

# ديدهتلا ىلع زكري يذلا ISE 2.2 NAC نيوكت Rapid7 مادختساب (TC-NAC)

## تايوتحمل

[عمدقمل](#)

[سياسال تابلطتم](#)

[تابلطتم](#)

[عمدختسمل تانوكمل](#)

[نيوكتلا](#)

[يوتسمل ىلع قفدت ططخم](#)

[هنيوكت وىلاتلا يئوضلا حسامل رشن](#)

[ىلاتلا يئوضلا حسامل رشن 1. ةوطخلا](#)

[ىلاتلا يئوضلا حسامل نيوكت 2. ةوطخلا](#)

[ISE نيوكت](#)

[TC-NAC تامدخ نيومت 1. ةوطخلا](#)

[ىلاتلا يئوضلا حسامل ةداهش داريتسا 2. ةوطخلا](#)

[يئوضلا NEXPOSE حسامل TC-NAC ليثم نيوكت 3. ةوطخلا](#)

[VA صحف ليغشتل ليوختلا فيرعت فلم نيوكت مق 4. ةوطخلا](#)

[ليوختلا جهن نيوكت 5. ةوطخلا](#)

[ةحصلا نم ققحتلا](#)

[ةيوهلا تامدخ كرحم](#)

[يئوضلا Nexpose حسامل](#)

[اهحالص او ءاطخال فاشكتسا](#)

[ISE ىلع ءاطخال احيحصت](#)

[ةلص تاذا تامولعم](#)

## عمدقمل

هئاطخاً فاشكتسا وديدهتلا ىلع زكري يذلا NAC نيوكت ةيفي دننتسمل اذه حضوي في مكحتلا ةزيم كلحي تت 2.2 (ISE) ةيوهلا عمدخ كرحم ىلع Rapid7 مادختساب اهحالص او تاسايس ءاشن ةينام (TC-NAC) ديهتلا ىلع زكترت يتلا ةكبشلا ىل لوصلو ديهتلا تائيهام نم اهلابقتسا متي يتلا فعضلا وديدهتلا تامس ىل اذانتسا ضيوفت فعضلا نم اكمو.

## سياسال تابلطتم

### تابلطتم

ةيلاتلا عيضاوملاب ةساسا ةفرعم كي دل نوكت ناب Cisco ي صوت

- Cisco نم ةيوهلا عمدخ كرحم
- Nexpose رثاتلل ةيلبائل يئوضلا حسامل

## ةمدختسمل اتانوكملا

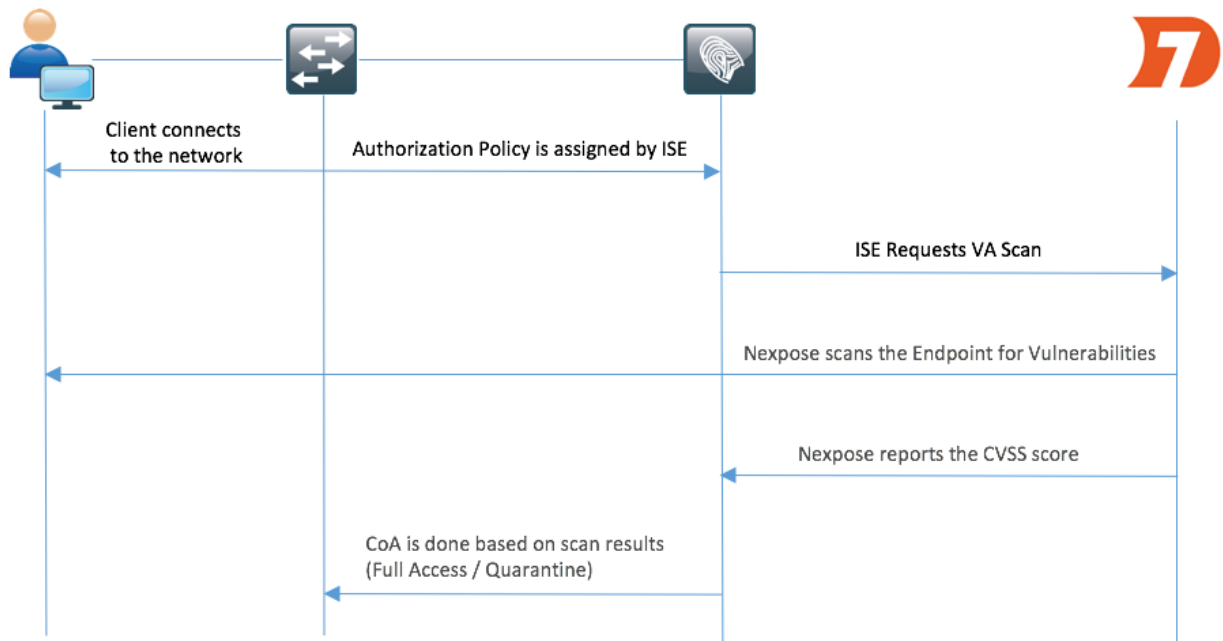
ةيلالات ةيدامل اتانوكملا وجماربال اتارادصلإ لىل دنن تسمل اذف ةدراول اتامل عمل دنن تس

- Cisco Identity Service Engine، رادصلإ 2.2
- Cisco Catalyst 2960S Switch 15.2(2a)E1
- Rapid7 Nexpose Vulnerability Scan Enterprise Edition
- Windows 7 ليغش التل ماظنل 1 ةمدخل ةمزح
- Windows Server 2012 R2 ليغش التل ماظن

ةصاخ ةيلعمل عم ةئيب يف ةدوجوملا ةزهجال نم دنن تسمل اذف ةدراول اتامل عمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنن تسمل اذف يف ةمدختسمل ةزهجال اعيمج تادب رما يال لمحتمل ريثاتلل كمهف نم دكأتف، ةرشابم كتكبش

## نيوكتل

### ىوتسمل يلاع قفدت ططخم



قفدتلا وه اذف:

1. عبرمب فيرعت فلم نييغت متي و دودحم لوصوحنم متي و ةكبشلاب لي عمل لصتي. هنيكمت مت يذلل فعضللا نطاوم مييقت رايخإ
2. VA حسم ناك و ةقداصلما ثودح دكؤت MNT ةدقع لىل syslog ةلاسرس PSN ةدقع لسرت لي وختلا جهنل ةجيتن
3. Admin WebApp مادختساب) TC-NAC ةدقع لىل ليئوضلا حسملا لاسراب MNT ةدقع موقت

تانايايابل هذه مادختساب:

- MAC ناوع
- IP ناوع
- حسملل ينمزلال لصالال
- يروال لصالال نيكم ت
- يلال ال PSN

4. ليغشتل Nexpose Scan حسامب (Docker ةيواحي في نمضمال) Nexpose TC-NAC لصلتي .  
ةجالال دن ع حسمال

5. ISE لبق نم ةبولطمال ةياهنال لةطقن صحب Nexpose ل ئيوضال حسامال موقوي .

6. ISE لئال ئيوضال حسمال جئاتن Nexpose ل ئيوضال حسامال لسري .

7. TC-NAC لئال رخأ ةرم صبال جئاتن لاسرا متي .

- MAC ناوع
- CVSS جئاتن ةفاك
- (CVEIDs) ةصال لةيراجتال تافرعمال او ناوعال) فعضال طاقن عيجم

8. ةوطخال نم تانايايابل عيجم عم PAN ثيحتب TC-NAC موقوي .

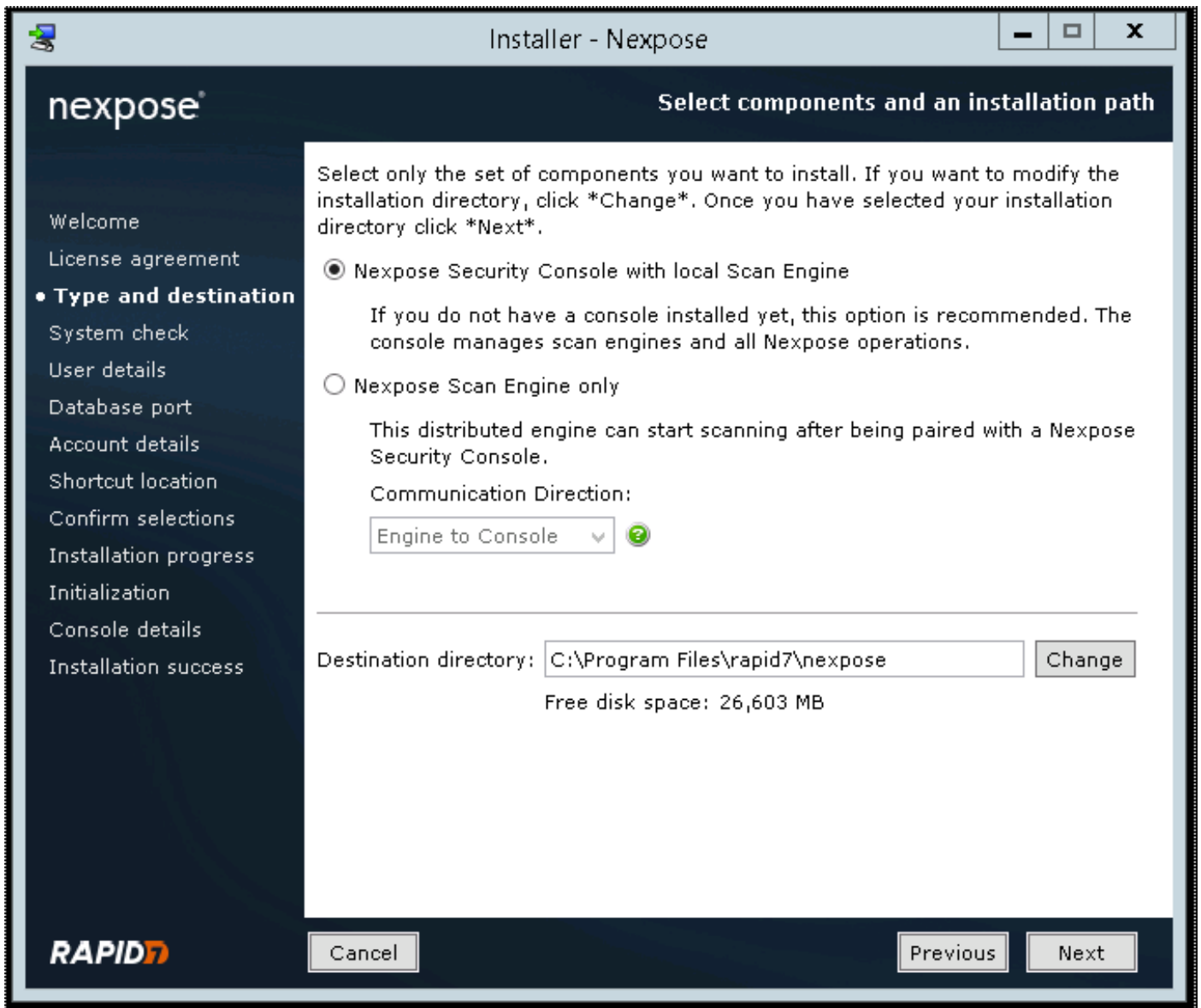
9. هنيوكت مت يذال لئوختال جهنال اق فو ةجالال دن ع CoA ليغشت متي .

## هنيوكتو يلالال ئيوضال حسامال رشن

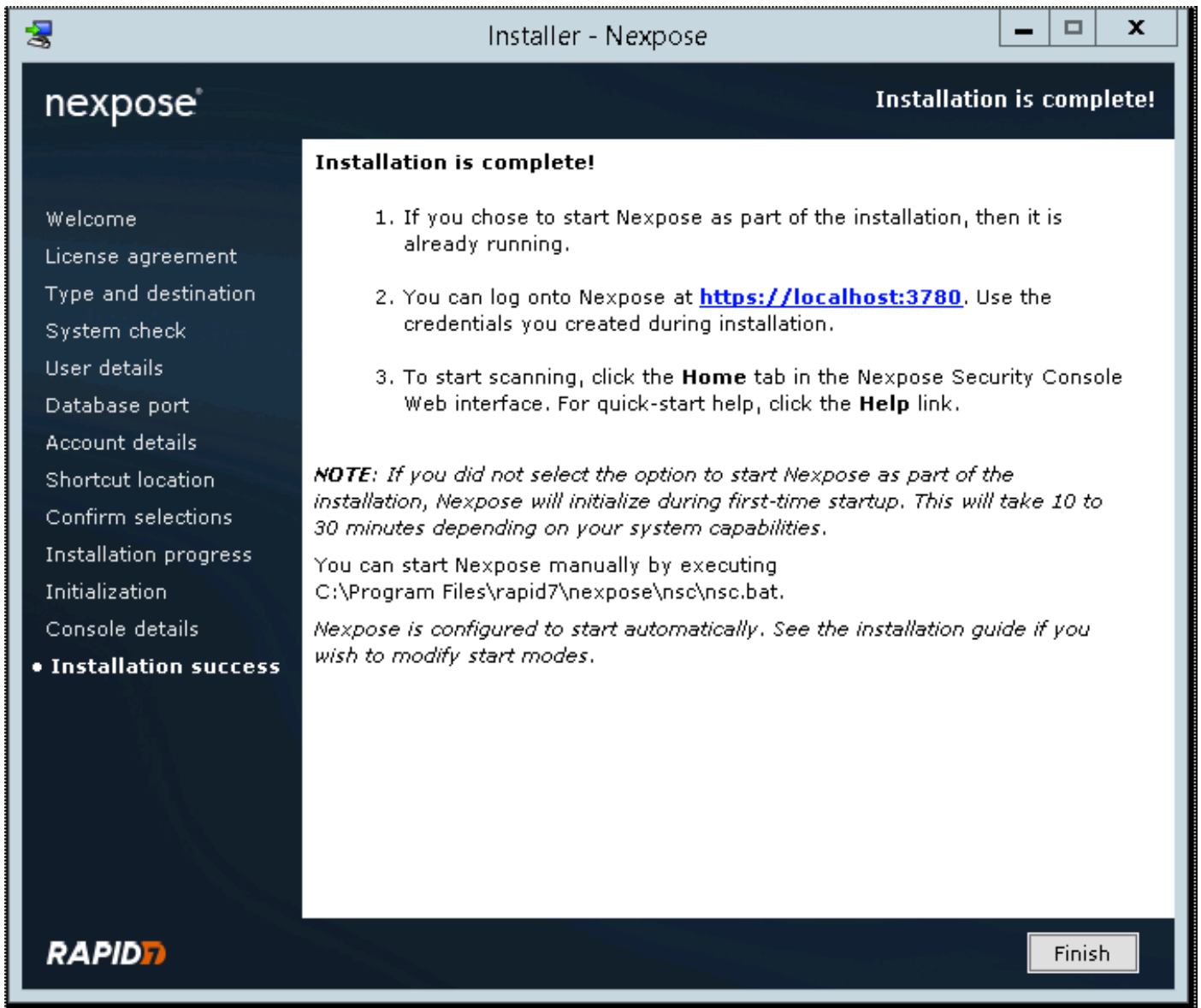
يسدنه م ةراشتسا لئجري ، ةيللم عم ضارغال دنن سمال اذه في Nexpose نئوكت مت : ريذحت  
مئمصتال تارابتعال Rapid7

### ياللال ئيوضال حسامال رشن 1. ةوطخال

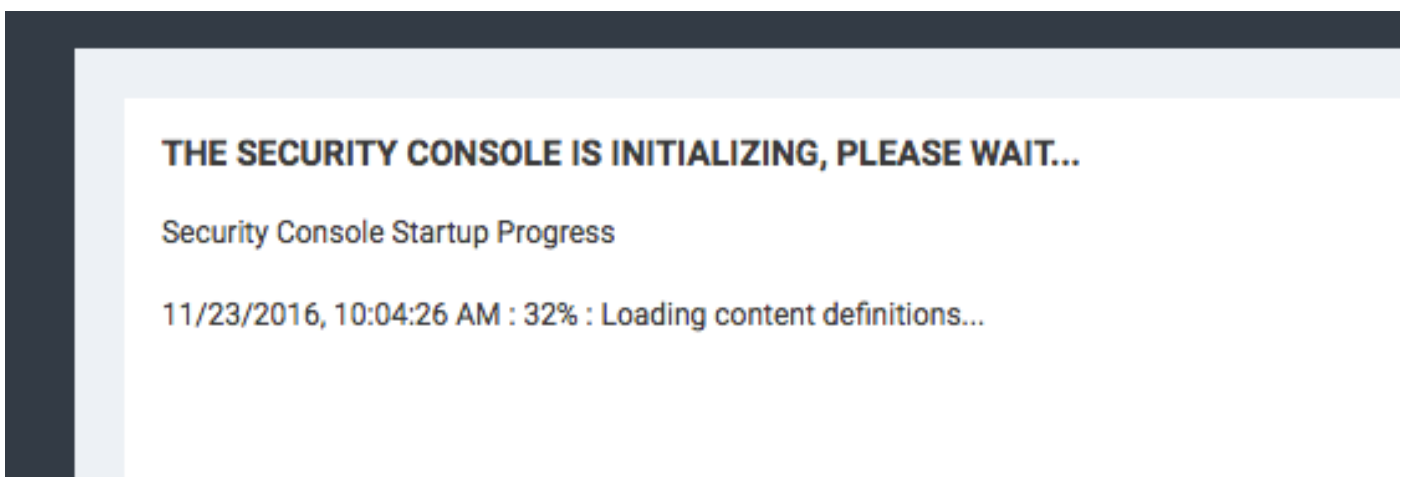
و Linux لئوختال ماظن قوف تبتمال ، OVA فلم نم Nexpose ئيوضال حسامال رشن نكمي  
لئزنن تبت مق . Windows Server 2012 R2 لئوختال متي ، دنن سمال اذه في  
دح ، ةهول او عونل نئوكت دن ع . تبتتال ةيللم ع ادباو بيولال لئوختال Rapid7 ع قوم نم ةروصلال  
يلل حمال ئيوضال حسمال كحم عم Nexpose نامال مكحت ةدحو



حسام ىل لوصولا بجي، ليغشتلا دع ب. مداخل ديهمت ةداع امت، تيبتتلا لامتك درجم ب  
ةروصلال يف حضورم وه امك، 3780 ذفنم ربع يئوضلال Nexpose:



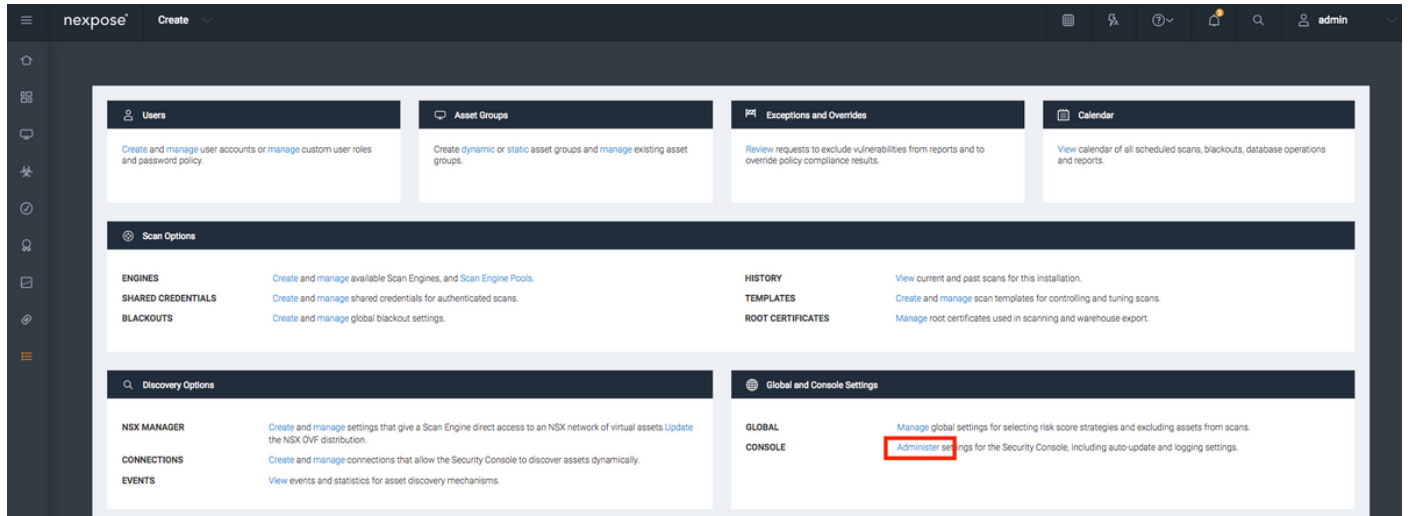
نام الة مكحت ةدحو لى غشت ءدب ةى لمعب ىئوضلا حساملا رمى؁ ةروصولا ىف حضوم وه امك



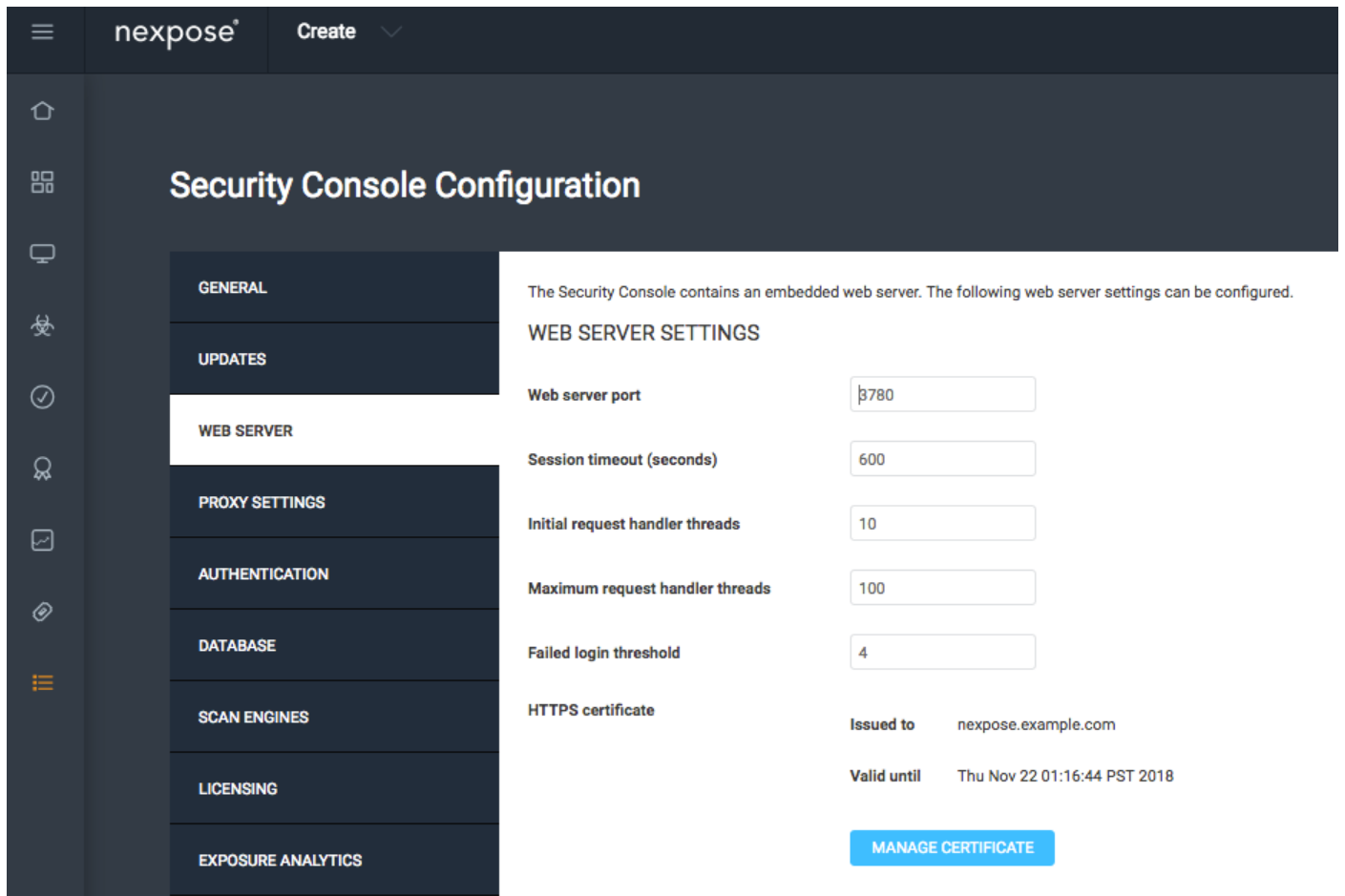
ىجرى .صىخرتلا حاتفم رىفوت بچى (GUI) ةىموسررلا مدختسمللا ةهجاو ىلى لوصولل كلذ دعب  
تاىلمع لى غشت متى الو؁ ىئوضلا Nexpose حسام نم Enterprise رادصا مزلى هنا ةظحال  
م Community رادصا ناك اذا حساملا

ىلاتلا ىئوضلا حساملا نىوكت 2. ةوطخل

رادصا متي Nexpose يئوضلا حساملا يلع تيبتتلا ةداهش يف يلاؤالا ةوطخلا لثمتت ISE (LAB) ل لوؤسم ةداهشك CA ةداهش سفن ةطساوب دنتسمل اذه يف ةدوجوملا ةداهشلا وه امك ،مكحتلا ةدحو تحت ةرادا دح .مكحتلا ةدحو تادادعإو ةماع تادادعإ > ةرادا يلا لقتنا . ةروصولا يف حضوم



ةروصولا يف حضوم وه امك ،ةداهشلا ةرادا يلع رقنا:



يرخأ تانايب ي أو عئاشلا مسالا لخدأ .ةديج ةداهش عاشنا يف رقنا ،ةروصولا يف حضوم وه امك ISE ةردق نم دكأت .Nexpose يئوضلا حساملا فيرعت ةداهش يف اهيلع لوصحلا يف بغيرت DNS مادختساب Nexpose ل يئوضلا حساملا ب صاخلا FQDN لحد

## 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

ةف رطلا ةدحولا لىا (CSR) ةداهشلا عيقوت بلط ري دصت

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

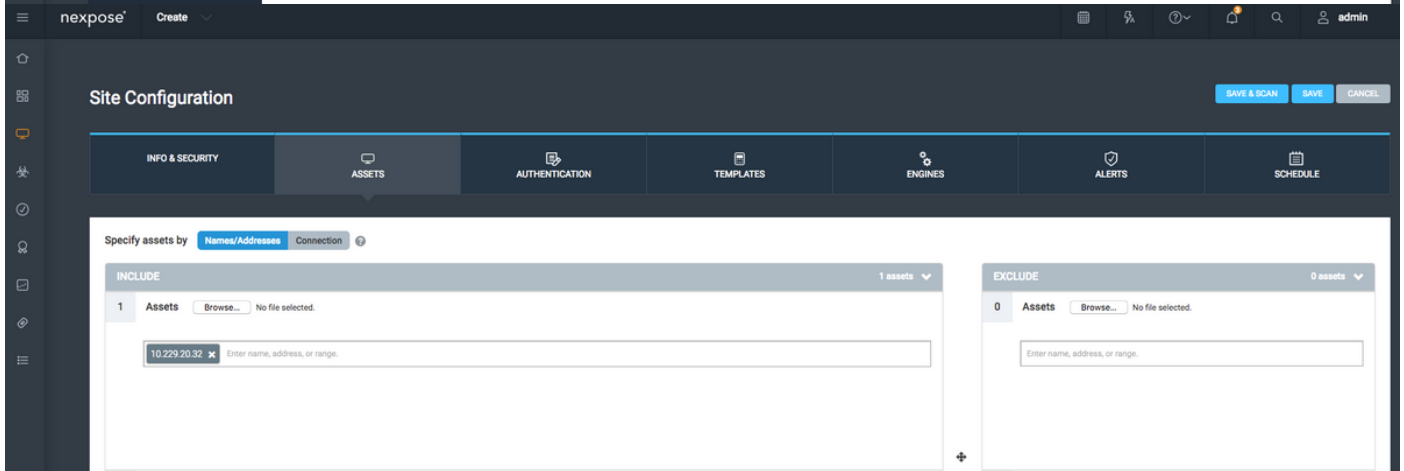
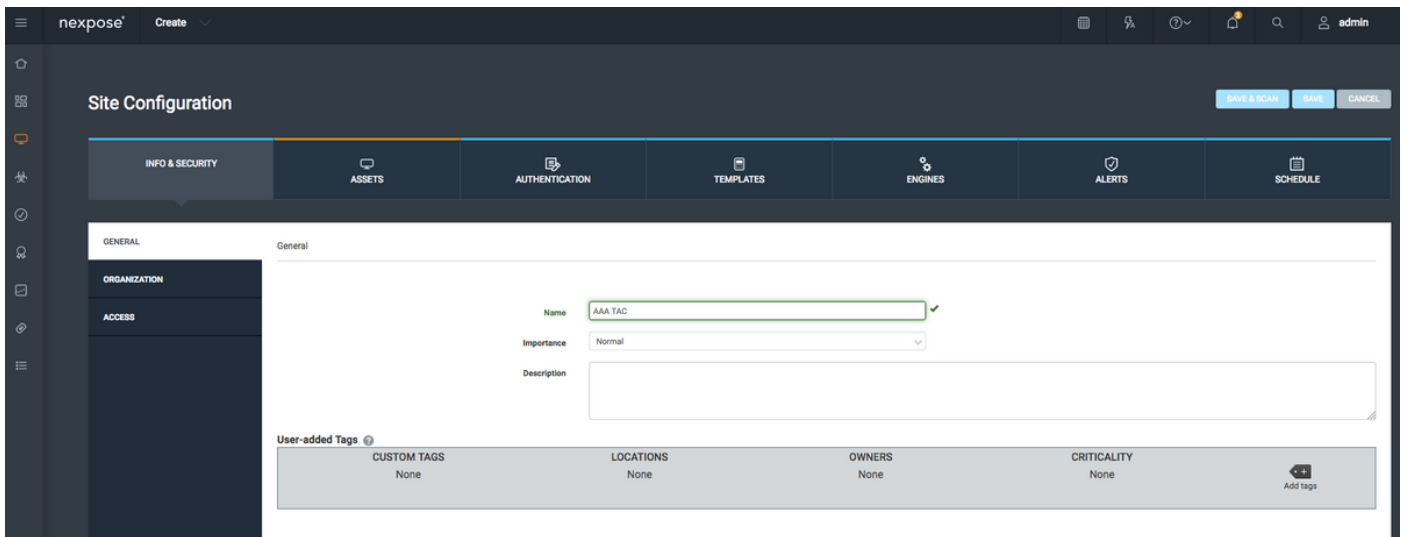
LATER

(CA) ق دصملا عجرملا مادختساب CSR عيقوت لىا جاتحت، ةطقنلا هذه دنع









لقتنا . هب قوٹومل انزخملا في ISE ةداهش ىلع تعقوي تاللا قدصملا عجرملا ةداهش داري ت سا  
 تاداهشلا داري ت سا > ةرادا > رذجال تاداهش > ةرادا ىل



## ISE نيوكت

### TC-NAC تامدخ نيكمت 1. ةوطخل

يلي ام طحال ISE. ةدقع ىلع TC-NAC تامدخ نيكمت

- اري بك اصيخرت ديدهتلا ىلع زكترت ي تاللا NAC ةمدخ بلطتت
- ىلع زكترت ي تاللا NAC ةمدخل ةلصفنم (PSN) ةسايس ةمدخ ةدقع ىللا ةجاحب تنأ ديدهتلا
- رشنلا في طقف ةدحاو ةدقع ىلع تاديدهتلا ىلع زكترت ي تاللا NAC ةمدخ نيكمت نكمي
- تارغثلا مي يقت ةمدخل دروم لكل ئيها مل طقف دحاو ليثم ةفاضلا كنكمي



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

Vendor \*

Instance Name \*

مق. طابترالا اذه قوف رقنا. ةلاحلا نيوكتل ةزهاج ىلا ليثملا ليوحت متي ،اهتفاضل درجمب  
مسا دح. 3780 وه يضارتفا لكش ب ،ذفنملاو (يئوضلا حساملا) فيضملا نيوكتب  
نم ال اعقوملا ىلا لوصول عم رورملا ةملاك و مدختسملا

### 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.

ىلع روثعلا نكمي و، ISE 2.2 لوؤسم ليلدي في ديج لكشبة مدمقتملا تادادعإل قيثوت مت ليغشت أدبي. زاجنإو كلذ دعب في تقطوط. دننسملا اذه في عجارملا مسق في طباترالا فراعملا دءاق ليزنتو ءطشنلا ءلألإل Nexpose ليلثم لاقننا تايلمع.

Third Party Vendors

Vendor Instances

Refresh Add Trash Edit Restart Stop Filter

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
Rapid7	Rapid7 Nexpose	VA	nexpose.example.com	Connected	Active

VA صحف ليغشتل ليلوختلا فيرعت فلم نيوكتب مق 4 ءوطخل

صيصخت تافلم > ليلوختلا > ءئاننلا > ءسايصل رصانع > ءسايصل لىل لقتنا مبيقت رايءخالا ءناخ دء ءكرتشملا ماهملا تحت. ديدج فيرعت فلم ءفاضل. ليلوختلا ءكبشلا ميمصتل اءوفو بلطال بسح حسمل ليلنمزلال لصال ديدحت بءي. تارءثلا

هءه AV ءاوزأ لىل ليلوختلا فيرعت فلم يوتءي

```
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
```

يقيءل ضرءل نأ نم مءرلا لىل، لوصولا لوبق ءمزء لءاء ءكبشلا ءزهء لىل اءلاسرا مءي و TC-NAC ءءق MNT دءري. صحفلا ليلغشت ءرورضب (MNT) ءبقارملا ءءق مءلء وه انه م Nexpose يءوئلل حساملاب لاصلال

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Global Exceptions Policy Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

\* Name: Rapid7

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Assess Vulnerabilities

Adapter Instance: Rapid7

Trigger scan if the time since last scan is greater than: 48

Enter value in hours (1-9999)

Advanced Attributes Settings

Select an item =

Attributes Details

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

## ل.ي وخت ل جهن ني وكت 5. ة وطل ل

- في هني وكت مت يذلا ل دي وخت ل ل دي وخت ل ل في رعت فلم مادخت س ل ل ل دي وخت ل ل جهن ني وكت ب مق ة د عاق ددحو، **ضي وفت ل ة سايس > ضي وفت > ة سايس** ل ل ل ق ت نا. 4. ة وطل ل ل نم ت ان و ذ ال ر ي غ ت ب مق. (ر ي رحت) **Edit** ق و ف ر ق نا م ت، **basic\_authenticated\_access** ص ح ف ا ر ج ل ل ل ك ل ذ ي د و ي. ا ث ي د ح ه و ا ش ن ل م ت ي ذ ل ا **Standard Rapid7** ل ل **PermitAccess** ظ ف ح ي ف ر ق نا. ن ي م د خ ت س م ل ا ة ف ا ك ل ت ا ر غ ث ل ل
- **> ضي وفت > جهن** ل ل ل ق ت نا. ا ه ي ل ع ي ح ص ر ج ح ض ر ف م ت ي ت ل ا ة ز ه ج ال ل د ا م ت ع ا جهن ا ش ن ل **ءاشن ل > ط و ر ش ل ل** ل ل ل ق ت نا. **ءا ن ث ت س ل د ع ا ق ءا ش ن ل و ت ا ء ا ن ث ت س ل > ل دي وخت ل ل جهن** ع ي س و ت ب مق. **دي د ه ت ل د د ح و ل ف س ال ر ي ر م ت ل ا ب مق**، **ء م س د ي د ح ت > (م د ق ت م ر ا ي خ) د ي د ج ط ر ش ر ب ك ا ل ل ل دي وخت ل ل ل م ا ع ر ي ي غ ت ب مق**. **Nexpose-CVSS\_BASE\_SCORE** د د ح و د ي د ه ت ل ة م س **ضي وفت** في رعت فلم ي ط ع ي ن ا ب ج ي. ك ب ص ا خ ل ل ن ا م ال جهن ل ا ق ف و ة م ي ق ل ا خ د ا ب مق و نم ي م ح م ل ا ر ي غ ز ا ه ج ل ل ا د و د ح م ال و ص و ي ح ص ل ل ر ج ح ل ا

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
✓	Exception Rule	if Threat:Rapid7 Nexpose-CVSS_Base_Score GREATER 1	then Quarantine

Standard

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

## تحصيل نم ققحتلا

### ةيوهلا تامدخ كرحم

لئغشت متي ،صحفلا ءاهتنا دنع VA لئوئوضلا حسملا لئغشتب لوالا لاصتالا موقئ هتقباطم ةلاح ئف دئدج جهن قئبطل CoA ةقداصم ةداع

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	⊙		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	✓			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	✓			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	✓			alice	3C-97-0E-52-3F-D9	Nortel-Device	Default >> D...	Default >> B...	Rapid7	10.229.20.32	Switch_2960	FastEthernet1/0/5	Profilled

ةياهنلا طاقن > قئبطل ةئورئ لئقننا ،ءافاشتكا مت ئتلا فعضلا نم اك نم ققحتلل حسام لالخنم هل ةاطعمل تامالعمل مادختساب ةياهن ةطقن لكل فعضلا طاقن نم ققحت ئوئوضلا 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

عقب طم ال ضيوفت ل اس ايس ة يور كن كمي ، ةرشابم ل TC-NAC ال جس > تاي لمع ل ي ف  
 ة ق ب ط م ل ض ي و ف ت ل ا س ا ي س ة ي و ر ك ن ك م ي ، ة ر ش ا ب م ل TC-NAC ال ج س > ت ا ي ل م ع ل ي ف  
 CVSS\_BASE\_SCORE ل ع ل ي ص ا ف ت ل و

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

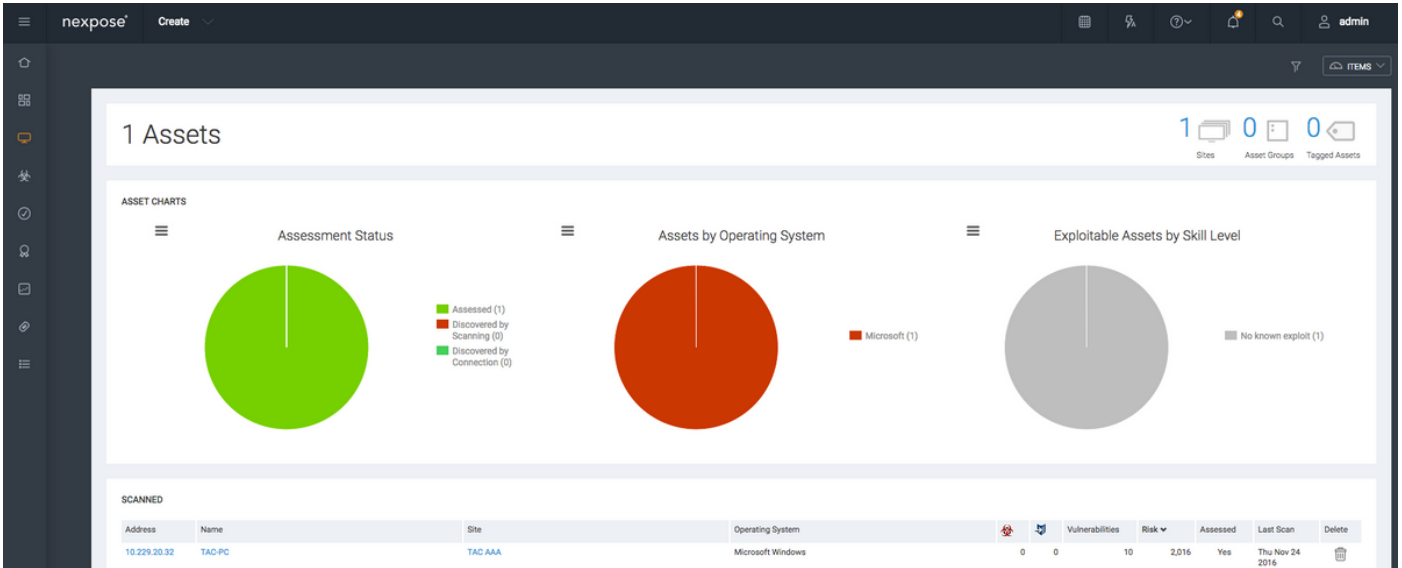
## يئوض ل Nexpose ح سام

ديق ة ل ا ح ل TC-NAC Nexpose Scan ال ا ل ا ق ت ن ا ة ط س ا و ب VA ح س م ل ي غ ش ت م ت ي ا م د ن ع  
 ط ا ق ت ل ل ي غ ش ت ب ت م ق ا ذ ا ، ة ي ا ه ن ل ا ة ط ق ن م ق ق ح ت ل ا ي ف يئوض ل ح سام ل ا ا ب ي و ، م د ق ت ل ل  
 د ن ع يئوض ل ح سام ل و ا ة ي ا ه ن ل ا ة ط ح م ن ي ب م ز ح ل ا ل د ا ب ت ي ر ت س ، ة ي ا ه ن ل ا ة ط ق ن ل ع Wireshark  
 ة ي س ي ئ ر ل ا ة ح ف ص ل ل ن م ض ج ئ ا ت ن ل ا ر ف و ت ت ، يئوض ل ح سام ل ا ا ه ت ن ا د ر ج م ب . ة ط ق ن ل ا ه ذ ه



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			

حسمل جئاتن عم ةرفوتم ةديج ةياهن ةطقن كانه نأ يرت نأ كنكمي ،لوصول ةحفص تحت فعض طاقن 10 فاشتكا متيوليغشتلا ماظن ديحت متيوليغ، ةيئوضلا



ةمئاقلا لىإ Nexpose ةيئوضلا حسملا كلقني ةياهنلا ةطقنل IP ناوئع يف رقت امئع ةمالعو ةيئوضلا مساكلذ يف امب تامولعمل نم ديزملا ةيؤر كنكمي شيح ،ةديجلا فعضلا طاقن نم ةلصفم ةمئاقو

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

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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude
<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	Exclude

ةروصولا يف لماكل فصولا ضرع متي ،اهسفن فعضلا ةلاح يف رقت امئع

**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, 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"> <li>Negotiated with the following insecure cipher suites:               <ul style="list-style-type: none"> <li>TLS 1.0 ciphers:                   <ul style="list-style-type: none"> <li>TLS_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul> </li> </ul> </li> </ul>	Nov 24th, 2016	Exclude

# اه حال صوا ءاطخ ال فاشكت سا

## ISE يلع ءاطخ ال حي حصت

لجس ني وكت > ليجست > م اظنل > ءرادال يلى لقتنا، ISE يلع ءاطخ ال حي حصت ني كمتل va-runtime و va-service لجس ال يوتسم نوكم ريغتب مقو، TC-NAC ءدق ءدحو، ءاطخ ال حي حصت ءاطخ ال حي حصت يلى.

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

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

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

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

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

Edit Reset to Default

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

رطس ءهجاو نم ءرشابم اه يلع لوصح ال كنكمي. varuntime.log - اه صحف بولطم ال الجس ال ISE رم او:

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

ءني عم ءي اهن ءطقنل صحف ال ءارجال تاءاشرا TC-NAC Docker يقلت

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

## قاي س ل ل ل ي د ي ف ة ي ن م أ ل ا ت ا ر غ ث ل ا ت ا ن ا ي ب ع ي م ج ن ي ز خ ت م ت ي ، ة ج ي ت ن ل ل ا م ا ل ت س ا | د ر ج م ب و

```
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": "4.3000019", "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": "4.3000019", "vulnerabilityTitle": "TLS/SSL Server is enabling the
BEAST attack", "vulnerabilityVendor": "Rapid7 Nexpose"}, {"vulnerabilityId": "tlsv1_0-
enabled", "cveIds": "", "cvssBaseScore": "4.3000019", "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": "4.3000019", "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": "4.3000019", "vulnerabilityTitle": "TLS/SSL Server is enabling the BEAST
attack", "vulnerabilityVendor": "Rapid7 Nexpose"}, {"vulnerabilityId": "tlsv1_0-
enabled", "cveIds": "", "cvssBaseScore": "4.3000019", "vulnerabilityTitle": "TLS Server Supports TLS
version 1.0", "vulnerabilityVendor": "Rapid7 Nexpose"}]]}
```

## ة ه ج ا و ن م ة ر ش ا ب م ا ه ي ل ع ل و ص ح ل ا ك ن ك م ي . Catalyervice.log - ا ه ص ح ف م ت ي س ي ت ل ا ت ا ل ج س ل ا س ل ا ISE: ر م ا و ا ر ط س :

## لوحمال ىل فعضلا مېيقت بلط لاسرا مت

```
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"]}
```

## يہتنني ىتح صحفلا ةلاح نم قئاقد 5 لك AdapterMessageListener ققحتي

```
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-
fe4e9fadadb","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-fe4e9fadadb","TC-NAC.VendorName","Rapid7
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}]]
```

## جئاتن عم CVE ىل عل لوحمال لصرحي

```
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"]}
```

## ةلص تاذا تامولعم

- [تادنتس مل او ینقتلا معدلا - Cisco Systems](#)
- [رادصإلا تاظحالم ISE 2.2](#)
- [ةزهجالا تېبثت لېلد ISE 2.2](#)
- [ةیقرت لېلد ISE 2.2](#)
- [كرحم لوؤسم لېلد ISE 2.2](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت م م م ي دقت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه  
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا