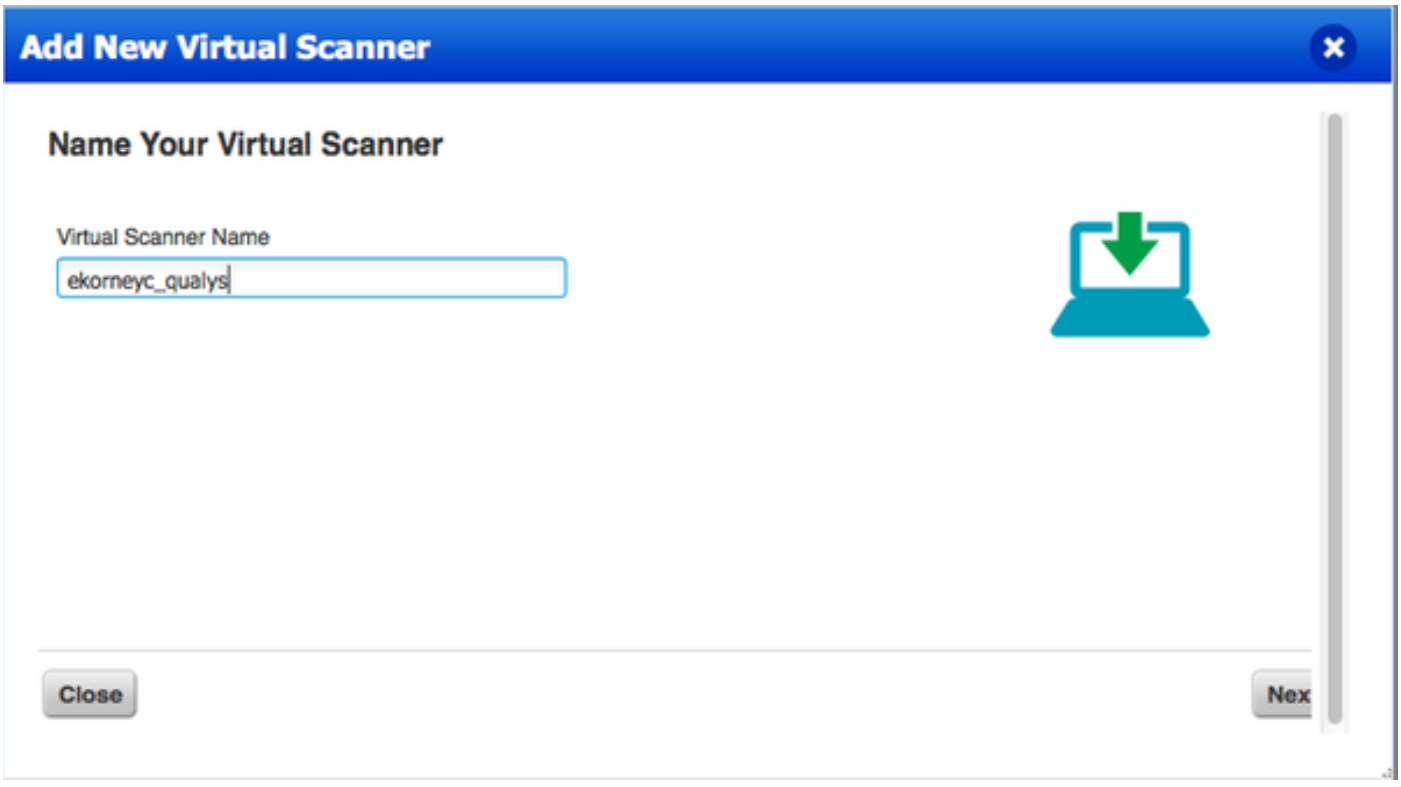
O varredor de Qualys pode ser distribuído do arquivo dos ÓVULOS. Entre à nuvem de Qualys e navegue às varreduras > aos dispositivos e selecione o dispositivo novo > virtual do varredor



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 seleto do varredor e para selecionar **eu tenho minha imagem**



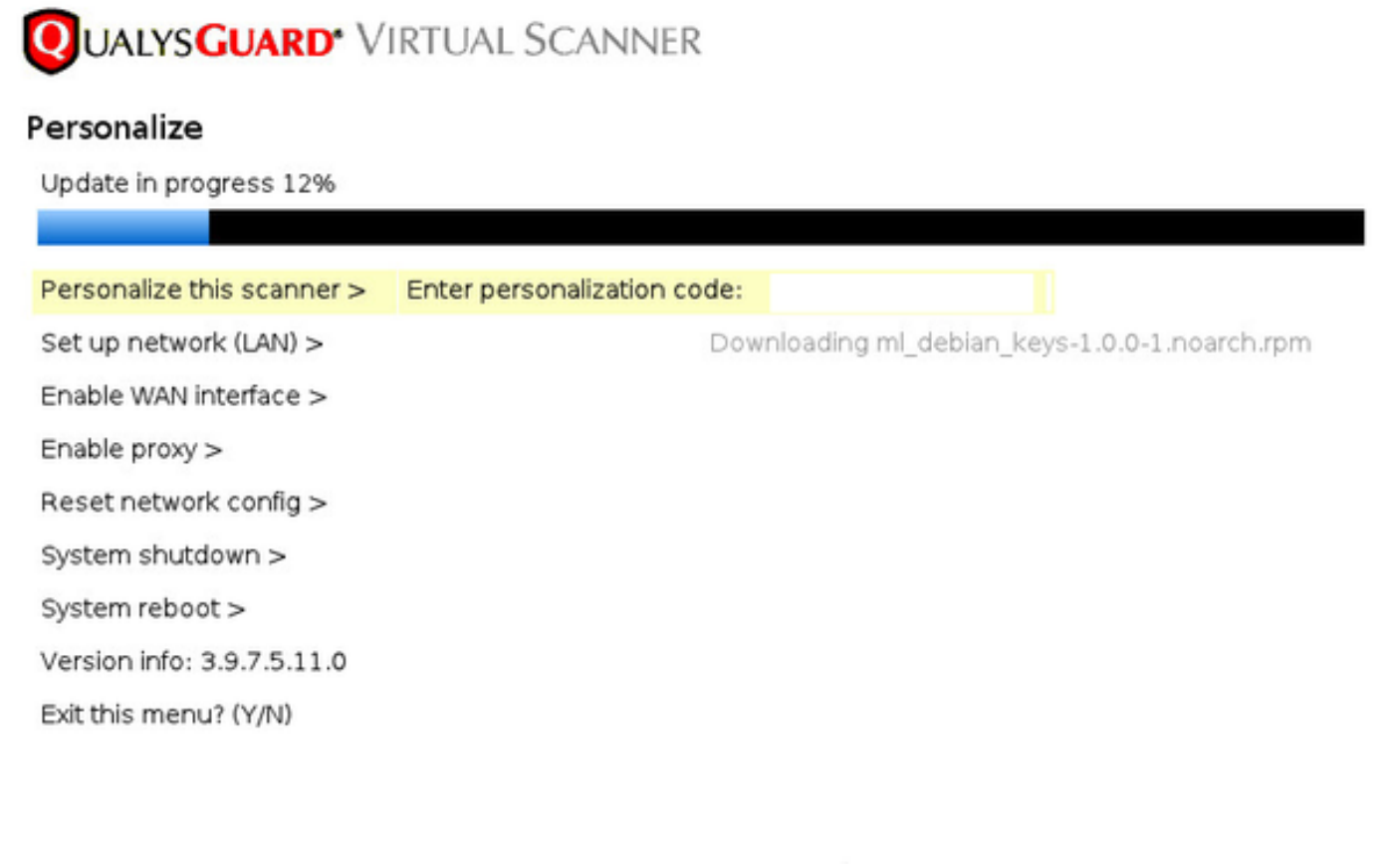
Depois que dando entrada com o nome do varredor você é dado o código de autorização que você usará mais tarde.

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

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



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

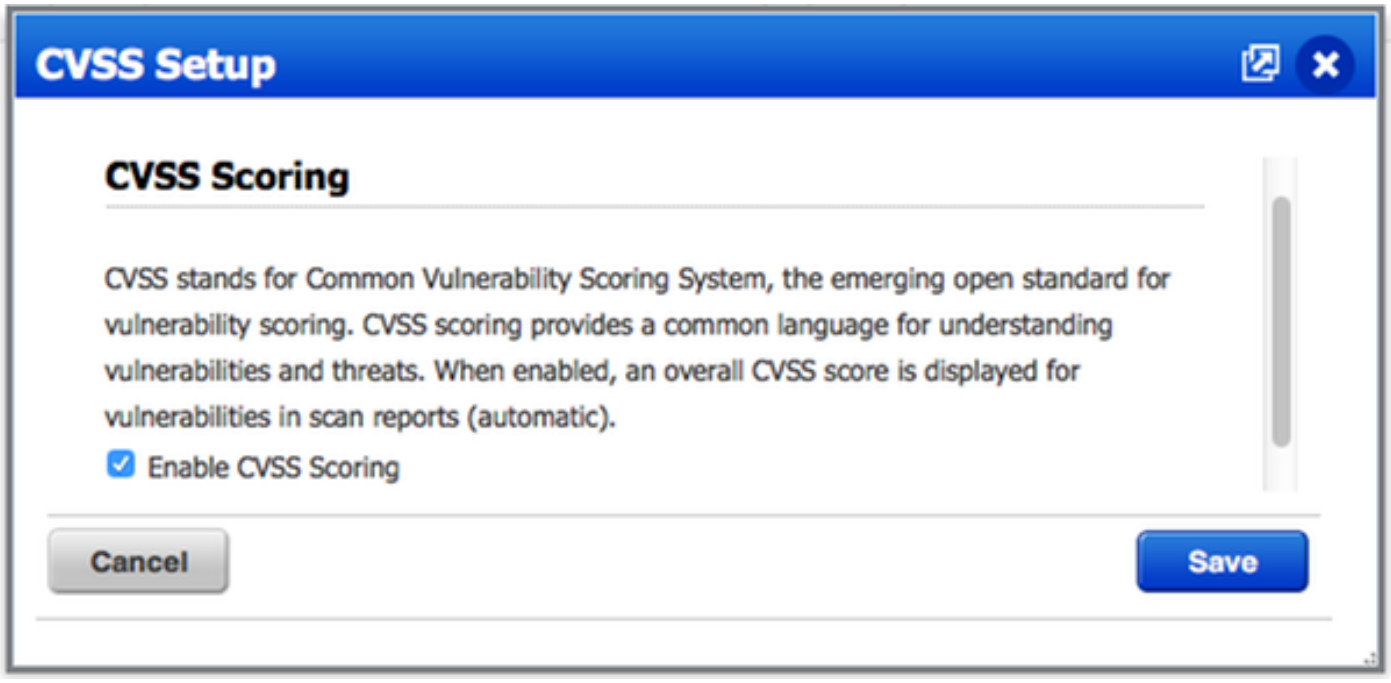
Esverdeie o sinal conectado à esquerda indica que o varredor está pronto, você pode igualmente ver o IP LAN, o IP de WAN, a versão do varredor e as assinaturas.

Configurar o ISE

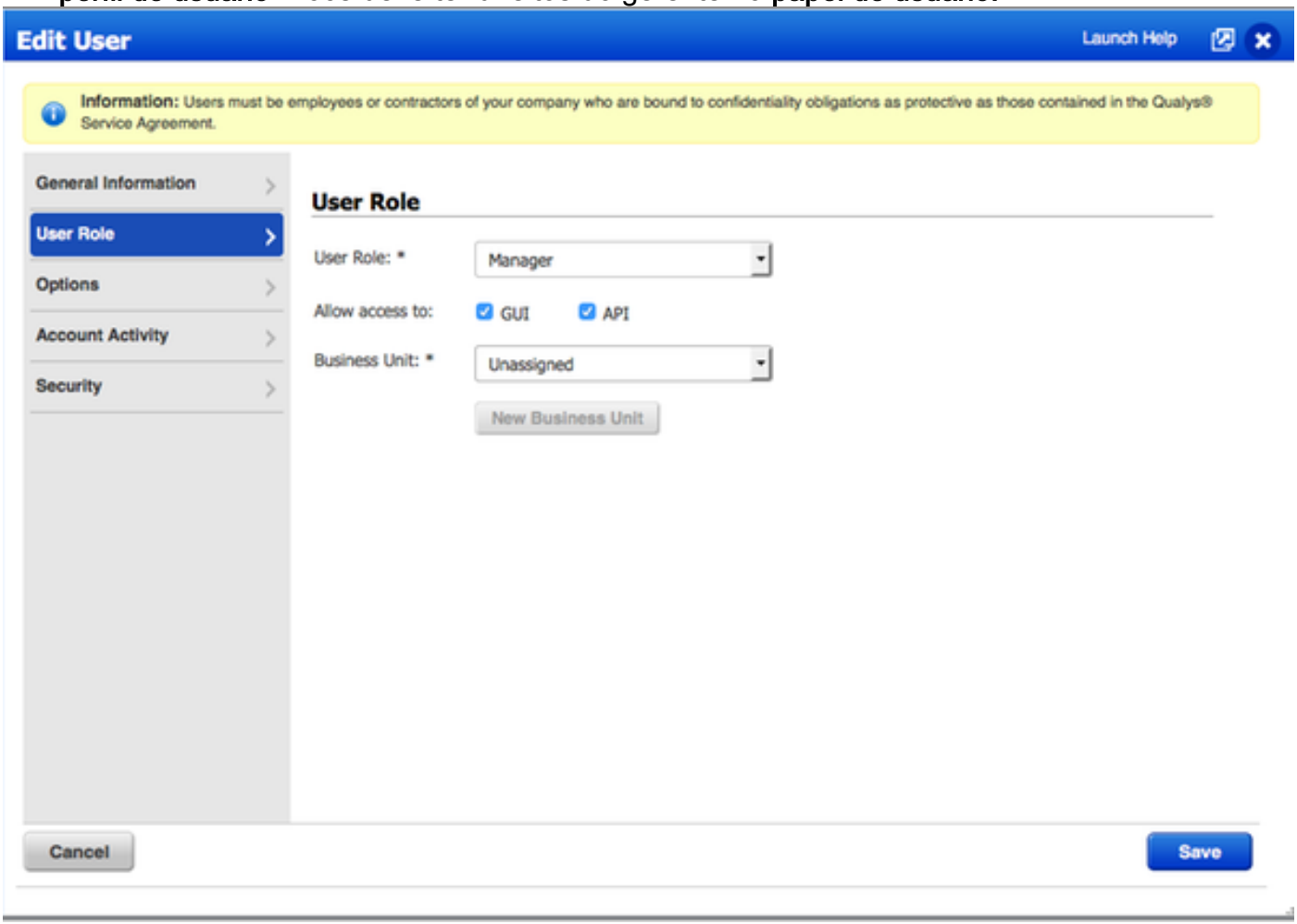
Embora você configurou o varredor e a nuvem de Qualys, você ainda tem que ajustar ajustes da nuvem para certificar-se muito bem da integração com trabalhos ISE. Note, ele deve ser feito antes que você configure o adaptador com o GUI, porque a base de conhecimentos que contém marcar CVSS está transferida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

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

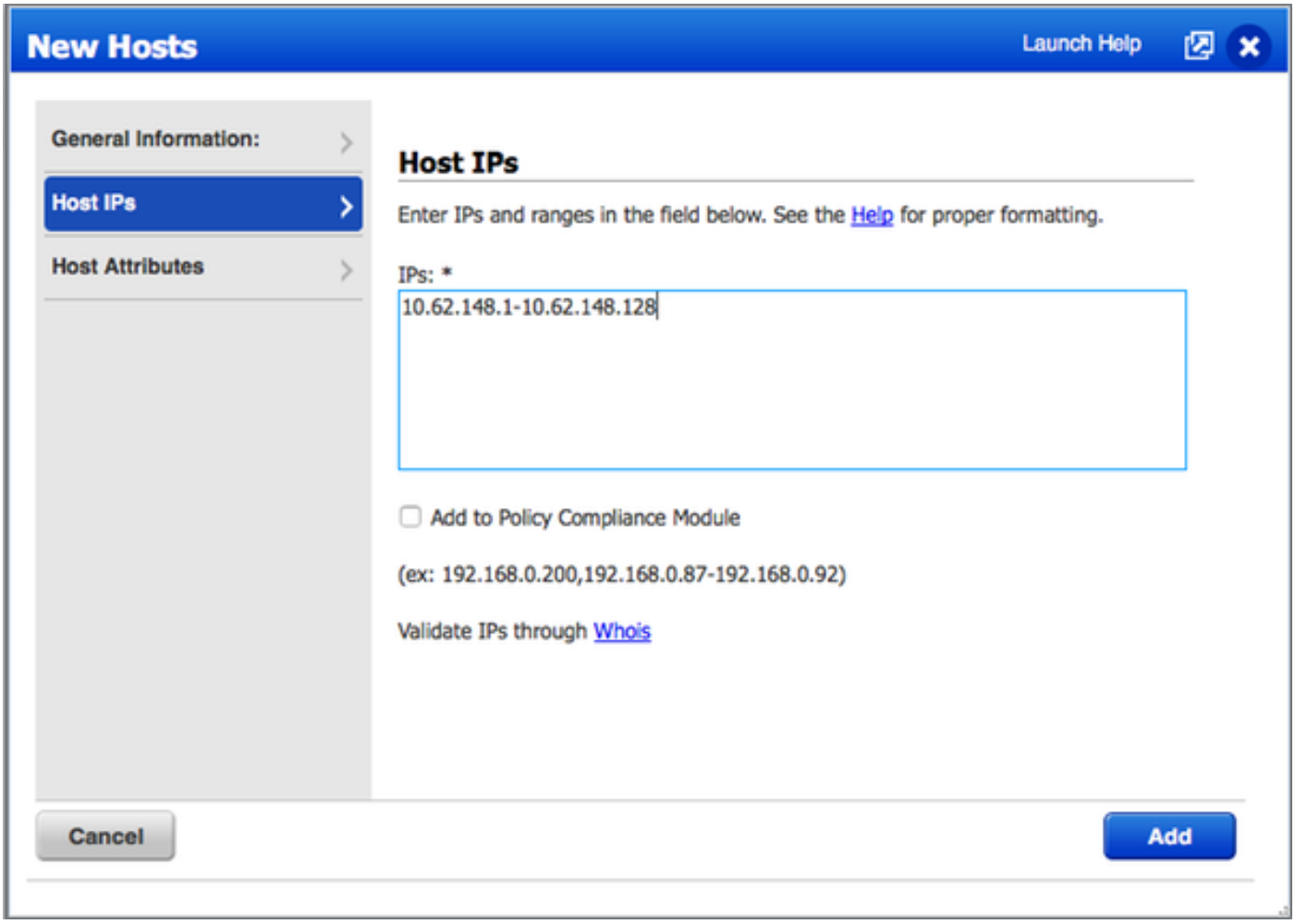
- Permita CVSS que marca no Gerenciamento > nos relatórios da vulnerabilidade > Setup > CVSS > permitem marcar CVSS



- 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.**



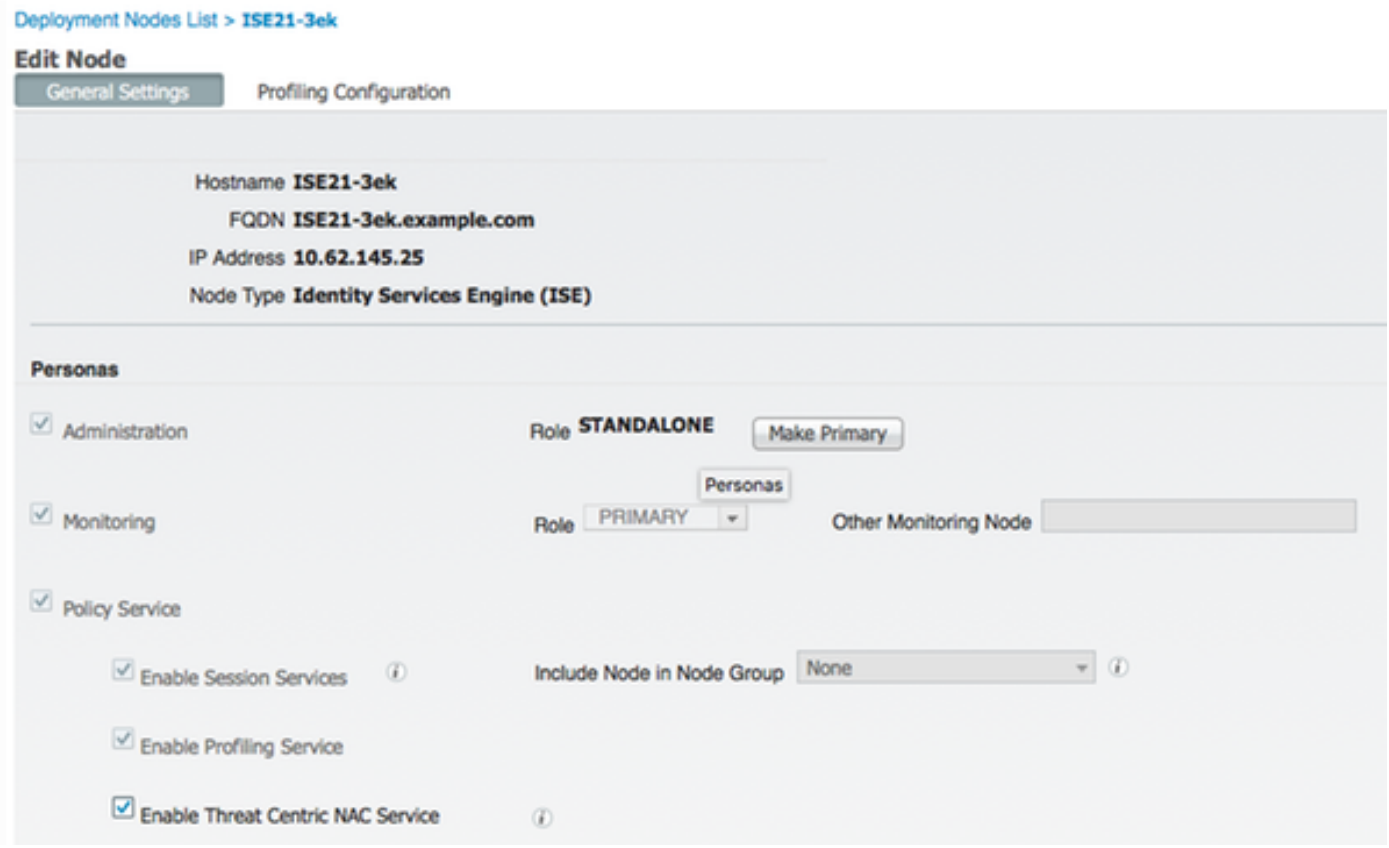
- Assegure-se de que os IP address/sub-redes dos valores-limite que exigem a avaliação da vulnerabilidade estejam adicionados a Qualys no Gerenciamento da vulnerabilidade > nos ativos > nos ativos do host > novo > anfitriões seguidos IP



Etapa 2. Permita serviços TC-NAC

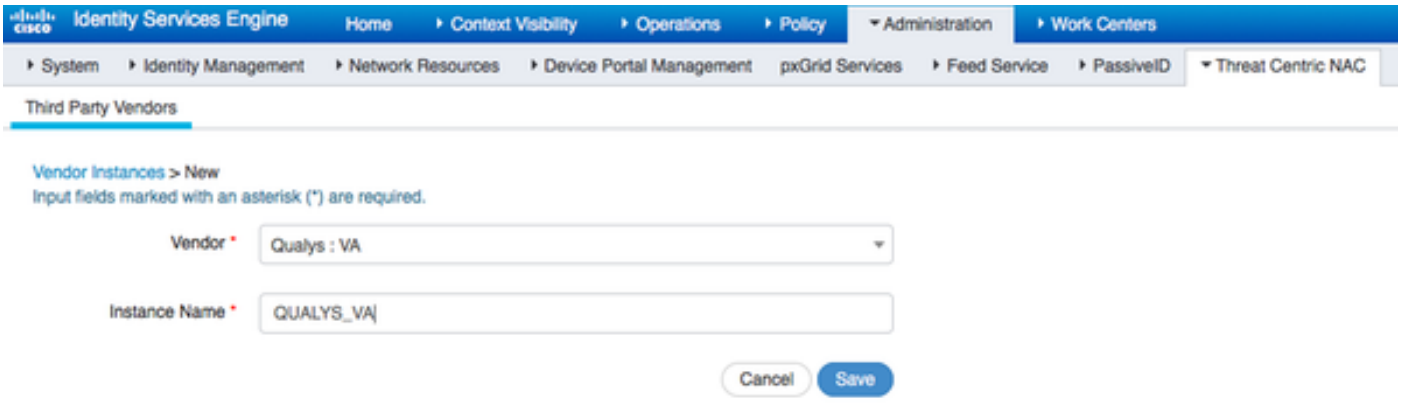
Permita serviços TC-NAC sob a administração > o desenvolvimento > editam o nó. A verificação **permite a caixa de seleção céntrica do serviço da ameaça** NAC.

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

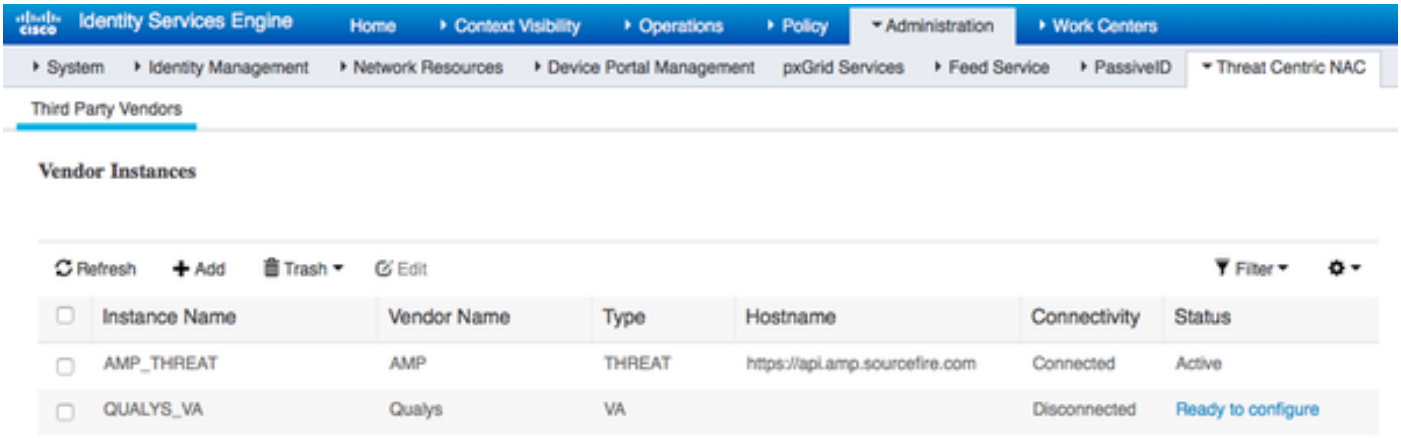


Etapa 3. Configurar a Conectividade do adaptador de Qualys à estrutura ISE VA

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

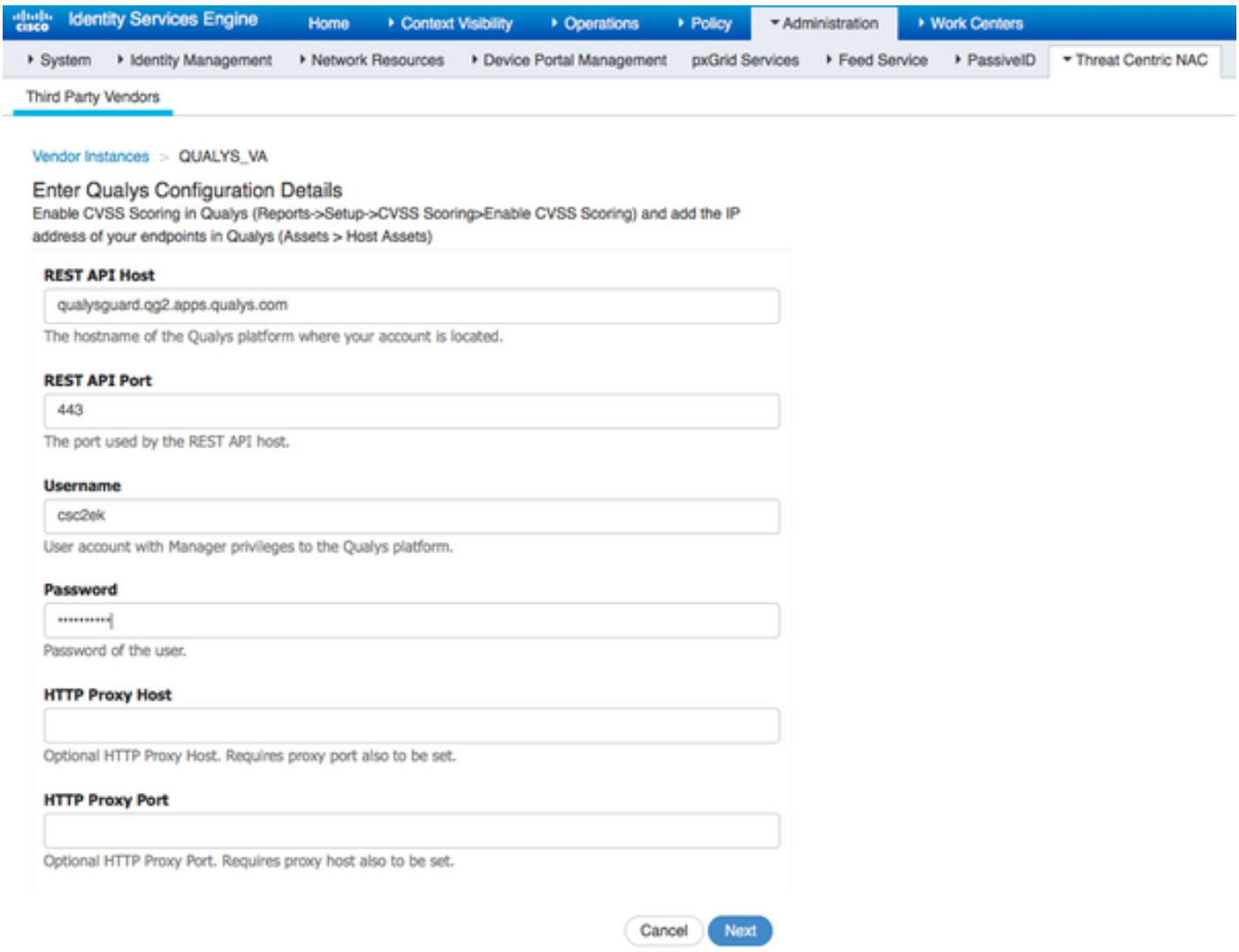


Quando as transições do exemplo de Qualys **a se aprontar para configurar o** estado, clicarem sobre **pronto para configurar a** opção no estado.

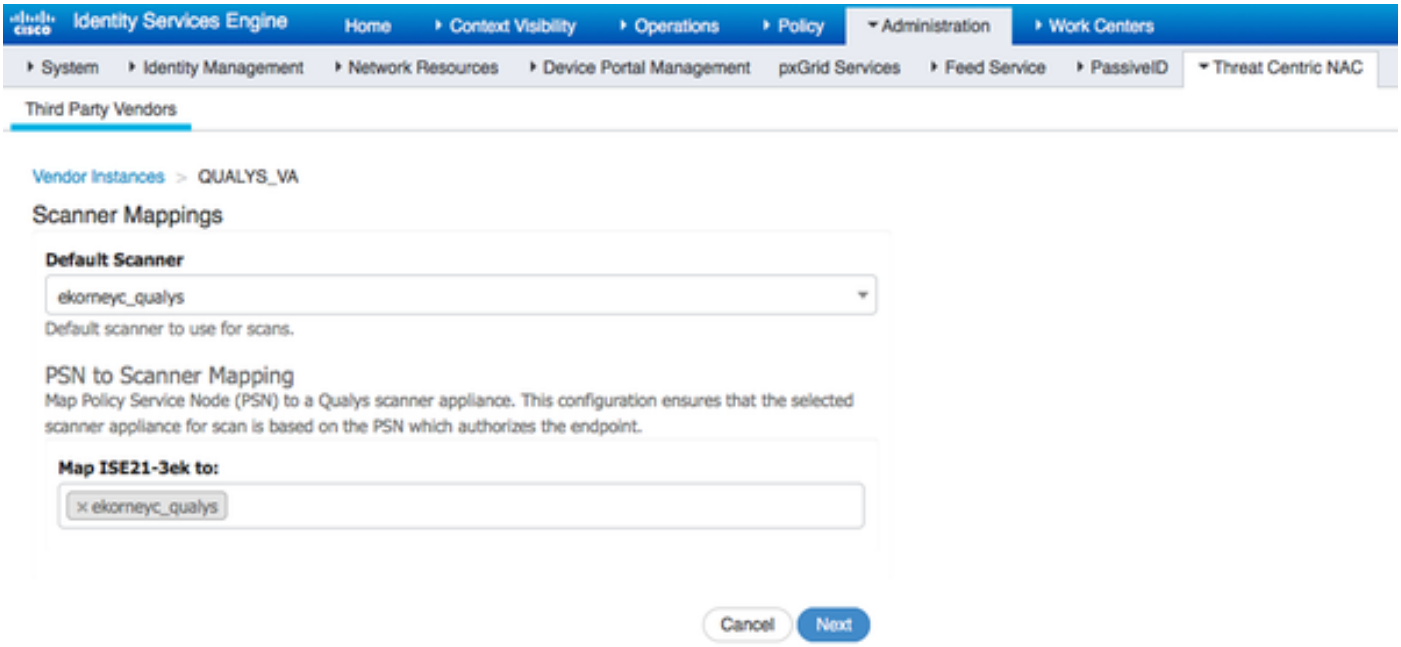


O host do RESTO API deve ser esse que você se usa para a nuvem de Qualys, onde sua conta é encontrada. Neste exemplo - qualysguard.qg2.apps.qualys.com

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

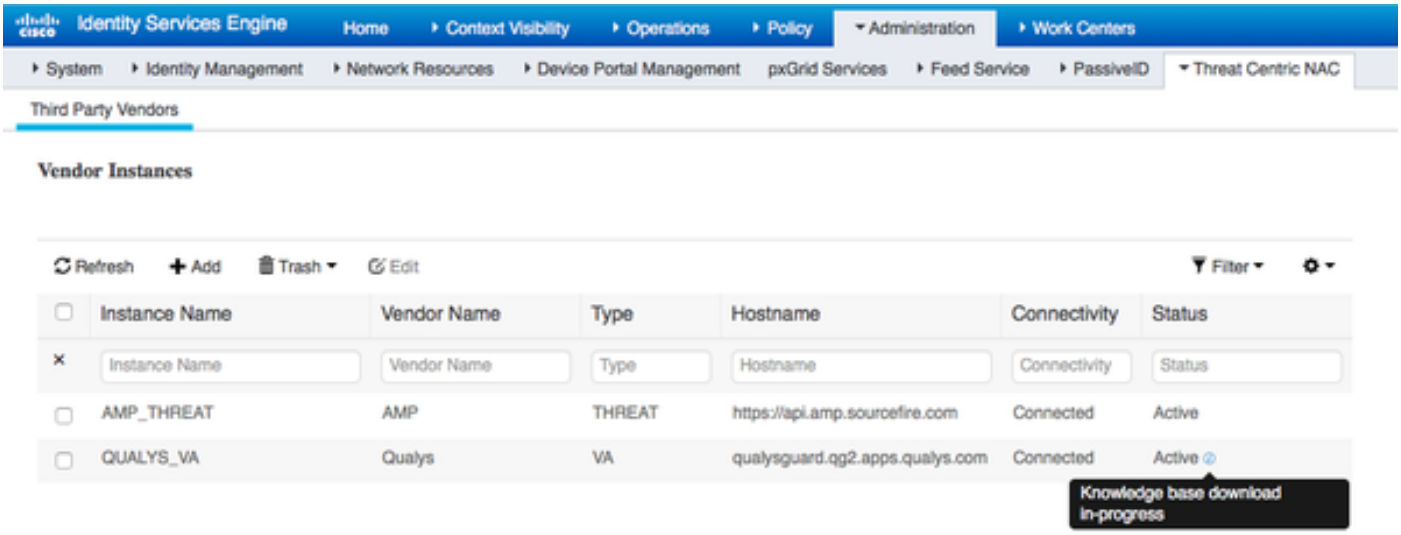


O ISE transfere a informação sobre os varredores que são conectados à nuvem de Qualys, você pode configurar o PSN ao mapeamento do varredor nesta página. Assegura-se de que o varredor selecionado esteja escolhido com base no PSN que autoriza o valor-limite.



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

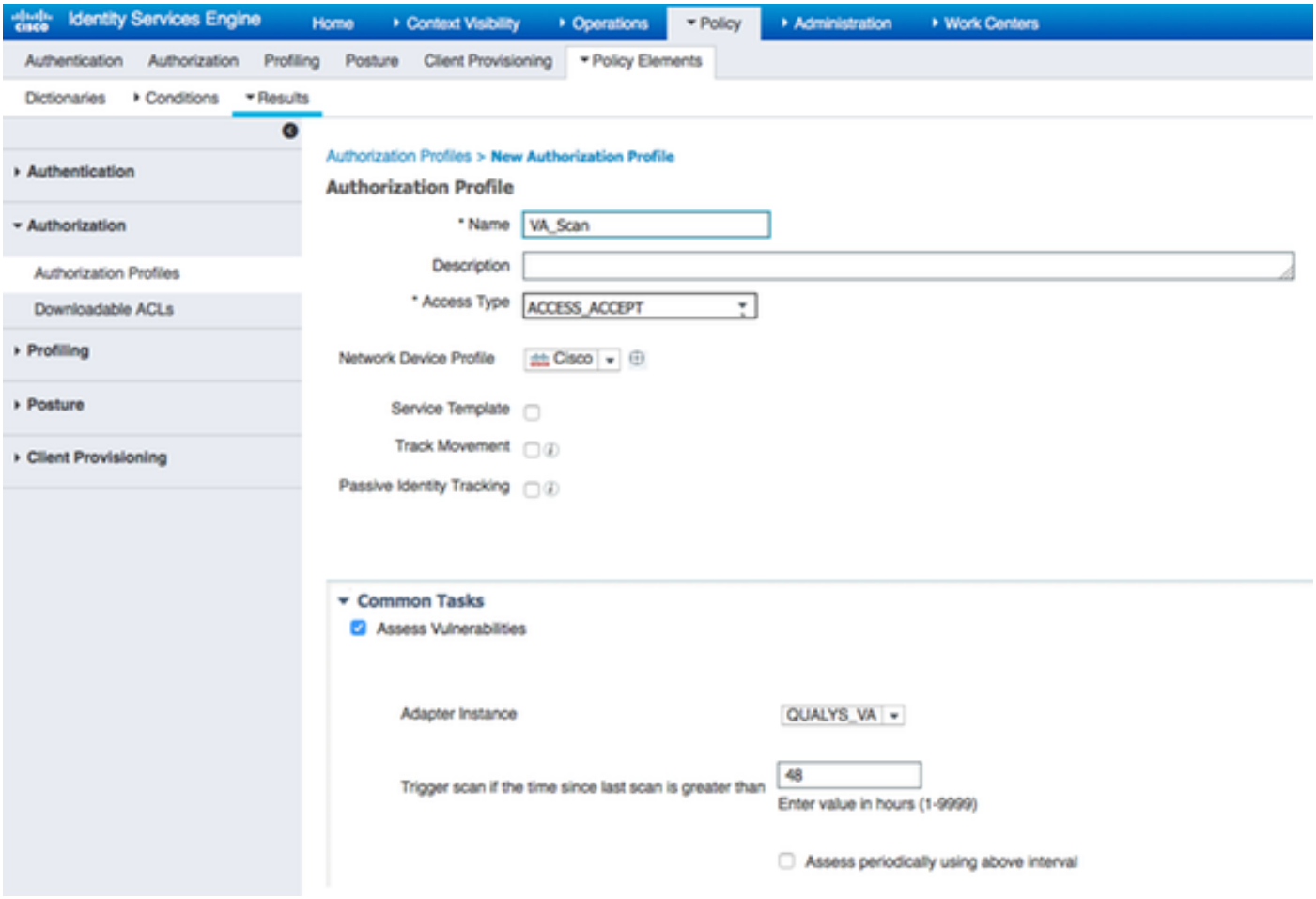
Navegue à política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização. Adicionar o perfil novo. Sob **tarefas comuns** selecione a caixa de seleção da **avaliação da vulnerabilidade**.
O intervalo por encomenda da varredura deve ser selecionado de acordo com seu 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

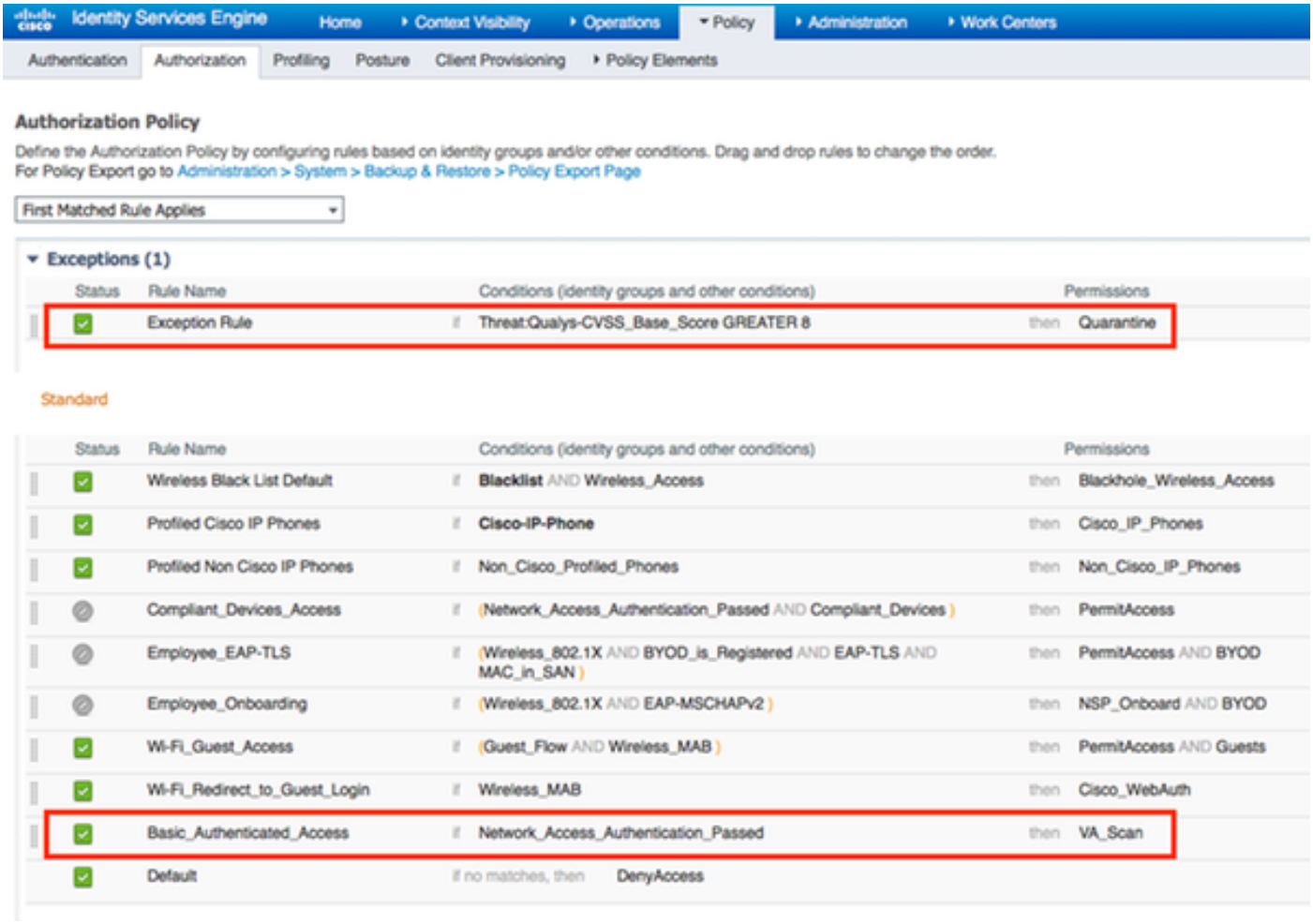
São enviados aos dispositivos de rede dentro do pacote de aceitação acesso, embora o propósito real deles seja dizer o nó MNT que a varredura deve ser provocada. O MNT instrui o nó TC-NAC para comunicar-se com a nuvem de Qualys.



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 **salvaguarda**.

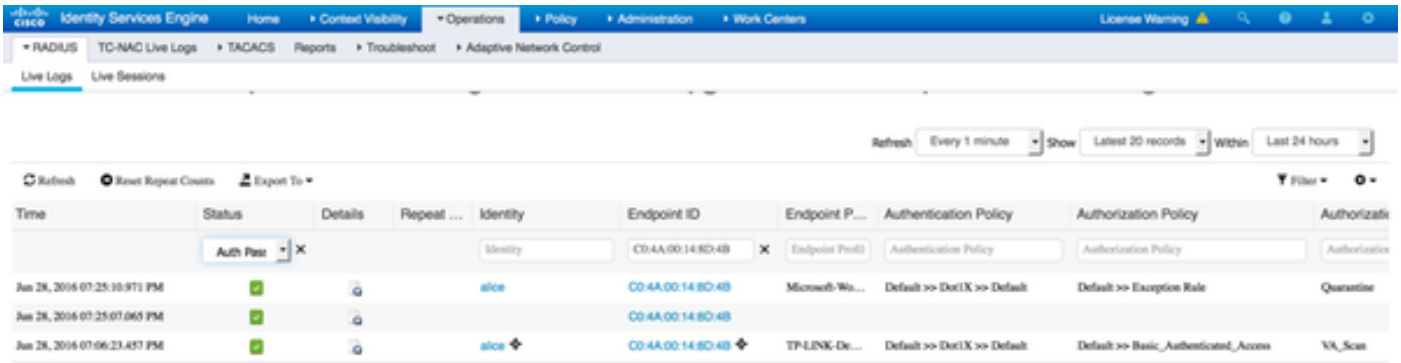
- Crie a política da autorização para máquinas Quarantined. Navegue à política > à autorização > à política > às exceções da autorização e crie uma **regra da exceção**. Clique sobre circunstâncias > criam a condição nova (opção avançada) > atributo seleto, enrolam para baixo e selecionam a **ameaça**. 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.



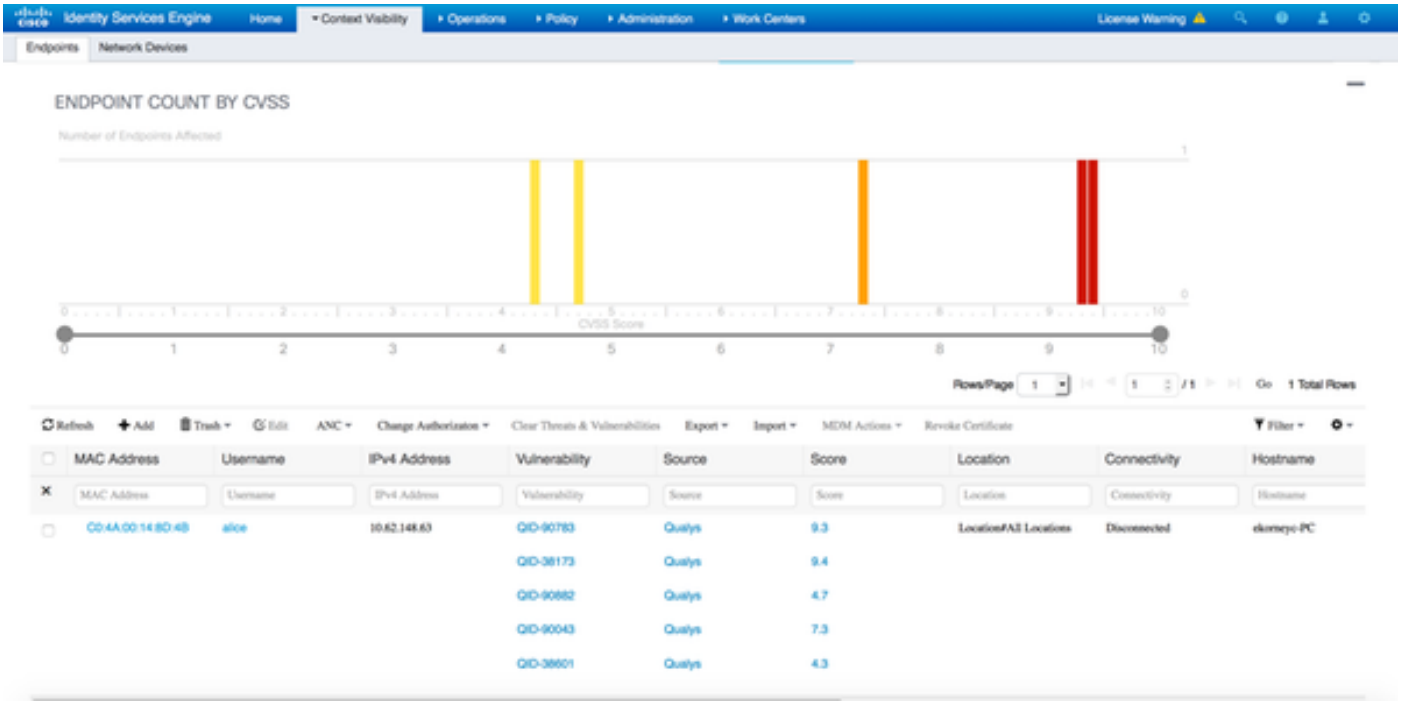
Verificar

Identity Services Engine

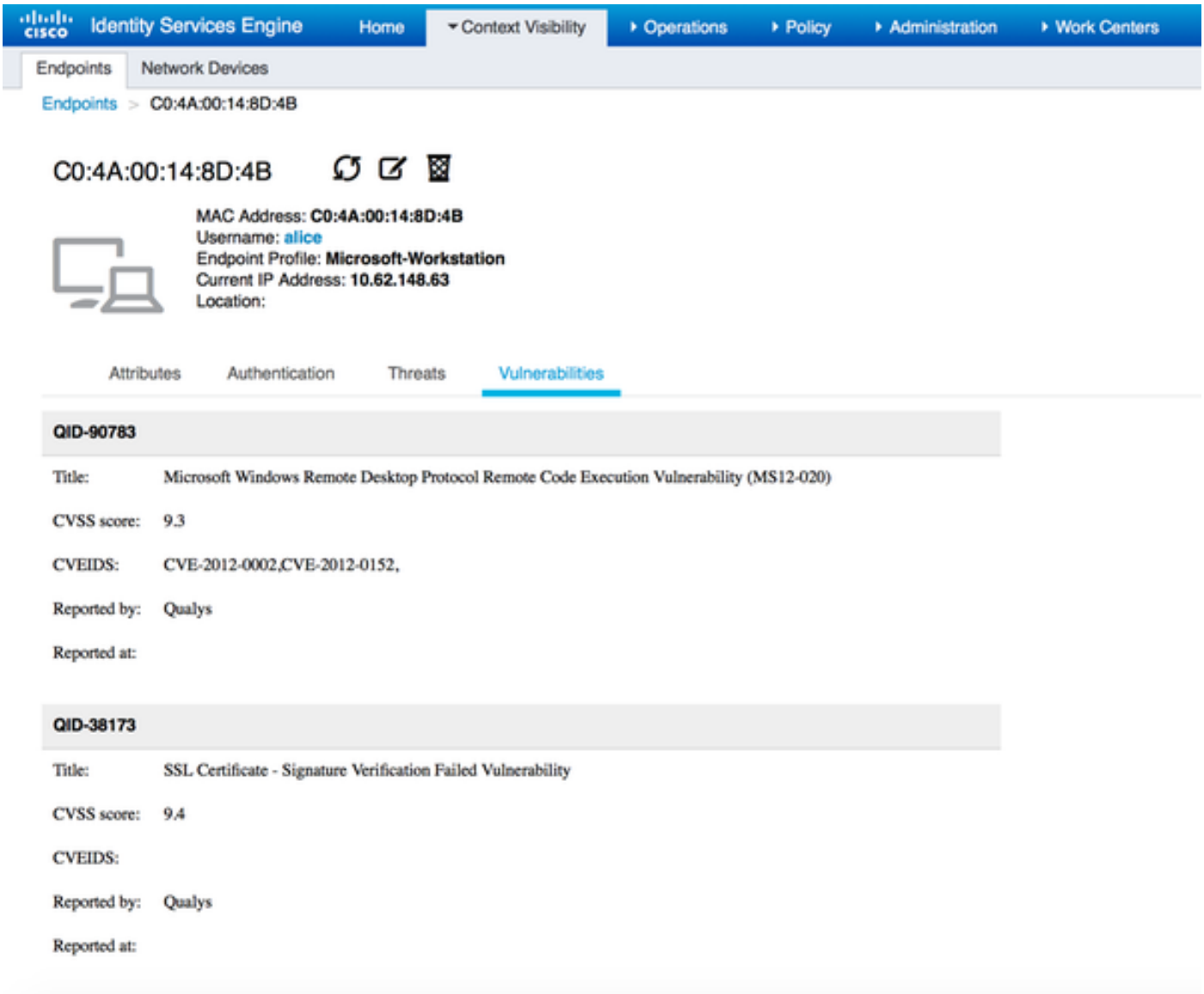
A primeira varredura VA dos disparadores da conexão. Quando a varredura é terminada, o Reauthentication CoA está provocado para aplicar a política nova se é combinado.



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.

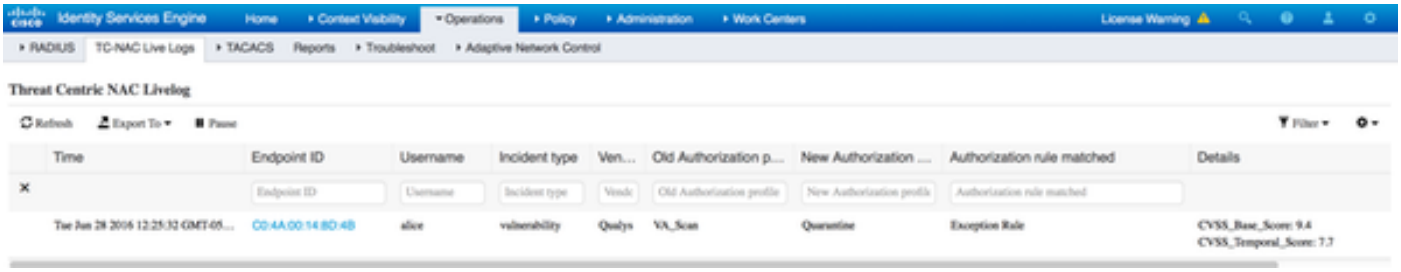


Ao selecionar o ponto final particular, mais detalhes sobre cada vulnerabilidade aparecem, incluindo o **título** e os **CVEID**.



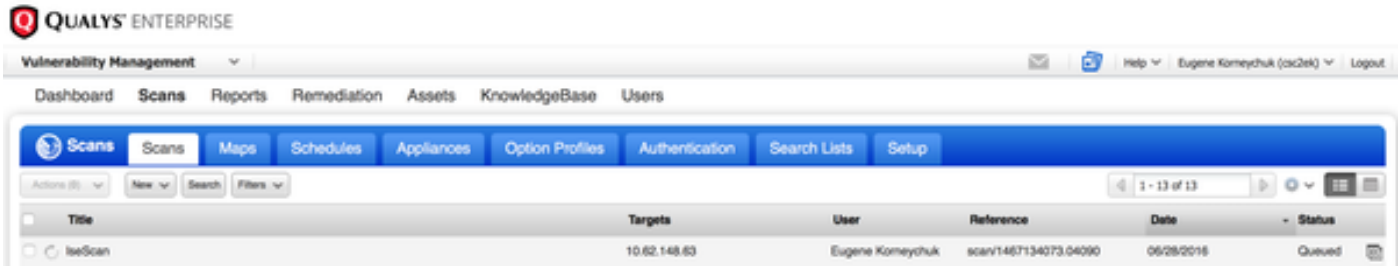
Nas operações > no TC-NAC vivem os logs, você pode ver velho contra as políticas novas da autorização aplicadas e os detalhes em CVSS_Base_Score.

> 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.

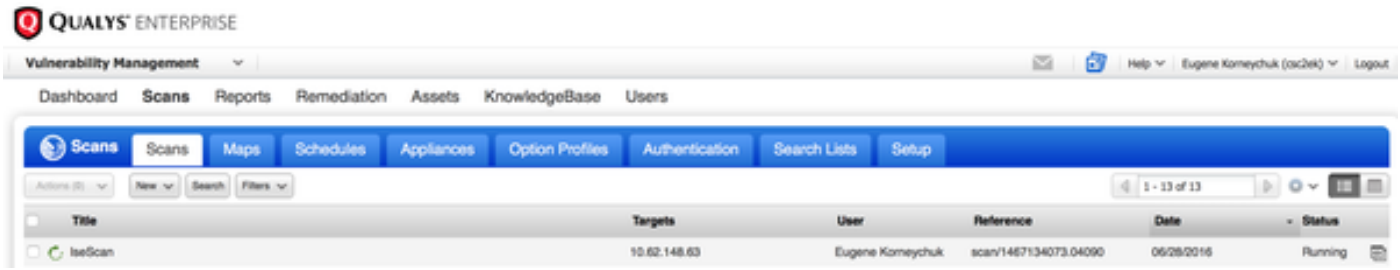


Nuvem de Qualys

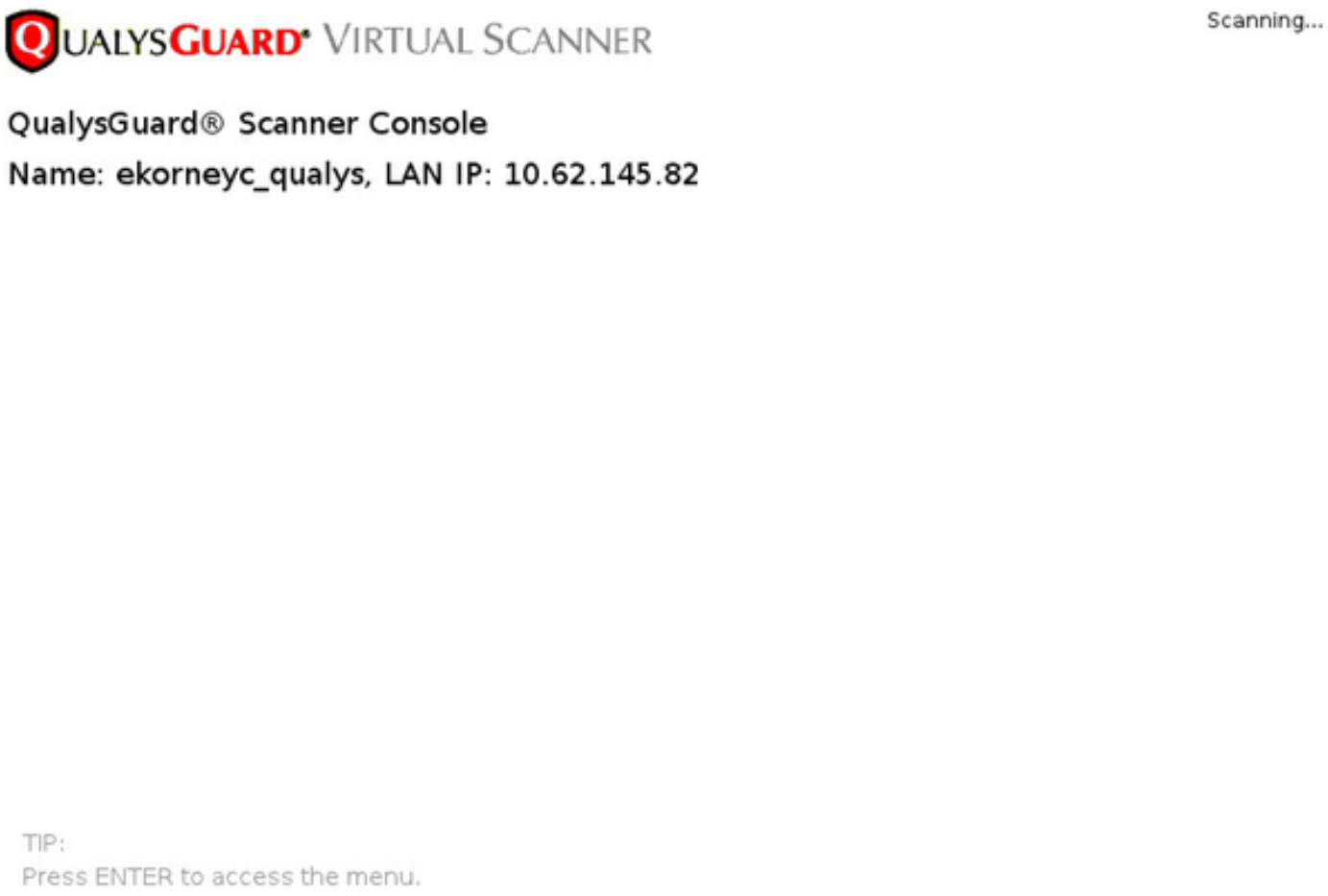
Quando a varredura VA é provocada por TC-NAC Qualys enfileira a varredura, ele pode ser visto em varreduras > em varreduras



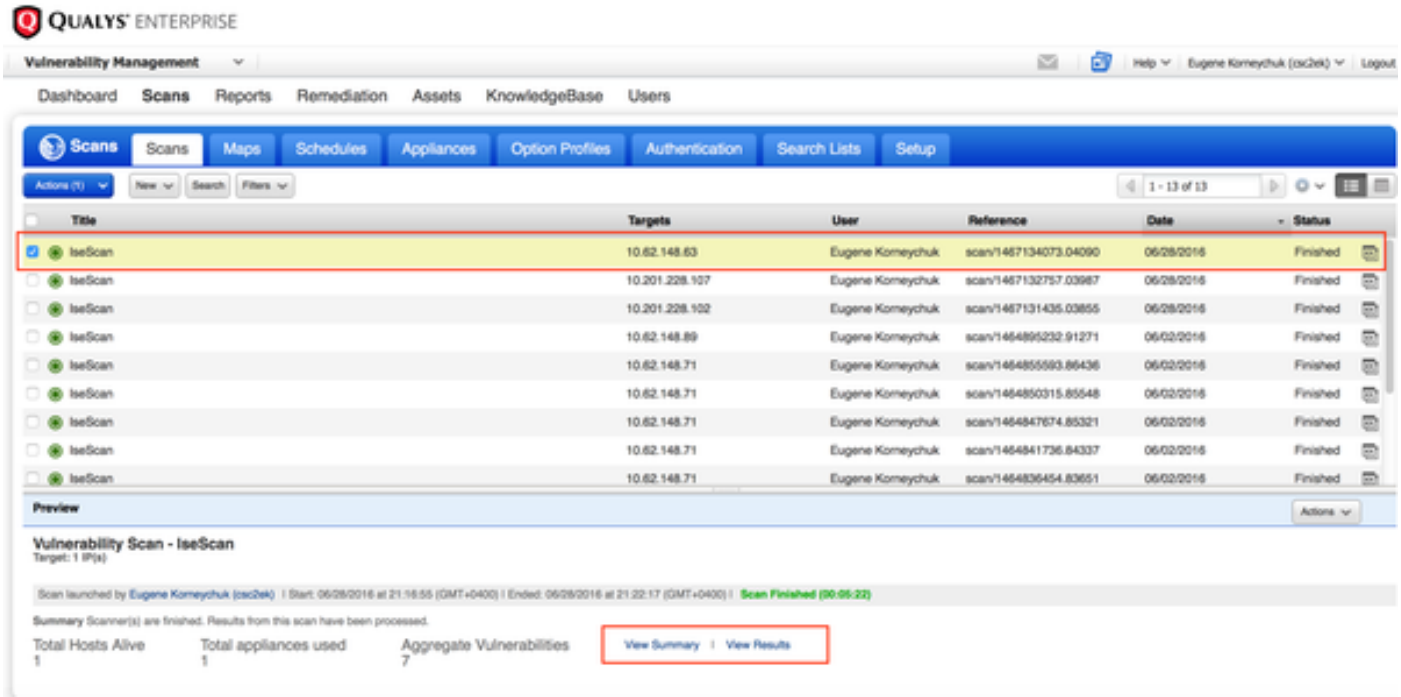
Mais tarde transições a ser executado, significando a nuvem de Qualys instruiu o varredor de Qualys para executar a exploração real



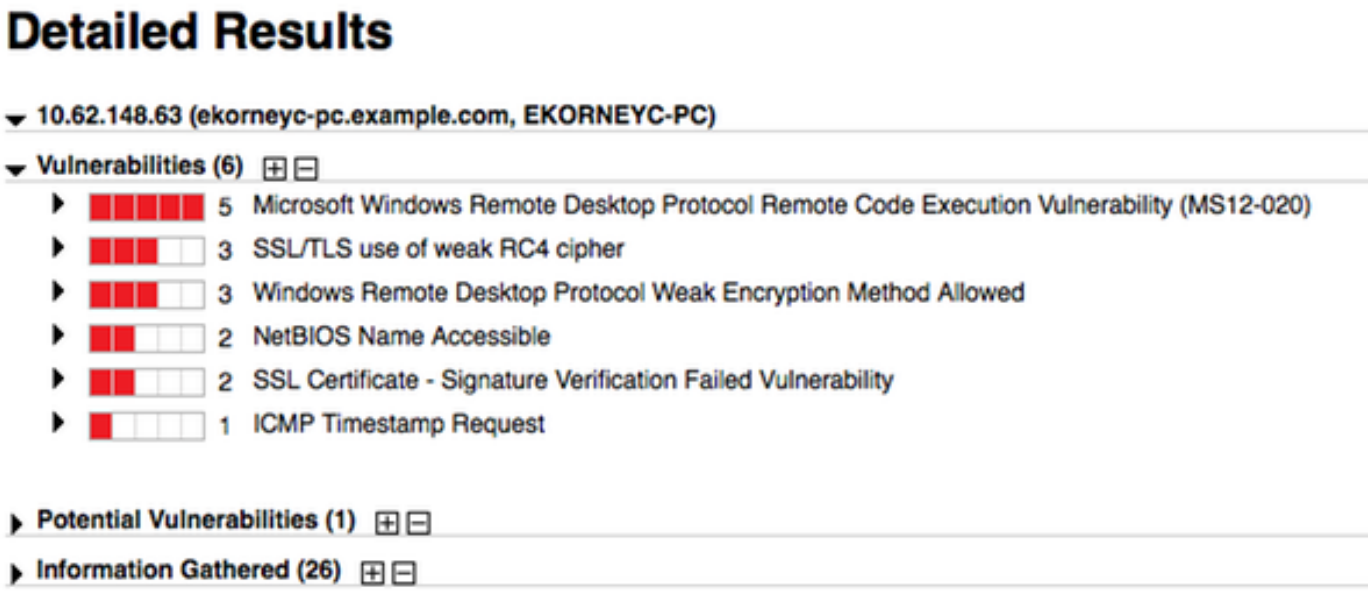
Quando o varredor executar a varredura, você deve ver a “exploração…” sinal no canto superior direito do protetor de Qualys



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**.



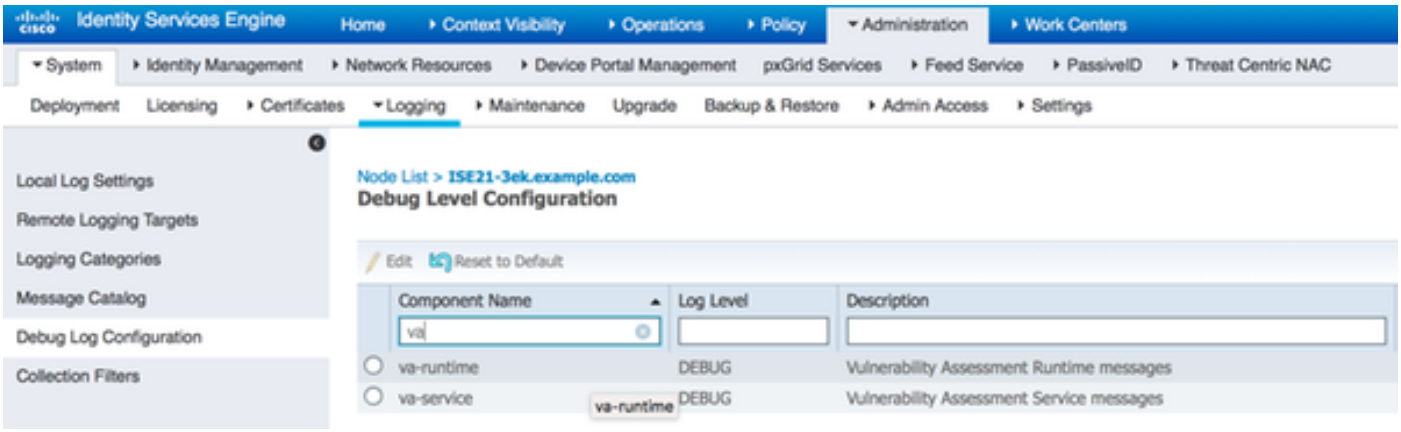
No relatório próprio você pode ver os **resultados detalhados**, onde as vulnerabilidades detectadas são mostradas.



Troubleshooting

Debuga no ISE

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



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,"vuln
erabilities":["{\"vulnerabilityId\":\"QID-90783\",\"cveIds\":\"CVE-2012-0002,CVE-2012-
0152,\",\"cvssBaseScore\":\"9.3\",\"cvssTemporalScore\":\"7.7\",\"vulnerabilityTitle\":\"Microso
ft (certificado do MS12-020)\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
38173\",\"cveIds\":\"\",\"cvssBaseScore\":\"9.4\",\"cvssTemporalScore\":\"6.9\",\"vulnerabilityT
itle\":\"SSL - assinatura falhada do
Allowed\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"vulnerabilityT
itle\":\"SMB do método de criptografia fraca do protocolo do Desktop remoto do
Vulnerability\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90882\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.7\",\"cvssTemporalScore\":\"4\",\"vulnerabilityTit
le\":\"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"}, certificado {"vulnerabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL -
vulnerabilidade falhada da verificação de assinatura”, “vulnerabilityVendor”: “Qualys”}, método
de criptografia fraca do protocolo do Desktop remoto {"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
permitido”, “vulnerabilityVendor”: “Qualys”}, assinatura {"vulnerabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
desabilitada ou SMB que assina não exigido”, “vulnerabilityVendor”: “Qualys”}, uso do
{"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 atá-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