# 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 on 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** 

3	Installer - Nexpose - 🗖 🗙
nexpose	Select components and an installation path
Welcome License agreement • <b>Type and destination</b> System check User details Database port Account details Shortcut location Confirm selections Installation progress Initialization	<ul> <li>Select only the set of components you want to install. If you want to modify the installation directory, click *Change*. Once you have selected your installation directory click *Next*.</li> <li>Nexpose Security Console with local Scan Engine If you do not have a console installed yet, this option is recommended. The console manages scan engines and all Nexpose operations. Nexpose Scan Engine only This distributed engine can start scanning after being paired with a Nexpose Security Console. Communication Direction: Engine to Console Image: Security Console Ima</li></ul>
Console details Installation success	Destination directory: C:\Program Files\rapid7\nexpose Change Free disk space: 26,603 MB
RAPID	Cancel Previous Next

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

=	nexpose <sup>*</sup> Create $\vee$					<b>%</b>	@~	đ	۹	admin	
	<ul> <li>Users</li> </ul>	Asset Groups	24 Exceptions and Overrides		m c	lendar					
	Create and manage user accounts or manage custom user roles	Create dynamic or static asset groups and manage existing asset	Review requests to exclude vulnera	abilities from reports and to	View ca	endar of all	scheduled sca	ans, blackout:	s, database	operations	
	and password policy.	groups.	override policy compliance results.		and rep	orts.					
	Scan Options										
	ENGINES Create and manage available Scan Err SHABED CREDENTIALS Create and manage shared credential	ngines, and Scan Engine Pools.	HISTORY	View current and past scans for this Create and manage scan templates	installation.	and tuning	scans				
	BLACKOUTS Create and manage global blackout s	lettings.	ROOT CERTIFICATES	Manage root certificates used in sca	inning and wa	rehouse exp	port.				
	Q. Discovery Options		Global and Console Settings								
	NSX MANAGER Create and manage settings that give the NSX OVF distribution.	a Scan Engine direct access to an NSX network of virtual assets.Update	GLOBAL	Manage global settings for selecting	g risk score st	ategies and	d excluding ass	ets from sca	ns.		
	CONNECTIONS Create and manage connections that a	allow the Security Console to discover assets dynamically.	GONGOLL	Harminister searings for the decarry	conduite, more	any auto a	poore and rogg	ying secongo.			
	EVENTS View events and statistics for asset die	scovery mechanisms.									

Klik op Certificaat beheren, zoals in de afbeelding weergegeven:

≡	nexpose <sup>®</sup> Create V		
Û			
	Security Console Cont	figuration	
ç	GENERAL	The Security Console contains an embedded	d web server. The following web server settings can be configured.
<b></b>	UPDATES	WEB SERVER SETTINGS	
$\oslash$	WEB SERVER	Web server port	3780
â	PROXY SETTINGS	Session timeout (seconds)	600
Ø	AUTHENTICATION	initial request handler threads	100
0	DATABASE	Failed login threshold	4
	SCAN ENGINES	HTTPS certificate	Issued to nexpose.example.com
	LICENSING		Valid until Thu Nov 22 01:16:44 PST 2018
	EXPOSURE ANALYTICS		MANAGE CERTIFICATE

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)	nexpose.example.com
Country (two letter country ISO code. e.g. US)	
State/Province	
Locality/City	
Organization	
Organizational unit	
Valid for (years)	10
	CREATE BACK

Exporteren certificaataanvraag (CSR) bij de terminal.



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

Th the Se	e Security Console has generated a certificate signing request for the current certificate. You may copy CSR below and send it to your CA for signature. The signed certificate can later be imported into the curity Console using the 'Import Signed Certificate' button
	BEGIN NEW CERTIFICATE REQUEST
N	IIIEYzCCAksCAOAwHiEcMBoGA1UEAxMTbmV4cG9zZS5leGFtcGxlLmNvbTCCAilw
D	OYJKoZlhycNAOEBBOADggIPADCCAgoCggIBAIWOyIrdSOIrDwLMaHEISgHZoG4G
0	yg3oC9MeML7s1TugD0K4pvmlZ0h1E+B6bK7Z0B3QAnf9/VxKaur/Q/yCNj1AcYH
G	B+Sq4bAfqHFIKlsidni3e00LW7h8TPmD57N0z0v4X8v6D0z42YF8TNSmScbeTZ5
q	4gc9DH6RuYU0EYawclWs+7wTVRDt+hvFL6v6e6relXF7Nlp8ssgC02ZvDGzLnzb
m	wJFNG13BILZvkhiMzZVsnnGWAn9IahaORNftXW5JHYdFVs84WeB+DKX1KWneiaL
r:	ay1voSprJXincC3xAXHWQGFknY8d8eoaEM82fUdzz6Y/jOgUH6ToZ5mEAsKINg
J	EQpzLxjQsnAZRG8dy9+J52S6Zm7RXyCg0p7MRKlykE0MGEqR5TF0ZWCfTxomvzp
S	0WExoXpWL8oZb0tPHheWaQSmPStzeuQpiFXNjth/XQ0gHpc48v+1DdDeZI/wrLd
j8	4GMbFuYvBq+x08prU/kGEVftVABGHnjnstGN+qM8CU93mq/6NNPmz8XCgAxCOm
w	/oD2cQFCdp1XBC7cUdvkXMIJwqQXtpd8uz9ZLvK+afJT8cBphledh1Fy+v7Mu+m
0	eNlx41XDaudLii/SuYBB03DLbN6Inu7Vp+5/3W59lcfmHlt+3oEJAnWx2vVCLgD

Importeer het door CA afgegeven certificaat door op het invoercertificaat te klikken.

This dialog enables you to create and manage the HTTPS certificate used by the Security Console web server. By default the Security Console uses a self-signed X.509 certificate which is created during installation. This certificate can be replaced by a custom self-signed certificate or a certificate signed by a trusted Certification Authority (CA) like Verisign, Thawte or your own CA. You may perform one or more of the following operations:

- Create New Certificate: 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 CSR.
- Generate CSR: Once you have created a custom certificate you may generate a Certificate Signing Request (CSR) for the current certificate. You may copy the generated CSR and send it to your Certification Authority.
- 3. Import Certificate / Certificate Chain: After you obtain a signed certificate from your CA you may import it to the Security Console. The Security Console will only accept a certificate that matches the current certificate/keypair. Make sure that the certificate has not been changed since you generated the CSR for this certificate.

The signed certificate **must** be based on a Certificate Signing Request generated by the Security Console. The Security Console does not allow you to import an arbitrary keypair/certificate generated by you.

CLOSE

View current certificate.

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.

≡	nexpose	Create 🔨
仚		Asset Group
		Dynamic Asset Group
		Report
_	0	Site
Ţ	0	Tags

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.

=	nexpose	Create 🗸						■ %	ූ <sup>6</sup>
	Site Cor	nfiguration							SAVE & SCAN SAVE CANCEL
		NFO & SECURITY	ASSETS		I TEMPLAT	S ENGINI	is	ALERTS	SCHEDULE
	GENERAL		General						
	ORGANIZATI	ION		Nama					
	ACCESS			Importance	Normal	~			
				Description					
									li
			User-added Tags  CUSTOM TAGS		LOCATIONS	OWNERS		CRITICALITY	
			None		None	None		None	Add tags
	nexpose'	Create 🗸							ද්
	Site Cor	nfiguration							SAVE & SCAN SAVE CANCEL
									<b>—</b>
			ASSETS	AUTHENTICATION	I TEMPLAT	S ENGINI	s	ALERTS	SCHEDULE
	Specify as	ssets by Names/Address	connection						
	INCLUD	Assets Browse No	file selected.			1 assets 🗸	D D	Assets Browse No file selected.	0 assets 🗸
		10.229.20.32 × Enter name	e, address, or range.					Enter name, address, or range.	
							÷		

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

≡	nexpose	Create V		5×	@~	<u>م</u> ۹	ද උ admin
	cu	STOM CERTIFICATES 💿					^ ×
쓧		MPORT CERTIFICATES					
	Die	tinguished Name	SHA-1 Fingerprint			Expired	a On Delete
0	Ch	ir LAB CA, DC-kexample, DC-kom	FD729A388533726FF8450	358A2F7EB27I	EC8A1178	02/12/	2025
8							
ø	PR	ESET CERTIFICATES 💿					
	Di	tinguished Name	SHA-1 Fingerprint			Expirer	a On
Č.	01	InDigiCent Assumed ID Root CA, OUHwww.digicent.com, 0-DigiCent Inc, C-US	056388630D62D75A8BC8/	NB1E4BDFB5A	899B24D43	11/10/	/2031
=	CP	I+TC TrustCenter Class 2 CA II, 0U-TC TrustCenter Class 2 CA, 0+TC TrustCenter GmbH, C+DE	AE5083ED7CF45CBC8F610	621FE685D79	4221156E	12/31/	/2025
	Ð	AAILADDRESS-premium-serveri@thawte.com, CN=Thawte Premium Server CA, OU-Dertification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA	E0AB05942072549305606	2023670F7CD:	2EFC6666	01/02/	/2021

## **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 Identity Services Engine	Home + C	Context Visibility	Belicy	Administration	► Work Centers
▼System Identity Management	Network Reso	ources	ment pxGrid Servic	ces Feed Sen	vice
Deployment Licensing Certification	ates + Logging	Maintenance Upgrade	Backup & Restore	Admin Access	<ul> <li>Settings</li> </ul>
System      Identity Management     Deployment     Licensing      Certifica      Deployment     ✓      ✓	Network Reso ates      Logging	Policy Service	ment pxGrid Servic Backup & Restore lek ing Configuration SE22-1ek SE22-1ek.example. 0.48.23.86 dentity Services En	Admin Access Admin Access com gine (ISE) Role STANDA Role PRIMA	VIONE Make Primary VIONE Other Monitoring Node
			Personas v/ces tric NAC Service trin Service	Include Node     Use Interface	in Node Group None v (i) GigabitEthernet 0 v

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)

dentity Services Engine	Home   Context Visibility   Operations   Polic	Y Administrat	tion Vork Centers						Licens
System Identity Management     Deployment Licensing Certificate	Network Resources     Device Portal Management     pxGi     p	id Services Fe	eed Service	ric NAC					Click here to do wireless setup
0									
- Certificate Management	Trusted Certificates								
System Certificates	🖊 Edit 💠 Import 🔀 Export 🗙 Delete 🔎 View								SI
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Tue, 13 May 2025	<b>Z</b>
Certificate Signing Requests	Cisco CA Manufacturing	Ø Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 2029	<b>Z</b>
Certificate Periodic Check Setti	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	2
Certificate Authority	Cisco Root CA 2048	Ø Disabled	Endpoints Infrastructure	5F F8 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	Image: A start and a start and a start a st
	LAB CA#LAB CA#00005	Enabled	Infrastructure Endpoints	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	Infrastructure Cisco Services Endpoints	-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	<b>~</b>
	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.

dentity Services En	gine Home	Context Visib	lity • Operations	Policy	<ul> <li>Administration</li> </ul>	n 💦	Work Centers
System Identity Mana	gement • Networ	k Resources	evice Portal Managemen	t pxGrid S	ervices Feed	Service	Threat Centric NAC
Third Party Vendors							
Vendor Instances > New Input fields marked with an a	isterisk (*) are require	ed.					
Vendor *	Rapid7 Nexpose	VA			•		
Instance Name *	Rapid7						
				Cancel	ave		

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.exan	nple.com
The hostname o	f the Nexpose Security Console Host.
Nexpose port	
3780	
The port of the	Nexpose Security Console host.
Username	
admin	
Username to ac	cess Nexpose Security Console.
Password	
Password	
Password 	user.
Password Password of the	user.
Password Password of the Http proxy Ho	user. st
Password Password of the Http proxy Ho	user. st
Password Password of the Http proxy Ho	user. st oxy host. Requires proxy port also to be set.
Password Password of the Http proxy Ho Optional http pr	user. st bxy host. Requires proxy port also to be set. t
Password Password of the Http proxy Ho Optional http pr Http proxy po	user. st oxy host. Requires proxy port also to be set. t

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 Voltooien**. Instantieovergangen naar **actieve** toestand en downloads met kennisbasis openen.

dentity	y Services Engine	Home   Contex	tt Visibility → O	perations   Policy	✓Administration	Work Centers
System	Identity Managemen	Network Resources	Device Portal	Management pxGrid Serv	vices Feed Service	Threat Centric NAC     ■
Third Party Ve	endors					
Vendor Ins	stances n <b>∔</b> Add	<b>Trash ▼ ⓒ</b> Edit Re	start Stop			〒 Filter マ 🌣 マ
Inst	ance Name	Vendor Name	Туре	Hostname	Connectiv	ity Status
Rap	id7	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.

dentity Services Engine	Home  Context Visibility  Operations  Policy  Administration  Work Centers
Global Exceptions Policy Authentication	n Authorization Profiling Posture Client Provisioning   Policy Elements
Dictionaries Conditions Results	
0	* Name Rapid7
Authentication	Description
- Authorization	* Access Type ACCESS_ACCEPT T
Authorization Profiles	Network Device Profile 🚓 Cisco 💌 🕀
Downloadable ACLs	Service Templete
▶ Profiling	Track Movement
▶ Posture	Passive Identity Tracking ()
Client Provisioning	
	<ul> <li>Common Tasks</li> <li>Assess Vulnerabilities</li> <li>Adapter Instance</li> <li>Rapid7 •</li> <li>Trigger scan if the time since last scan is greater than 48 Enter value in hours (1-9999)</li> <li>Advanced Attributes Settings</li> <li>Select an item • = • • • • • • • • • • • • • • • • •</li></ul>

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.

-strate Identi	y Services Engine Home +	Context Visibility	k Centers	License Warning 🔺 🤍 🔍 🎯 Ö
Global Excep	tions Policy Authentication Authoriza	ation Profiling Posture Client Provisioning   Policy Elements		Click here to do wireless setup and visibility setup Do not show this again.
Authorizati Define the Aut For Policy Exp First Matched	on Policy orization Policy by configuring rules based et go to Administration > System > Backup Rule Applies	t on identity groups and/or other conditions. Drag and drop rules to change the order & Restore > Policy Export Page		
<ul> <li>Exception</li> </ul>	ns (1)	A control on a first solid control on a static control and the control of the con		
ii 🔽	Fulle Name	Conditions (identity groups and other conditions)	Permissions	
Standard				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Access	Edit I 🕶
	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones	Edit I 🕶
	Profiled Non Cisco IP Phones	If Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit I 👻
0	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices )	then PermitAccess	Edt I 👻
0	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD	Edit I 🕶
0	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD	Edit I 👻
	Wired_Guest_Access	If (Guest_Flow AND Wired_MAB)	then PermitAccess AND Guests	Edit I 👻
	Wi-FI_Guest_Access	If (Guest_Flow AND Wireless_MAB )	then PermitAccess AND Guests	Edit I 👻
	Wired_Redirect_to_Guest_Login	if Wired_MAB	then Cisco_WebAuth	Edit i v
0	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth	Edit i 🕶
	Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then Rapid7	Edit I 🕶
	Default	if no matches, then DenyAccess		Edt I 👻

# 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.

dentity	Services Engine	Home Conte	xt Visibility	• Operations	Policy	Administration	Work Centers							License	e Warning 🔺 🔍		0
▼RADIUS 1	Threat-Centric NAC Live I	.ogs + TACACS	Troublesho	ot Adaptive	Network Contro	ol Reports							Click her	e to do wireless setur	and visibility setup	to not show this again	X
Live Logs Li	ive Sessions																
		Misconfigured Su	pplicants O		Misconfig	ured Network Devic	tes O	RADIUS Drops	0	с	lient Stopped Responding 0		Repe	at Counter 0			
		0				0		0			0			0			
											Refre	h Every 1 minute	• Sho	Latest 20 reco	rds 🚽 Within	Last 24 hours	•
C Refresh	Reset Repeat Count	s 🚊 Export To 🗸														▼ Filter -	۰.
Time		Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Profiles	IP Address	N	etwork Device	Device Port	Identity Grou	up
×		Status -	]		Identity		Endpoint ID	Endpoint Profi	Authentication	Authorization	Authorization Profiles	IP Address		Network Device	Device Port	Identity Group	ip
Nov 24, 3	2016 01:45:41.438 PM	0	0	0	alice		3C:97:0E:52:3F:0	09 Nortel-Device	Default >> D	Default >> E	Quarantine	10.229.20.32			FastEthernet1/0/5	5	
Nov 24, 3	2016 01:45:40.711 PM	<b>2</b>	0		alice		3C:97:0E:52:3F:0	9 Nortel-Device	Default >> D	Default >> E	Quarantine	10.229.20.32	S	witch_2960	FastEthernet1/0/5	Profiled	
Nov 24, 3	2016 01:45:39.166 PM	2	0				3C:97:0E:52:3F:0	99					s	witch_2960			
Nov 24, 3	2016 01:32:00.564 PM	<b>~</b>	0		alice		3C:97:0E:52:3F:0	99	Default >> D	Default >> B	Rapid7	10.229.20.32	S	witch_2960	FastEthernet1/0/5	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.

cisco Identity	y Services Engine Home		<ul> <li>Operations</li> </ul>	Policy	Administration	Work Centers
Endpoints	Users Network Devices					
Endpoints >	3C:97:0E:52:3F:D9					
		_				
3C:97:0	E:52:3F:D9 ØØ	8				
Ę	MAC Address: 3C:97:0E:52:3 Username: alice Endpoint Profile: Nortel-Devic Current IP Address: 10.229.20 Location: Location → All Loc	F:D9 ee 0.32 ations				
Ap	plications Attributes	Authentication T	hreats Vulr	erabilities		
ssl-cve-201	16-2183-sweet32					
Title:	TLS/SSL Birthday attacks on 6	4-bit block ciphers (SWEE	ET32)			
CVSS score	e: 5					
CVEIDS:	CVE-2016-2183					
Reported by	y: Rapid7 Nexpose					
Reported at	t: Thu Nov 24 05:42:52 CET 201	6				
aal atatia l	au alabara					
SSI-STATIC-K	ey-cipners					
Title:	TLS/SSL Server Supports The	Use of Static Key Ciphers	3			
CVSS score	e: 2.5999999					
CVEIDS:						
Reported by	y: Rapid7 Nexpose					
Reported at	t: Thu Nov 24 05:42:52 CET 201	6				
rc4-cve-20	13-2566					
Title:	TLS/SSL Server Supports RC4	Cipher Algorithms (CVE-	2013-2566)			
CVSS score	e: 4.30000019					
CVEIDS:	CVE-2013-2566					
Reported by	y: Rapid7 Nexpose					
Reported at	t: Thu Nov 24 05:42:52 CET 201	6				

In Operations > TC-NAC Live Logs kunt u autorisatiebeleid zien toegepast en details zien over CVSS\_Base\_Score.

dentity Services Engine Home	Context Visibility     Operat	tions Policy	Administration	Work Center	5			License Warning 🔺 🔍		•	5
RADIUS Threat-Centric NAC Live Logs     1	TACACS Troubleshoot A	daptive Network Contro	Reports					Click here to do wireless setup and visibility setup D	to not show thi	is again.	×
Threat Centric NAC Livelog											
C Refresh 🚨 Export To 👻 🔳 Pause									▼ Filter ▼	۰۰	
Time	Endpoint ID	Username	Incident type	Vendor	Old Authorization profile	New Authorization profile	Authorization rule matched	Details			
×	Endpoint ID	Username	Incident type	Vendor	Old Authorization profile	New Authorization profile	Authorization rule matched				
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**.

SITES										
Name	Assets	Vulnerabilities	Risk 🗸		Scan Engine	Туре	Scan Status	Scan	Edit	Delete
TAC AAA	1	10		2,016	Local scan engine	Static	Scan finished on Thu, Nov 24th, 2016	C	0	1
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

=	nexpo	se	Create											⊙~ (	5° c		admin
Û																	🗅 items 🗸
먦		TAC A	AA   View all :	sites													
Q																	
44		1	DDRESSES	10.229.20	0.32	OS	Kicrosoft Windows 🔀	RISK SC	CORE 😡			U	SER-ADDED TA	GS 🕜			
~		ŀ	ARDWARE	Unknown		CPE		ORIC	SINAL		CUSTOM TAGS			OWN	ERS		
Ø		1	LIASES	TAC-PC		LAST SCAN	Nov 24, 2016 4:42:07 AM (6 minutes ago)	2,0	10		None			NO	ne		
Q		F L	INIQUE	Unknown		NEXT SCAN	Not set	CONTEX	T-DRIVEN		LOCATIONS			CRITIC	ALITY		Add tags
Ø		1	DENTIFIERS					2,0	)16		None			Nor	ne		
		9	ATE	TAC AAA													
0		s	CAN ASSET NO	W CR	EATE ASSET REPORT DELETE ASSET	SEND LOG											
≔																	_
≡	nexpos	e'	Create												đ		😤 admin
ŵ																	
_																	
		VUL	NERABILITIE	s													
88		VUL	NERABILITIE details about dis	S	nerabilities. To use one of the exception controls	s on a vulnerability, se /alidated with Metaso	lect a row. To use the control with all displayed displayed vulneration of a first sector unbilithed exclored and the sector of	abilities, select the top row a	ind use Selec	rt Visible. Car	icel all selections using Clear All. (						
88 <b>P</b>		VUL View Expo	NERABILITIE details about dir sures: 發 Susc	S scovered vult	nerabilities. To use one of the exception control alware attacks 🖗 Metaspioit-exploitable 🐞 V	s on a vulnerability, se Validated with Metasp	fect a row. To use the control with all displayed displayed valueration . To use the control with all displayed wither a control to the control of the contr	abilities, select the top row a	ind use Selec	rt Visible. Car	icel all selections using Clear All. (	•					
8		VUL View Expo	NERABILITIE details about dir sures: 🔮 Susc	S scovered vul reptible to ma RECALL	nersbillities. To use one of the exception control alware attacks @ Metasploit-exploitable @ Y RESUBNIT	s on a vulnerability, se Validated with Metasp	Net a row. To use the control with all displayed displayed vulneral to ${\bf A}_{\rm p}$ Validated with published exploit	abilities, select the top row a	ind use Selec	rt Visible. Car	ncet all selections using Clear All. (	•		Το	stal Vulnerab	ilities Sele	lected: 0 of 10
器 D 父		VUL View Expo	NERABILITIE details about din sures: & Susc EXCLUDE	S scovered vulr eptible to m RECALL	nersölliles. To use one of the exception commo alware attacks @ Metasploit exploitable @ v RESUBMIT	s on a vulnerability, se /alidated with Metasp	Ret a row. To use the control with all displayed displayed vulneral ioit. 👗 Exploit published 🐴 Validated with published exploit	abilities, select the top row a	ind use Selec	t Visible. Car CVSS	noet all selections using Clear All. ( Risk Published 0	э • м	udified On	To Severity v	stal Vulnerab	ilities Sele	iected: 0 of 10 ceptions
器 <b>〕</b>		VUL View Expo	NERABILITIE details about dir sures: 🛞 Susc EXCLUDE TItle TLS/SSL Bir	S scovered vulk eptible to ma RECALL thday attack	nerabilities. To use one of the exception common alware attacks @ Metasploit-exploitable @ v RESUBNIT us on 64-bit block ciphers (BWEET22)	s on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral to $\underline{X}$ Exploit published $\frac{1}{2}$ Validated with published exploit	abilities, select the top row a	and use Selec	t Visible. Car CVSS	Risk Published 0 425 Wed Aug 24	n M 2016 Fr	odified On Sep 02 2016	To Severity ~ Severe	tal Winerab	Allties Self B Ext 1 2	ected: 0 of 10 ceptions Exclude
品 日 冬 〇 〇		VUL View Expo	NERABILITIE details about dis sures: Susc EXCLUDE TIS/SSL Bin TLS/SSL Bin TLS Server 1 TLS Server 1	S scovered vulk eptible to mining the scovered vulk eptible to mining the scovered vulk eptitic scovered vulk eptitics and scovered vulk eptitics scovered vulk eptitics scovered vulk epiterics scove	nerabilities. To use one of the exception control where attacks (2) Metasplot-explorable (3) v RESUBMT as on 64-bit block ciphers (DWEET32) 5 version 1.0 5 version 1.0	s on a vulnerability, se validated with Metasp	fect a row. To use the control with all displayed displayed vulneral ion 3. Exploit published in Validated with published exploit	abilities, select the top row <i>t</i>	and use Selec	CVSS 4.3	Risk Published 0	m M 2016 Fr 1014 TP	odified On Sep 02 2016 u Nov 12 2015	Severe Severe Severe Severe	stel Vulnerab	filties Self Ex 1 2 1 2	ected: 0 of 10 ceptions Exclude Exclude
88 ● � ⊘ Q3			NERABILITIE details about din sures: 😥 Susc EXCLUDE TLS/SSL Bin TLS/SSL Bin TLS/SSL Se TLS/SSL Se	IS scovered vulk septible to m RECALL thday attack Supports TLS river Supports	nersbillies. To use one of the exception controls where attacks IP Metasplot-exploitable IP ( RESUBMIT Is on 64-bit block ciphers (UWEET32) S version 1.0 Is RC4 Cipher Algorithms (CVE2013-2566) Ion the BEAT stack	s on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral ion T. Exploit published with published exploit	abilities, select the top row a	and use Selec	t Visible. Car CVSS 4.3 4.3 4.3	Risk Published 0 425 Wed Aug 24 324 Tue Oct 14 397 Tue Beo 6	M M 2016 Fr 2014 TP 2013 TP	dified On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016	To Severity ~ Severe Severe Severe Severe	stal Vulnerab	Allties Self B Exc 1 @ 1 @ 1 @	ected: 0 of 10 ceptions Exclude Exclude Exclude
88 ♥ ♥ ♥		VUL View Expo	NERABILITIE details about dii details about dii EXCLUDE TLS/SSL Bii TLS/SSL Bii TLS/SSL Se TLS/SSL Se TLS/SSL Se	S scovered vult eptible to mi RECALL thday attack Supports TLS river Supports river support river is enabli	nersbillies. To use one of the exception controls alware attacks @ Metasplot-exploitable @ V RESUBMIT as on 64-bit block ciphers (SWEET32) a version 1.0 as RC4 Cipher Algorithms (CVE2013-2566) ing the BEAT attack. Commonly Used Prime Numbers	s on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral lot 3. Exploit published 👋 Validated with published exploit	abilities, select the top row 4	and use Selec	CVSS 4.3 4.3 4.3 2.6	Risk Published O 425 Wed Aug 24 324 Tue Oct 14 377 Tue Mari 448 Tue Sep 66 91.0 Wed May 23	M 2016 Fr 2013 TP 2013 TP 2011 TP 2015 TP	odified On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Feb 18 2016	To Severity ~ Severe Severe Severe Severe Moderate	Instancer	Alties Still B Ext 1 @ 1 @ 1 @ 1 @	ected: 0 of 10 ceptions Exclude Exclude Exclude Exclude
88 <b>0</b> ↔ ⊘ Q2		VUL	NERABILITIE details about dii details about dii DEXCLUDE EXCLUDE TILS/SSL Bin TILS/SSL Se TILS/SSL Se TILS/SSL Se TILS/SSL Se Diffie Helim	S scovered vulk eptible to mu RECALL thday attack Supports TLS river Supports river Supports river is enablit river is Using an group sm	nersbillies. To use one of the exception control alware attacka @ Metaspiot-exploitable @ V RESUBMT as on 64-bit block ciphers (SWEET32) S version 1.0 as RC4 Opher Algorithms (CVE:2013-2566) ling the BAST attack Commonly Used Prime Numbers aller than 2048 bits	s on a vulnerability, ss	lect a row. To use the control with all displayed displayed vulneral ion 3. Exploit published and Validated with published exploit	abilities, select the top row a	end use Selec	t Visible. Car CVSS 4.3 4.3 4.3 2.6 2.6	Risk Published 0 425 Wed Aug 24 324 Tue Oct 14 327 Tue Mar 12 448 Tue Strol Mar 22 91.0 Wed May 22 91.0 Wed May 22	M 2016 Fr 2013 TP 2013 TP 2015 TP 2015 TP	xdified On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Jun 16 2016	Severity ~ Severo Severo Severo Severo Severo Severo Moderate	tal Vulnerab	Alletes Self 9 Exc 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2	ected: 0 of 10 coptions Exclude Exclude Exclude Exclude Exclude Exclude
88 ● ★ ⊘ ♀		VUL View Expo	NERABILITIE details about di sures: & Susc EXCLUDE TLS/SSL Bi TLS/SSL Se TLS/SSL Se TLS/SSL Se Diffie-Hellm TLS/SSL Se	S scovered vulk eptible to mi RECALL thday attack Supports TLS river Supports river senabil river is using an group sm river Supports	Intersalilities. To use one of the exception control alware attacka P Metaspiot-exploitable V RESUMIT as on 64-bit block ciphers (SWEET32) S version 1.0 8 RC4 Cipher Algorithms (CVE:2013-2564) ing the BEAST attack Commonly Used Prime Numbers aller than 2048 bits as The Used Flatck Kay Ciphers	s on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral tort 🚡 Exploit published 👘 Validated with published exploit	abilities, select the top row a	and use Selec	t Visible. Car CVSS 4.3 4.3 2.6 2.6 2.6 2.6	Risk Published 0 425 Wed Aug 24 324 Tue Oct 14 397 Tue Mar 12 448 Tue Step 0 91.0 Wed May 22 91.0 Wed May 22 240 Sun Feb 01	M M 2016 Fr 2013 Tr 2013 Tr 2015 Tr 2015 Tr 2015 W	vdiffied On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2015 vd Sep 30 2015	To Severity - Sever Sever Sever Sever Moderate Moderate	stal Vulnerab	Iltries Sel Exc P C P C	ected: 0 of 10 ceptions Exclude Exclude Exclude Exclude Exclude Exclude Exclude Exclude
88 ● 🛠 ⊘ 🔉 🕑 🖽			NERABILITIE details about di sures: & Susc EXCLUDE EXCLUDE TIS'SSL Bis TLS'SSL Se TLS'SSL Se TLS'SSL Se TLS'SSL Se Diffie Helim TLS'SSL Se Diffie Helim TLS'SSL Se	S scovered vult eptible to mi RECALL thday attack Supports TLS river Support river is using an group sm river Support imp response	Intersbillides. To use one of the exception control alware attacks RESUBMIT as on 64-bit block ciphers (BWEET32) S version 1.0 8 RC4 Cipher Algorithms (CVE-2013-2566) ing the BEATS attack 4. Commonly Used Prime Numbers allier than 2048 bits 3 The Used of Static Key Ciphers e	s on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral tort 🚡 Exploit published 👘 Validated with published exploit	abilities, select the top row a	and use Selec	CVSS CVSS 4.3 4.3 2.6 2.6 2.6 2.6 0 0 0	Risk Published 0 425 Wed Aug 24 324 Tue Oct 14 397 Tue Mar 12 48 Tue Sep 06 91.0 Wed May 22 240 Sun Feb 01 0.0 Fri Aug 01	2016 Fr 2016 Fr 2013 TF 2013 TF 2015 TF 2015 TF 2015 TF 2015 TF	diffed On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2015 rd Sep 30 2015 rd Sep 30 2015	To Severity ~ Severe Severe Severe Moderate Moderate Moderate	tal Winerab	altries Sel Exc Por	ected: 0 of 10 ceptions Exclude Exclude Exclude Exclude Exclude Exclude Exclude Exclude Exclude
88 ▶ ☆ ⊘ ♀ ==			NERABILITIE details about di sures: Susc EXCLUDE TLS/SSL Bie TLS/SSL Se TLS/SSL Se TLS/SSL Se TLS/SSL Se TLS/SSL Se Diffe-Hellm TLS/SSL Se Diffe-Hellm TLS/SSL Se	S scovered vuli eptible to mi RECALL thday attack Supports TLS river Supports river Supports river is Using an group sm river Support imp respons Traffic Ampl	nersbillies. To use one of the exception common alware attacks in the exception and in the exception of the exception and in the exception of	s on a vulnerability, se	lect a row. To use the control with all displayed displayed vulneral lot 🚡 Exploit published 👘 Validated with published exploit	abilities, select the top row a	and use Select	cvss cvss 4.3 2.6 2.6 2.6 0 0 0 0	Risk Published 0 425 Wed Aug 24 324 Tue Oct 14 397 Tue Mar 12 448 Tue Bep 66 91.0 Wed May 22 91.0 Wed May 22 91.0 Wed May 22 40 Sun Feb 01 0.0 Fir Aug 01 0.0 Sun Feb 00	2016 Fr 2016 Fr 2013 TF 2013 TF 2015 TF 2015 TF 2015 TF 2015 TF 2015 TF 2015 W	diffed On Sep 02 2016 u Nov 12 2015 u Apr 28 2016 u Feb 18 2016 u Jun 16 2016 u Nov 12 2015 rd Sep 30 2015 rd Sep 30 2015 rd Sep 30 2015 rd Sep 30 2015	To Severity ~ Severe Severe Severe Severe Moderate Moderate Moderate	stal Vulnerab	lities Self Exi Q	ected: 0 of 10 Deceptions Declude Declude Declude Declude Declude Declude Declude Declude Declude
88 <b>₽</b> ★ ⊘ & ⊵ @ ≡			NERABILITIE details about di sures: Susc EXCLUDE TLS:SSL Bit TLS:SSL Bit TLS:SSL Se TLS:SSL Se TLS:SSL Se Diffe-Hellm TLS:SSL Se Diffe-Hellm TLS:SSL Se	S scovered vuli eptible to mi RECALL thday attack Supports TLS river Supports river Support river Support my respons Traffic Ampli river Support	nersbillies. To use one of the exception common alware stacks in Metasploit-exploitable in v RESURMT as on 64-bit block ciphers (SWEET32) S version 1.0 S ve	s on a volnerability, se	fect a row. To use the control with all displayed displayed vulneral lot	shifties, select the top row a	and use Select	cvss standard data data data data data data data	Risk         Published           1         425         Wed Aug 2           3         324         Tue Oct 141           3         327         Tue Mar 12           4         4         Tue Step 66           9         10.         Wed May 20           2         240         Sun Feb 01           0         0.         Sun Feb 01           0         Sun Feb 01         Sun Feb 01	2016 Fr 2016 Fr 2013 TF 2013 TF 2015 TF 2015 TF 2015 TF 2015 TF 2015 TF 2015 W 2019 M	xdified On Sep 02 2016 u Nov 12 2015 u Pob 18 2016 u John 16 2016 u John 16 2016 u John 16 2016 u John 12 2012 xd Dec 10 2014 yn Feb 15 2016	Severity - Sever Sever Sever Sever Moderate Moderate Moderate Moderate	stal Vulnerab	<ul> <li>dittes Seld</li> <li>Ex</li> <li>1</li> <li>2</li> <li>2</li> <li>2</li> <li>3</li> <li>4</li> <li>4&lt;</li></ul>	ested: 0 of 10 experions 0 Ectude 0 Ectude

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

	nexpose	Create 🗸										~ d <sup>2</sup>		≗ admin
														🛆 гтемз
		VULNERABILITY INFO	RMATION											
		OVERVIEW												
		Title						Severity	Vulnerability ID	CVSS		Published	Modified	
Q		TLS/SSL Birthday attacks	on 64-bit block ciphers (SWEET:	32)				Severe (5)	ssi-cve-2016-2183-sweet32	5 (AV:N/AC:L/Au	:N/C:P/I:N/A:N)	Aug 24, 2016	Sep 2, 201	6
		DESCRIPTION Legacy block ciphers having should be the exhaustive se with up to 2 to the power of with 64-bit blocks, the birthe	g a block size of 64 bits are vuln arch of the key, with complexity n queries, but most modes of o fay bound corresponds to only 5	erable to a practical collision a 2 to the power of k. However, peration (e.g. CBC, CTR, GCM, 32 GB, which is easily reached i	ttack when the block sit OCB, etc.) a n practice. (	used in CBC mo te n is also an in re unsafe with n Once a collision	de. All versions of the SSL/TLS protocols that support cipher suites oportant security parameter, defining the amount of data that can be once than 2 to the power of half n blocks of message (the birthday be between the cipher blocks accurs it is possible to use the collision t	which use 3DES as t encrypted under the ound). With a moden to extract the plain te	he symmetric encryption cipher are affect same kay. This is particularly important w block cipher with 128-bit blocks such as at data.	td. The security of rhen using commo AES, the birthday b	a block cipher is oft n modes of operatic ound corresponds t	en reduced to the k n: we require block o 256 exabytes. Ho	ey size k: the be : ciphers to be so wever, for a bloc	st attack soure sk cipher
		AFFECTS												
		Asset 🗸	Name	Site	Port	Status	Proof				La	it Scan	Exceptions	
		10.229.20.32	TAC-PC	TAC AAA	3389	Vulnerable Version	Negotiated with the following insecure cipher suites:     TLS 1.0 ciphers:         TLS_RSA_WITH_3DES_EDE_CBC_SHA				No	v 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**.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼ System  → Identity Management	Network Resources     Device Portal Management     pxGrid Service     Feed Service     PassiveID     Threat Centric NAC
Deployment Licensing   Certificat	es  Logging  Maintenance Upgrade Backup & Restore  Admin Access  Settings
0	
Local Log Settings	Node List > ISE21-3ek.example.com Debug Level Configuration
Remote Logging Targets	
Logging Categories	/ Edit Contraction Default
Message Catalog	Component Name   Log Level Description
Debug Log Configuration	va o
Collection Filters	O va-runtime DEBUG Vulnerability Assessment Runtime messages
	O 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","ondemandScanInt erval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c217 5761-0e2b-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","ondemandScanInte
rval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c2175
761-0e2b-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\":\"\",\"cvsBaseScore\":\"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": "2.59999999", "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:

```
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": "2.5999999", "vulnerabilityTitle": "TLS/SSL Server Supports
The Use of Static Key Ciphers", "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": "tls-dh-
prime-under-2048-bits", "cveIds":"", "cvssBaseScore":"2.5999999", "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
```

#### De adapter krijgt CVE's samen met de CVSS-scores.

2016-11-24 12:36:28,143 DEBUG [SimpleAsyncTaskExecutor-2][]

Nexpose", "TC-NAC.AdapterInstanceName", "Rapid7"]}]

which the scan is in progress: 1"}

:::::- 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

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

2016-11-24 12:36:28,880 DEBUG [endpointPollerScheduler-5][] cpm.va.service.util.VaServiceUtil -

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

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"] }

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

[{"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-

:::::- VA SendSyslog systemMsg :

cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter : {"AdapterInstanceName": "Rapid7", "AdapterInstanceUid": "7a2415e7-980d-4c0c-b5ed-

2016-11-24 12:32:05,783 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -

Aanvraag tot Kwetsbaarheidsbeoordeling ingediend bij adapter.

```
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