

Konfigurieren von ISE 2.2 Threat-Centric NAC (TC-NAC) mit Rapid7

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Übergeordnetes Flussdiagramm](#)

[Bereitstellen und Konfigurieren des Nexpose-Scanners](#)

[Schritt 1: Bereitstellen des Nexpose-Scanners](#)

[Schritt 2: Konfigurieren Sie den Nexpose-Scanner.](#)

[ISE konfigurieren](#)

[Schritt 1: Aktivieren Sie TC-NAC-Services.](#)

[Schritt 2: Importieren des Zertifikats des Nexpose-Scanners.](#)

[Schritt 3: Konfigurieren Sie die TC-NAC-Instanz des Nexpose Scanners.](#)

[Schritt 4: Konfigurieren des Autorisierungsprofils zum Auslösen der VA-Prüfung](#)

[Schritt 5: Konfigurieren von Autorisierungsrichtlinien](#)

[Überprüfen](#)

[Identity Services Engine](#)

[Nexus-Scanner](#)

[Fehlerbehebung](#)

[Debugger auf der ISE](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Threat-Centric NAC mit Rapid7 auf Identity Service Engine (ISE) 2.2 konfiguriert und behoben wird. Mit der Threat Centric Network Access Control (TC-NAC)-Funktion können Sie Autorisierungsrichtlinien erstellen, die auf den Bedrohungs- und Schwachstellenattributen basieren, die von den Adaptern für Bedrohungen und Schwachstellen empfangen wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Identity Service Engine
- Schwachstellen-Scanner

Verwendete Komponenten

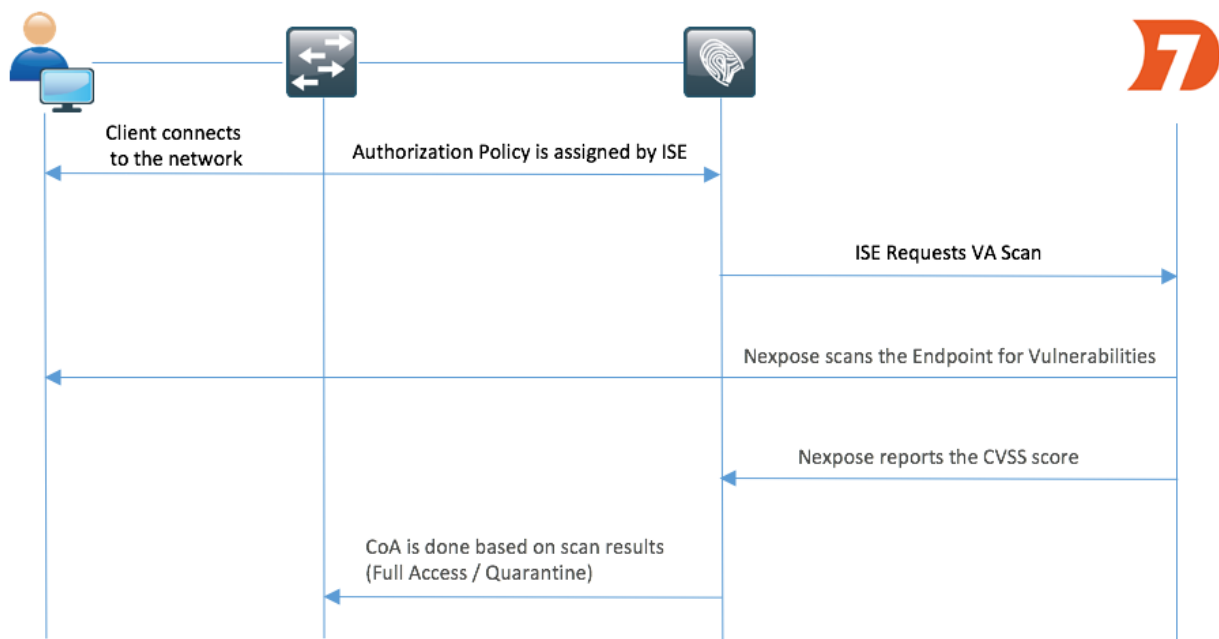
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Service Engine Version 2.2
- Cisco Catalyst 2960S Switch 15.2(2a)E1
- Rapid7 Nexpose Vulnerability Scanner Enterprise Edition
- Windows 7 Service Pack 1
- Windows Server 2012 R2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Übergeordnetes Flussdiagramm



Dies ist der Fluss:

1. Der Client stellt eine Verbindung zum Netzwerk her, der Zugriff ist beschränkt, und das Kontrollkästchen **Schwachstellen bewerten** ist aktiviert.
2. Der PSN-Knoten sendet eine Syslog-Meldung an den MNT-Knoten, in der bestätigt wird, dass die Authentifizierung erfolgt ist, und der VA-Scan war das Ergebnis der Autorisierungsrichtlinie.

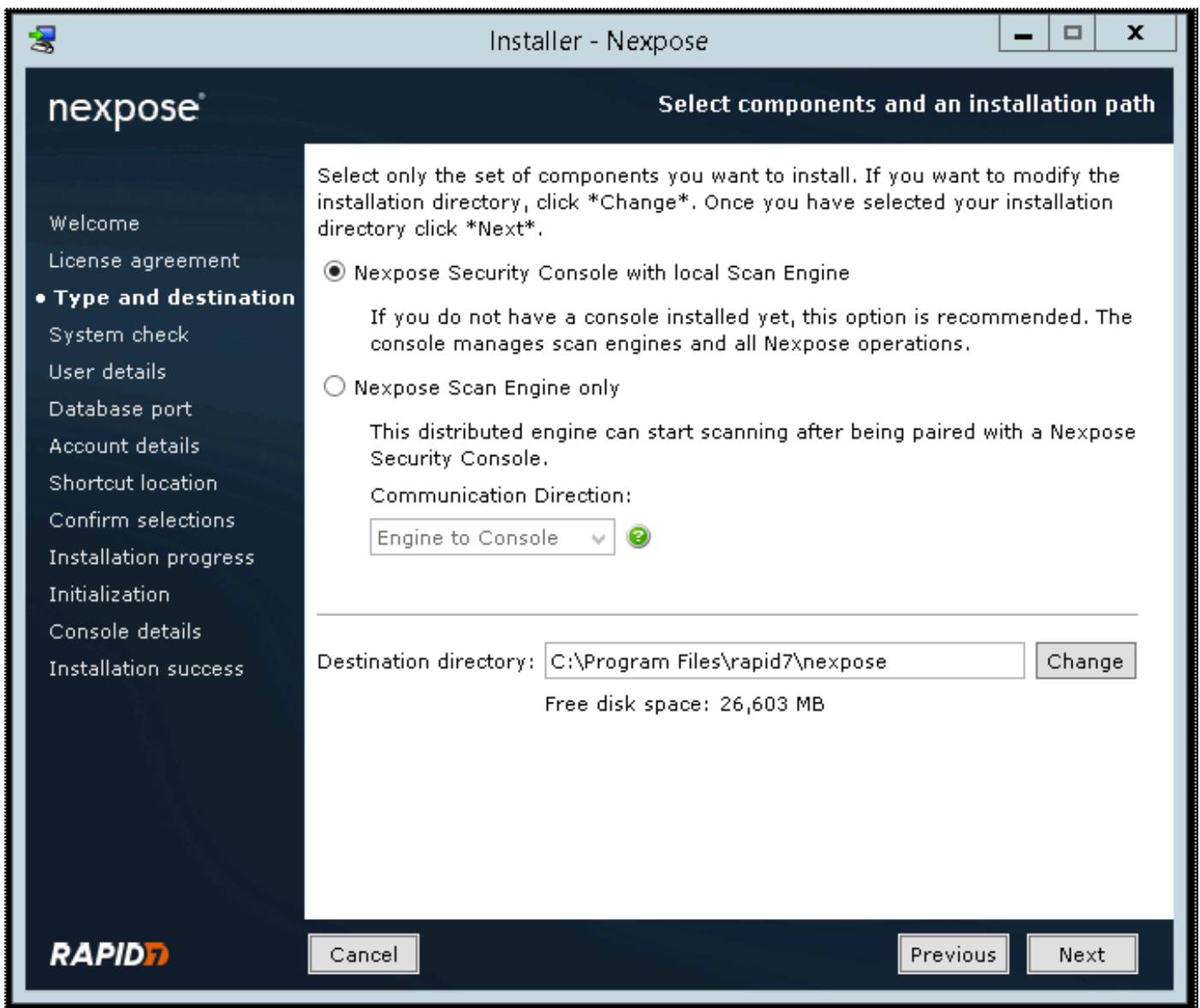
3. Der MNT-Knoten sendet SCAN mithilfe der folgenden Daten an den TC-NAC-Knoten (unter Verwendung von Admin WebApp):
 - MAC-Adresse
 - IP-Adresse
 - Scan-Intervall
 - Periodischer Scan aktiviert
 - Ursprungs-PSN
4. Nexpose TC-NAC (in Docker-Container eingebettet) kommuniziert mit dem Nexpose Scanner, um bei Bedarf einen Scan auszulösen.
5. Nexpose Scanner scannt den von der ISE angeforderten Endpunkt.
6. Nexpose Scanner sendet die Ergebnisse der Prüfung an die ISE.
7. Die Ergebnisse der Prüfung werden an TC-NAC zurückgesendet:
 - MAC-Adresse
 - Alle CVSS-Bewertungen
 - Alle Sicherheitslücken (Titel, CVEIDs)
8. TC-NAC aktualisiert PAN mit allen Daten aus Schritt 7.
9. CoA wird bei Bedarf gemäß konfigurierter Autorisierungsrichtlinie ausgelöst.

Bereitstellen und Konfigurieren des Nexpose-Scanners

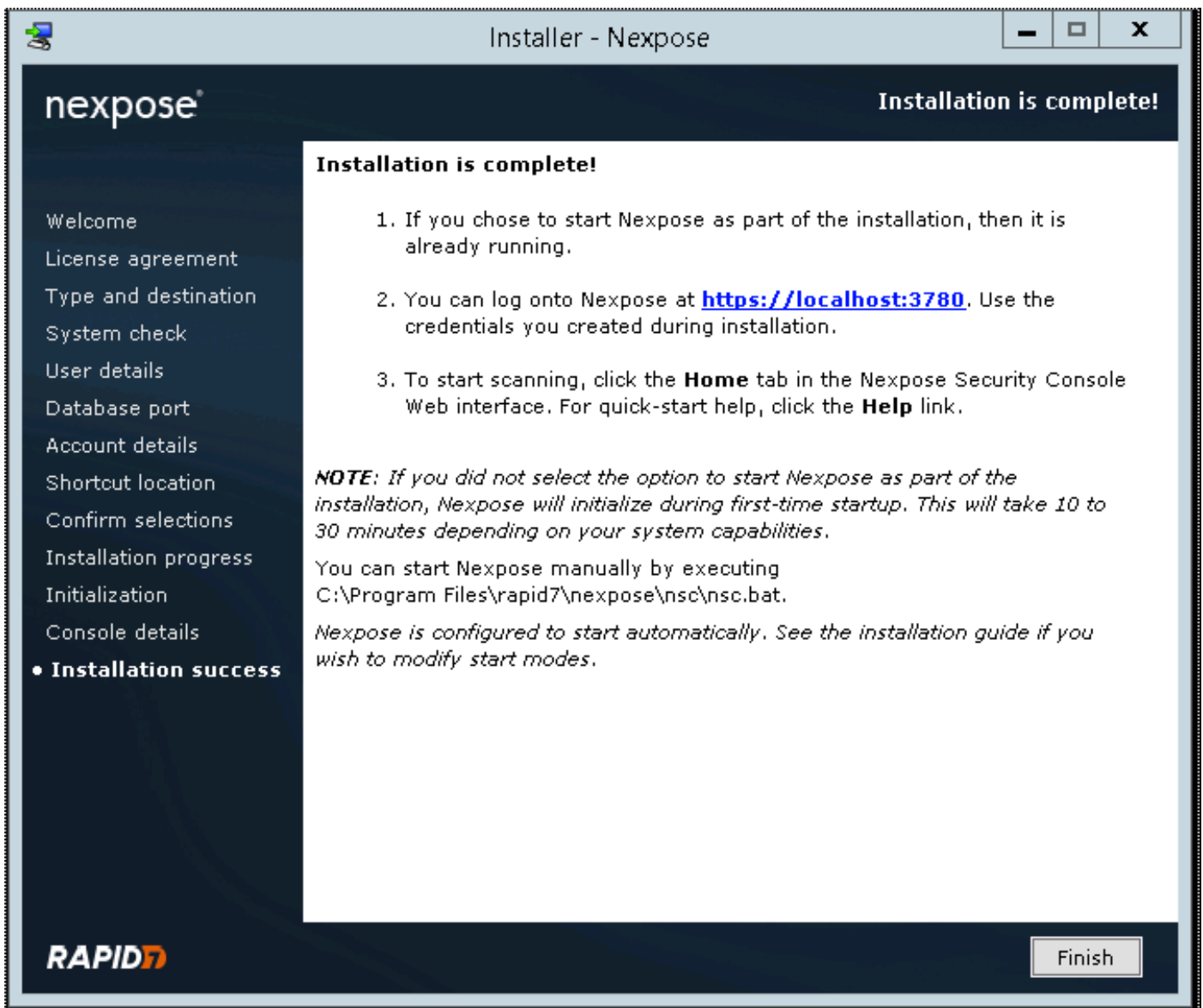
Vorsicht: Die Konfiguration in diesem Dokument für die Übungszwecke erfolgt nicht. Fragen Sie die Rapid7-Techniker, um Einzelheiten zum Design zu erfahren.

Schritt 1: Bereitstellen des Nexpose-Scanners

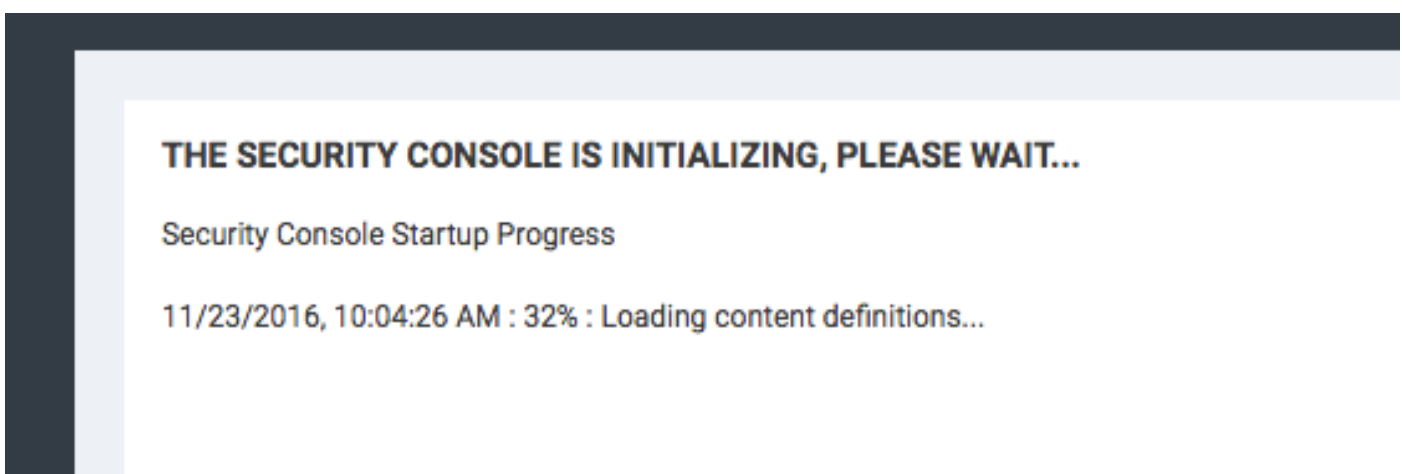
Der Nexpose-Scanner kann aus einer OVA-Datei bereitgestellt und auf Linux- und Windows-Betriebssystemen installiert werden. In diesem Dokument wird die Installation unter Windows Server 2012 R2 durchgeführt. Laden Sie das Image von der Rapid7-Website herunter und starten Sie die Installation. Wenn Sie **Typ und Ziel** konfigurieren, wählen Sie **Nexpose Security Console with local Scan Engine (Sicherheitskonsole mit lokalem Scan Engine)** aus.



Nach Abschluss der Installation wird der Server neu gestartet. Nach dem Start sollte der Zugriff auf den Nexpose-Scanner über den 3780-Port erfolgen, wie im Bild gezeigt:



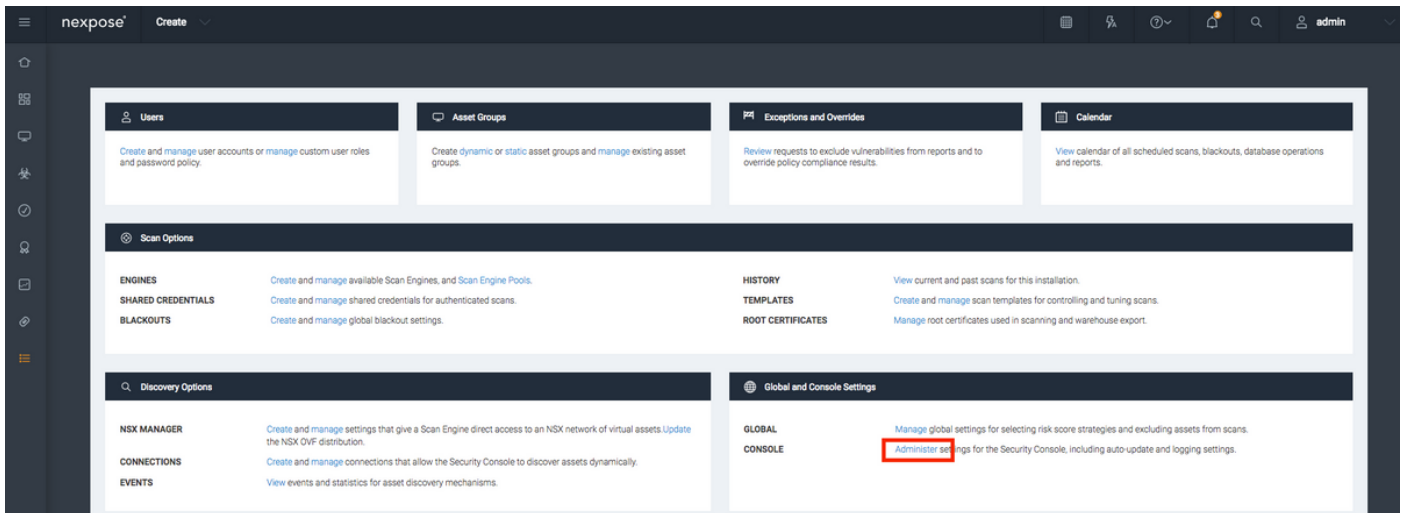
Wie im Bild gezeigt, durchläuft der Scanner den Systemstartprozess der Sicherheitskonsole:



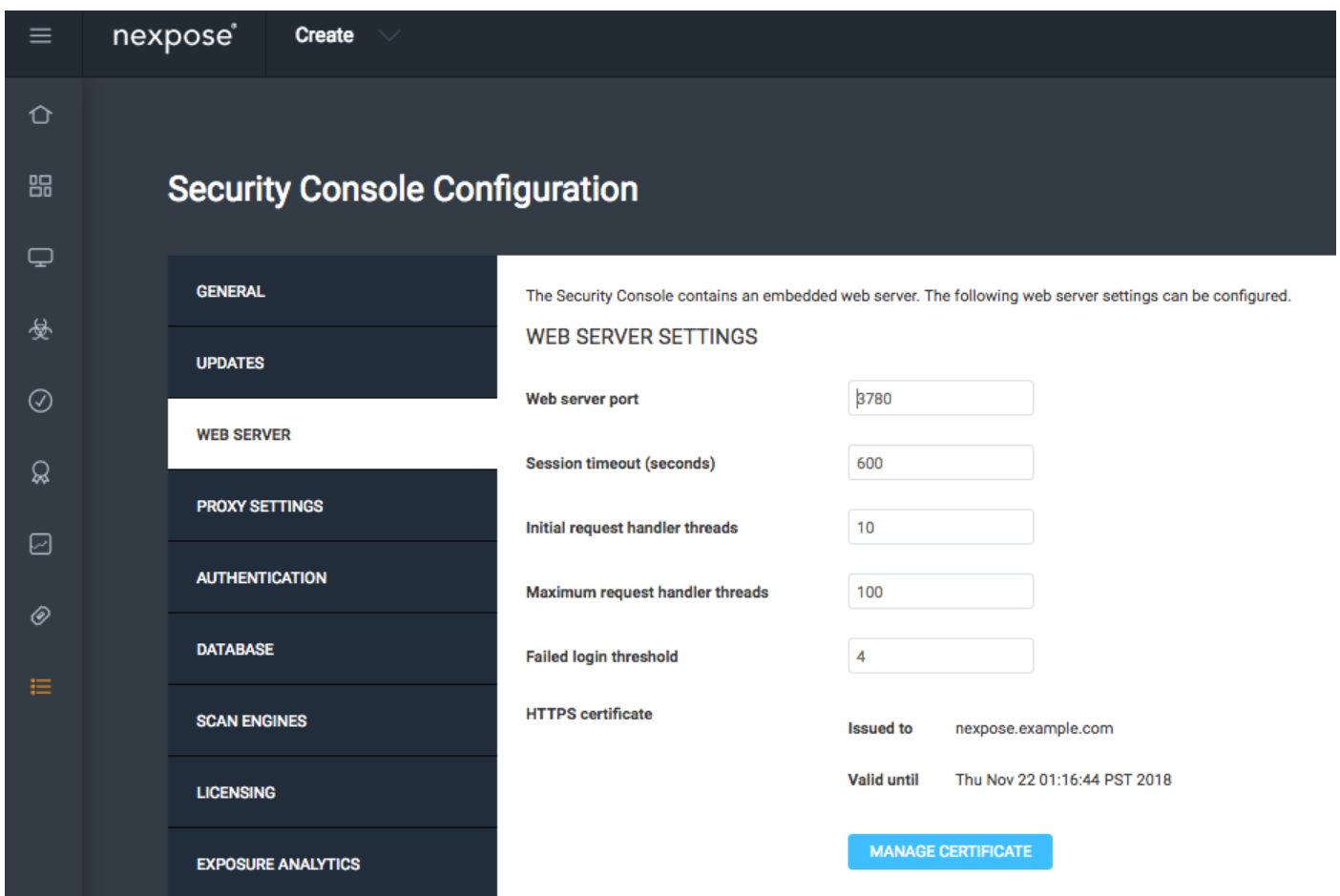
Anschließend sollte der Lizenzschlüssel bereitgestellt werden, um Zugriff auf die GUI zu erhalten. Beachten Sie, dass die Enterprise Edition des Nexpose Scanners erforderlich ist. Wenn Community Edition installiert ist, werden Prüfungen nicht ausgelöst.

Schritt 2: Konfigurieren Sie den Nexpose-Scanner.

Der erste Schritt besteht in der Installation des Zertifikats auf dem Nexpose Scanner. Das Zertifikat in diesem Dokument wird von derselben Zertifizierungsstelle ausgestellt wie das Administratorzertifikat für die ISE (LAB CA). Navigieren Sie zu **Administration > Global and Console Settings**. Wählen Sie **Administration** unter **Console** aus, wie im Bild gezeigt.



Klicken Sie auf **Zertifikat verwalten**, wie im Bild gezeigt:



Klicken Sie, wie im Bild gezeigt, in **Neues Zertifikat erstellen**. Geben Sie **Common Name** und alle anderen Daten ein, die Sie im Identitätszertifikat des Nexpose Scanners speichern möchten. Stellen Sie sicher, dass die ISE in der Lage ist, Nexpose Scanner FQDN mit DNS aufzulösen.

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

Exportieren der CSR-Anfrage (Certificate Signing Request) in das 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

An diesem Punkt müssen Sie den CSR mit der Zertifizierungsstelle (Certificate Authority, CA) unterzeichnen.

Manage Certificate



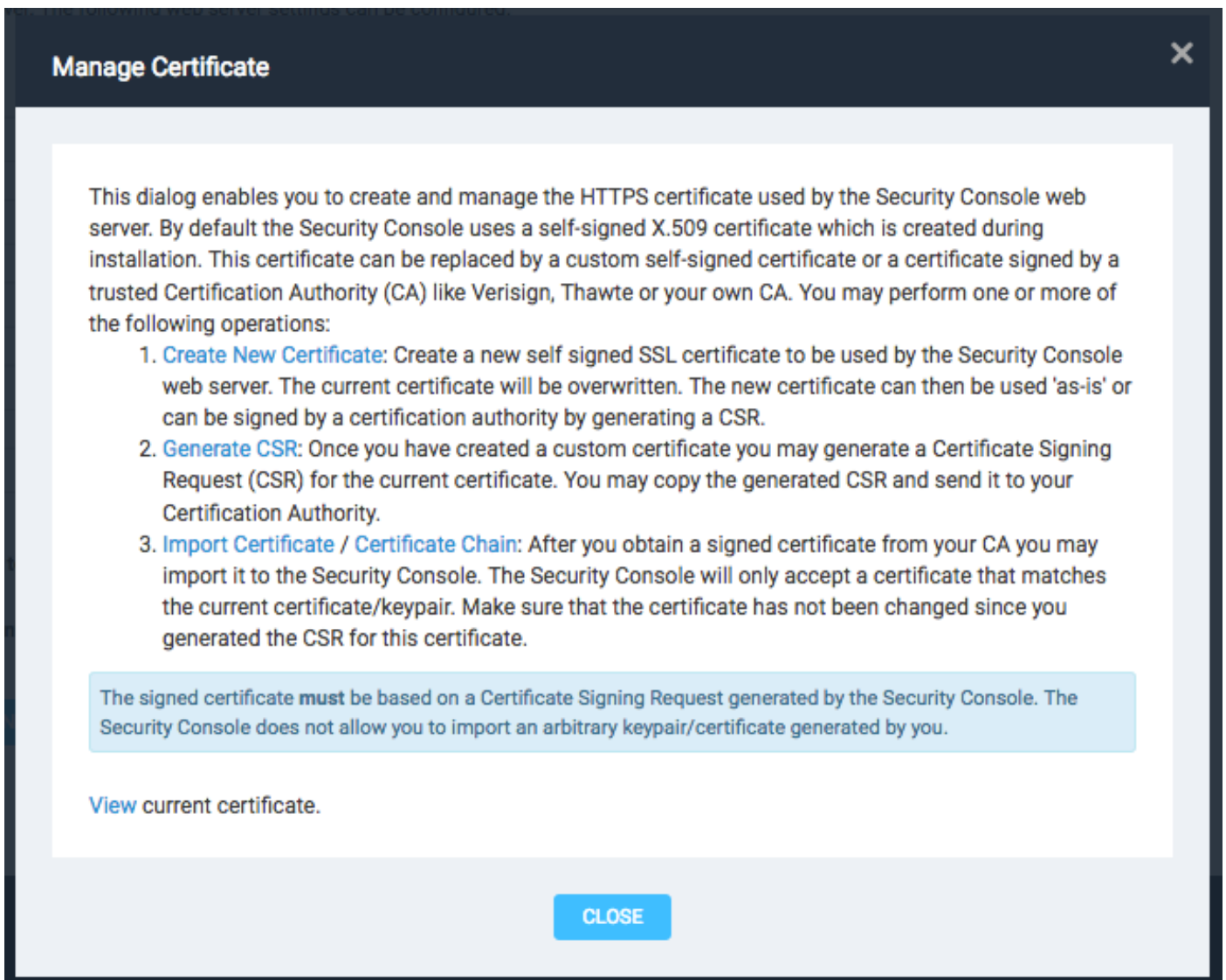
The Security Console has generated a certificate signing request for the current certificate. You may copy the CSR below and send it to your CA for signature. The signed certificate can later be imported into the Security Console using the 'Import Signed Certificate' button.

-----BEGIN NEW CERTIFICATE REQUEST-----

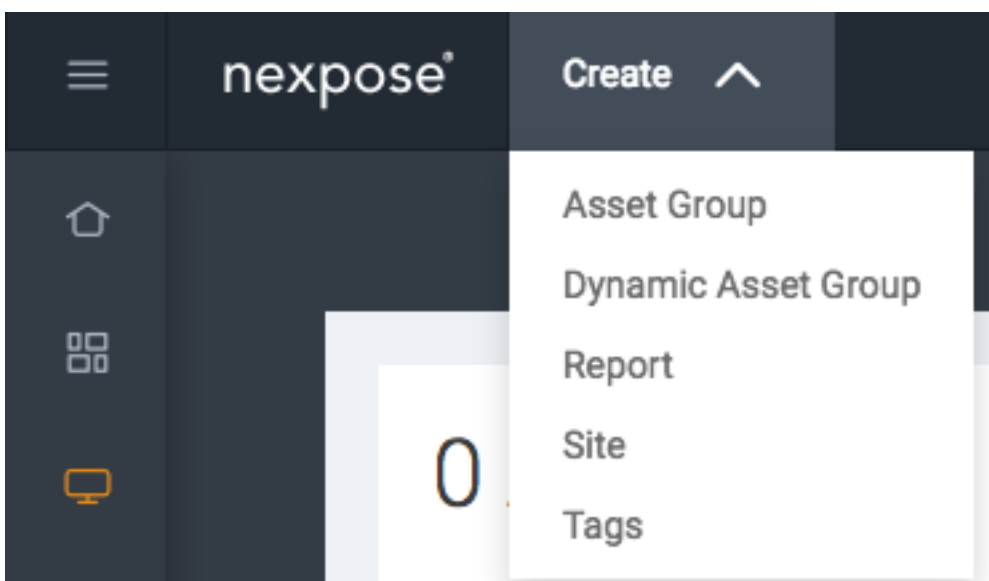
```
MIIEYzCCAksCAQAwHjEcmBoGA1UEAxMTbmV4cG9zZS5leGFtcGxlLmNvbTCCAILw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAIW0yIrdSOlrDwLMAHEISqHZoG4G
oyg3oC9MeML7s1TugD0K4pvmlZOh1E+B6bK7ZOB3QAnf9/VxKaur/Q/yCNj1AcYH
GB+Sq4bAfqHFIKlsjdnj3eOOLW7h8TPmD57NOzOv4X8v6DOz42YF8TNSmScheTZ5
q4qc9DH6RuYUOEYawclWs+7wTVRDt+hyFL6v6e6reIXF7Nlp8ssqC02ZvDGzLnzb
mwJFNG13BILZykhjMzZVsnnGWAn9IghqQRNftXW5JHYdFVs84WeB+DKX1KWneigL
rsay1voSprJXjncC3xAXHWQGFknY8d8eoaEM82fUdzz6Y/jOqUH6ToZ5mEAsKINg
JEQpzLxjQsnAZRG8dy9+J52S6Zm7RXyCg0p7MRKlykEOMGEqR5TF0ZWCFtxomvzp
S0WExoXpWL8oZbOtPHheWaQSmPStzeuQpiFXNjth/XQ0gHpc48v+1DdDeZl/wrLd
j84GMbFuYvBq+x08prU/kGEVftVABGHnjnstGN+qM8CU93mq/6NNPmz8XCgAxCOm
w/oD2cQFCdp1XBC7cUdvkXMIJwqQXtpd8uz9ZLvK+afJT8cBphledh1Fy+v7Mu+m
OeNlx41XDaudLii/SuYBB03DLbN6Inu7Vp+5/3W59lcfmHlt+3oEJAnWx2vVCLgD
NF/0050W-0050CTA-1MBAQ-1DANP-1-1H100-00AQUFAAQCA-1FANQ100KBT-10
```

BACK

Importieren Sie das von der Zertifizierungsstelle ausgestellte Zertifikat, indem Sie auf **Zertifikat importieren** klicken.

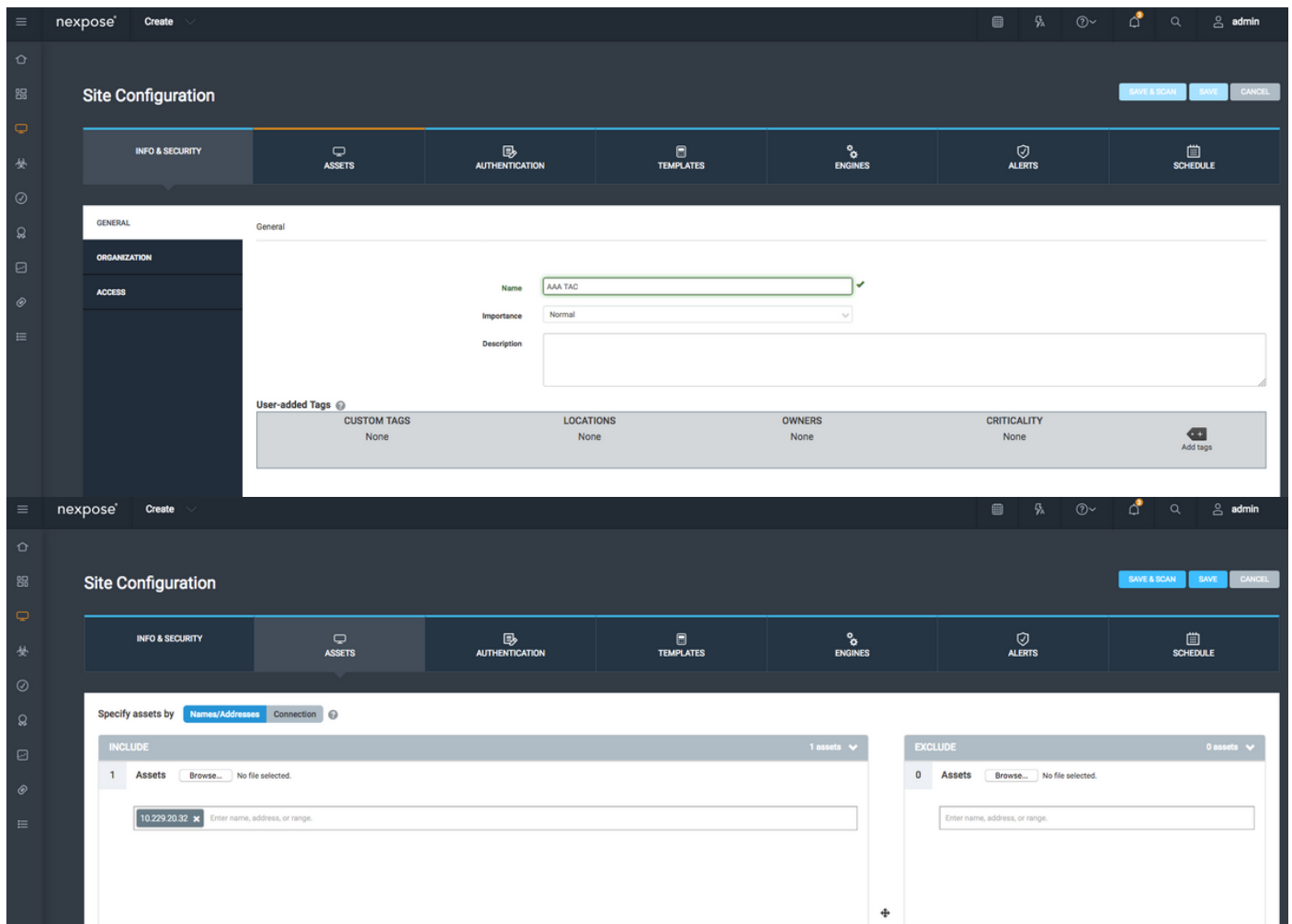


Konfigurieren einer Site Die Website enthält Ressourcen, die Sie scannen können sollten, und das Konto, das für die Integration der ISE mit dem Nexpose Scanner verwendet wird, sollte über Berechtigungen zum Verwalten von Standorten und zum Erstellen von Berichten verfügen. Navigieren Sie zu **Erstellen > Standort**, wie im Bild gezeigt.



Geben Sie, wie im Bild gezeigt, den **Namen** der Website auf der Registerkarte **Info & Security** ein. Die Registerkarte "**Assets**" sollte IP-Adressen der gültigen Ressourcen und Endpunkte enthalten,

die für die Schwachstellenüberprüfung qualifiziert sind.



Importieren Sie ein CA-Zertifikat, das das ISE-Zertifikat signiert hat, in den vertrauenswürdigen Speicher. Navigieren Sie zu **Administration > Root Certificates > Manage > Import Certificates**.



ISE konfigurieren

Schritt 1: Aktivieren Sie TC-NAC-Services.

Aktivieren Sie TC-NAC Services auf einem ISE-Knoten. Beachten Sie:

- Für den Threat Centric NAC-Service ist eine Apex-Lizenz erforderlich.
- Sie benötigen einen separaten Policy Service Node (PSN) für den Threat Centric NAC-Service.

- Der Threat Centric NAC-Service kann auf nur einem Knoten in einer Bereitstellung aktiviert werden.
- Sie können pro Anbieter nur eine Instanz eines Adapters für den Vulnerability Assessment Service hinzufügen.

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. The left sidebar shows 'Deployment' > PAN Failover. The main content area is titled 'Edit Node' for 'ISE22-1ek'. The 'General Settings' tab is active, showing: Hostname ISE22-1ek, FQDN ISE22-1ek.example.com, IP Address 10.48.23.86, and Node Type Identity Services Engine (ISE). Under the 'Personas' section, 'Administration' (Role: STANDALONE), 'Monitoring' (Role: PRIMARY), and 'Policy Service' are checked. Under 'Policy Service', 'Enable Threat Centric NAC Service' is checked, and 'Use Interface' is set to GigabitEthernet 0. Other services like 'Enable SXP Service', 'Enable Device Admin Service', and 'Enable Passive Identity Service' are unchecked.

Schritt 2: Importieren des Zertifikats des Nexpose-Scanners.

Importieren Sie das Zertifikat der Nexpose Scanner-Zertifizierungsstelle in den Trusted Certificates Store in der Cisco ISE (**Administration > Certificates > Certificate Management > Trusted Certificates > Import**). Stellen Sie sicher, dass die entsprechenden Root- und Zwischenzertifikate in den Cisco ISE Trusted Certificates Store importiert (oder vorhanden) werden.

The screenshot shows the 'Trusted Certificates' section in 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 > Certificates. The left sidebar shows 'Certificate Management' > Certificate Authority. The main content area displays a table of trusted certificates. The 'Nexpose Security Console' certificate is highlighted.

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	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	Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Cisco Root CA 2048	Disabled	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	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	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 80 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	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	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	✓

Schritt 3: Konfigurieren Sie die TC-NAC-Instanz des Nexpose Scanners.

Hinzufügen von Rapid7-Instanzen unter **Administration > Threat Centric NAC > Drittanbieter**.

Third Party Vendors

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

Vendor *

Instance Name *

Nach dem Hinzufügen wechselt die Instanz zum Status **Bereit zu Konfigurieren**. Klicken Sie auf diesen Link. Konfigurieren Sie **Nexpose Host** (Scanner) und **Port**, standardmäßig ist dies 3780. Geben Sie **Benutzername** und **Kennwort** mit Zugriff auf die richtige Site an.

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.

Cancel

Next

Die erweiterten Einstellungen sind im ISE 2.2 Admin Guide gut dokumentiert. Sie finden den Link im Abschnitt Referenzen dieses Dokuments. Klicken Sie in **Weiter** und **Beenden**. Nexpose Instance wechselt in den **aktiven** Status, und der Download der Wissensdatenbank wird gestartet.

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

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

Schritt 4: Konfigurieren des Autorisierungsprofils zum Auslösen der VA-Prüfung

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**. Neues Profil hinzufügen Aktivieren Sie unter **Häufige Aufgaben** das Kontrollkästchen **Schwachstellenbewertung**. Das On-Demand-Scan-Intervall sollte entsprechend Ihrem Netzwerkdesign ausgewählt werden.

Das Autorisierungsprofil enthält diese av-pair-Kräfte:

```
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
```

Sie werden innerhalb des Access-Accept-Pakets an Netzwerkgeräte gesendet, obwohl der eigentliche Zweck dieser Geräte darin besteht, dem Überwachungsknoten (MNT) mitzuteilen, dass der Scan ausgelöst werden soll. MNT weist den TC-NAC-Knoten an, mit dem Nexpose Scanner zu kommunizieren.

The screenshot shows the configuration page for an Authorization Profile in Cisco ISE. The profile is named 'Rapid7' and has an Access Type of 'ACCESS_ACCEPT'. The Network Device Profile is set to 'Cisco'. The 'Common Tasks' section is expanded, showing 'Assess Vulnerabilities' checked. The 'Adapter Instance' is set to 'Rapid7' and the 'Trigger scan if the time since last scan is greater than' is set to '48' hours. The 'Advanced Attributes Settings' section shows a list of attributes, and the 'Attributes Details' section shows the following attributes:

```
Access Type = ACCESS_ACCEPT
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
```

Schritt 5: Konfigurieren von Autorisierungsrichtlinien

- Konfigurieren Sie die Autorisierungsrichtlinie, um das in Schritt 4 konfigurierte neue

Autorisierungsprofil zu verwenden. Navigieren Sie zu **Richtlinien > Autorisierung > Autorisierungsrichtlinie**, suchen Sie die Regel **Basic_Authenticated_Access**, und klicken Sie auf **Bearbeiten**. Ändern Sie die Berechtigungen von **PermitAccess** in den neu erstellten **Standard Rapid7**. Dies führt zu einer Schwachstellenüberprüfung für alle Benutzer. Klicken Sie in **Speichern**.

- Erstellen einer Autorisierungsrichtlinie für isolierte Computer. Navigieren Sie zu **Richtlinien > Autorisierung > Autorisierungsrichtlinie > Ausnahmen**, und erstellen Sie eine **Ausnahmeregel**. Navigieren Sie jetzt zu **Bedingungen > Neue Bedingung erstellen (Erweiterte Option) > Attribut auswählen**, scrollen Sie nach unten, und wählen Sie **Bedrohung aus**. Erweitern Sie das **Threat**-Attribut, und wählen Sie **Nexpose-CVSS_Base_Score** aus. Ändern Sie den Operator in **Greater Than**, und geben Sie einen Wert gemäß Ihrer Sicherheitsrichtlinie ein. Das **Quarantäne**-Autorisierungsprofil sollte eingeschränkten Zugriff auf das anfällige System ermöglichen.

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	Edit

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
✓	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones	Edit
✓	Profiled Non Cisco IP Phones	If Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit
⊙	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess	Edit
⊙	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN)	then PermitAccess AND BYOD	Edit
⊙	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPV2)	then NSP_Onboard AND BYOD	Edit
✓	Wired_Guest_Access	If (Guest_Flow AND Wired_MAB)	then PermitAccess AND Guests	Edit
✓	Wi-Fi_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests	Edit
✓	Wired_Redirect_to_Guest_Login	If Wired_MAB	then Cisco_WebAuth	Edit
⊙	Wi-Fi_Redirect_to_Guest_Login	If Wireless_MAB	then Cisco_WebAuth	Edit
✓	Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then Rapid7	Edit
✓	Default	If no matches, then	DenyAccess	Edit

Überprüfen

Identity Services Engine

Die erste Verbindung löst VA Scan aus. Wenn die Prüfung abgeschlossen ist, wird die CoA-Neuauthentifizierung ausgelöst, um neue Richtlinien anzuwenden, wenn sie abgeglichen werden.

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	None!-Device	Default >> D...	Default >> E...	Quarantine	10.229.20.32	Switch_2960	FastEthernet1/0/5	
Nov 24, 2016 01:45:40.711 PM	✓			alice	3C-97:0E:52:3F:D9	None!-Device	Default >> D...	Default >> E...	Quarantine	10.229.20.32	Switch_2960	FastEthernet1/0/5	Profiled
Nov 24, 2016 01:45:39.166 PM	✓			alice	3C-97:0E:52:3F:D9						Switch_2960		
Nov 24, 2016 01:32:00.564 PM	✓			alice	3C-97:0E:52:3F:D9		Default >> D...	Default >> B...	Rapid7	10.229.20.32	Switch_2960	FastEthernet1/0/5	

Um zu überprüfen, welche Schwachstellen erkannt wurden, navigieren Sie zu **Context Visibility > Endpoints**. Überprüfen Sie die Schwachstellen pro Endpunkt mit den vom Nexpose Scanner angegebenen Punktzahlen.

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

Unter Operations > TC-NAC Live Logs (Vorgänge > TC-NAC Live-Protokolle) werden Autorisierungsrichtlinien und Einzelheiten zu CVSS_Base_Score angezeigt.

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

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

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
X	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

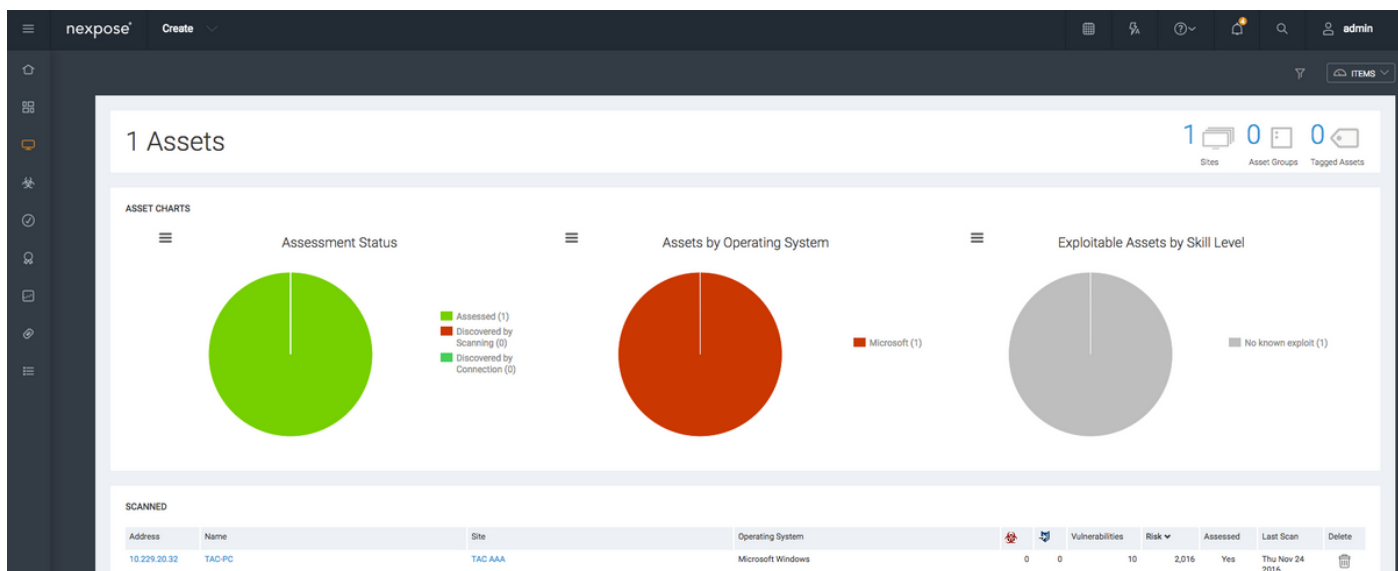
Nexus-Scanner

Wenn der VA-Scan durch die Übertragung des TC-NAC Nexpose Scan in den **In-Progress-**Zustand ausgelöst wird, und der Scanner beginnt, den Endpunkt zu überprüfen. Wenn Sie die Wireshark-Erfassung auf dem Endpunkt ausführen, wird an dieser Stelle der Paketaustausch zwischen der Endstation und dem Scanner angezeigt. Nach Abschluss des Scanners sind die Ergebnisse unter **Startseite** verfügbar.

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](#)

Auf der Seite **Assets (Ressourcen)** können Sie sehen, dass neue Endgeräte mit den Ergebnissen des Scan verfügbar sind, das Betriebssystem identifiziert wird und 10 Schwachstellen erkannt werden.



Wenn Sie auf die **IP-Adresse des Endpunkts** klicken, wird der Nexpose-Scanner zum neuen Menü weitergeleitet, in dem Sie weitere Informationen wie Hostname, Risikobewertung und eine detaillierte Liste der Schwachstellen sehen können

The screenshot shows the details page for the asset 'TAC AAA'. It displays various metadata fields:

- ADDRESSES:** 10.229.20.32
- HARDWARE:** Unknown
- ALIASES:** TAC-PC
- HOST TYPE:** Unknown
- UNIQUE IDENTIFIERS:** SITE: TAC AAA
- OS:** Microsoft Windows
- CPE:** [Icon]
- LAST SCAN:** Nov 24, 2016 4:42:07 AM (6 minutes ago)
- NEXT SCAN:** Not set
- RISK SCORE:** ORIGINAL: 2,016; CONTEXT DRIVEN: 2,016
- CUSTOM TAGS:** None
- OWNERS:** None
- LOCATIONS:** None
- CRITICALITY:** None

At the bottom, there are buttons: [SCAN ASSET NOW](#), [CREATE ASSET REPORT](#), [DELETE ASSET](#), and [SEND LOG](#).

The 'VULNERABILITIES' section shows a list of 10 vulnerabilities. The first one is selected:

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	

Showing 1 to 10 of 10 | [Export to CSV](#) | Rows per page: 10 | 1 of 1

Wenn Sie auf die **Schwachstelle** selbst klicken, wird eine vollständige Beschreibung im Bild angezeigt.

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, GCM, 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

Fehlerbehebung

Debugger auf der ISE

Um das Debuggen auf der ISE zu aktivieren, navigieren Sie zu **Administration > System > Logging > Debug Log Configuration**, wählen Sie TC-NAC Node aus, und ändern Sie die **Protokollstufeva-runtime** und **va-service**-Komponente in **DEBUG**.

Identity Services Engine Administration > System > Logging > Debug Log Configuration

Node List > ISE21-3ek.example.com

Debug Level Configuration

Component Name: va

Component Name	Log Level	Description
<input type="radio"/> va-runtime	DEBUG	Vulnerability Assessment Runtime messages
<input type="radio"/> va-service	DEBUG	Vulnerability Assessment Service messages

Protokolle, die überprüft werden sollen - varuntime.log. Sie können sie direkt über die ISE-CLI entfernen:

```
ISE21-3ek/admin# show logging application varuntime.log tail
```

TC-NAC Docker erhielt Anweisungen zur Durchführung der Prüfung auf einen bestimmten Endpunkt.

```
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","ondemandScanInte
```

```
rval":"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}
```

Sobald das Ergebnis empfangen wurde, werden alle Schwachstellendaten im Kontextverzeichnis gespeichert.

```
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"}]}
```

Protokolle zu überprüfen - vaservice.log. Sie können sie direkt über die ISE-CLI entfernen:

```
ISE21-3ek/admin# show logging application vaservice.log tail
```

Anfrage zur Schwachstellenbewertung wurde an Adapter gesendet.

```
2016-11-24 12:32:05,783 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcInstance":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"]}
```

AdapterMessageListener überprüft alle 5 Minuten den Status der Prüfung, bis sie abgeschlossen ist.

```
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","isAutoInsertSelfAcInstance":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"]}
Adapter erhält CVE's zusammen mit den 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":"2.5999999","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
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"]}
```

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)
- [ISE 2.2 Versionshinweise](#)
- [ISE 2.2 Hardware-Installationsanleitung](#)
- [ISE 2.2-Upgrade-Leitfaden](#)
- [ISE 2.2 Engine - Administratoranleitung](#)