

Configurazione di ISE 2.2 Threat-Centric NAC (TC-NAC) con Rapid7

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Diagramma di flusso ad alto livello](#)

[Distribuire e configurare lo scanner Nexpose](#)

[Passaggio 1. Distribuire lo scanner Nexpose.](#)

[Passaggio 2. Configurare lo scanner Nexpose.](#)

[Configurare ISE](#)

[Passaggio 1. Abilitare i servizi TC-NAC.](#)

[Passaggio 2. Importare il certificato dello scanner Nexpose.](#)

[Passaggio 3. Configurare l'istanza TC-NAC di Nexpose Scanner.](#)

[Passaggio 4. Configurare il profilo di autorizzazione per attivare la scansione VA.](#)

[Passaggio 5. Configurare i criteri di autorizzazione.](#)

[Verifica](#)

[Identity Services Engine](#)

[Scanner Nexpose](#)

[Risoluzione dei problemi](#)

[Debug su ISE](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi ai sistemi NAC basati sulle minacce con Rapid7 su Identity Service Engine (ISE) 2.2. La funzionalità TC-NAC (Threat Centric Network Access Control) consente di creare criteri di autorizzazione basati sugli attributi di minaccia e vulnerabilità ricevuti dagli adattatori minacce e vulnerabilità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco Identity Service Engine
- Nexpose Vulnerability Scanner

Componenti usati

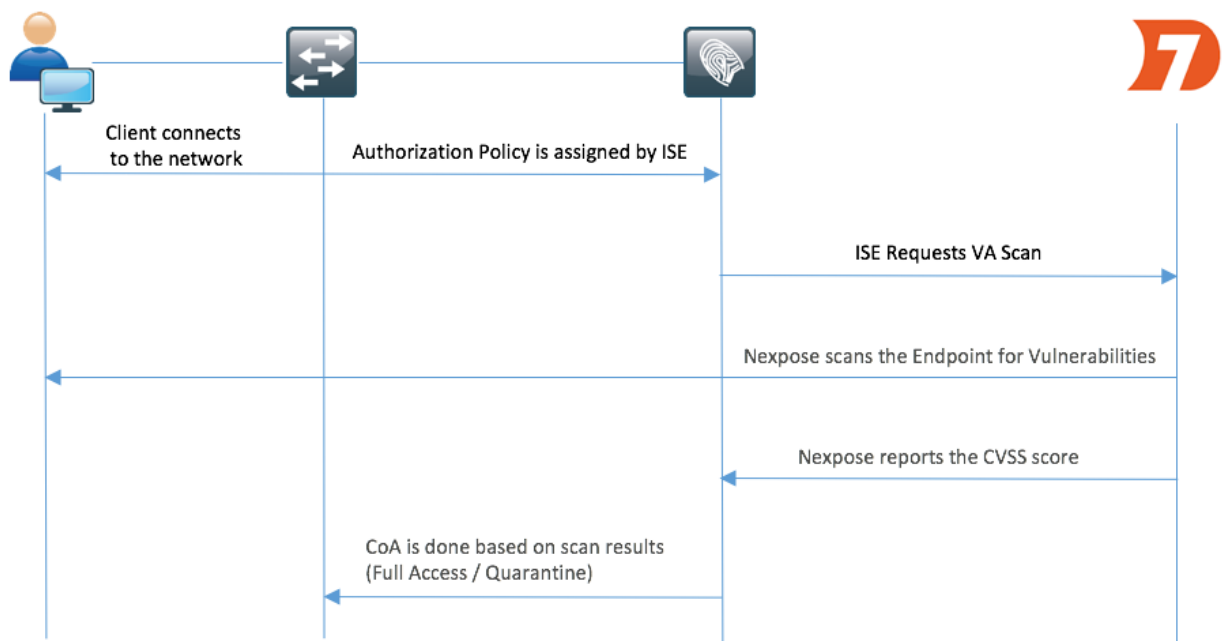
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Service Engine versione 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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Diagramma di flusso ad alto livello



Questo è il flusso:

1. Il client si connette alla rete, viene concesso un accesso limitato e viene assegnato un profilo con la casella di controllo **Valuta vulnerabilità** abilitata.
2. Il nodo PSN invia un messaggio Syslog al nodo MNT per confermare l'autenticazione e l'analisi VA è il risultato dei criteri di autorizzazione.

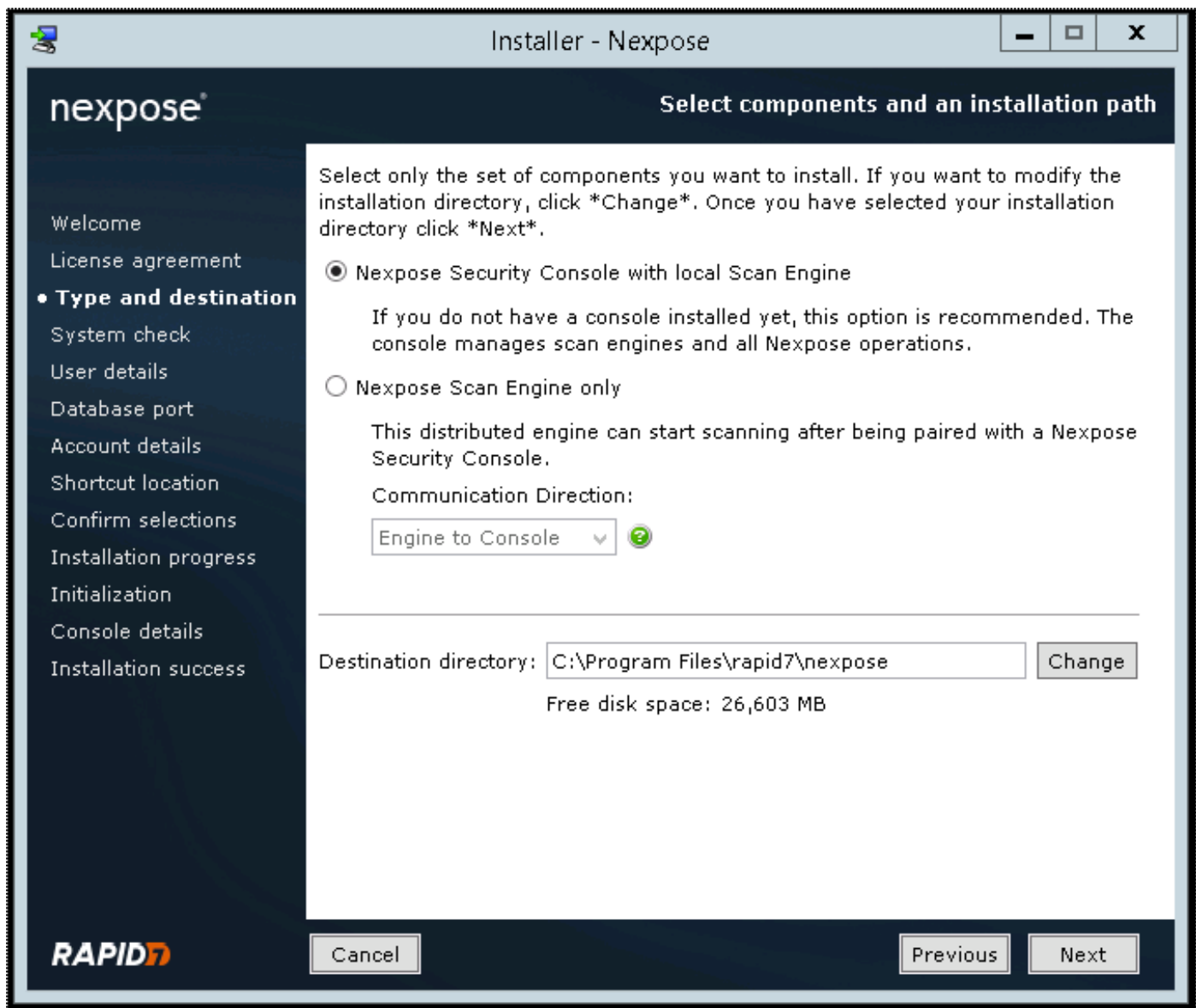
3. Il nodo MNT invia SCAN al nodo TC-NAC (utilizzando Admin WebApp) utilizzando questi dati:
 - Indirizzo MAC
 - Indirizzo IP
 - Intervallo di scansione
 - Scansione periodica abilitata
 - PSN di origine
4. Nexpose TC-NAC (incapsulato nel contenitore Docker) comunica con lo scanner Nexpose per attivare la scansione, se necessario.
5. Nexpose Scanner esegue la scansione dell'endpoint richiesto da ISE.
6. Nexpose Scanner invia i risultati della scansione ad ISE.
7. I risultati della scansione vengono inviati al TC-NAC:
 - Indirizzo MAC
 - Tutti i punteggi CVSS
 - Tutte le vulnerabilità (titolo, CVEID)
8. TC-NAC aggiorna la PAN con tutti i dati del passaggio 7.
9. Il CoA viene attivato se necessario in base ai criteri di autorizzazione configurati.

Distribuire e configurare lo scanner Nexpose

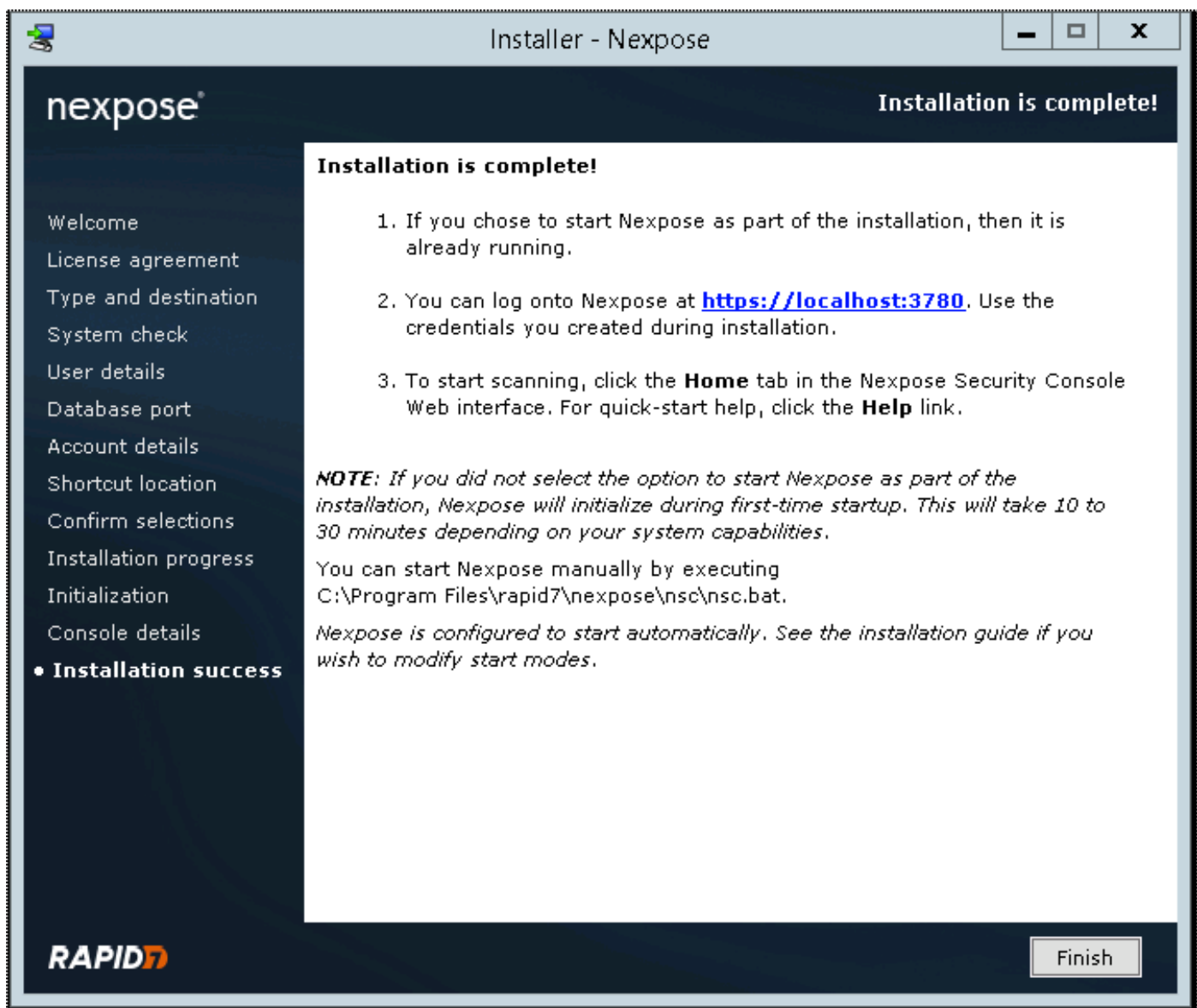
Attenzione: La configurazione di Nexpose in questo documento viene eseguita per scopi di laboratorio. Consultare i tecnici Rapid7 per le considerazioni di progettazione

Passaggio 1. Distribuire lo scanner Nexpose.

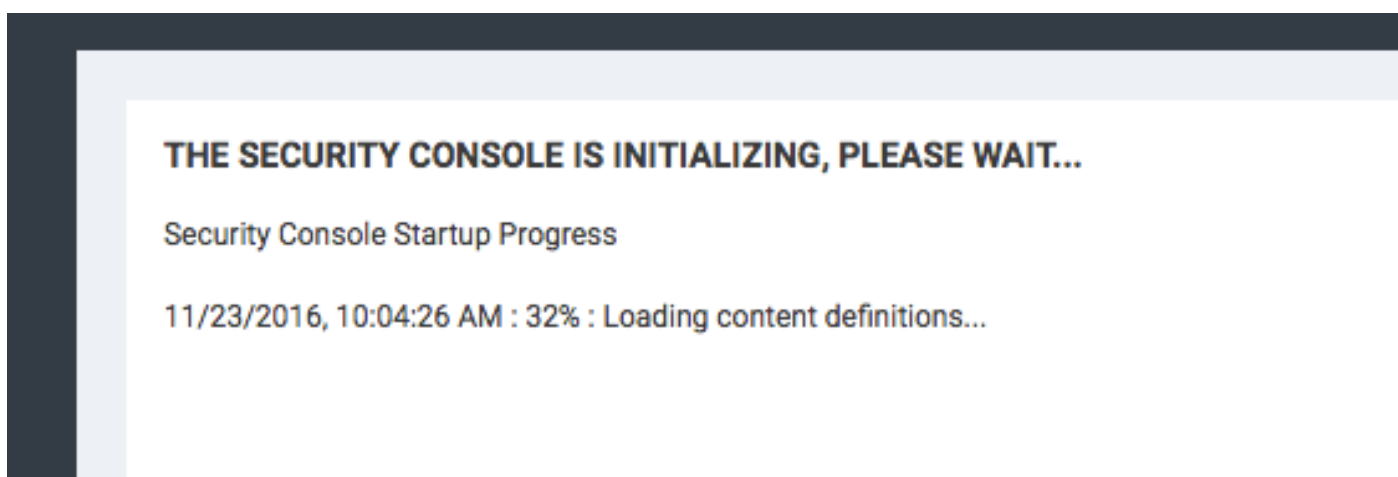
Nexpose scanner può essere distribuito da file OVA, installato sul sistema operativo Linux e Windows. In questo documento l'installazione viene eseguita in Windows Server 2012 R2. Scaricare l'immagine dal sito Web Rapid7 e avviare l'installazione. Quando si configura il **tipo e la destinazione**, selezionare **Nexpose Security Console con Scan Engine locale**



Al termine dell'installazione, il server viene riavviato. Dopo il lancio, lo scanner Nexpose deve essere accessibile tramite la porta 3780, come mostrato nell'immagine:



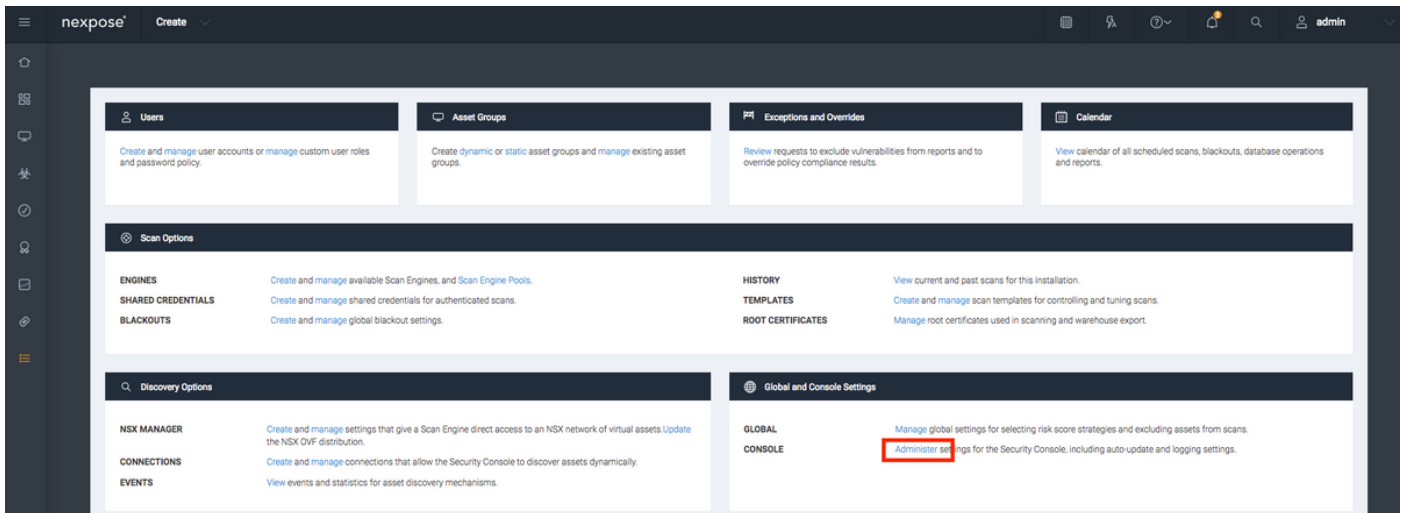
Come mostrato nell'immagine, lo scanner esegue il processo di avvio della console di sicurezza:



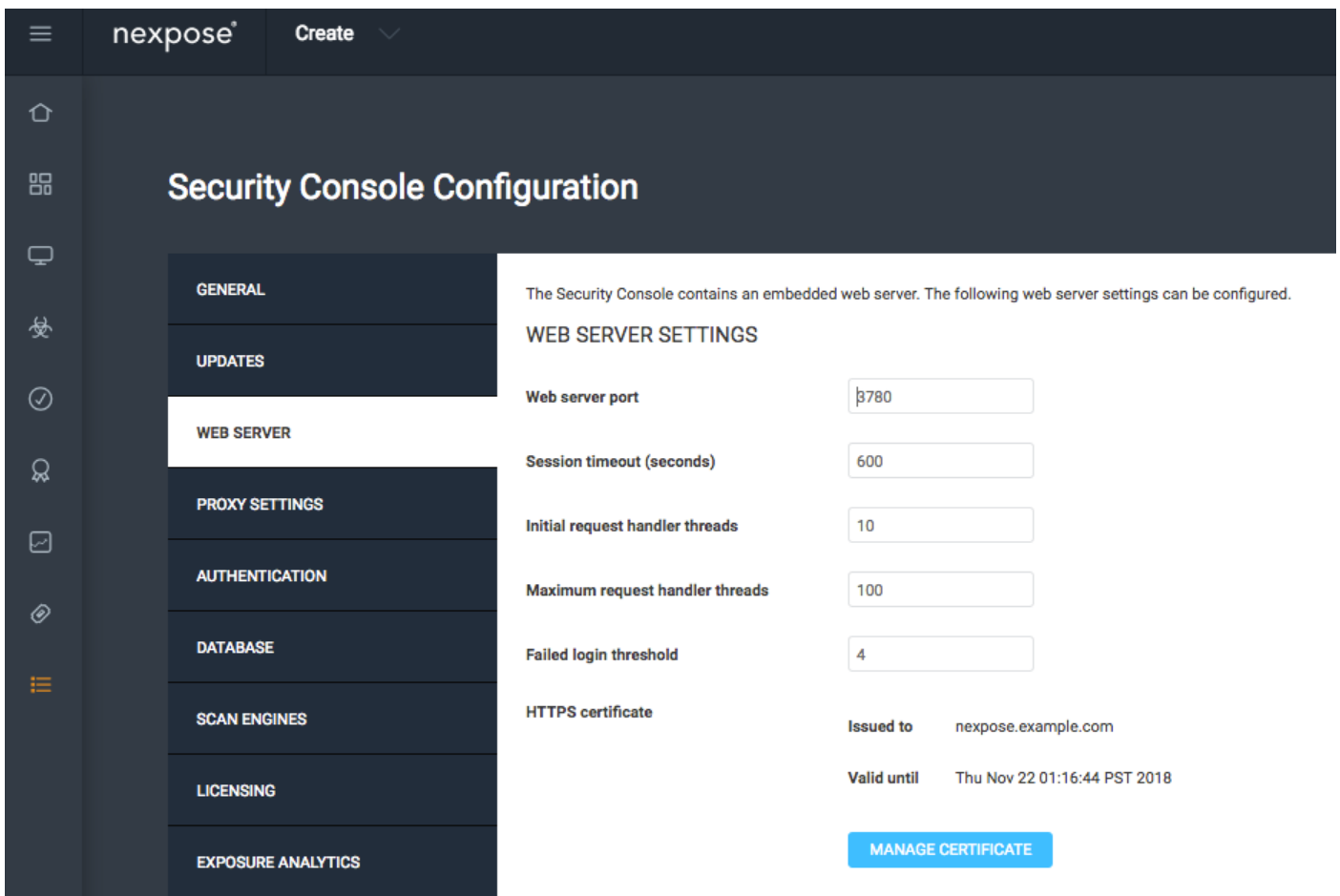
Quindi, per accedere alla GUI, occorre fornire la chiave di licenza. Si noti che è richiesta l'edizione Enterprise di Nexpose Scanner, le analisi non vengono attivate se è installata l'edizione Community.

Passaggio 2. Configurare lo scanner Nexpose.

Il primo passaggio consiste nel reinstallare il certificato su Nexpose Scanner. Il certificato descritto in questo documento viene emesso dalla stessa CA che ha emesso il certificato di amministratore per ISE (LAB CA). Selezionare **Amministrazione > Impostazioni globali e console**. Selezionare **Amministra in Console**, come mostrato nell'immagine.



Fare clic su **Gestisci certificato**, come illustrato nell'immagine:



Come mostrato nell'immagine, fare clic su in **Crea nuovo certificato**. Immettere il **Nome comune** ed eventuali altri dati che si desidera includere nel certificato di identità di Nexpose Scanner. Verificare che ISE sia in grado di risolvere l'FQDN dello scanner Nexpose con DNS.

Manage Certificate



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

Common name (fully qualified domain name)

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

State/Province

Locality/City

Organization

Organizational unit

Valid for (years)

CREATE

BACK

Esportare la richiesta di firma del certificato (CSR) nel terminale.

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

A questo punto è necessario firmare il CSR con CA (Certification Authority).

Manage Certificate



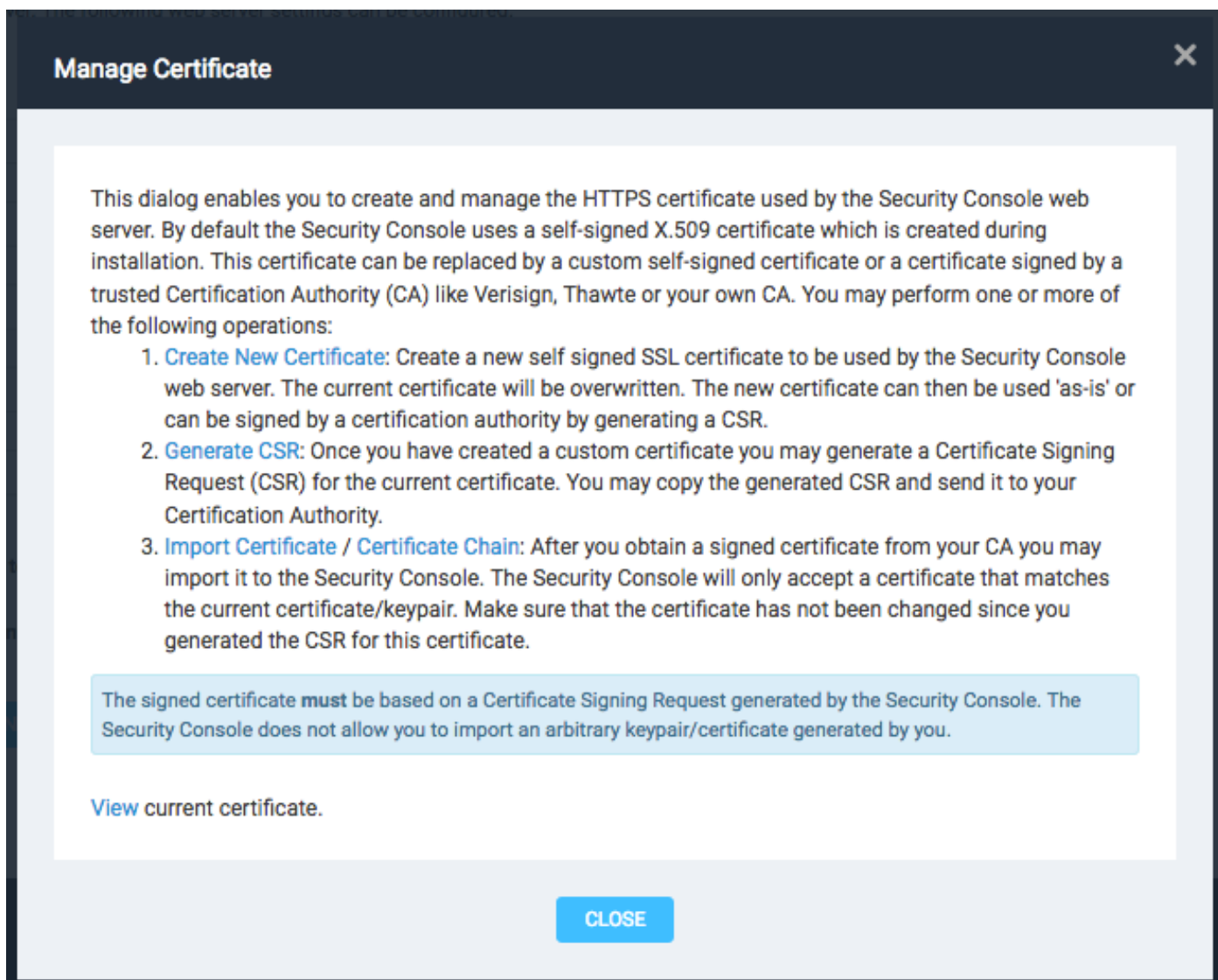
The Security Console has generated a certificate signing request for the current certificate. You may copy the CSR below and send it to your CA for signature. The signed certificate can later be imported into the Security Console using the 'Import Signed Certificate' button.

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

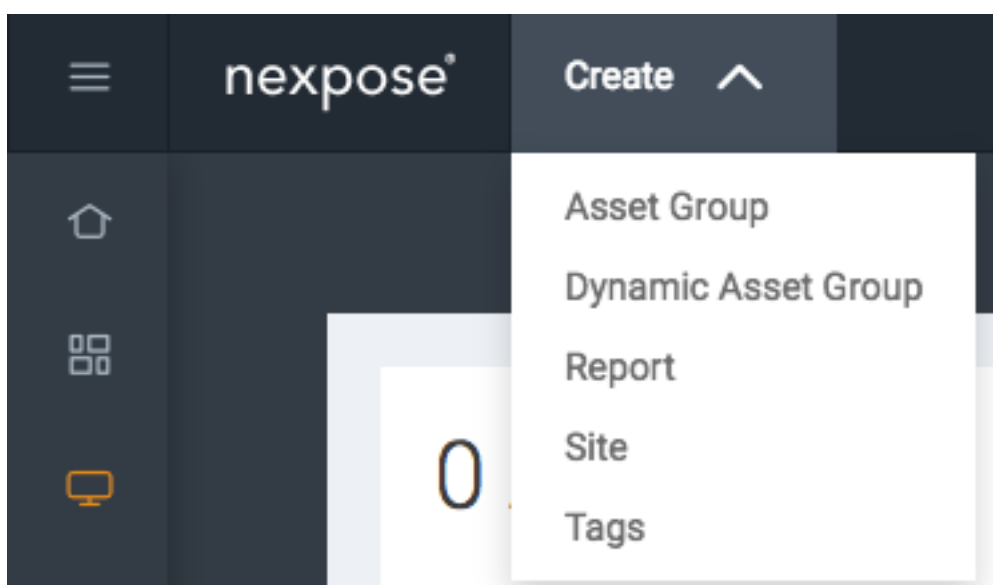
```
MIIEYzCCAksCAQAwHjEcmBoGA1UEAxMTbnV4cG9zZS5leGFtcGxlLmNvbTCCAILw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAIW0yIrdSOlrDwLMAHEISqHZoG4G
oyg3oC9MeML7s1TugD0K4pvmIZOh1E+B6bK7ZOB3QAnf9/VxKaur/Q/yCNj1AcYH
GB+Sq4bAfqHFIKIsjdnj3eOOLW7h8TPmD57NOzOv4X8v6DOz42YF8TNSmScheTZ5
q4qc9DH6RuYUOEYawclWs+7wTVRdt+hyFL6v6e6reIXF7Nlp8ssqC02ZvDGzLnzb
mwJFNG13BILZykhjMzZVsnGWAn9IghqQRNftXW5JHYdFVs84WeB+DKX1KWneigL
rsay1voSprJXjncC3xAXHWQGFknY8d8eoaEM82fUdzz6Y/jOqUH6ToZ5mEAsKINg
JEQpzLxjQsnAZRG8dy9+J52S6Zm7RXyCg0p7MRKlykEOMGEqR5TF0ZWCFtxomvzp
S0WExoXpWL8oZbOtPHheWaQSmPStzeuQpiFXNjth/XQ0gHpc48v+1DdDeZI/wrLd
j84GMbFuYvBq+x08prU/kGEVftVABGHnjnstGN+qM8CU93mq/6NNPmz8XCgAxCOm
w/oD2cQFCdp1XBC7cUdvkXMIJwqQXtpd8uz9ZLvK+afJT8cBphledh1Fy+v7Mu+m
OeNlx41XDaudLii/SuYBB03DLbN6Inu7Vp+5/3W59lcfmHlt+3oEJANWx2vVCLgD
NE/0050W500500TA=MPAAG=ADANP=+L+H00=00AQUFAAGAA=FAANQ100KBT=0
```

BACK

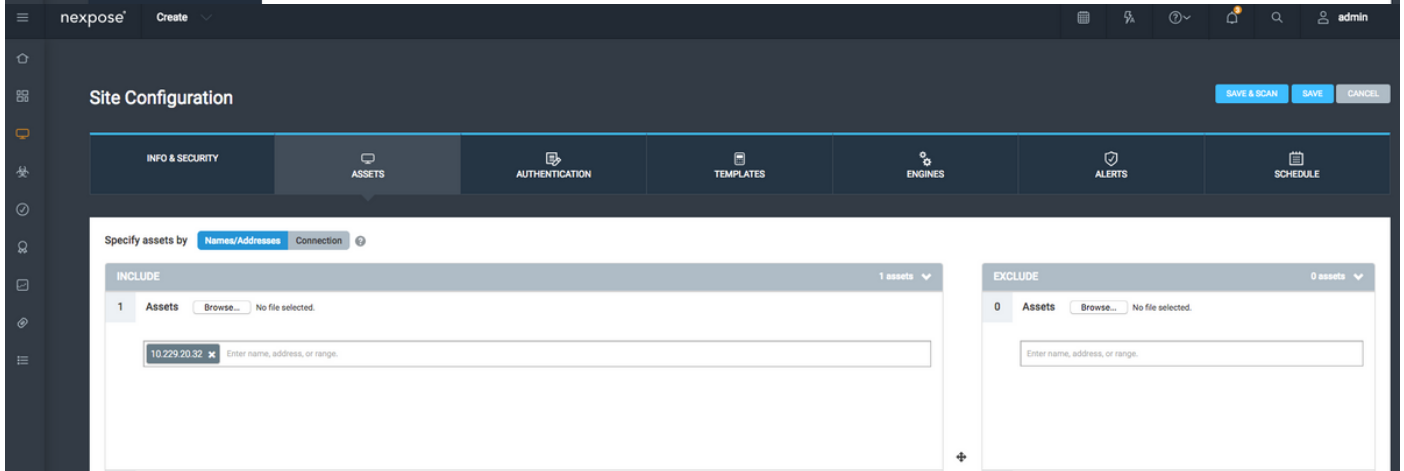
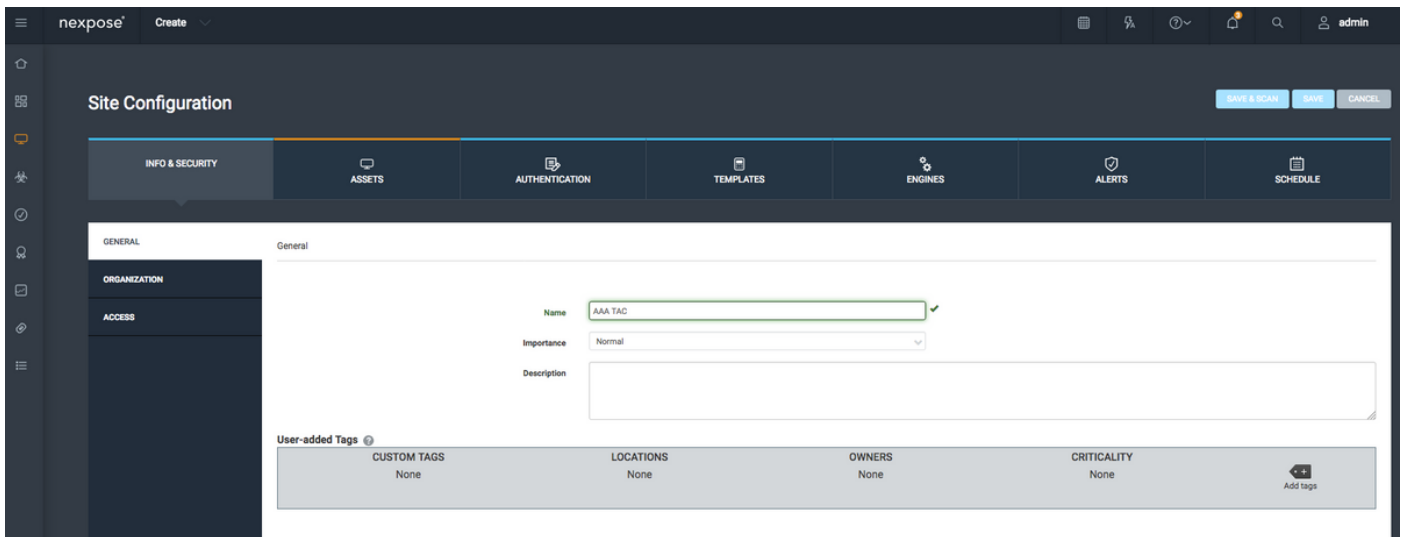
Importare il certificato rilasciato dalla CA facendo clic su **Importa certificato**.



Configurare un sito. Il sito contiene risorse che è possibile analizzare e l'account utilizzato per integrare ISE con Nexpose Scanner deve disporre dei privilegi per gestire i siti e creare i report. Passare a **Crea > Sito**, come mostrato nell'immagine.



Come mostrato nell'immagine, immettere il **Nome** del Sito nella scheda **Info & Security**. La scheda **Assets** deve contenere gli indirizzi IP delle risorse valide, gli endpoint idonei per l'analisi delle vulnerabilità.



Importare il certificato CA che ha firmato il certificato ISE nell'archivio protetto. Selezionare **Amministrazione > Certificati radice > Gestisci > Importa certificati**.



Configurare ISE

Passaggio 1. Abilitare i servizi TC-NAC.

Abilitare i servizi TC-NAC sul nodo ISE. Tenere presente quanto segue:

- Il servizio NAC incentrato sulle minacce richiede una licenza Apex.
- È necessario un PSN (Policy Service Node) distinto per il servizio NAC incentrato sulle minacce.
- Il servizio NAC incentrato sulle minacce può essere abilitato solo su un nodo in una distribuzione.

- È possibile aggiungere una sola istanza di una scheda per fornitore per il servizio di valutazione delle vulnerabilità.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation tree with 'Deployment' selected. The main content area is titled 'Deployment Nodes List > ISE22-1ek' and 'Edit Node'. The 'General Settings' tab is active, showing the following information:

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

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

- Administration: Role **STANDALONE** (Make Primary)
- Monitoring: Role **PRIMARY** (Other Monitoring Node:)
- Policy Service:
 - Enable Session Services: Include Node in Node Group: **None**
 - Enable Profiling Service
 - Enable Threat Centric NAC Service
 - Enable SXP Service: Use Interface: **GigabitEthernet 0**
 - Enable Device Admin Service
 - Enable Passive Identity Service
- pxGrid

Passaggio 2. Importare il certificato dello scanner Nexpose.

Importare il certificato CA dello scanner Nexpose nell'archivio Certificati attendibili di Cisco ISE (Amministrazione > Certificati > Gestione certificati > Certificati attendibili > Importa). Verificare che i certificati radice e intermedi appropriati siano importati (o presenti) nell'archivio dei certificati protetti di Cisco ISE

The screenshot shows the Cisco ISE Administration console with the 'Certificate Management' section selected. The 'Trusted Certificates' table is displayed, showing a list of certificates with their status and details.

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

Passaggio 3. Configurare l'istanza TC-NAC di Nexpose Scanner.

Aggiungere Rapid7 Instance in Administration > Threat Centric NAC > Vendor di terze parti.

Vendor Instances > New

Input fields marked with an asterisk (*) are required.

Vendor *

Instance Name *

Una volta aggiunta, l'istanza passa allo stato **Pronta per la configurazione**. Fare clic su questo collegamento. Configurare **Nexpose Host** (Scanner) e **Port**. Per impostazione predefinita, il valore è 3780. Specificare **Nome utente** e **Password** con accesso al sito corretto.

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.

Le impostazioni avanzate sono ben documentate nella Guida dell'amministratore di ISE 2.2. Il link è disponibile nella sezione Riferimenti di questo documento. Fare clic su **Avanti** e **Fine**. Nexpose Instance passa allo stato **Attivo** e viene avviato il download della Knowledge Base.

Third Party Vendors

Vendor Instances

Refresh + Add Trash Edit Restart Stop Filter

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

Passaggio 4. Configurare il profilo di autorizzazione per attivare la scansione VA.

Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione**. Aggiungi nuovo profilo. In **Operazioni comuni** selezionare la casella di controllo **Valutazione vulnerabilità**. L'intervallo di scansione su richiesta deve essere selezionato in base alla progettazione della rete.

Il profilo di autorizzazione contiene le seguenti coppie av:

```
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
```

Vengono inviati ai dispositivi di rete all'interno di un pacchetto di accettazione dell'accesso, anche se il loro vero scopo è quello di dire al nodo MNT (Monitoring) che deve essere attivata la scansione. MNT indica al nodo TC-NAC di comunicare con Nexpose Scanner.

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

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

Passaggio 5. Configurare i criteri di autorizzazione.

- Configurare il criterio di autorizzazione per utilizzare il nuovo profilo di autorizzazione configurato nel passaggio 4. Passare a **Criterio > Autorizzazione > Criterio di autorizzazione**, individuare la regola **Basic_Authenticated_Access** e fare clic su **Modifica**. Modificare le autorizzazioni da **PermitAccess** al nuovo **Standard Rapid7** creato. In questo modo viene eseguita una scansione delle vulnerabilità per tutti gli utenti. Fare clic su in **Salva**.
- Crea criteri di autorizzazione per computer in quarantena. Passare a **Criterio > Autorizzazione > Criterio di autorizzazione > Eccezioni** e creare una **regola di eccezione**. Passare quindi a **Condizioni > Crea nuova condizione (opzione avanzata) > Seleziona attributo**, scorrere verso il basso e selezionare **Minaccia**. Espandere l'attributo **Threat** e selezionare **Nexpose-CVSS_Base_Score**. Modificare l'operatore in **Maggiore di** e immettere un valore in base ai criteri di sicurezza. Il profilo di autorizzazione della **quarantena** deve consentire un accesso limitato alla macchina vulnerabile.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Global Exceptions Policy Authentication Authorization Profiling Posture Client Provisioning Policy Elements

License Warning

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

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Exception Rule	if Threat:Rapid7 Nexpose-CVSS_Base_Score GREATER 1	then Quarantine

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profilled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profilled Non Cisco IP Phones	if Non_Cisco_Profild_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
<input checked="" type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN)	then PermitAccess AND BYOD
<input checked="" type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPV2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wired_Guest_Access	if (Guest_Flow AND Wired_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wired_Redirect_to_Guest_Login	if Wired_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then Rapid7
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Verifica

Identity Services Engine

La prima connessione attiva VA Scan. Al termine dell'analisi, la riautenticazione CoA viene attivata per applicare nuovi criteri, se corrispondenti.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

License Warning

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

Live Logs Live Sessions




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

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

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

Per verificare quali vulnerabilità sono state rilevate, selezionare **Context Visibility > Endpoints**. Verificare le vulnerabilità degli endpoint con i punteggi assegnati dallo scanner Nexpose.

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

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



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

Applications Attributes Authentication Threats **Vulnerabilities**

ssl-cve-2016-2183-sweet32

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

ssl-static-key-ciphers

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

rc4-cve-2013-2566

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

In Operazioni > TC-NAC Live Logs, è possibile visualizzare i criteri di autorizzazione applicati e i dettagli su CVSS_Base_Score.

Threat Centric NAC LiveLog

Refresh Export To Pause

Filter

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

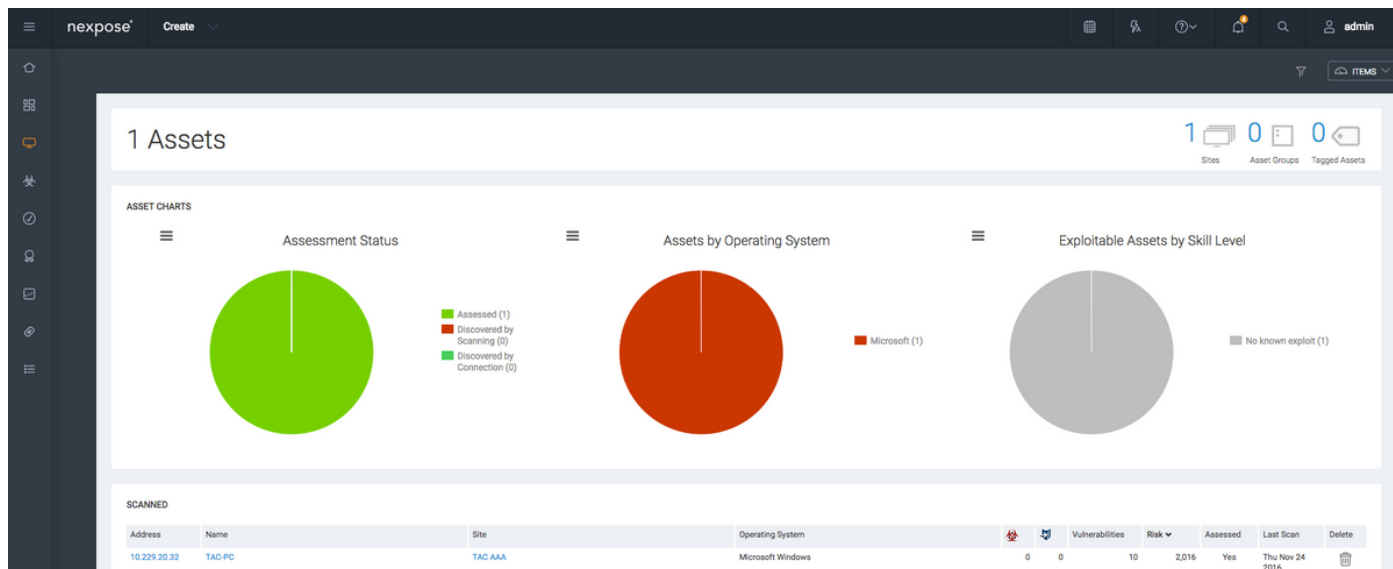
Scanner Nexpose

Quando l'analisi VA viene attivata da TC-NAC Nexpose Scan, le transizioni allo stato **In corso** e lo scanner inizia a eseguire il probe dell'endpoint. Se si esegue l'acquisizione wireshark sull'endpoint, a questo punto si verificherà lo scambio di pacchetti tra l'endpoint e lo scanner. Al termine dell'esecuzione dello scanner, i risultati saranno disponibili nella **home page**.

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](#)

Nella pagina **Asset**, è possibile verificare la presenza di un nuovo endpoint con i risultati dell'analisi, l'identificazione del sistema operativo e il rilevamento di 10 vulnerabilità.



Quando si fa clic sull'indirizzo IP dell'endpoint, Nexpose Scanner visualizza il nuovo menu, in cui è possibile visualizzare ulteriori informazioni, tra cui nome host, punteggio Risk e elenco dettagliato delle vulnerabilità

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 SDES Cipher Suite	0	0.0	Sun Feb 01 2009	Mon Feb 15 2016	Moderate	1	

Quando si fa clic su nella **Vulnerabilità** stessa, nell'immagine viene visualizzata una descrizione completa.

VULNERABILITY INFORMATION

OVERVIEW

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

DESCRIPTION

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption cipher are affected. The security of a block cipher is often reduced to the key size k; the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter; defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, CCM, CCM, 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

Risoluzione dei problemi

Debug su ISE

Per abilitare i debug su ISE, selezionare **Amministrazione > Sistema > Registrazione > Configurazione log di debug**, selezionare **TC-NAC Node** e modificare il componente **Log Level va-runtime** e **va-service** in **DEBUG**.

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

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

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

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

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

Edit Reset to Default

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

Registri da controllare - `varuntime.log`. È possibile archiviarlo direttamente dalla CLI di ISE:

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

TC-NAC Docker ha ricevuto istruzioni per eseguire la ricerca di un endpoint specifico.

```
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","isPeriodicScanEn
abled":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}
```

Una volta ricevuto il risultato, tutti i dati di Vulnerabilità vengono memorizzati nella directory di contesto.

```
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"}]}
```

Registri da controllare - vaservice.log. È possibile archiviarlo direttamente dalla CLI di ISE:

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

Richiesta di valutazione della vulnerabilità inviata alla scheda.

```
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 controlla ogni 5 minuti lo stato dell'analisi fino al completamento.

```
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"]}]]
```

L'adattatore ottiene i CVE insieme ai punteggi CVSS.

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

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)
- [Note sulla release di ISE 2.2](#)
- [Guida all'installazione dell'hardware ISE 2.2](#)
- [Guida all'aggiornamento a ISE 2.2](#)
- [Guida per l'amministratore di ISE 2.2 Engine](#)