تكوين ISE 2.2 NAC الذي يركز على التهديد (TC-NAC) باستخدام Rapid7

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين NAC الذي يركز على التهديد واستكشاف أخطائه وإصلاحها باستخدام Rapid7 على محرك خدمة الهوية (ISE) 2.2. تتيح لك ميزة التحكم في إمكانية إنشاء سياسات (TC-NAC) الوصول إلى الشبكة التي ترتكز على التهديد والضعف التي يتم استقبالها من معايير التهديد وتفويض الاستجابة إلى سمات التهديد والضعف ومكامن الضعف.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمة الهوية من Cisco
- الماسح الضوئي للقابلية للتأثر Nexpose

المكونات المستخدمة

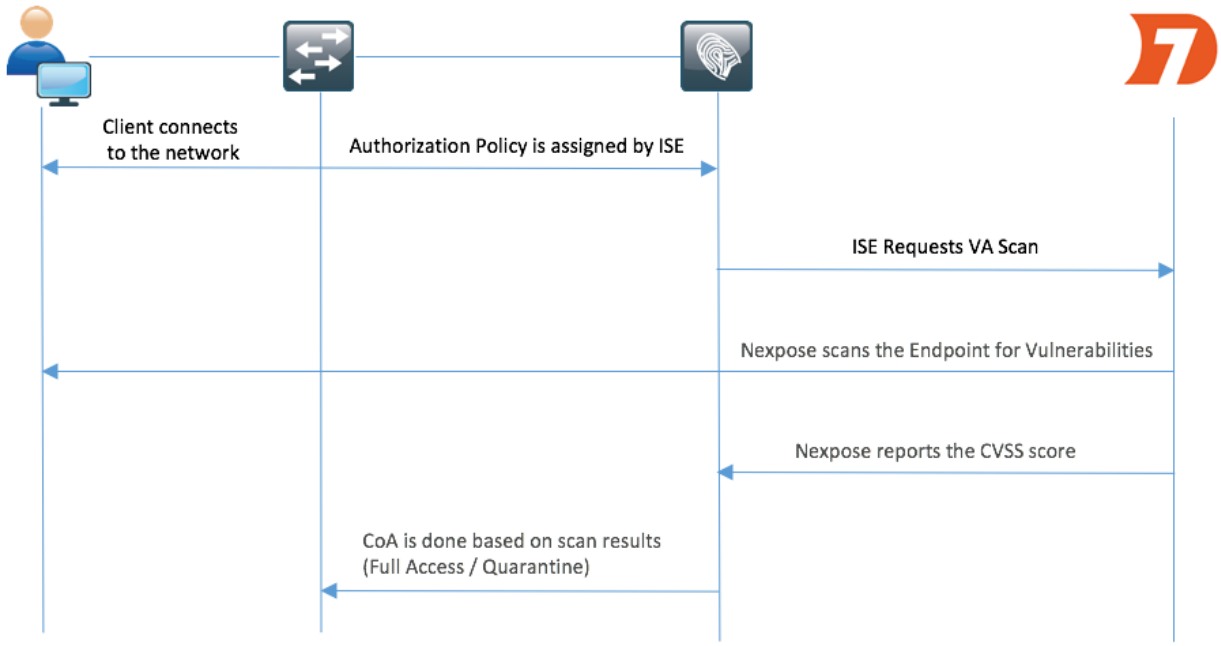
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Identity Service Engine، الإصدار 2.2
- المحول Cisco Catalyst 2960S Switch 15.2(2a)E1
- Rapid7 Nexpose Vulnerability Scan Enterprise Edition
- حزمة الخدمة 1 لنظام التشغيل Windows 7
- نظام التشغيل Windows Server 2012 R2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

مخطط تدفق عالي المستوى



هذا هو التدفق:

1. يتصل العميل بالشبكة ويتم منح وصول محدود ويتم تعيين ملف تعريف بمربع إختيار **تقييم مواطن الضعف** الذي تم تمكينه.

2. ترسل عقدة PSN رسالة syslog إلى عقدة MNT تؤكد حدوث المصادقة وكان مسح VA نتيجة لنهج التخويل.

3. تقوم عقدة MNT بإرسال المسح الضوئي إلى عقدة TC-NAC (باستخدام Admin WebApp)

باستخدام هذه البيانات:
- عنوان MAC
- عنوان IP
- الفاصل الزمني للمسح
- تمكين الفحص الدوري
- PSN الأصلي

4. يتصل Nexpose TC-NAC (المضمن في حاوية Docker) بماسح Nexpose Scan لتشغيل المسح عند الحاجة.

5. يقوم الماسح الضوئي لـ Nexpose بفحص نقطة النهاية المطلوبة من قبل ISE.

6. يرسل الماسح الضوئي لـ Nexpose نتائج المسح الضوئي إلى ISE.

7. يتم إرسال نتائج الفحص مرة أخرى إلى TC-NAC:
- عنوان MAC
- كافة نتائج CVSS
- جميع نقاط الضعف (العنوان والمعرفات التجارية الخاصة (CVEIDs))

8. يقوم TC-NAC بتحديث PAN مع جميع البيانات من الخطوة 7.

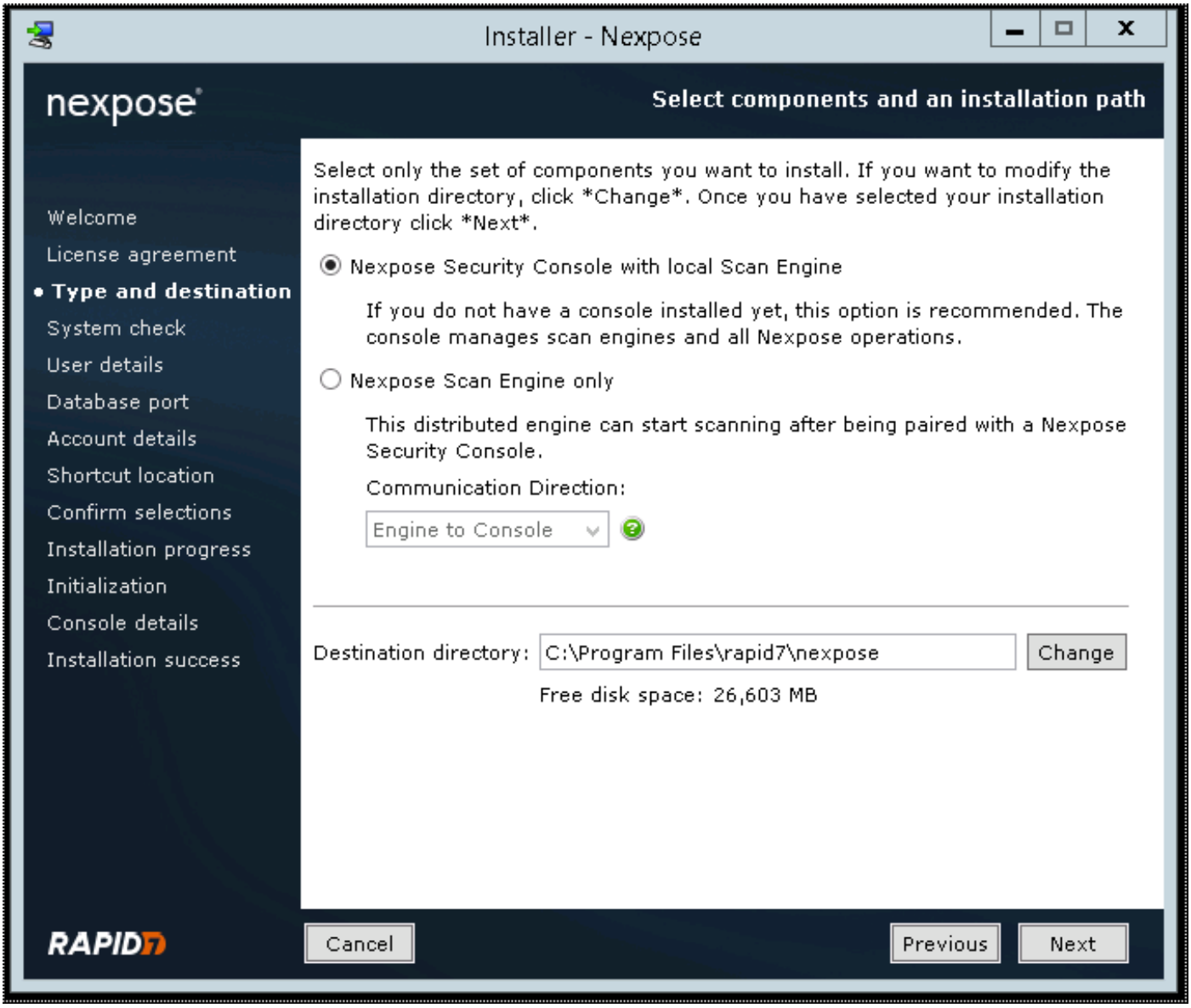
9. يتم تشغيل CoA عند الحاجة وفقا لنهج التخويل الذي تم تكوينه.

نشر الماسح الضوئي التالي وتكوينه

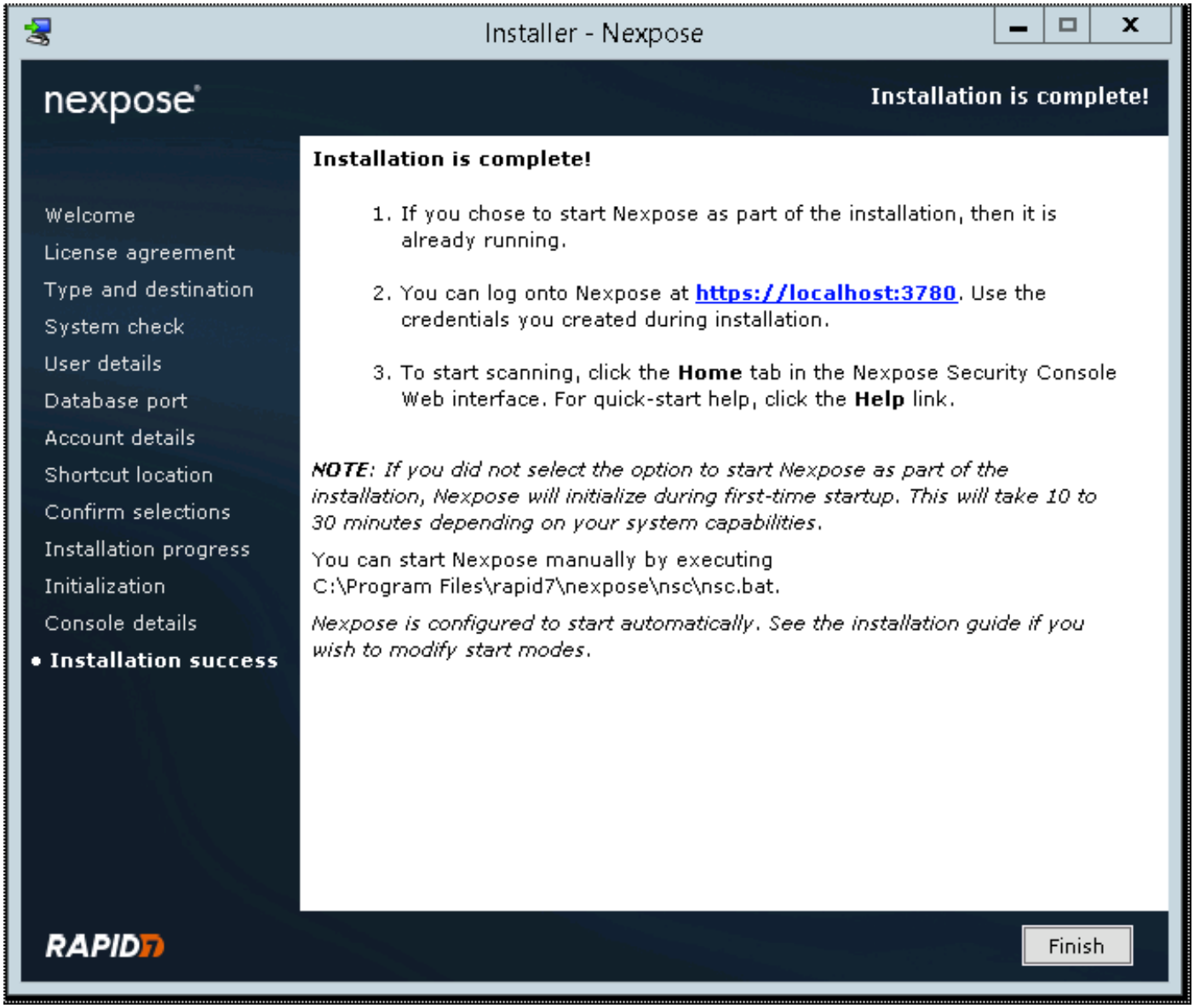
تحذير: تم تكوين Nexpose في هذا المستند لأغراض معملية، يرجى إستشارة مهندسي Rapid7 لاعتبارات التصميم

الخطوة 1. نشر الماسح الضوئي التالي.

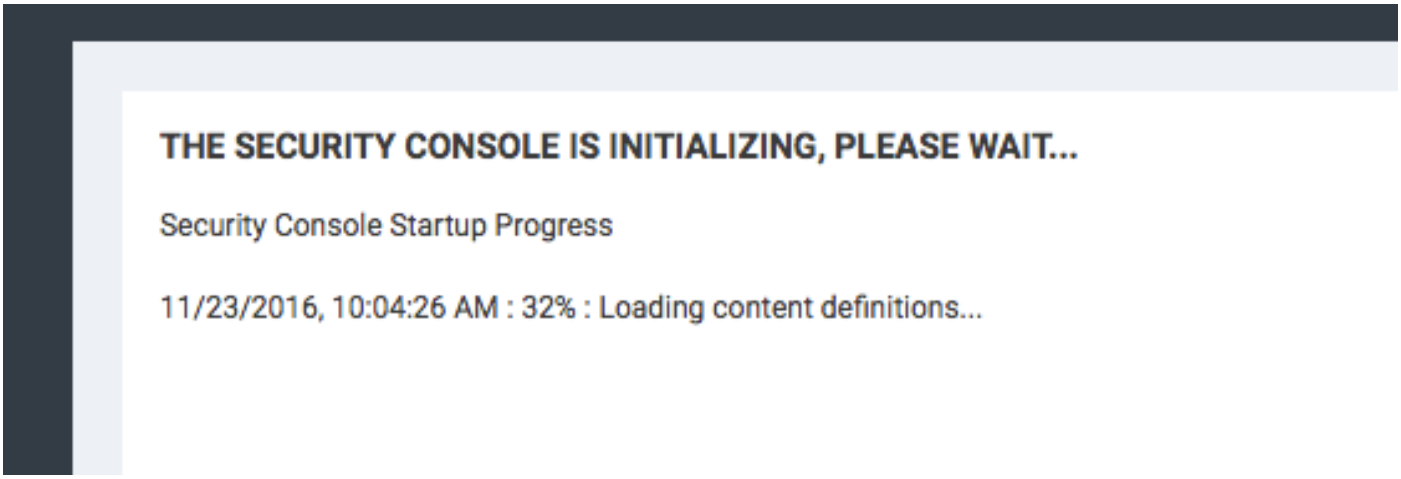
يمكن نشر الماسح الضوئي Nexpose من ملف OVA، المثبت فوق نظام التشغيل Linux و Windows. في هذا المستند، يتم التثبيت على Windows Server 2012 R2. قم بتنزيل الصورة من موقع Rapid7 على الويب وابدأ عملية التثبيت. عند تكوين **النوع والوجهة**، حدد **وحدة تحكم الأمان Nexpose مع محرك المسح الضوئي المحلي**



بمجرد اكتمال التثبيت، تتم إعادة تمهيد الخادم. بعد التشغيل، يجب الوصول إلى ماسح Nexpose الضوئي عبر منفذ 3780، كما هو موضح في الصورة:



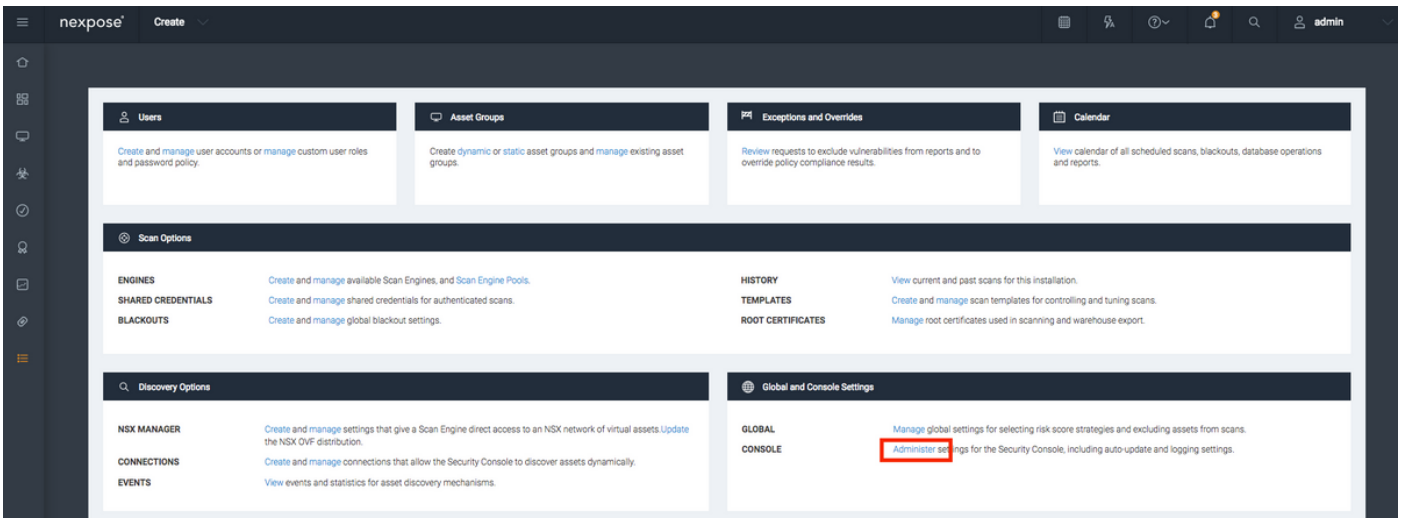
كما هو موضح في الصورة، يمر الماسح الضوئي بعملية بدء تشغيل وحدة تحكم الأمان:



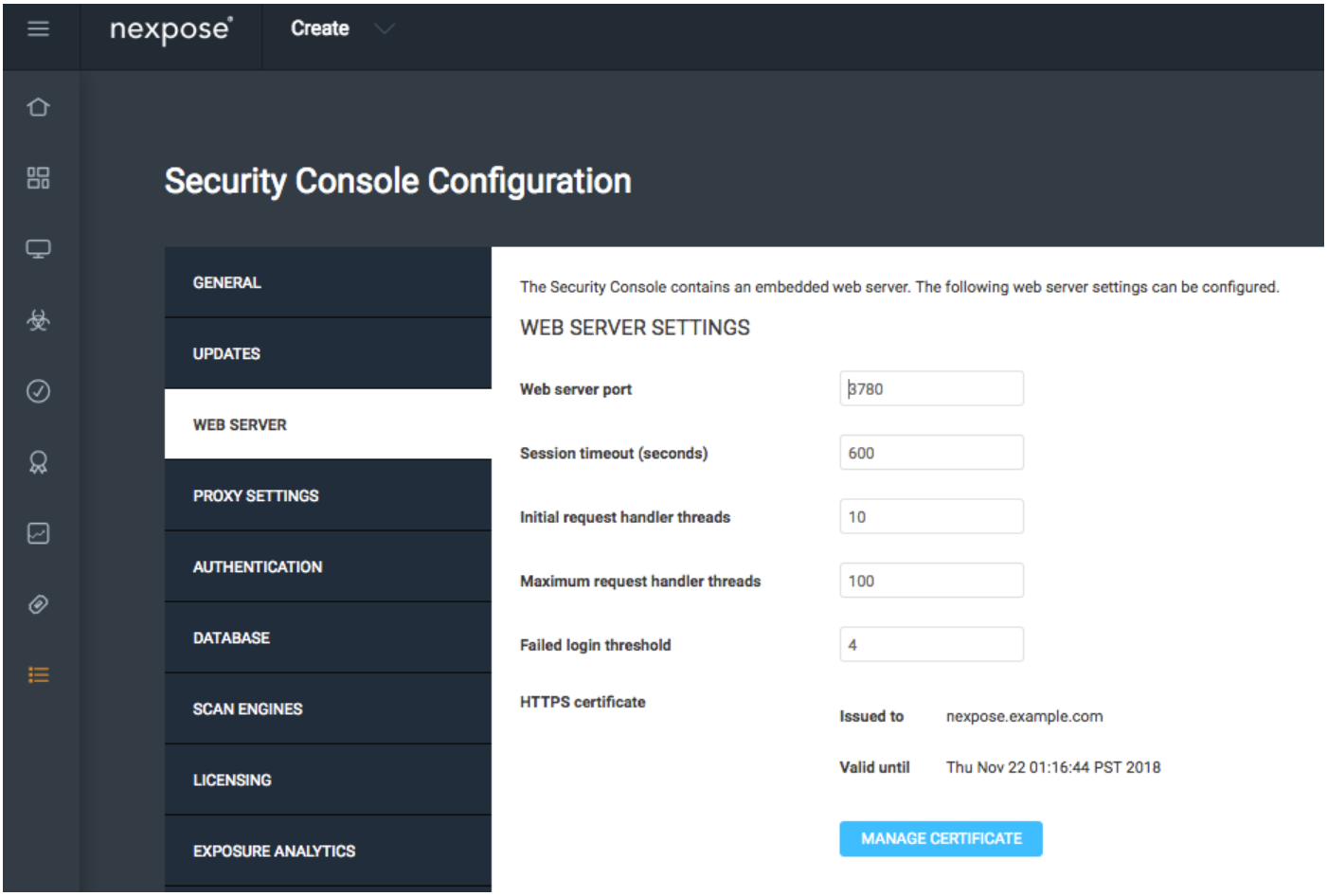
بعد ذلك للوصول إلى واجهة المستخدم الرسومية (GUI) يجب توفير مفتاح الترخيص. يرجى ملاحظة أنه يلزم إصدار Enterprise من ماسح Nexpose الضوئي، ولا يتم تشغيل عمليات المسح إذا كان إصدار Community مثبتا.

الخطوة 2. تكوين الماسح الضوئي التالي.

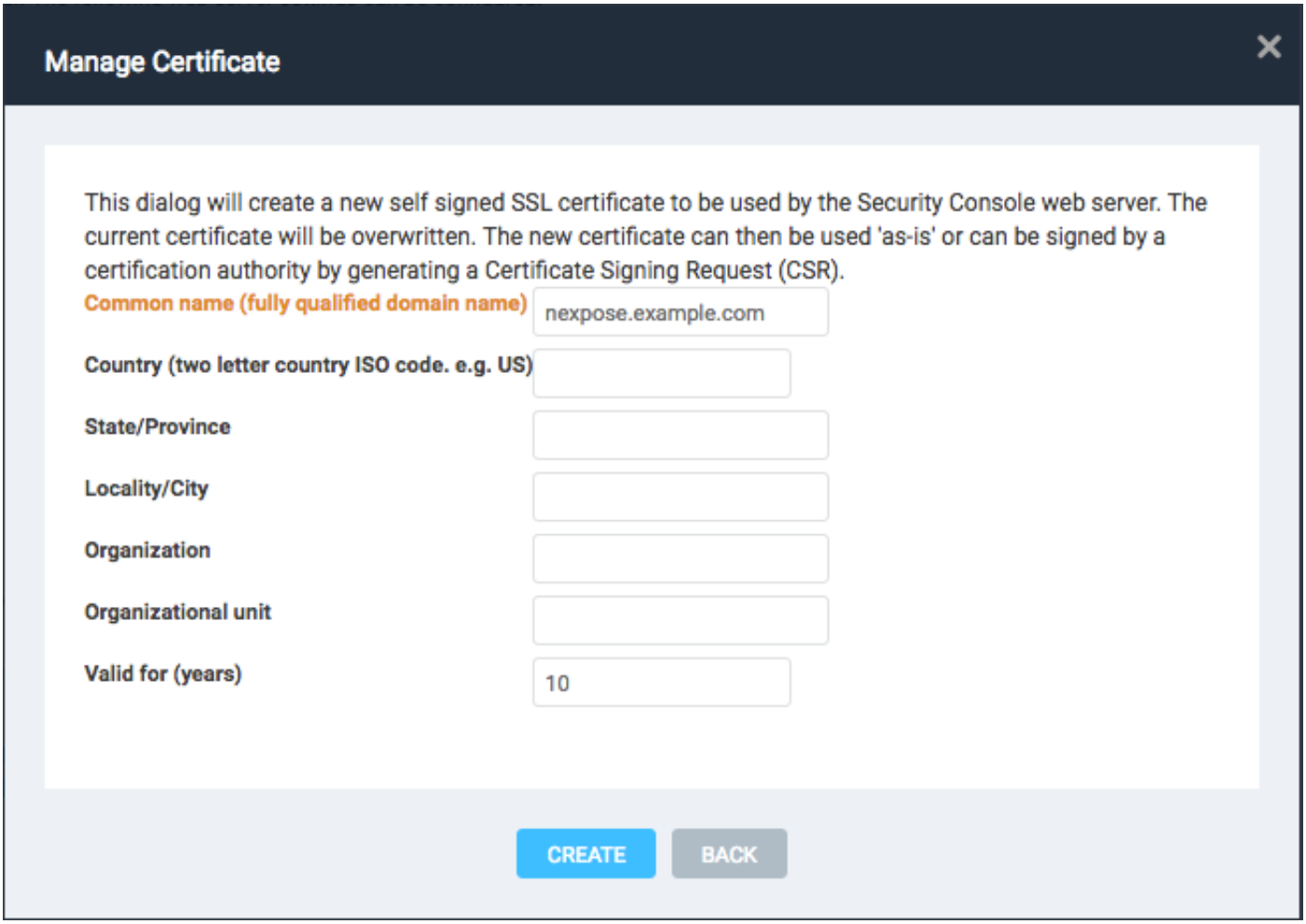
تتمثل الخطوة الأولى في شهادة التثبيت على الماسح الضوئي Nexpose. يتم إصدار الشهادة الموجودة في هذا المستند بواسطة نفس شهادة CA كشهادة مسؤول ل ISE (LAB CA). انتقل إلى **إدارة > إعدادات عامة وإعدادات وحدة التحكم**. حدد **إدارة** تحت **وحدة التحكم**، كما هو موضح في الصورة.



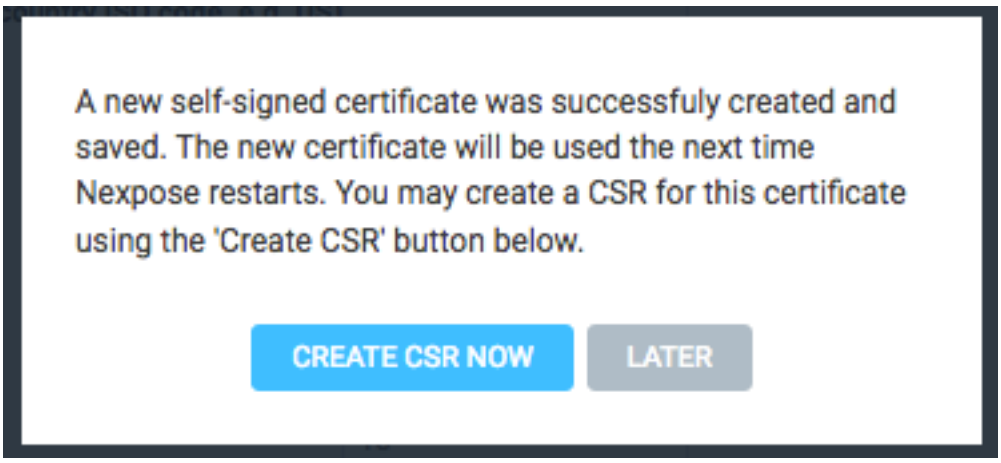
انقر على **إدارة الشهادة**، كما هو موضح في الصورة:



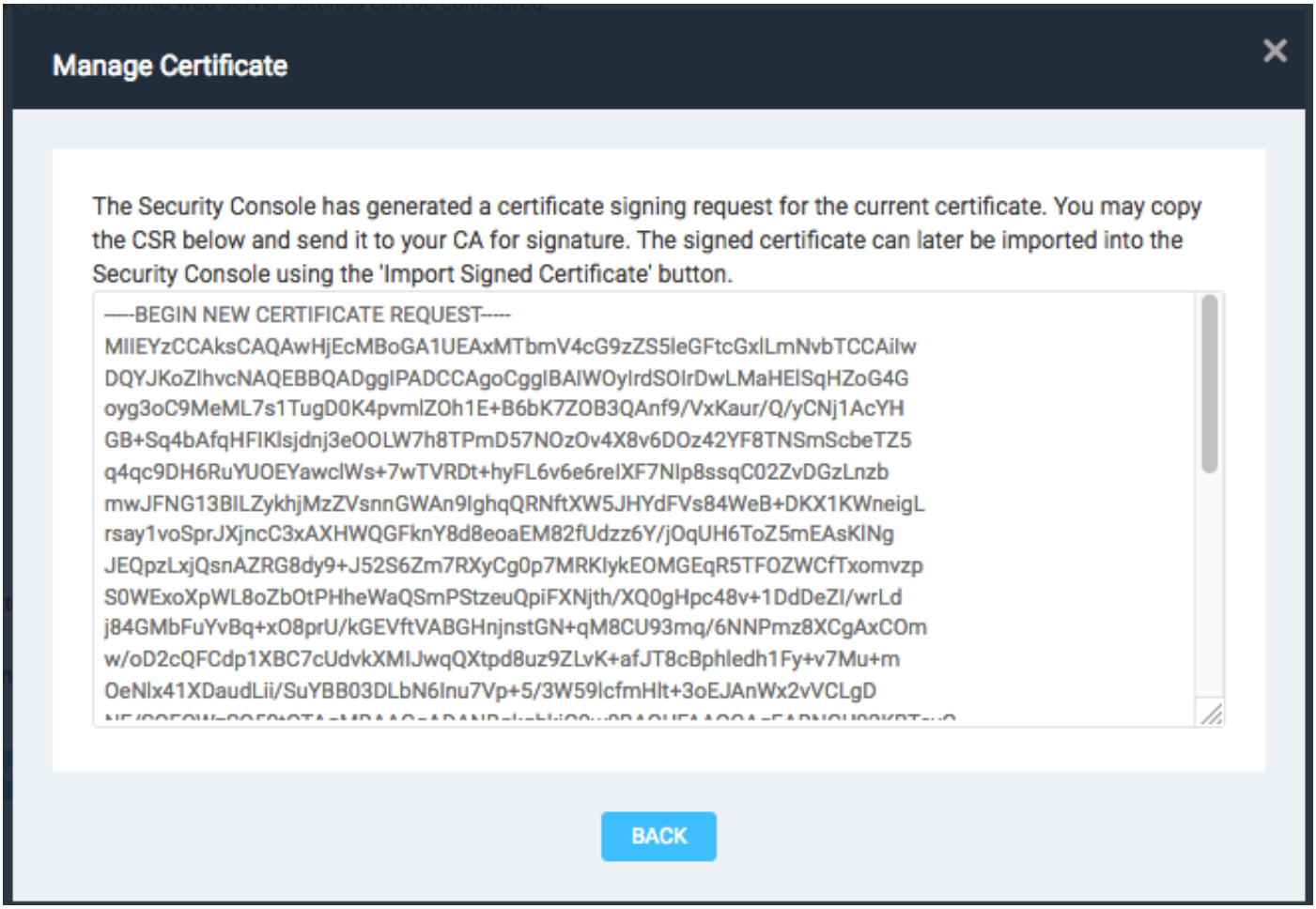
كما هو موضح في الصورة، انقر في **إنشاء شهادة جديدة**. أدخل **الاسم الشائع** وأي بيانات أخرى ترغب في الحصول عليها في شهادة تعريف الماسح الضوئي Nexpose. تأكد من قدرة ISE على حل FQDN الخاص بالماسح الضوئي ل Nexpose باستخدام DNS.



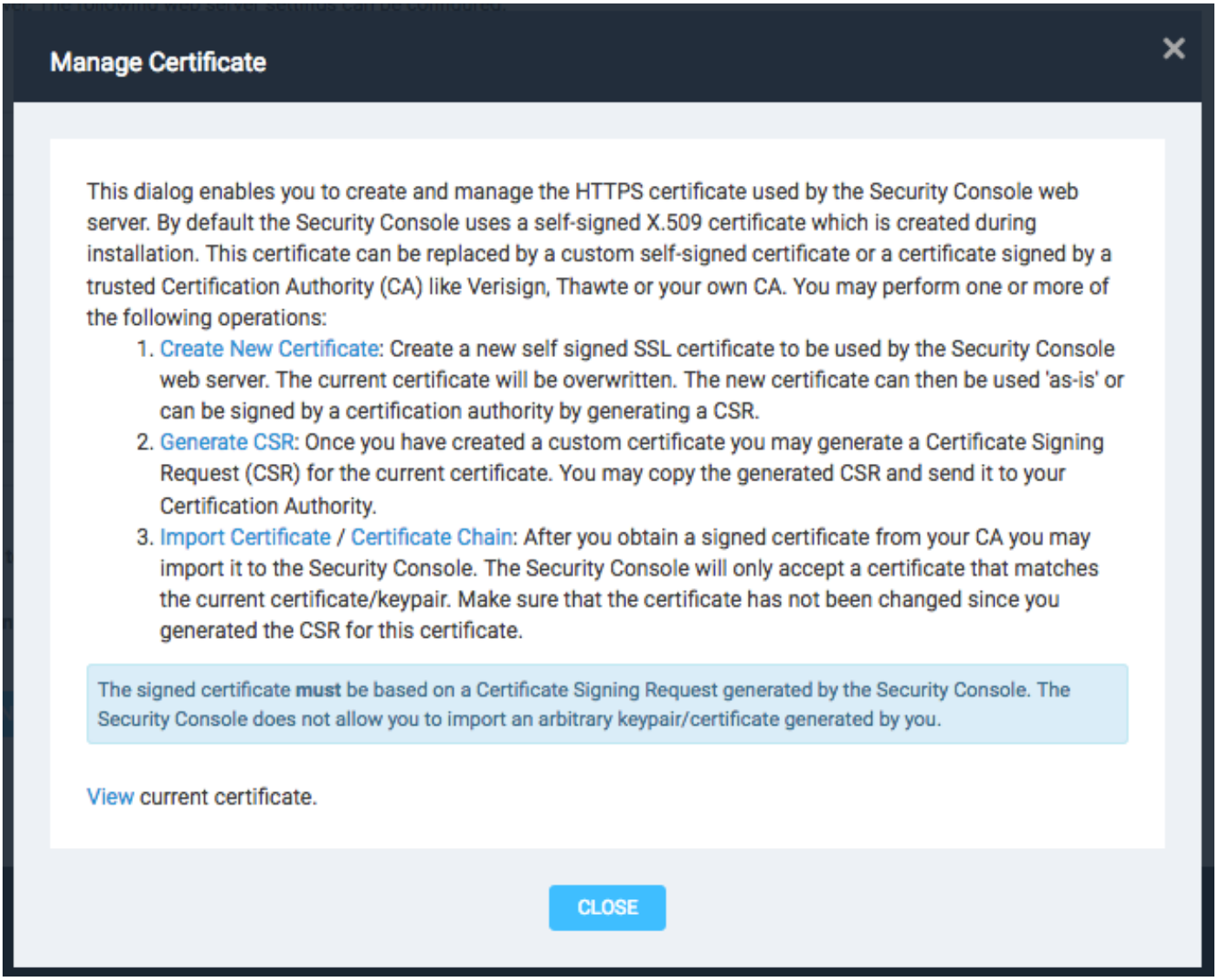
تصدير طلب توقيع الشهادة (CSR) إلى الوحدة الطرفية.



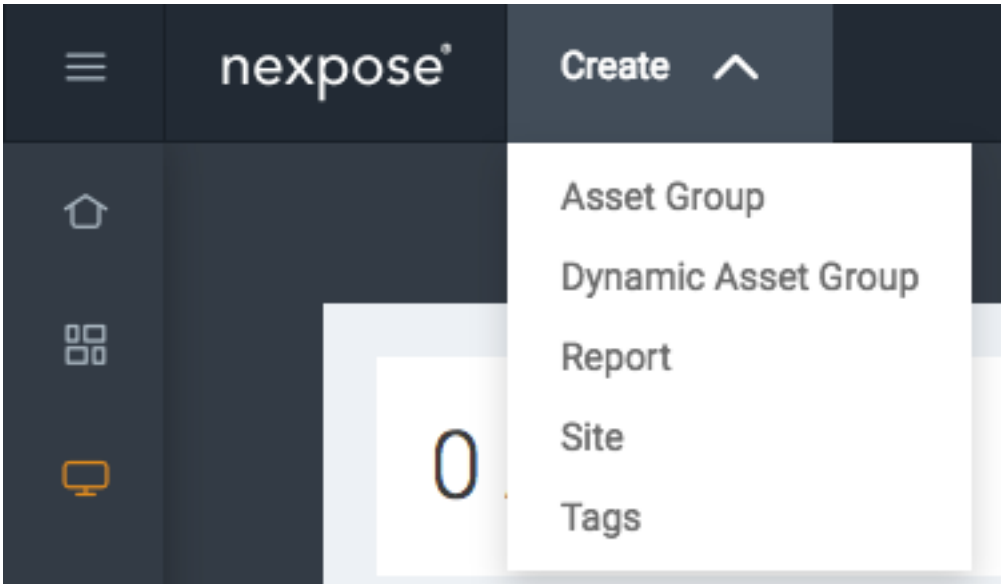
عند هذه النقطة، تحتاج إلى توقيع CSR باستخدام المرجع المصدق (CA).



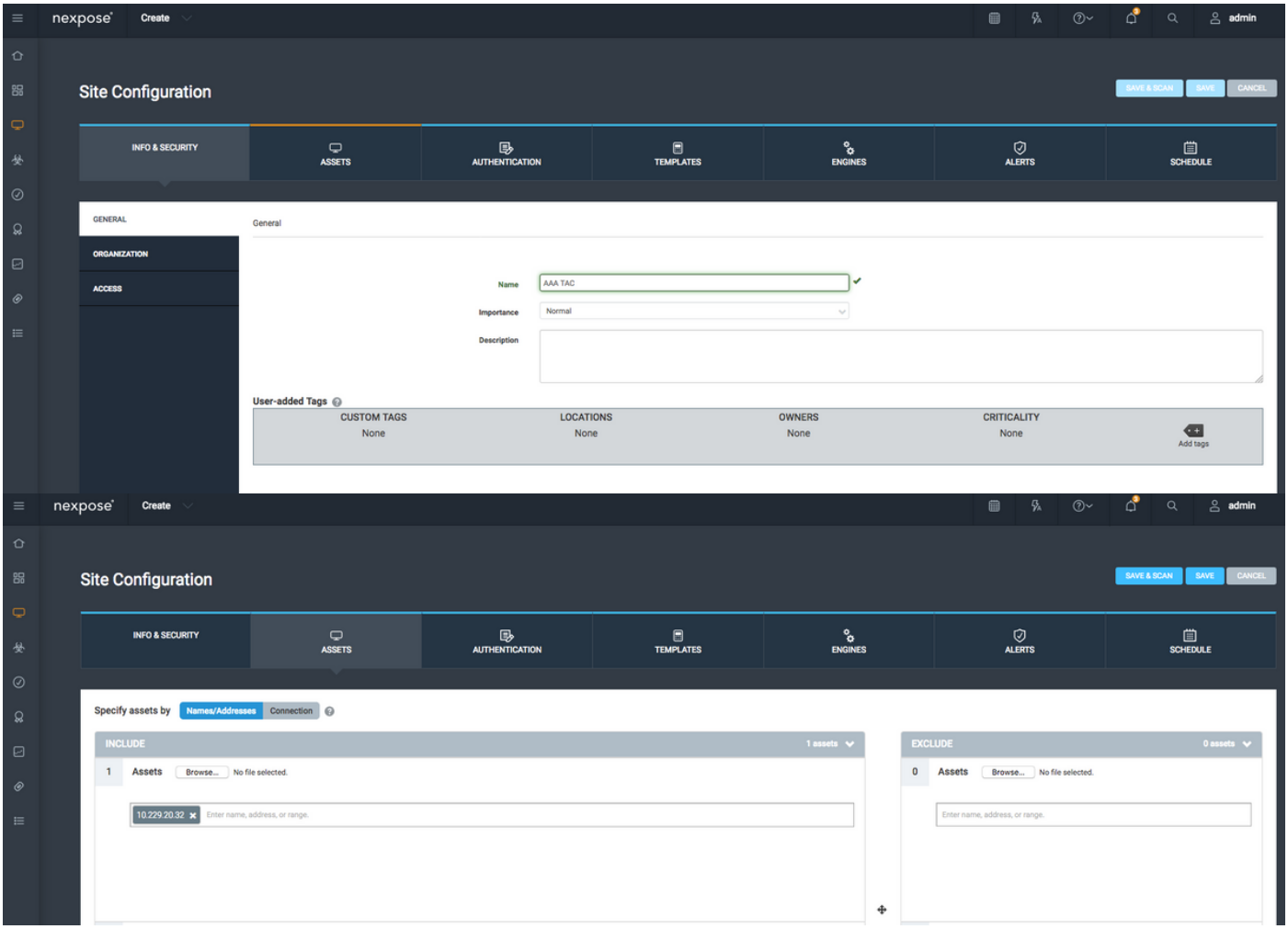
قم باستيراد الشهادة التي أصدرها المرجع المصدق بالنقر على **استيراد شهادة**.



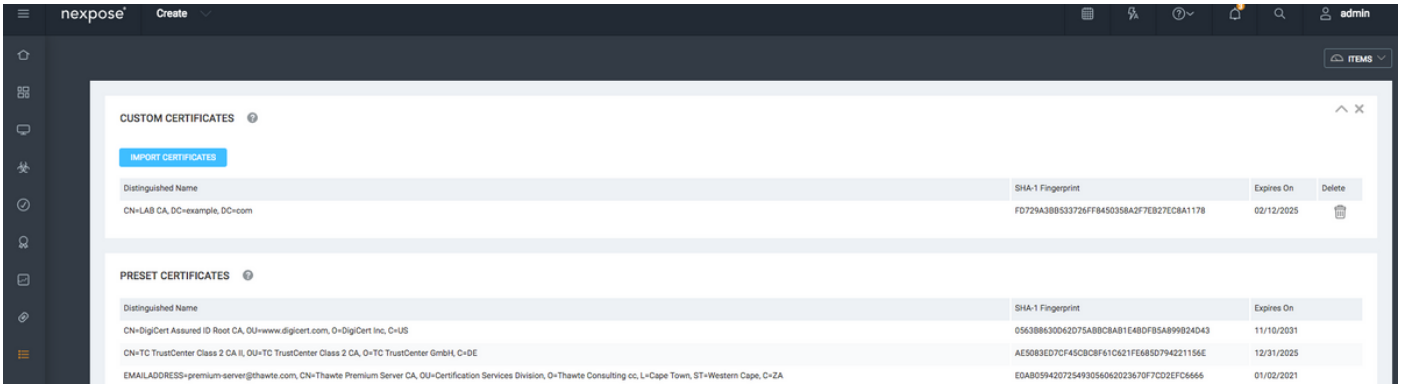
تكوين موقع. يحتوي الموقع على الأصول التي يجب أن تتمكن من مسحها، كما يجب أن يكون للحساب المستخدم في دمج ISE مع Nexpose Scanner امتيازات لإدارة المواقع وإنشاء التقارير. انتقل إلى **إنشاء > موقع**، كما هو موضح في الصورة.



كما هو موضح في الصورة، أدخل **اسم** الموقع في علامة التبويب **معلومات أو أمان**. يجب أن تحتوي علامة التبويب **الأصول** على عناوين IP للأصول الصالحة ونقاط النهاية المؤهلة للمسح الضوئي للقابلية للتأثر.



إستيراد شهادة المرجع المصدق التي وقعت على شهادة ISE في المخزن الموثوق به. انتقل إلى **إدارة > شهادات الجذر > إدارة > إستيراد الشهادات**.

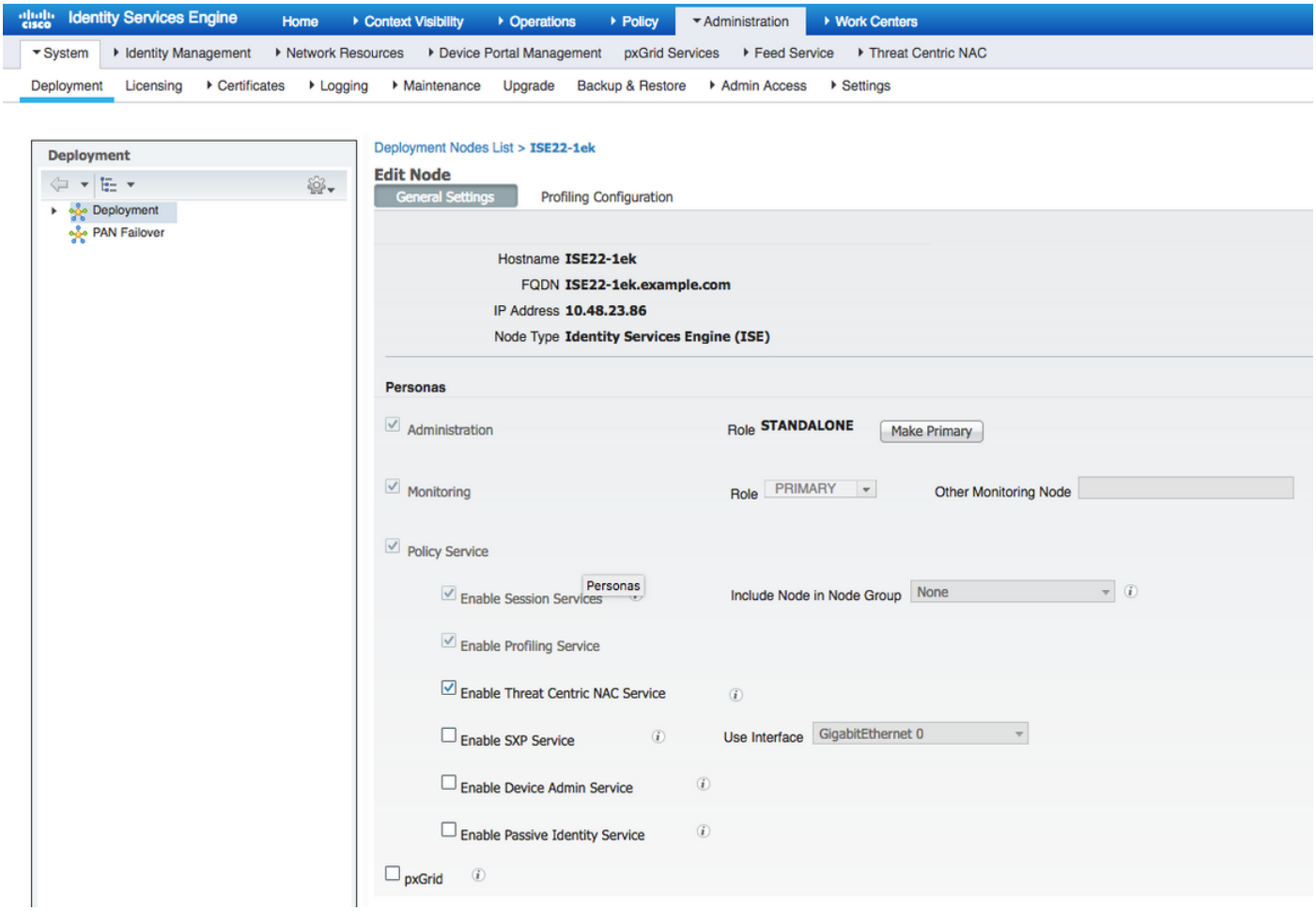


تكوين ISE

الخطوة 1. تمكين خدمات TC-NAC.

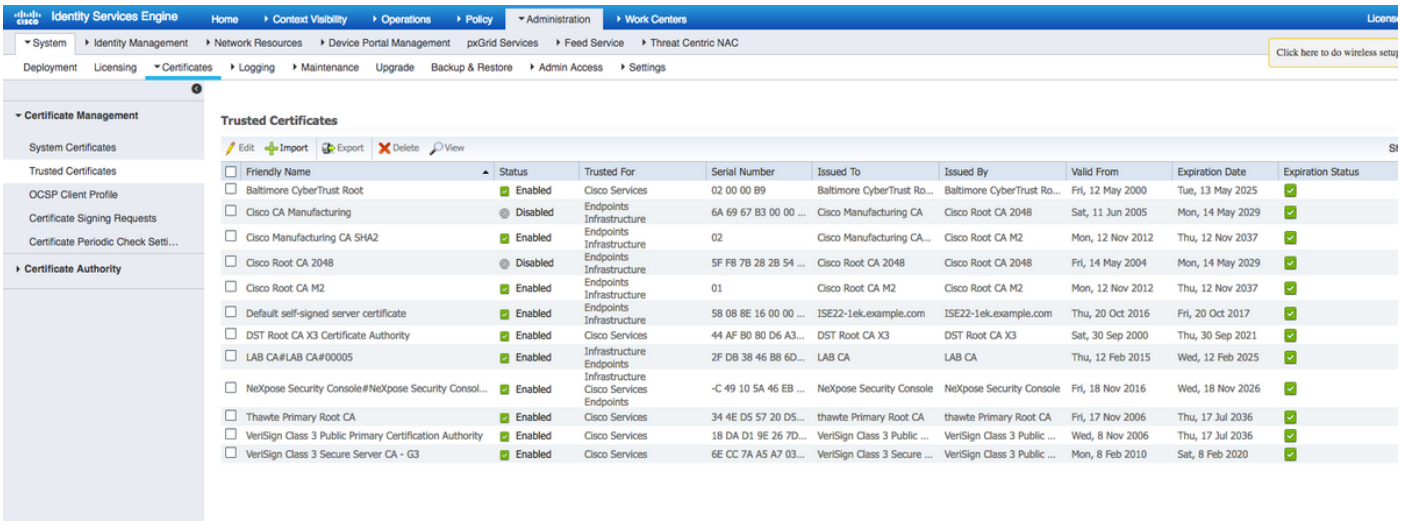
تمكين خدمات TC-NAC على عقدة ISE. لاحظ ما يلي:

- تتطلب خدمة NAC التي ترتكز على التهديد ترخيصا كبيرا.
- أنت بحاجة إلى عقدة خدمة سياسة (PSN) منفصلة لخدمة NAC التي ترتكز على التهديد.
- يمكن تمكين خدمة NAC التي ترتكز على التهديدات على عقدة واحدة فقط في النشر.
- يمكنك إضافة مثيل واحد فقط لمهايئ لكل مورد لخدمة تقييم الثغرات.



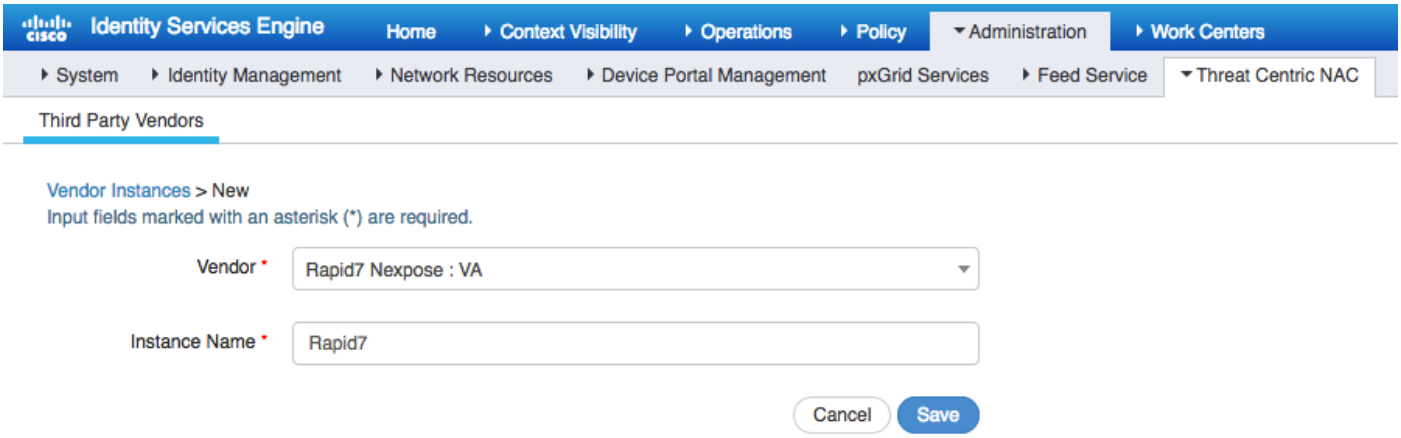
الخطوة 2. إستيراد شهادة الماسح الضوئي التالي.

قم باستيراد شهادة مرجع مصدق Nexpose Scan CA إلى مخزن الشهادات الموثوق بها في Cisco ISE (**إدارة > شهادات > إدارة شهادات > شهادات موثوق بها > إستيراد**). تأكد من إستيراد (أو وجود) الشهادات الوسيطة والجذرية المناسبة في مخزن Cisco ISE Trusted Certificates

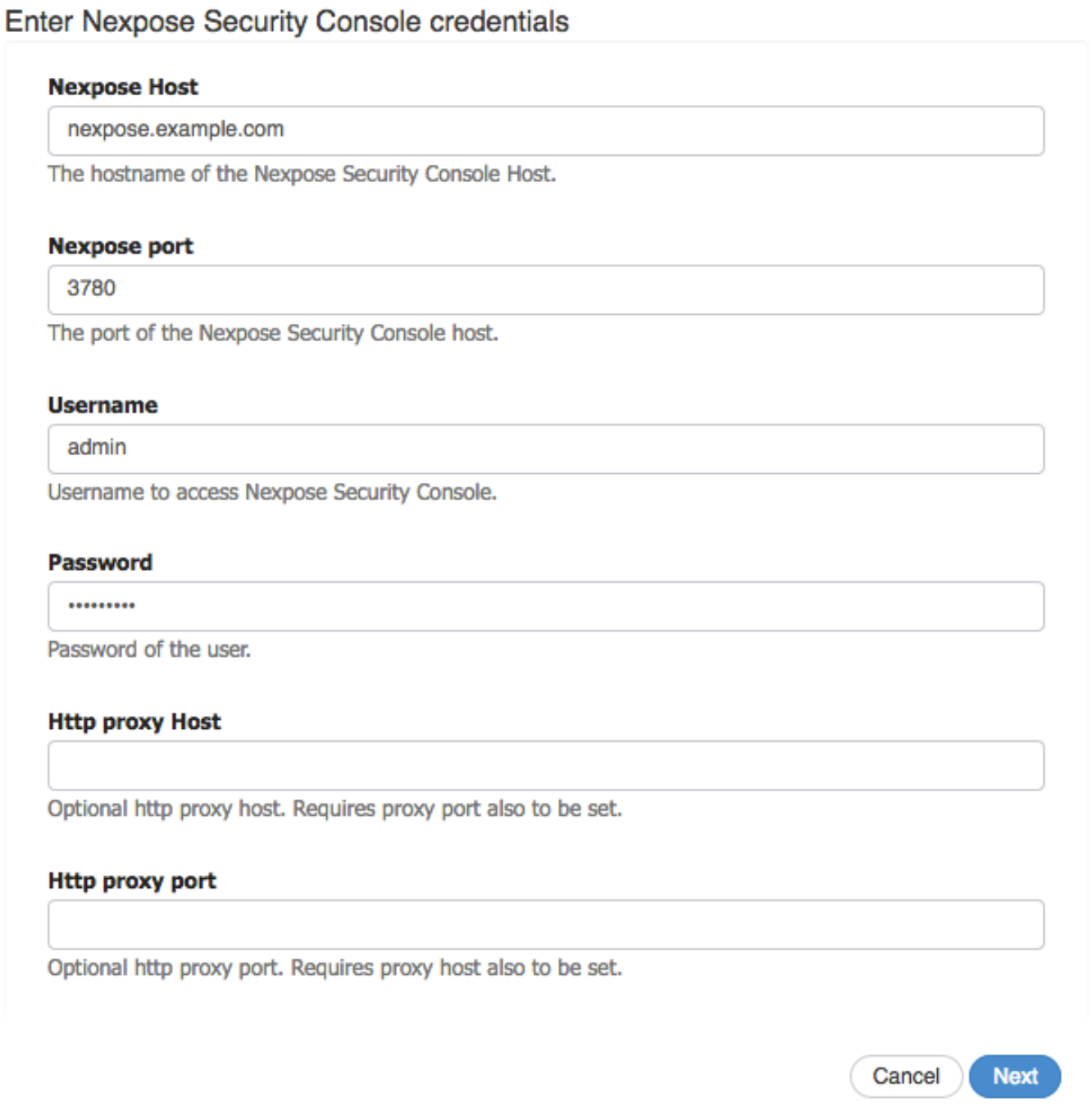


الخطوة 3. تكوين مثيل TC-NAC لماسح NEXPOSE الضوئي.

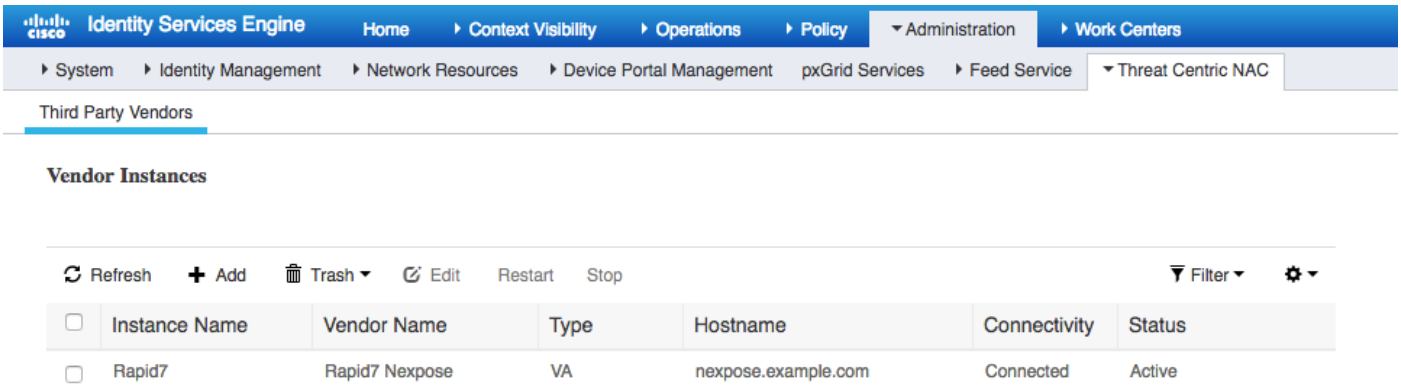
أضف نموذج Rapid7 في **الإدارة > NAC الذي يرتكز على التهديدات > موردي الجهات الخارجية**.



بمجرد إضافتها، يتم تحويل المثيل إلى **جاهزة لتكوين** الحالة. انقر فوق هذا الارتباط. قم بتكوين **المضيف** (الماسح الضوئي) و**المنفذ**، بشكل افتراضي هو 3780. حدد **اسم المستخدم** و**كلمة المرور** مع الوصول إلى الموقع الأيمن.



تم توثيق الإعدادات المتقدمة بشكل جيد في دليل مسؤول ISE 2.2، ويمكن العثور على الارتباط في قسم المراجع في هذا المستند. طقطقت في **بعد ذلك وإنجاز**. يبدأ تشغيل عمليات انتقال مثيل Nexpose إلى الحالة **النشطة** وتنزيل قاعدة المعارف.



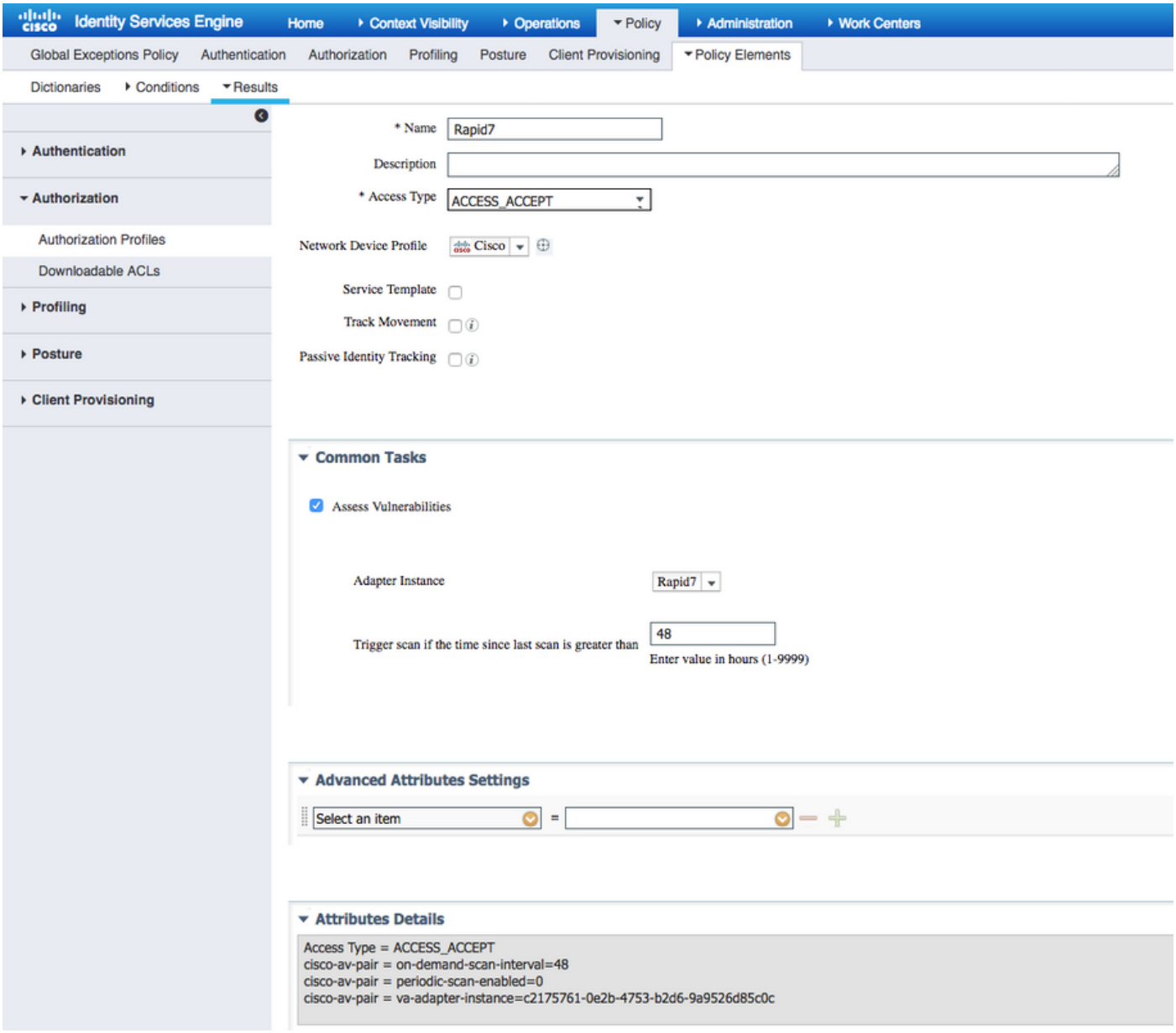
الخطوة 4. قم بتكوين ملف تعريف التخويل لتشغيل فحص VA.

انتقل إلى **السياسة > عناصر السياسة > النتائج > التخويل > ملفات تخصيص التخويل**. إضافة ملف تعريف جديد. تحت **المهام المشتركة** حدد **خانة الاختيار تقييم الثغرات.** يجب تحديد الفاصل الزمني للمسح حسب الطلب وفقا لتصميم الشبكة.

يحتوي ملف تعريف التخويل على أزواج AV هذه:

```
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
```

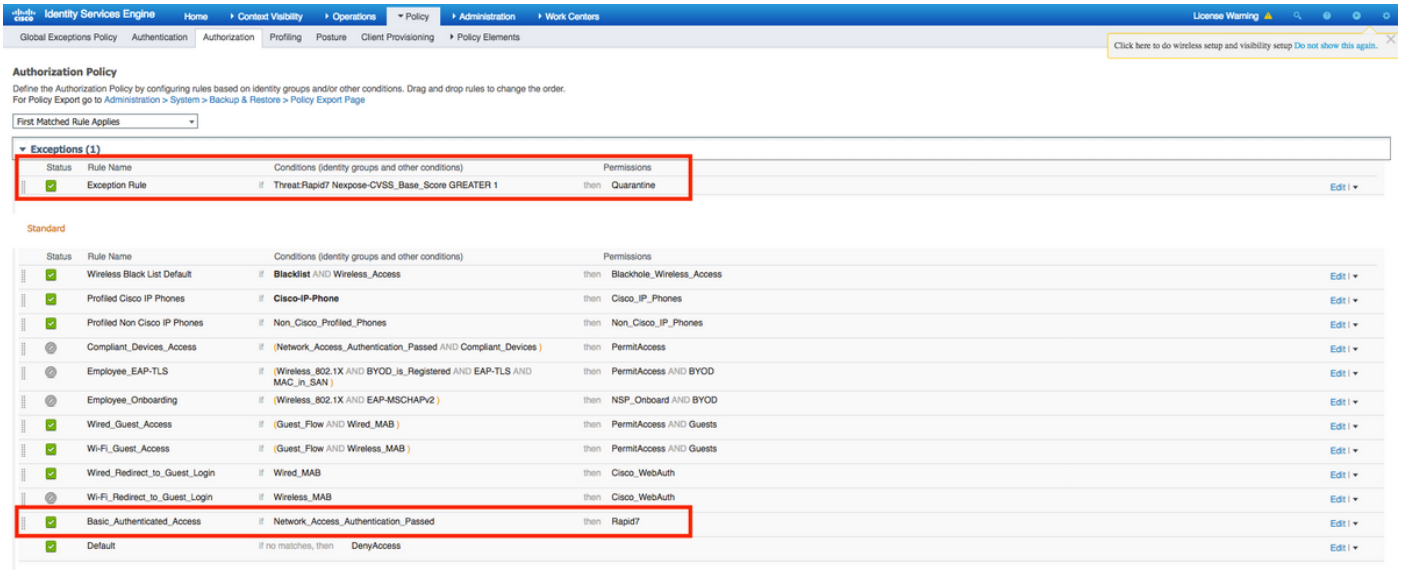
ويتم إرسالها إلى أجهزة الشبكة داخل حزمة قبول الوصول، على الرغم من أن الغرض الحقيقي منها هو إعلام عقدة المراقبة (MNT) بضرورة تشغيل الفحص. يرشد MNT عقدة TC-NAC للاتصال بالماسح الضوئي Nexpose.



الخطوة 5. تكوين نهج التخويل.

- قم بتكوين نهج التخويل لاستخدام ملف تعريف التخويل الجديد الذي تم تكوينه في الخطوة 4. انتقل إلى **سياسة > تفويض > سياسة التفويض**، وحدد قاعدة **basic_authenticated_access**، ثم انقر فوق **Edit (تحرير)**. قم بتغيير الأذونات من **PermitAccess** إلى **Standard Rapid7** الذي تم إنشاؤه حديثا. يؤدي ذلك إلى إجراء فحص الثغرات لكافة المستخدمين. انقر في **حفظ**.

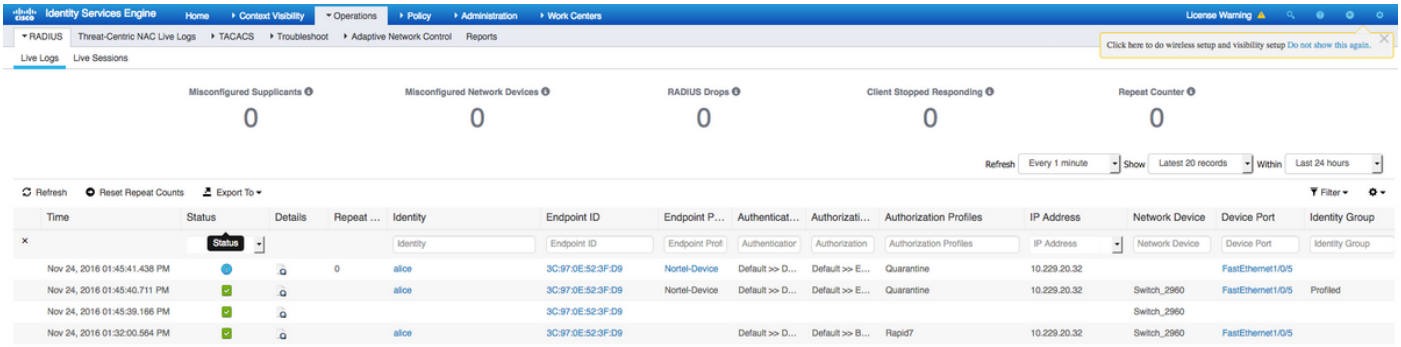
- إنشاء نهج اعتماد للأجهزة التي تم فرض حجر صحي عليها. انتقل إلى **نهج > تفويض > نهج التخويل > إستثناءات** وإنشاء **قاعدة إستثناء**. انتقل الآن إلى **الشروط > إنشاء شرط جديد (خيار متقدم) > تحديد سمة**، قم بالتمرير لأسفل وحدد **التهديد**. قم بتوسيع سمة **التهديد** وحدد **Nexpose-CVSS_BASE_SCORE**. قم بتغيير عامل التشغيل إلى **أكبر من** وقم بإدخال قيمة وقف النهج الأمان الخاص بك. يجب أن يعطي ملف تعريف تفويض **الحجر الصحي** وصولا محدودا للجهاز غير المحمي.



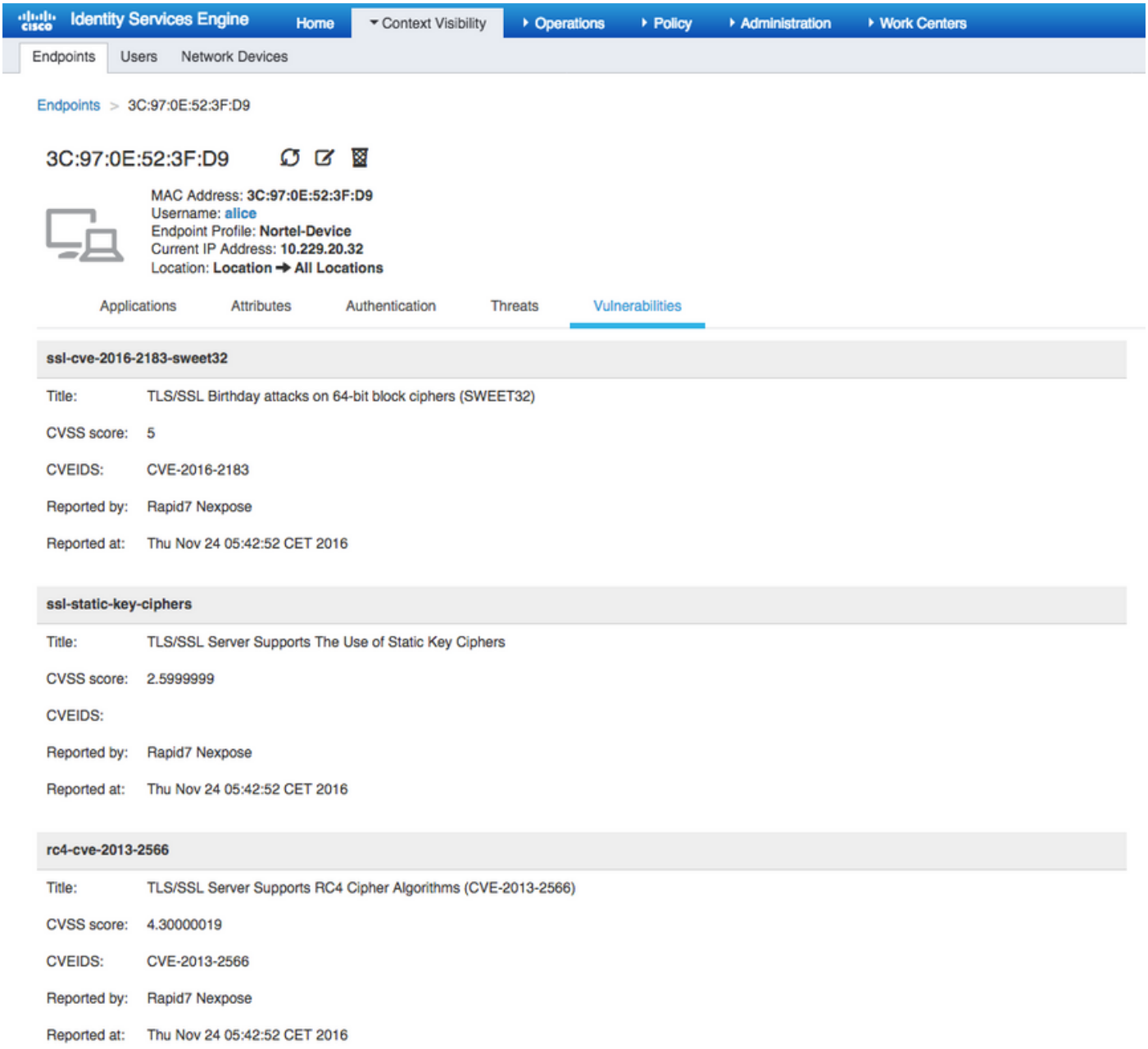
التحقق من الصحة

محرك خدمات الهوية

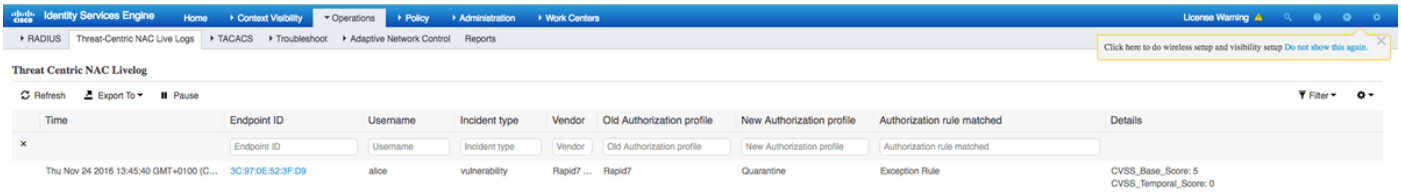
يقوم الاتصال الأول بتشغيل المسح الضوئي لـ VA. عند انتهاء الفحص، يتم تشغيل إعادة مصادقة CoA لتطبيق نهج جديد في حالة مطابقته.



للتحقق من مكامن الضعف التي تم اكتشافها، انتقل إلى **رؤية السياق > نقاط النهاية**. تحقق من نقاط الضعف لكل نقطة نهاية باستخدام العلامات المعطاة له من خلال ماسح Nexpose الضوئي.

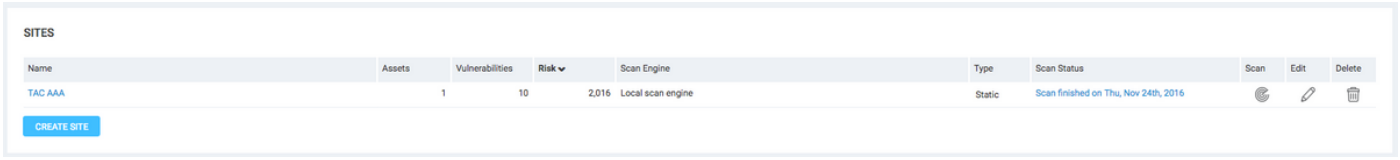


في العمليات > سجلات TC-NAC المباشرة، يمكنك رؤية سياسات التفويض المطبقة والتفاصيل على CVSS_BASE_SCORE.

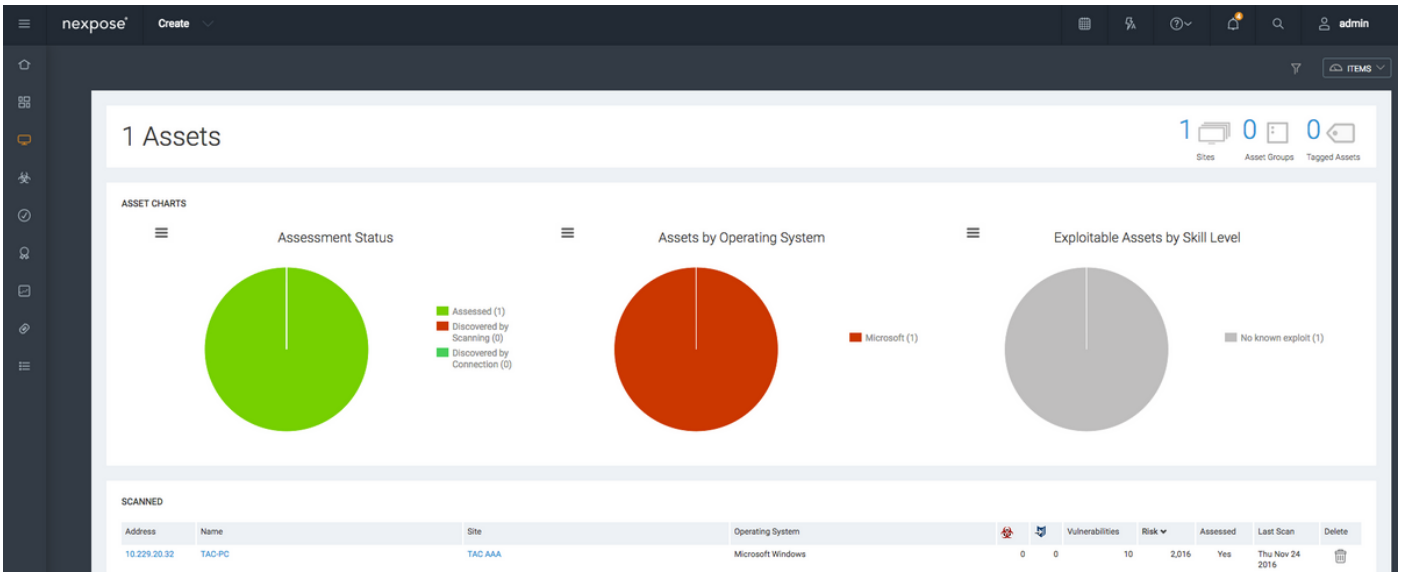


ماسح Nexpose الضوئي

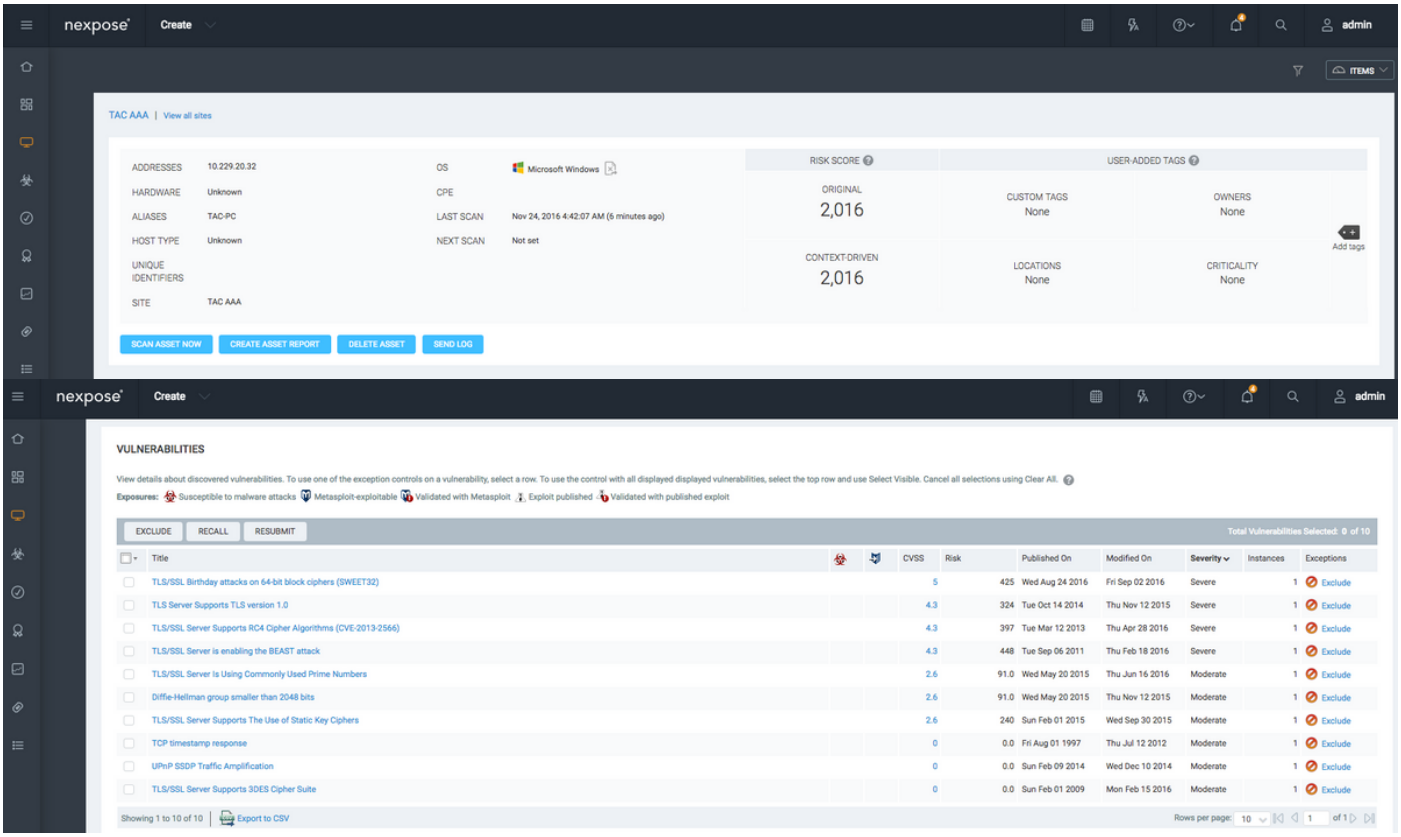
عندما يتم تشغيل مسح VA بواسطة انتقالات TC-NAC Nexpose Scan إلى حالة **قيد التقدم**، ويبدأ الماسح الضوئي في التحقق من نقطة النهاية، إذا قمت بتشغيل التقاط Wireshark على نقطة النهاية، سترى تبادل الحزم بين محطة النهاية والماسح الضوئي عند هذه النقطة. بمجرد انتهاء الماسح الضوئي، تتوفر النتائج ضمن **الصفحة الرئيسية**.



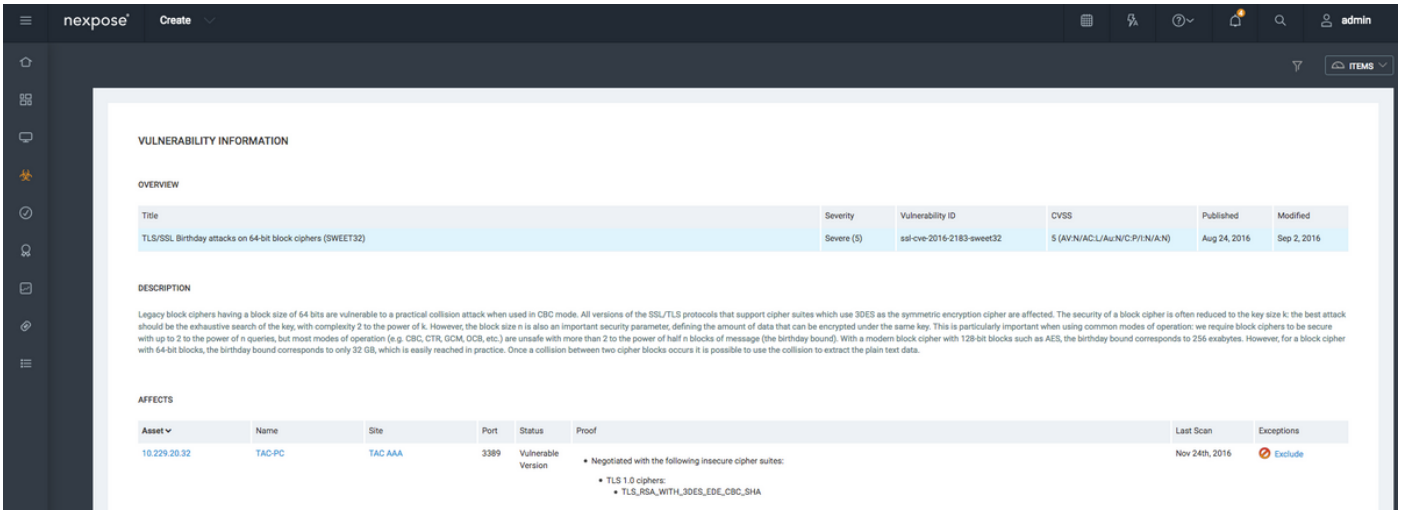
تحت **صفحة الأصول**، يمكنك أن ترى أن هناك نقطة نهاية جديدة متوفرة مع نتائج المسح الضوئي، وتم تحديد نظام التشغيل وتم اكتشاف 10 نقاط ضعف.



عندما تنقر في **عنوان IP لنقطة النهاية** ينقلك الماسح الضوئي Nexpose إلى القائمة الجديدة، حيث يمكنك رؤية المزيد من المعلومات بما في ذلك اسم المضيف وعلامة RISC وقائمة مفصلة من نقاط الضعف



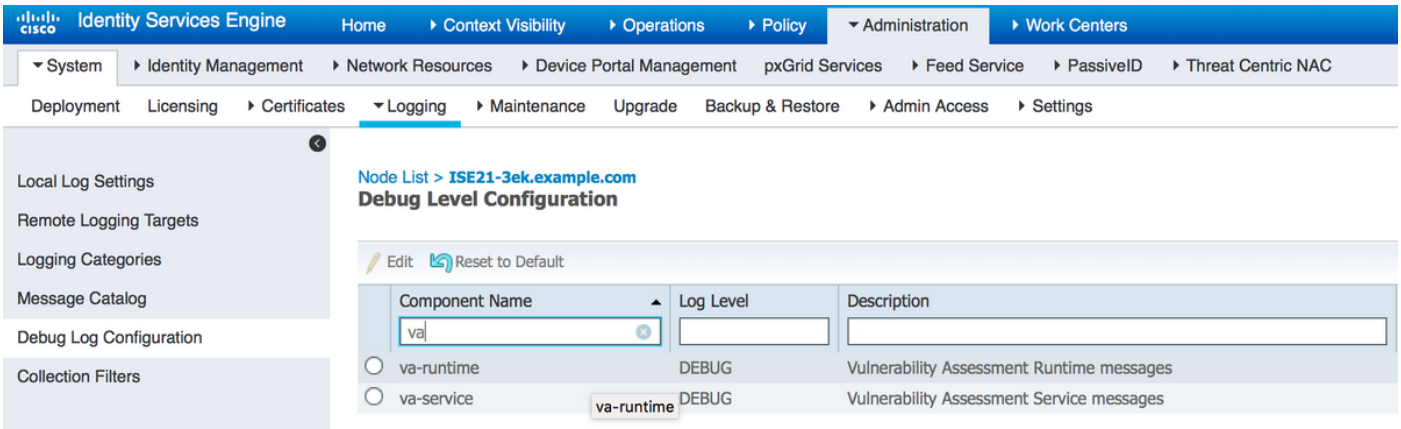
عندما تنقر في **حالة الضعف** نفسها، يتم عرض الوصف الكامل في الصورة.



استكشاف الأخطاء وإصلاحها

تصحيح الأخطاء على ISE

لتمكين تصحيح الأخطاء على ISE، انتقل إلى **الإدارة > النظام > تسجيل > تكوين سجل تصحيح الأخطاء**، وحدد عقدة TC-NAC، وقم بتغيير **مكون مستوى السجل va-runtime** و**va-service** إلى **تصحيح الأخطاء**.



السجلات المطلوب فحصها - varuntime.log. يمكنك الحصول عليها مباشرة من واجهة سطر أوامر ISE:

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

تلقى TC-NAC Docker إرشادات لإجراء الفحص لنقطة نهاية معينة.

```
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}

وبمجرد إستلام النتيجة، يتم تخزين جميع بيانات الثغرات الأمنية في دليل السياق.

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"}]}

السجلات التي سيتم فحصها - Catalyervice.log. يمكنك الحصول عليها مباشرة من واجهة رماوأ رطس ISE:

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

تم إرسال طلب تقييم الضعف إلى المحول.

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

يتحقق AdapterMessageListener كل 5 دقائق من حالة الفحص حتى ينتهي.

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

يحصل المحول على CVE مع نتائج 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":"2.5999999","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"]}

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- ISE 2.2 ملاحظات الإصدار
- دليل تثبيت الأجهزة ISE 2.2
- دليل ترقية ISE 2.2
- دليل مسؤول محرك ISE 2.2

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).