

ISE 2.2 Threat-Centric NAC (TC-NAC) configureren met Rapid7

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Snel stroomschema op hoog niveau](#)

[Scanner implementeren en configureren](#)

[Stap 1. Plaats een scanner voor blootstellen.](#)

[Stap 2. Stel een scanner bloot.](#)

[ISE configureren](#)

[Stap 1. Schakel TC-NAC-services in.](#)

[Stap 2. Voer een scanner in.](#)

[Stap 3. Configureer scanner en/of instantie van TC-NAC.](#)

[Stap 4. Het machtigingsprofiel configureren om VA Scan te starten.](#)

[Stap 5. Instellen van een vergunningsbeleid.](#)

[Verifiëren](#)

[Identity Services Engine](#)

[Scanner tonen](#)

[Problemen oplossen](#)

[Debugs op ISE](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Threat-Centric NAC kunt configureren en oplossen met Rapid7 op Identity Services Engine (ISE) 2.2. De optie Threat Centric Network Access Control (TC-NAC) stelt u in staat om autorisatiebeleid te maken dat is gebaseerd op de bedreigings- en kwetsbaarheidskenmerken die worden ontvangen van de bedreigings- en kwetsbaarheidsadapters.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco Identity Services Engine
- kwetsbaarheidsscanner tonen

Gebruikte componenten

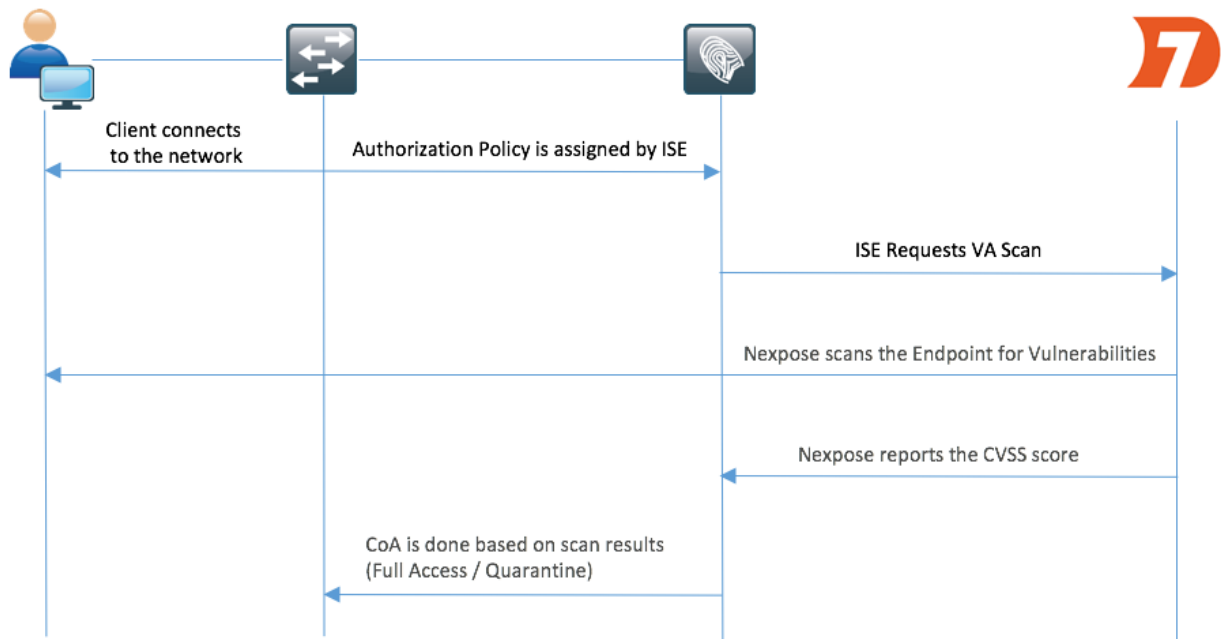
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 2.2
- Cisco Catalyst 2960S switch 15.2(2a)E1
- Rapid7 Nexus-scanner voor kwetsbaarheden en Enterprise Edition
- Windows 7 Service Pack 1
- Windows Server 2012 R2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Snel stroomschema op hoog niveau



Dit is de stroom:

1. De client verbindt zich met het netwerk, de beperkte toegang wordt verleend en het profiel met ingeschakeld selectieteken voor **Kwetsbaarheid** wordt toegewezen.
2. Het PSN-knooppunt verstuurt een systeemmeldingen naar het MNT-knooppunt, waarbij de authenticatie werd bevestigd, en de VA Scan was het resultaat van het autorisatiebeleid.
3. MNT-knooppunt vult SCAN met het TC-NAC-knooppunt (via Admin Webex) in met deze

gegevens:

- MAC-adres
- IP-adres
- Scaninterval
- Periodieke scan ingeschakeld
- van oorsprong PSN

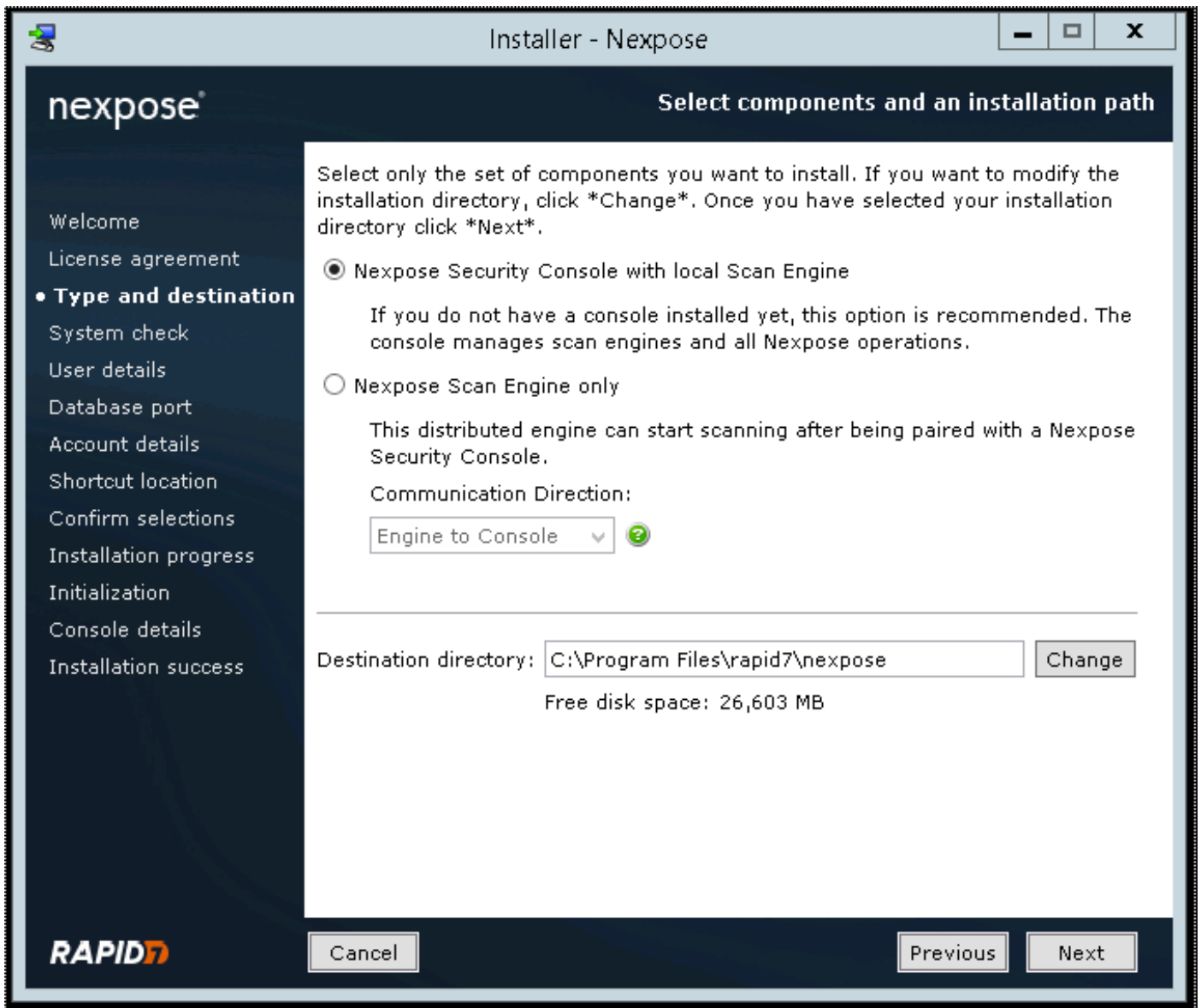
4. Stel TC-NAC (ingekapseld in Docker-container) bloot aan Nexpose Scanner om scan indien nodig te activeren.
5. Scanner blootgeven aan het door ISE gevraagde eindpunt.
6. Nexpose Scanner verstuurt de resultaten van de scan naar ISE.
7. Resultaten van de scan worden teruggestuurd naar TC-NAC:
 - MAC-adres
 - Alle CVSS-scores
 - Alle kwaliteiten (titel, EID)
8. TC-NAC werkt PAN bij met alle gegevens uit stap 7.
9. CoA wordt indien nodig geactiveerd volgens een beleid voor autorisatie.

Scanner implementeren en configureren

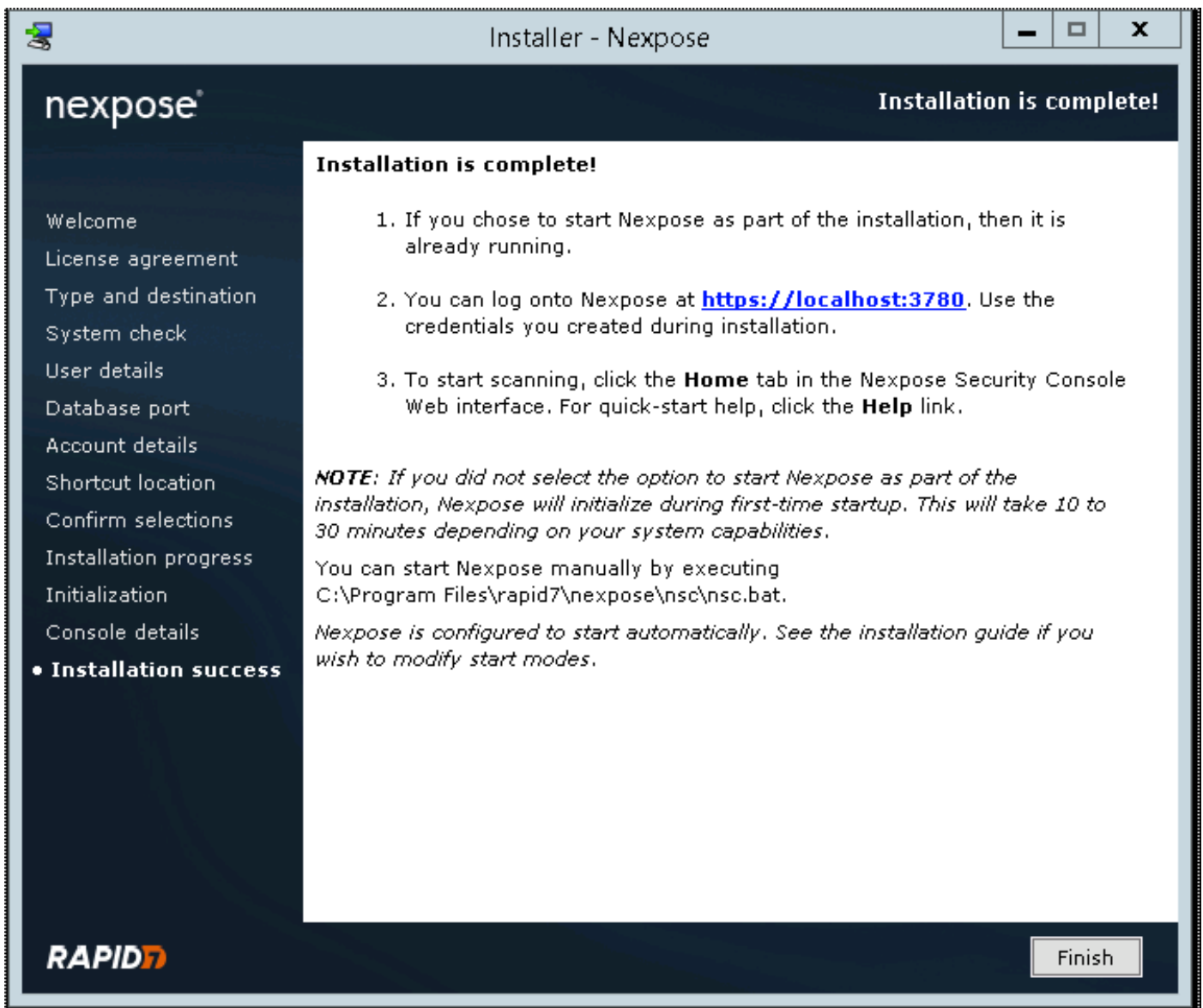
Voorzichtig: Stel dat de configuratie in dit document is uitgevoerd voor laboratoriumdoeleinden. Neem contact op met Rapid7-technici voor ontwerpoverwegingen

Stap 1. Plaats een scanner voor blootstellen.

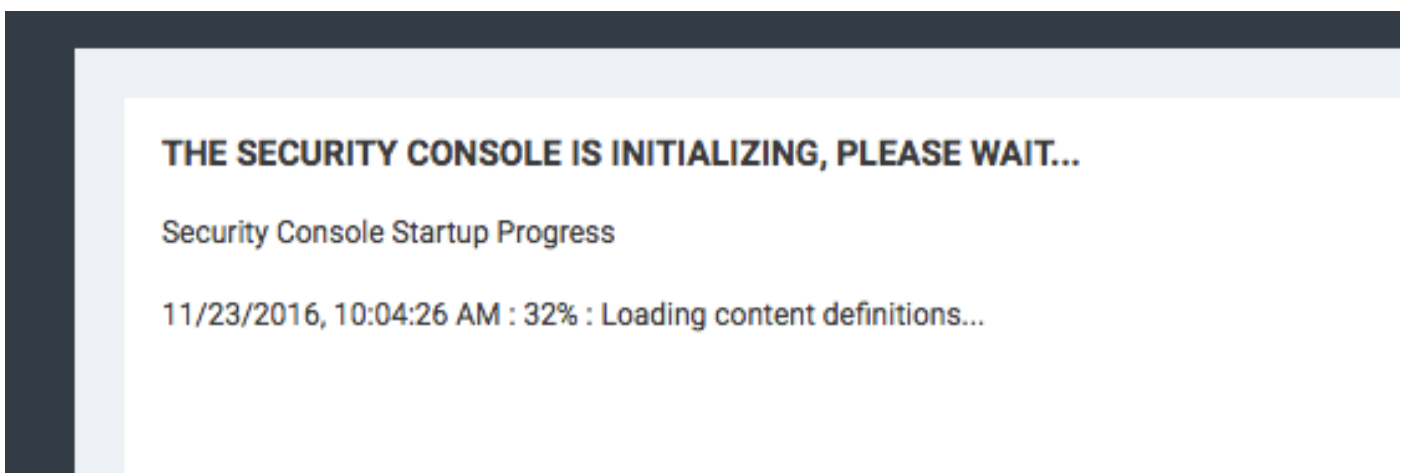
De scanner Nexpose kan worden uitgevoerd vanuit een OVA-bestand dat boven op Linux en Windows OS is geïnstalleerd. In dit document wordt de installatie uitgevoerd op Windows Server 2012 R2. Download de afbeelding van de website Rapid7 en start de installatie. Wanneer u **type en bestemming** instelt, selecteert u **Security console opnieuw instellen met lokale Scannen engine**



Nadat de installatie is voltooid, herstart de server. Na het lanceren moet de scanner Nexpose via 3780 poorten toegankelijk zijn, zoals in de afbeelding wordt weergegeven:



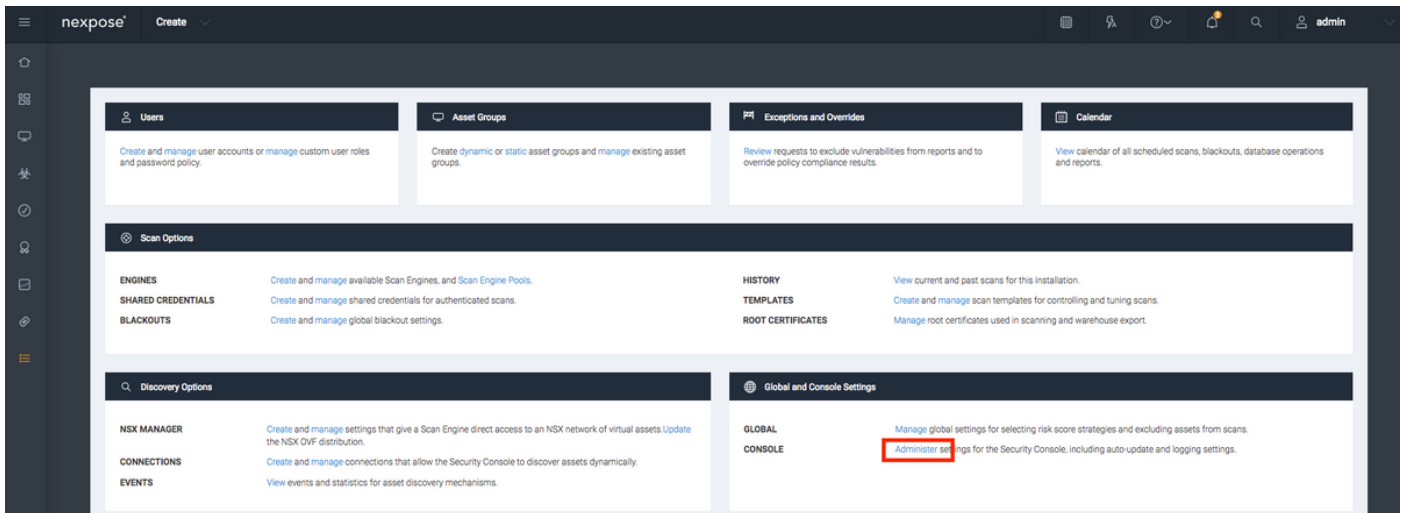
Zoals in de afbeelding wordt getoond, gaat de scanner door het opstartproces van de Security Console:



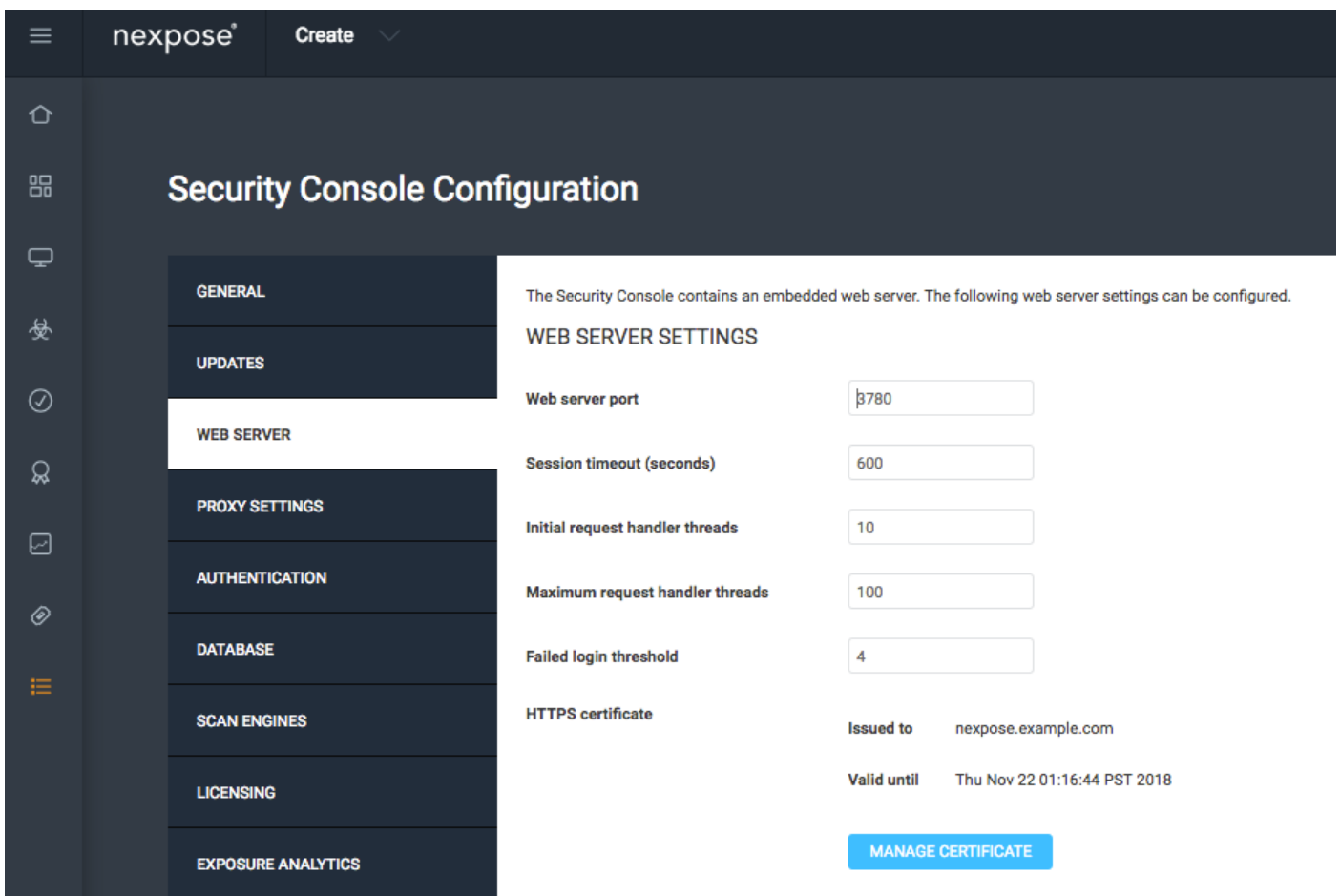
Om toegang tot de GUI te krijgen, dient de licentiesleutel te worden meegeleverd. Let op dat Enterprise Edition van Nexpose Scanner vereist is en dat er geen scans worden gegenereerd als Community Edition is geïnstalleerd.

Stap 2. Stel een scanner bloot.

De eerste stap is het installeren van certificaat op Nexpose Scanner. Het certificaat in dit document wordt afgegeven door dezelfde CA als het admincertificaat voor ISE (LAB CA). Navigeer naar **Administratie > Mondiale en Console-instellingen**. Selecteer **Beheers** onder **console**, zoals in de afbeelding.



Klik op **Certificaat beheren**, zoals in de afbeelding weergegeven:



Zoals in de afbeelding wordt weergegeven, klikt u op in **Nieuw certificaat maken**. Voer een **gemeenschappelijke naam** in en alle andere gegevens die u wilt hebben, in het identiteitsbewijs van scanner. Zorg ervoor dat ISE in staat is om Nexpose Scanner FQDN op te lossen met DNS.

Manage Certificate



This dialog will create a new self signed SSL certificate to be used by the Security Console web server. The current certificate will be overwritten. The new certificate can then be used 'as-is' or can be signed by a certification authority by generating a Certificate Signing Request (CSR).

Common name (fully qualified domain name)

Country (two letter country ISO code. e.g. US)

State/Province

Locality/City

Organization

Organizational unit

Valid for (years)

CREATE

BACK

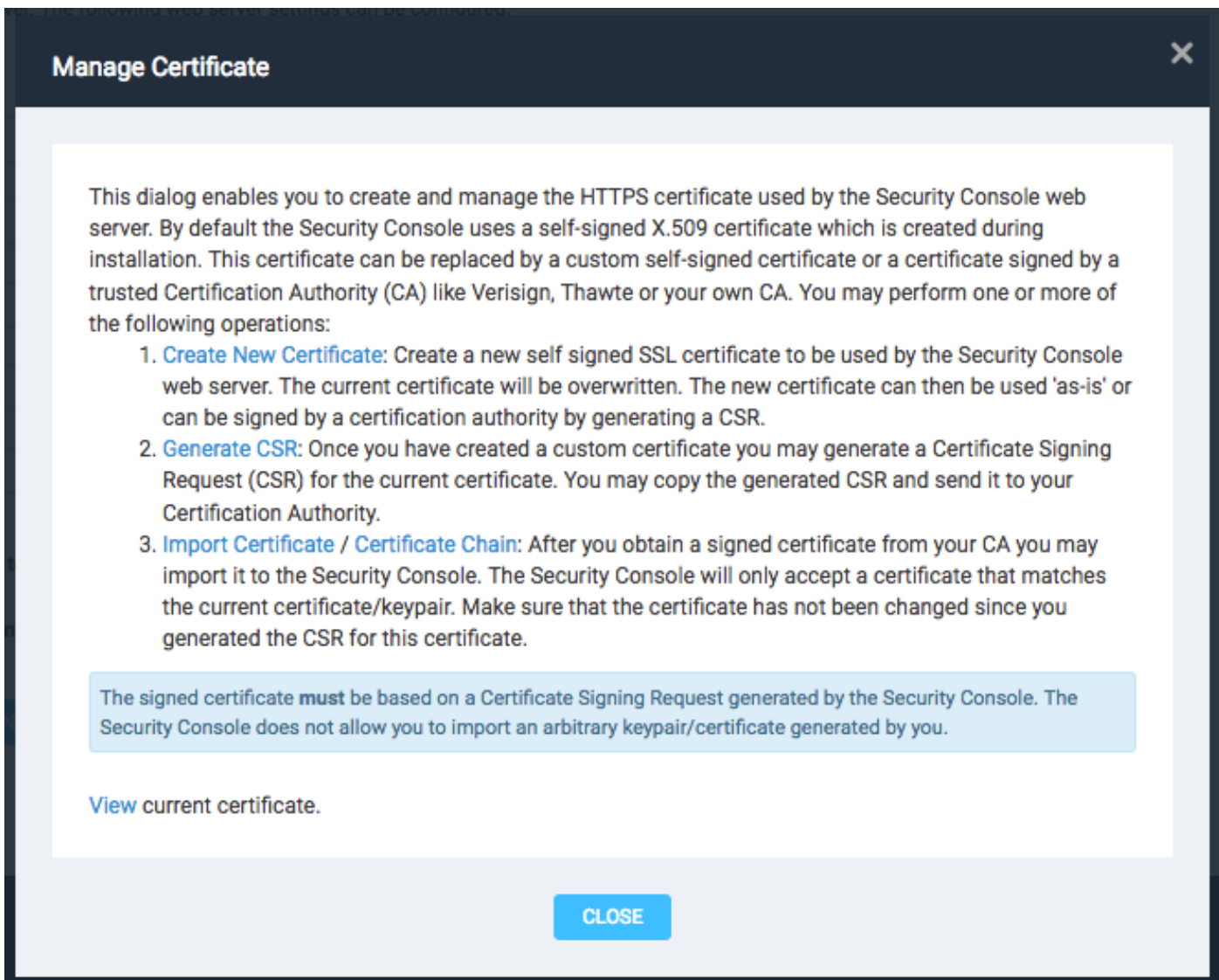
Exporteren certificaataanvraag (CSR) bij de terminal.

A new self-signed certificate was successfully created and saved. The new certificate will be used the next time Nexpose restarts. You may create a CSR for this certificate using the 'Create CSR' button below.

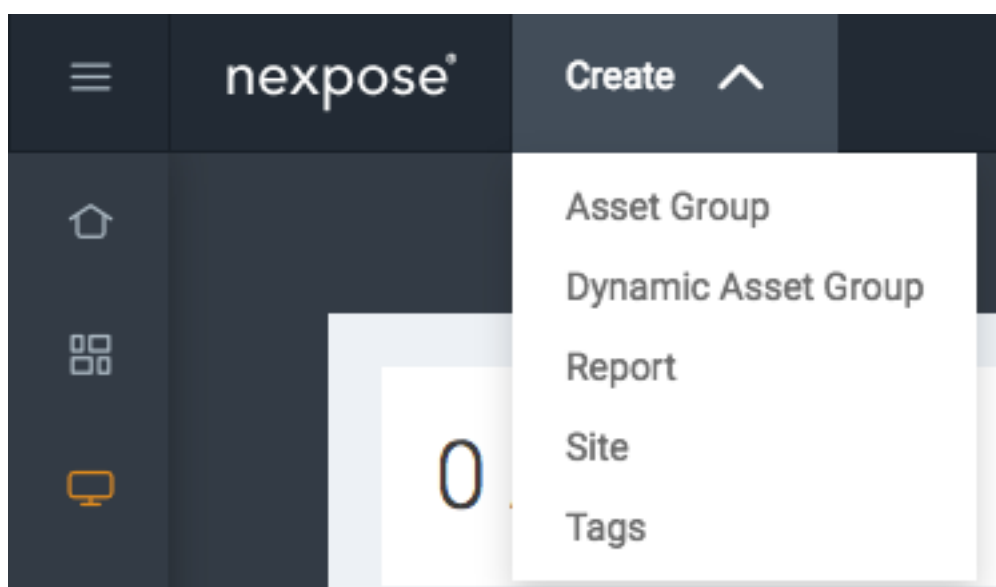
CREATE CSR NOW

LATER

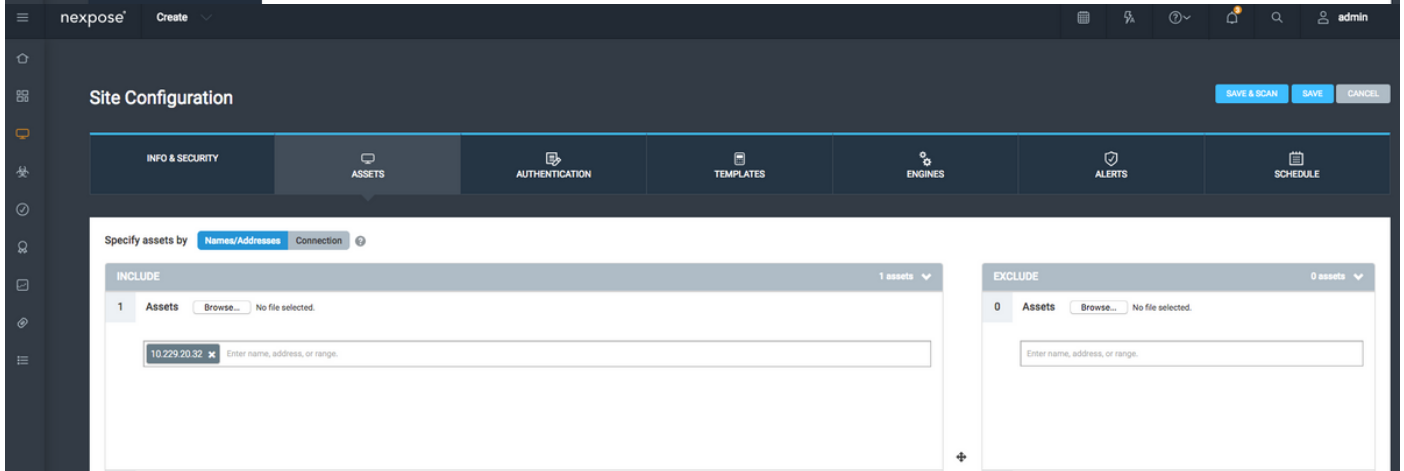
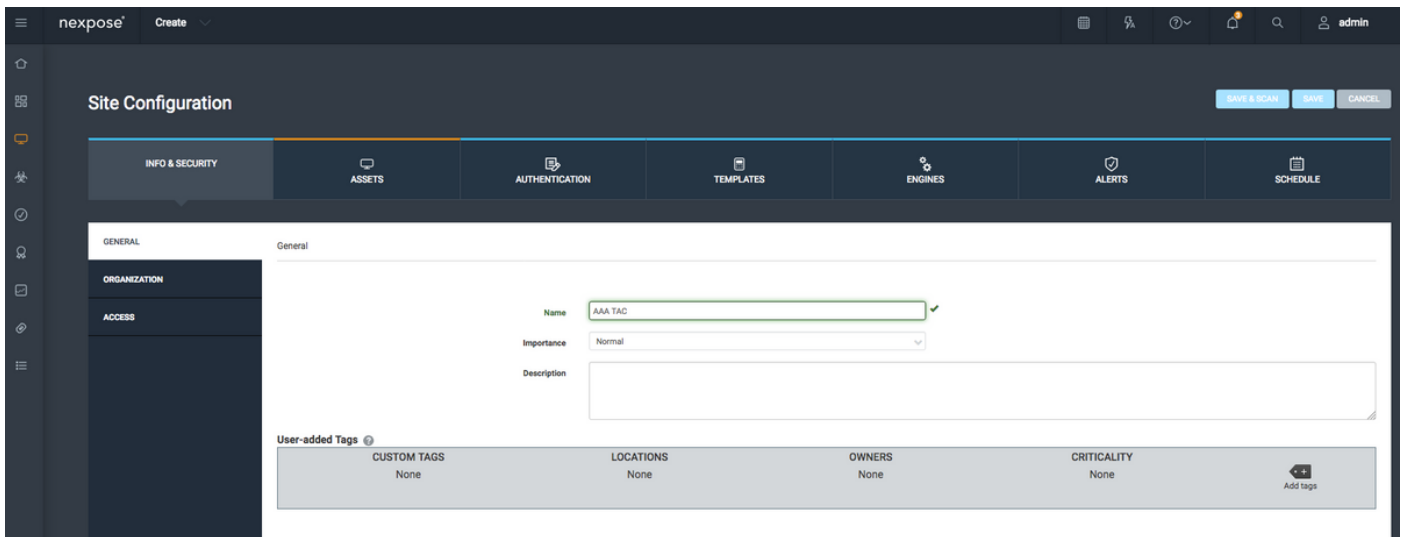
Op dit punt moet u de CSR ondertekenen met certificaatinstantie (CA).



Configureer een site. De website bevat Activa die u kunt scannen en de account die wordt gebruikt om ISE te integreren met Scanner openen, heeft rechten om websites te beheren en rapporten te maken. Blader naar **Maken > Site**, zoals in de afbeelding.



Zoals in de afbeelding wordt aangegeven, voert u de **naam** van de site in op het tabblad **Info & Security**. Het tabblad **Activa** moet ip-adressen bevatten van de geldige activa, endpoints die in aanmerking komen voor het scannen van kwetsbaarheden.



Importeer CA-certificaat dat ISE-certificaat heeft ondertekend in de vertrouwde winkel. Navigeer naar **Beheer > basiscertificaten > Bewerken > Importaatcertificaten**.



ISE configureren

Stap 1. Schakel TC-NAC-services in.

Schakel TC-NAC services in op ISE-knooppunt. Let op:

- De Threat Centric NAC-service vereist een Apex-licentie.
- U hebt een afzonderlijk knooppunt voor beleidsservices (PSN) nodig voor Threat Centric NAC-service.
- De verbinding van de centrum-NAC van de bedreiging kan op slechts één knoop in een plaatsing worden toegelaten.

- U kunt slechts één exemplaar van een adapter per verkoper toevoegen voor de Kwetsbaarheidsbeoordelingsdienst.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings.

The main content area is titled 'Deployment Nodes List > ISE22-1ek' and 'Edit Node'. It has two tabs: 'General Settings' (selected) and 'Profiling Configuration'. The 'General Settings' tab shows the following information:

- Hostname: ISE22-1ek
- FQDN: ISE22-1ek.example.com
- IP Address: 10.48.23.86
- Node Type: Identity Services Engine (ISE)

The 'Personas' section is expanded, showing the following configuration:

- Administration: Role STANDALONE, Make Primary button.
- Monitoring: Role PRIMARY, Other Monitoring Node field.
- Policy Service:
 - Enable Session Services: Includes a 'Personas' dropdown.
 - Enable Profiling Service
 - Enable Threat Centric NAC Service: Includes an 'i' icon.
 - Enable SXP Service: Includes an 'i' icon.
 - Enable Device Admin Service: Includes an 'i' icon.
 - Enable Passive Identity Service: Includes an 'i' icon.
 - pxGrid: Includes an 'i' icon.
 - Use Interface: GigabitEthernet 0
 - Include Node in Node Group: None

Stap 2. Voer een scanner in.

Importeer het Nexpose Scanner CA-certificaat in de Trusted Certificates-winkel in Cisco ISE (Beheer > Certificaten > certificaatbeheer > Vertrouwde certificaten > Importeren). Zorg ervoor dat de juiste basis- en intermediaire certificaten in de Cisco ISE Trusted Certificates-winkel worden geïmporteerd (of aanwezig zijn)

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings.

The main content area is titled 'Certificate Management' and 'Trusted Certificates'. It has a table with the following columns: Friendly Name, Status, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Expiration Status.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 2025	✓
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 2029	✓
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F FB 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	✓
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Default self-signed server certificate	Enabled	Endpoints Infrastructure	58 08 8E 16 00 00 ...	ISE22-1ek.example.com	ISE22-1ek.example.com	Thu, 20 Oct 2016	Fri, 20 Oct 2017	✓
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	✓
LAB CA#LAB CA#00005	Enabled	Endpoints Infrastructure	2F DB 38 46 B8 6D...	LAB CA	LAB CA	Thu, 12 Feb 2015	Wed, 12 Feb 2025	✓
Nexpose Security Console#Nexpose Security Consol...	Enabled	Endpoints Infrastructure	C- 49 10 5A 46 EB ...	Nexpose Security Console	Nexpose Security Console	Fri, 18 Nov 2016	Wed, 18 Nov 2026	✓
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Thu, 17 Jul 2036	✓
VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...	Wed, 8 Nov 2006	Thu, 17 Jul 2036	✓
VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public ...	Mon, 8 Feb 2010	Sat, 8 Feb 2020	✓

Stap 3. Configureer scanner en/of instantie van TC-NAC.

Voeg Rapid7 Instance toe aan Administration > Threat Centric NAC > Verkopers van derden.

Vendor Instances > New
Input fields marked with an asterisk (*) are required.

Vendor *

Instance Name *

Zodra toegevoegd, gaat de instantie over naar **Klaar om staat te configureren**. Klik op deze link. Configuratie **Host** (Scanner) en **Port**, standaard 3780. Specificeer **Gebruikersnaam** en **Wachtwoord** met toegang tot rechtse Site.

Enter Nexpose Security Console credentials

Nexpose Host

The hostname of the Nexpose Security Console Host.

Nexpose port

The port of the Nexpose Security Console host.

Username

Username to access Nexpose Security Console.

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.

Geavanceerde instellingen zijn duidelijk gedocumenteerd in ISE 2.2 Admin Guide, de link kan worden gevonden in het gedeelte Referenties van dit document. Klik op **Volgende** en op **Voltoeien**. Instantieovergangen naar **actieve** toestand en downloads met kennisbasis openen.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Third Party Vendors

Vendor Instances

Refresh Add Trash Edit Restart Stop Filter Settings

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
<input type="checkbox"/> Rapid7	Rapid7 Nexpose	VA	nexpose.example.com	Connected	Active

Stap 4. Het machtigingsprofiel configureren om VA Scan te starten.

Navigeer in **Policy > Policy Elementen > Resultaten > autorisatie > autorisatieprofielen**. Nieuw profiel toevoegen. Selecteer onder **Common Tasks** de optie **Kwetsbaarheidsassessments**. Het On-Demand scaninterval moet worden geselecteerd volgens uw netwerkontwerp.

autorisatieprofiel bevat die av-paren:

```
cisco-av-pair = on-demand-scan-interval=48  
cisco-av-pair = periodic-scan-enabled=0  
cisco-av-pair = va-adapter-instance=c2175761-0e2b-4753-b2d6-9a9526d85c0c
```

Ze worden naar netwerkapparaten verzonden binnen het pakket Access-Accept, hoewel het echte doel ervan is om MNT (Monitoring) Node te vertellen dat Scannen moet worden geactiveerd. MNT draagt TC-NAC knooppunt op om met Nexpose Scanner te communiceren.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a policy element named 'Rapid7'. The interface includes a navigation menu on the left with categories like Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main configuration area is divided into several sections:

- Basic Information:** Name is 'Rapid7', Access Type is 'ACCESS_ACCEPT', and Network Device Profile is 'Cisco'.
- Common Tasks:** 'Assess Vulnerabilities' is checked. The Adapter Instance is 'Rapid7' and the trigger scan interval is set to 48 hours.
- Advanced Attributes Settings:** A field for 'Select an item' is visible.
- Attributes Details:** Shows the configuration summary: Access Type = ACCESS_ACCEPT, cisco-av-pair = on-demand-scan-interval=48, cisco-av-pair = periodic-scan-enabled=0, and cisco-av-pair = va-adapter-instance=c2175761-0e2b-4753-b2d6-9a9526d85c0c.

Stap 5. Instellen van een vergunningsbeleid.

- Configureer beleid om het nieuwe autorisatieprofiel te gebruiken dat in stap 4 is geconfigureerd. Navigeer naar **beleid > autorisatie > autorisatiebeleid**, plaats **Basic_Authenticated_Access** regel en klik op **Bewerken**. Verander de toegangsrechten van **PermitAccess** tot de nieuwe **standaard Rapid7**. Dit veroorzaakt een kwetsbaarheidsscan voor alle gebruikers. Klik op in **Opslaan**.
- Maak een autorisatiebeleid voor geharde machines. Navigeer in **Policy > Authorization > Authorization Policy > Exceptions** en reinig een **Exception Rule**. navigeren nu naar **Voorwaarden > Nieuwe conditionering maken (geavanceerde optie) > Eigenschappen selecteren**, omlaag scrollen en **bedreigingen** selecteren. Vul het attribuut **Threat uit** en selecteer **Nexpose-CVSS_Base_Score**. Verander de operator in **grotere mate** en voer een waarde in volgens uw beveiligingsbeleid. **Quarantaine** autorisatieprofiel dient beperkte toegang tot de kwetsbare machine te bieden.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Global Exceptions Policy Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Click here to do wireless setup and visibility setup Do not show this again.

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 Threat:Rapid7 Nexpose-CVSS_Base_Score GREATER 1	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
✓	Profilled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profilled Non Cisco IP Phones	if Non_Cisco_Profilded_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
✓	Wired_Guest_Access	if (Guest_Flow AND Wired_MAB)	then PermitAccess AND Guests
✓	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
✓	Wired_Redirect_to_Guest_Login	if Wired_MAB	then Cisco_WebAuth
⊙	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
✓	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then Rapid7
✓	Default	if no matches, then	DenyAccess

Verifiëren

Identity Services Engine

De eerste verbinding voert een VA Scan in. Wanneer de scan is voltooid, wordt voor de toepassing van het nieuwe beleid van CoA een nieuwe echtheidscontrole op gang gebracht, indien het is afgestemd.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Click here to do wireless setup and visibility setup Do not show this again.

Live Logs Live Sessions




Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 0

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

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group
Nov 24, 2016 01:45:41.438 PM	⊙		0	alice	3C-97-0E-52-3F-D9	NoneI-Device	Default >> D...	Default >> E...	Quarantine	10.229.20.32			FastEthernet1/0/5
Nov 24, 2016 01:45:40.711 PM	✓			alice	3C-97-0E-52-3F-D9	NoneI-Device	Default >> D...	Default >> E...	Quarantine	10.229.20.32	Switch_2960		FastEthernet1/0/5 Profilled
Nov 24, 2016 01:45:39.166 PM	✓				3C-97-0E-52-3F-D9						Switch_2960		
Nov 24, 2016 01:32:00.564 PM	✓				3C-97-0E-52-3F-D9		Default >> D...	Default >> B...	Rapid7	10.229.20.32	Switch_2960		FastEthernet1/0/5

Om te verifiëren welke kwetsbaarheden werden gedetecteerd, navigeer naar **Context Visibility > Endpoints**. Controleer de zwakheden per eindpunt met de scores die het worden gegeven door Nexpose Scanner.

Endpoints > 3C:97:0E:52:3F:D9

3C:97:0E:52:3F:D9   



MAC Address: 3C:97:0E:52:3F:D9
 Username: **alice**
 Endpoint Profile: **Nortel-Device**
 Current IP Address: **10.229.20.32**
 Location: **Location** → All Locations

Applications Attributes Authentication Threats **Vulnerabilities**

ssl-cve-2016-2183-sweet32

Title: TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)
 CVSS score: 5
 CVEIDS: CVE-2016-2183
 Reported by: Rapid7 Nexpose
 Reported at: Thu Nov 24 05:42:52 CET 2016

ssl-static-key-ciphers

Title: TLS/SSL Server Supports The Use of Static Key Ciphers
 CVSS score: 2.5999999
 CVEIDS:
 Reported by: Rapid7 Nexpose
 Reported at: Thu Nov 24 05:42:52 CET 2016

rc4-cve-2013-2566

Title: TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)
 CVSS score: 4.30000019
 CVEIDS: CVE-2013-2566
 Reported by: Rapid7 Nexpose
 Reported at: Thu Nov 24 05:42:52 CET 2016

In Operations > TC-NAC Live Logs kunt u autorisatiebeleid zien toegepast en details zien over CVSS_Base_Score.

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

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Threat Centric NAC LiveLog

Refresh Export To Pause Filter

Time	Endpoint ID	Username	Incident type	Vendor	Old Authorization profile	New Authorization profile	Authorization rule matched	Details
Thu Nov 24 2016 13:45:40 GMT+0100 (C...)	3C:97:0E:52:3F:D9	alice	vulnerability	Rapid7 ...	Rapid7	Quarantine	Exception Rule	CVSS_Base_Score: 5 CVSS_Temporal_Score: 0

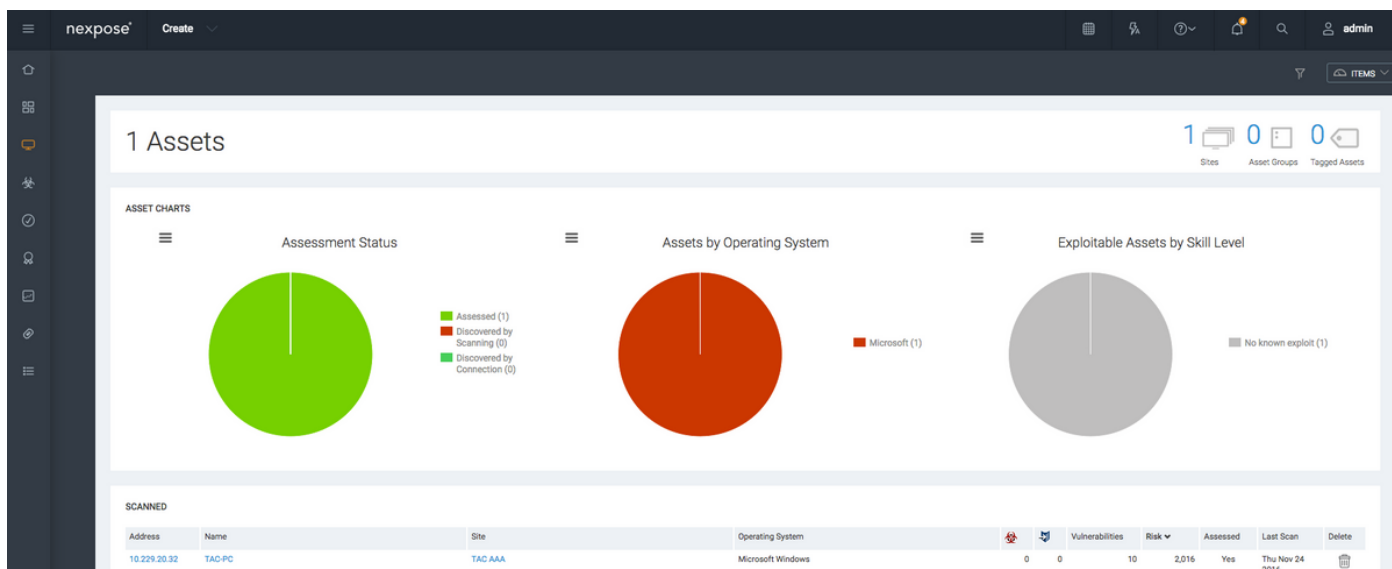
Scanner tonen

Wanneer de VA Scan wordt geactiveerd door TC-NAC Nexpose Scan transitions naar **In-Progress** status en de scanner begint het eindpunt te controleren en als u de Wireless Capture op het eindpunt uitvoert, ziet u op dit punt pakketuitwisseling tussen het eindstation en Scanner. Nadat het programma Scanner is voltooid, zijn de resultaten beschikbaar onder **Thuispagina**.

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
TAC AAA	1	10	2,016	Local scan engine	Static	Scan finished on Thu, Nov 24th, 2016			

[CREATE SITE](#)

Onder de pagina **Activa** kunt u zien dat er een nieuw eindpunt beschikbaar is met de resultaten van het Scannen, dat het besturingssysteem wordt geïdentificeerd en dat 10 kwetsbaarheden worden gedetecteerd.



Wanneer u in de Nexpose Scanner van het **IP-adres van het eindpunt** klikt, neemt u naar het nieuwe menu, waar u meer informatie kunt zien zoals hostname, Risc Score en gedetailleerde lijst van kwetsbaarheden

EXCLUDE	RECALL	RESUBMIT	Title	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	5	425	Wed Aug 24 2016	Fri Sep 02 2016	Severe	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS Server Supports TLS version 1.0	4.3	324	Tue Oct 14 2014	Thu Nov 12 2015	Severe	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)	4.3	397	Tue Mar 12 2013	Thu Apr 28 2016	Severe	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS/SSL Server is enabling the BEAST attack	4.3	448	Tue Sep 06 2011	Thu Feb 18 2016	Severe	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS/SSL Server is Using Commonly Used Prime Numbers	2.6	91.0	Wed May 20 2015	Thu Jun 16 2016	Moderate	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Diffie-Hellman group smaller than 2048 bits	2.6	91.0	Wed May 20 2015	Thu Nov 12 2015	Moderate	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS/SSL Server Supports The Use of Static Key Ciphers	2.6	240	Sun Feb 01 2015	Wed Sep 30 2015	Moderate	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP timestamp response	0	0.0	Fri Aug 01 1997	Thu Jul 12 2012	Moderate	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UPnP SSDP Traffic Amplification	0	0.0	Sun Feb 09 2014	Wed Dec 10 2014	Moderate	1	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS/SSL Server Supports 3DES Cipher Suite	0	0.0	Sun Feb 01 2009	Mon Feb 15 2016	Moderate	1	

Wanneer u in de kwetsbaarheid zelf klikt, wordt de volledige beschrijving in de afbeelding weergegeven.

VULNERABILITY INFORMATION

OVERVIEW

Title	Severity	Vulnerability ID	CVSS	Published	Modified
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Severe (5)	ssll-cve-2016-2183-sweet32	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	Aug 24, 2016	Sep 2, 2016

DESCRIPTION

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption cipher are affected. The security of a block cipher is often reduced to the key size k; the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter; defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, CCM, OCB, etc.) are unsafe with more than 2 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

AFFECTS

Asset	Name	Site	Port	Status	Proof	Last Scan	Exceptions
10.229.20.32	TAC-PC	TAC AAA	3389	Vulnerable Version	<ul style="list-style-type: none"> Negotiated with the following insecure cipher suites: <ul style="list-style-type: none"> TLS 1.0 ciphers: <ul style="list-style-type: none"> TLS_RSA_WITH_3DES_EDE_CBC_SHA 	Nov 24th, 2016	Exclude

Problemen oplossen

Debugs op ISE

Om diepgang op ISE in te schakelen, navigeer naar **Beheer > Systeem > Vastlegging > Loggen > Logconfiguratie van het Debug Log**, selecteer TC-NAC Node en wijzig de optielogniveau **va-run** en **va-service** component naar **DEBUG**.

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

Deployment > Licensing > Certificates > **Logging** > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Local Log Settings
Remote Logging Targets
Logging Categories
Message Catalog
Debug Log Configuration
Collection Filters

Node List > ISE21-3ek.example.com
Debug Level Configuration

Edit Reset to Default

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

Aanmelden voor controle - varuntime.log. U kunt deze direct staart vanaf ISE CLI:

```
ISE21-3ek/admin# toont bloggingstoepassing varuntime.log tail
```

TC-NAC Docker heeft instructie ontvangen om scan voor een bepaald eindpunt te uitvoeren.

```
2016-11-24 13:32:04,436 DEBUG [Thread-94][ ] va.runtime.admin.mnt.EndpointFileReader -:::- VA:
Read va runtime.
[{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","ondemandScanInterval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c2175761-0e2b-4753-b2d6-9a9526d85c0c","psnHostName":"ISE22-1ek","heartBeatTime":0,"lastScanTime":0},
{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEnabled":false,"heartBeatTime":0,"lastScanTime":0}]
2016-11-24 13:32:04,437 DEBUG [Thread-94][ ] va.runtime.admin.vaservice.VaServiceRemotingHandler
-:::- VA: received data from Mnt:
{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","ondemandScanInterval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c2175761-0e2b-4753-b2d6-9a9526d85c0c","psnHostName":"ISE22-1ek","heartBeatTime":0,"lastScanTime":0}
```

```
2016-11-24 13:32:04,439 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler
-:::- VA: received data from Mnt:
{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEn
abled":false,"heartBeatTime":0,"lastScanTime":0}
```

Zodra het resultaat ontvangen is slaat het alle Vulnerability gegevens in de Map van de Context op.

```
2016-11-24 13:45:28,378 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler
-:::- VA: received data from Mnt:
{"operationType":2,"isPeriodicScanEnabled":false,"heartBeatTime":1479991526437,"lastScanTime":0}
2016-11-24 13:45:33,642 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::- Got message from VaService:
[{"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","lastScanTime":1479962572758,"vuln
erabilities":[{"vulnerabilityId":"ssl-cve-2016-2183-sweet32","cveIds":"CVE-2016-
2183","cvssBaseScore":5,"vulnerabilityTitle":"TLS/SSL Birthday attacks on 64-bit block
ciphers (SWEET32)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-
static-key-
ciphers","cveIds":"","cvssBaseScore":2.5999999,"vulnerabilityTitle":"TLS/SSL
Server Supports The Use of Static Key Ciphers","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"rc4-cve-2013-2566","cveIds":"CVE-2013-
2566","cvssBaseScore":4.30000019,"vulnerabilityTitle":"TLS/SSL Server Supports RC4
Cipher Algorithms (CVE-2013-2566)","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"tls-dh-prime-under-2048-
bits","cveIds":"","cvssBaseScore":2.5999999,"vulnerabilityTitle":"Diffie-Hellman
group smaller than 2048 bits","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"tls-dh-
primes","cveIds":"","cvssBaseScore":2.5999999,"vulnerabilityTitle":"TLS/SSL Server
Is Using Commonly Used Prime Numbers","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"ssl-cve-2011-3389-beast","cveIds":"CVE-2011-
3389","cvssBaseScore":4.30000019,"vulnerabilityTitle":"TLS/SSL Server is enabling the
BEAST attack","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tlsv1_0-
enabled","cveIds":"","cvssBaseScore":4.30000019,"vulnerabilityTitle":"TLS Server
Supports TLS version 1.0","vulnerabilityVendor":"Rapid7 Nexpose"}]}]
2016-11-24 13:45:33,643 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::- VA: Save to context db,
lastscantime: 1479962572758, mac: 3C:97:0E:52:3F:D9
2016-11-24 13:45:33,675 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaPanRemotingHandler -:::- VA: Saved to elastic search:
{3C:97:0E:52:3F:D9=[{"vulnerabilityId":"ssl-cve-2016-2183-sweet32","cveIds":"CVE-2016-
2183","cvssBaseScore":5,"vulnerabilityTitle":"TLS/SSL Birthday attacks on 64-bit block
ciphers (SWEET32)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-static-key-
ciphers","cveIds":"","cvssBaseScore":2.5999999,"vulnerabilityTitle":"TLS/SSL Server
Supports The Use of Static Key Ciphers","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"rc4-
cve-2013-2566","cveIds":"CVE-2013-
2566","cvssBaseScore":4.30000019,"vulnerabilityTitle":"TLS/SSL Server Supports RC4
Cipher Algorithms (CVE-2013-2566)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tls-dh-
prime-under-2048-bits","cveIds":"","cvssBaseScore":2.5999999,"vulnerabilityTitle":"Diffie-
Hellman group smaller than 2048 bits","vulnerabilityVendor":"Rapid7 Nexpose"},
{"vulnerabilityId":"tls-dh-
primes","cveIds":"","cvssBaseScore":2.5999999,"vulnerabilityTitle":"TLS/SSL Server
Is Using Commonly Used Prime Numbers","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-
cve-2011-3389-beast","cveIds":"CVE-2011-
3389","cvssBaseScore":4.30000019,"vulnerabilityTitle":"TLS/SSL Server is enabling the
BEAST attack","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tlsv1_0-
enabled","cveIds":"","cvssBaseScore":4.30000019,"vulnerabilityTitle":"TLS Server
Supports TLS version 1.0","vulnerabilityVendor":"Rapid7 Nexpose"}]}
```

Aantekeningen die moeten worden gecontroleerd - vaservice.log. U kunt deze direct staart vanaf ISE CLI:

```
ISE21-3ek/admin# toont logapplicatie vaservice.log tail
```

Aanvraag tot Kwetsbaarheidsbeoordeling ingediend bij adapter.

```
2016-11-24 12:32:05,783 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA request submitted to
adapter","TC-NAC.Details","VA request submitted to adapter for processing","TC-
NAC.MACAddress","3C:97:0E:52:3F:D9","TC-NAC.IpAddress","10.229.20.32","TC-
NAC.AdapterInstanceUuid","c2175761-0e2b-4753-b2d6-9a9526d85c0c","TC-NAC.VendorName","Rapid7
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}
2016-11-24 12:32:05,810 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg res: {"status":"SUCCESS","statusMessages":["SUCCESS"]}
```

AdapterMessageList controleert elke 5 minuten de status van de scan tot deze is voltooid.

```
2016-11-24 12:36:28,143 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :
{"AdapterInstanceName":"Rapid7","AdapterInstanceUid":"7a2415e7-980d-4c0c-b5ed-
fe4e9fadadbd","VendorName":"Rapid7 Nexpose","OperationMessageText":"Number of endpoints queued
for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for
which the scan is in progress: 1"}
2016-11-24 12:36:28,880 DEBUG [endpointPollerScheduler-5][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","Adapter Statistics","TC-
NAC.Details","Number of endpoints queued for checking scan results: 0, Number of endpoints
queued for scan: 0, Number of endpoints for which the scan is in progress: 1","TC-
NAC.AdapterInstanceUuid","7a2415e7-980d-4c0c-b5ed-fe4e9fadadbd","TC-NAC.VendorName","Rapid7
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}
De adapter krijgt CVE's samen met de CVSS-scores.
```

```
2016-11-24 12:45:33,132 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :
{"returnedMacAddress":"","requestedMacAddress":"3C:97:0E:52:3F:D9","scanStatus":"ASSESSMENT_SUCC
ESS","lastScanTimeLong":1479962572758,"ipAddress":"10.229.20.32","vulnerabilities":[{"vulnerabil
ityId":"tlsv1_0-enabled","cveIds":"","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS
Server Supports TLS version 1.0","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"rc4-cve-2013-2566","cveIds":"CVE-2013-
2566","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS/SSL Server Supports RC4 Cipher
Algorithms (CVE-2013-2566)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-cve-
2016-2183-sweet32","cveIds":"CVE-2016-2183","cvssBaseScore":"5","vulnerabilityTitle":"TLS/SSL
Birthday attacks on 64-bit block ciphers (SWEET32)","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"ssl-static-key-
ciphers","cveIds":"","cvssBaseScore":"2.59999999","vulnerabilityTitle":"TLS/SSL Server Supports
The Use of Static Key Ciphers","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tls-
dh-primes","cveIds":"","cvssBaseScore":"2.59999999","vulnerabilityTitle":"TLS/SSL Server Is Using
Commonly Used Prime Numbers","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tls-dh-
prime-under-2048-bits","cveIds":"","cvssBaseScore":"2.59999999","vulnerabilityTitle":"Diffie-
Hellman group smaller than 2048 bits","vulnerabilityVendor":"Rapid7
Nexpose"}, {"vulnerabilityId":"ssl-cve-2011-3389-beast","cveIds":"CVE-2011-
3389","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS/SSL Server is enabling the BEAST
attack","vulnerabilityVendor":"Rapid7 Nexpose"}]}
2016-11-24 12:45:33,137 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Endpoint Details sent to IRF is
{"3C:97:0E:52:3F:D9":[{"vulnerability":{"CVSS_Base_Score":5.0,"CVSS_Temporal_Score":0.0},"time-
stamp":1479962572758,"title":"Vulnerability","vendor":"Rapid7 Nexpose"}]}
2016-11-24 12:45:33,221 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA successfully
```

```
completed","TC-NAC.Details","VA completed; number of vulnerabilities found: 7","TC-  
NAC.MACAddress","3C:97:0E:52:3F:D9","TC-NAC.IpAddress","10.229.20.32","TC-  
NAC.AdapterInstanceUuid","c2175761-0e2b-4753-b2d6-9a9526d85c0c","TC-NAC.VendorName","Rapid7  
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}]  
2016-11-24 12:45:33,299 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -  
:::::- VA SendSyslog systemMsg res: {"status":"SUCCESS","statusMessages":["SUCCESS"]}
```

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [ISE 2.2 Releaseopmerkingen](#)
- [ISE 2.2 hardwareinstallatiehandleiding](#)
- [ISE 2.2 upgrade-gids](#)
- [ISE 2.2 Besturingsgids voor de motor](#)