تكوين ISE 2.1 NAC الذي يركز على التهديد (TC-NAC) مع Qualys

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين NAC الذي يركز على التهديد باستخدام Qualys on Identity Services Engine (ISE) 2.1. تتيح لك ميزة التحكم في الوصول إلى الشبكة التي ترتكز على التهديد (TC-NAC) إمكانية إنشاء سياسات تفويض استنادا إلى سمات التهديد والضعف التي يتم استقبالها من موائيات التهديد ومكامن الضعف.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمة الهوية من Cisco
- Qualys ScanGuard

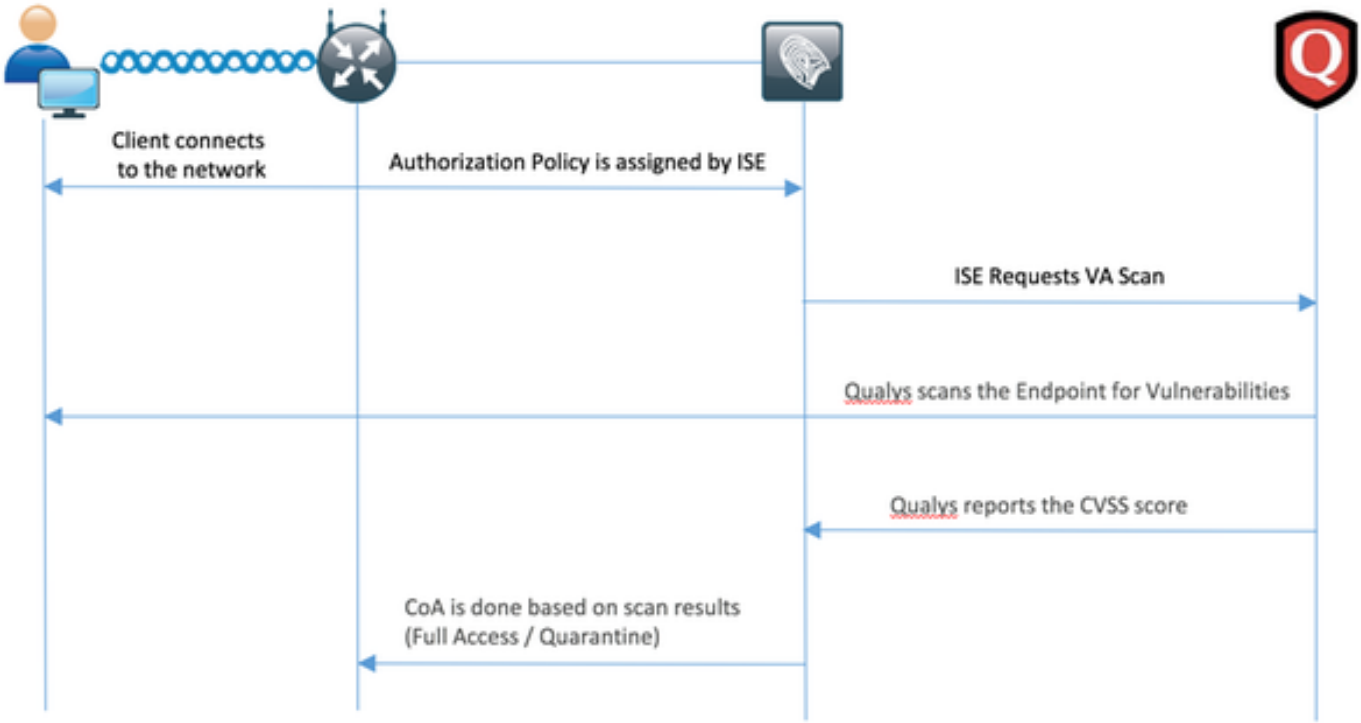
المكونات المستخدمة

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

- Cisco Identity Service Engine، الإصدار 2.1
- وحدة التحكم في شبكة LAN اللاسلكية (WLC) 8.0.121.0
- Qualys Guard Scan 8.3.36-1، Signatures 2.3.364-2
- حزمة الخدمة 1 لنظام التشغيل Windows 7

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. Qualys TC-NAC (مضمن في حاوية Docker) يتصل بسحابة Qualys (عبر REST API) لتشغيل المسح عند الحاجة

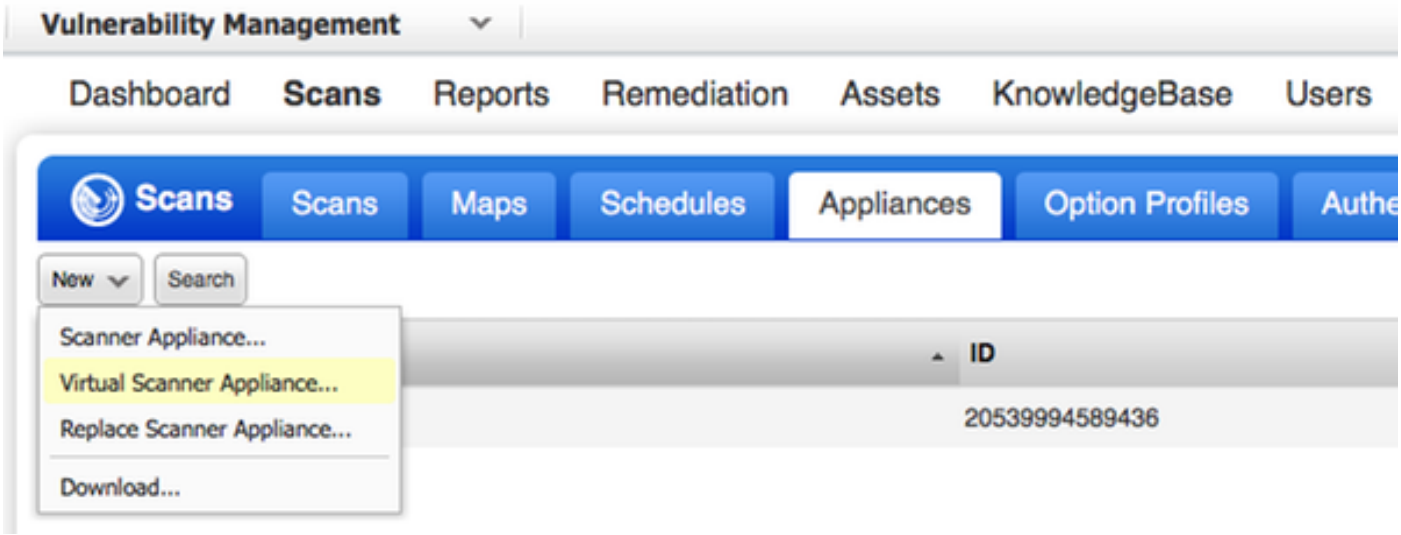
5. Qualys Cloud يرشد Qualys Scan لمسح نقطة النهاية
6. يرسل ماسح Qualys الضوئي نتائج المسح الضوئي إلى سحابة Qualys
7. يتم إرسال نتائج الفحص مرة أخرى إلى TC-NAC:
   - عنوان MAC
   - كافة نتائج CVSS
   - كافة نقاط الضعف (QID، العنوان، CVEIDs)
8. يقوم TC-NAC بتحديث PAN مع جميع البيانات من الخطوة 7.
9. يتم تشغيل CoA عند الحاجة وفقا لنهج التخويل الذي تم تكوينه.

تكوين سحابة Qualys والماسح الضوئي

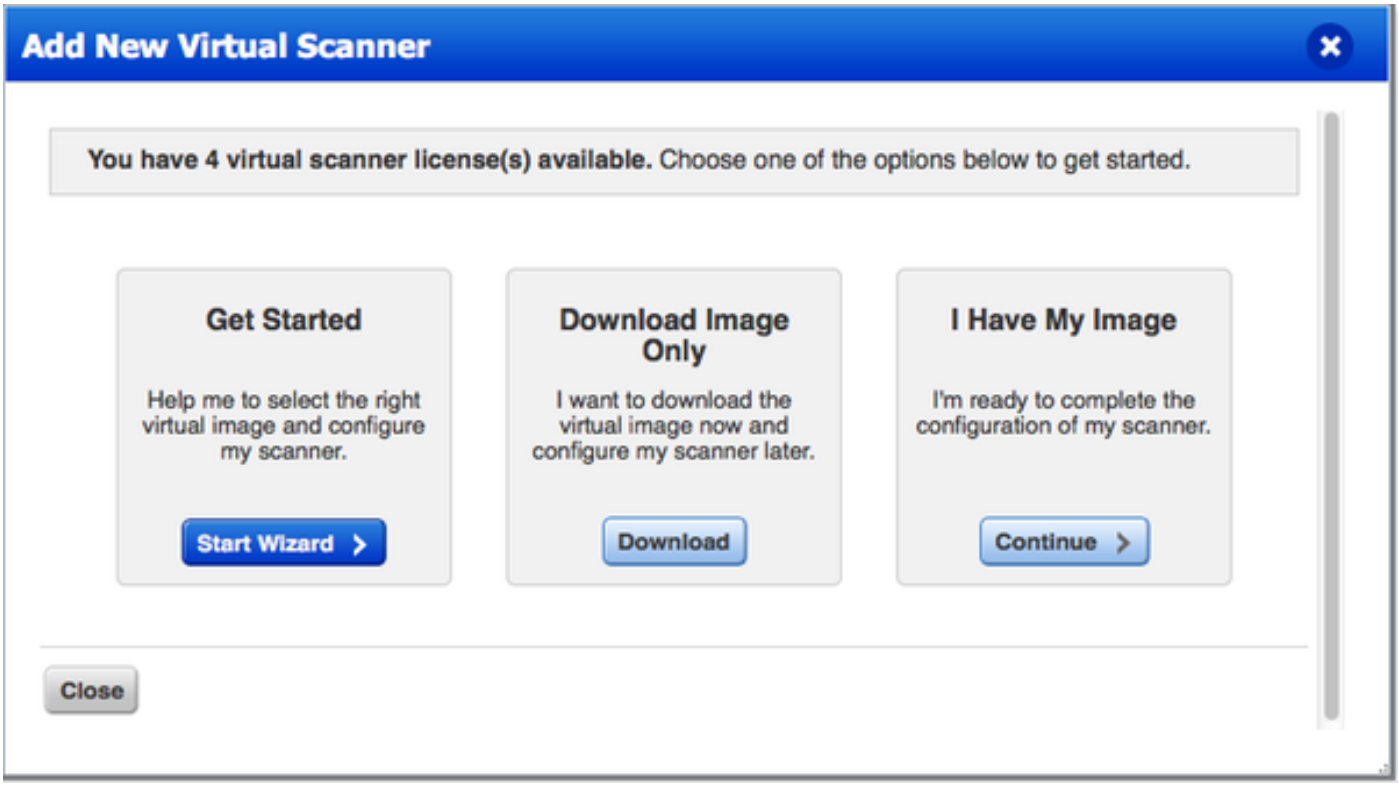
> **تحذير**: يتم إجراء التكوين المتنوع في هذا المستند لأغراض معملية، يرجى التشاور مع مهندسي Qualys لاعتبارات التصميم

الخطوة 1. نشر ماسح Qualys الضوئي

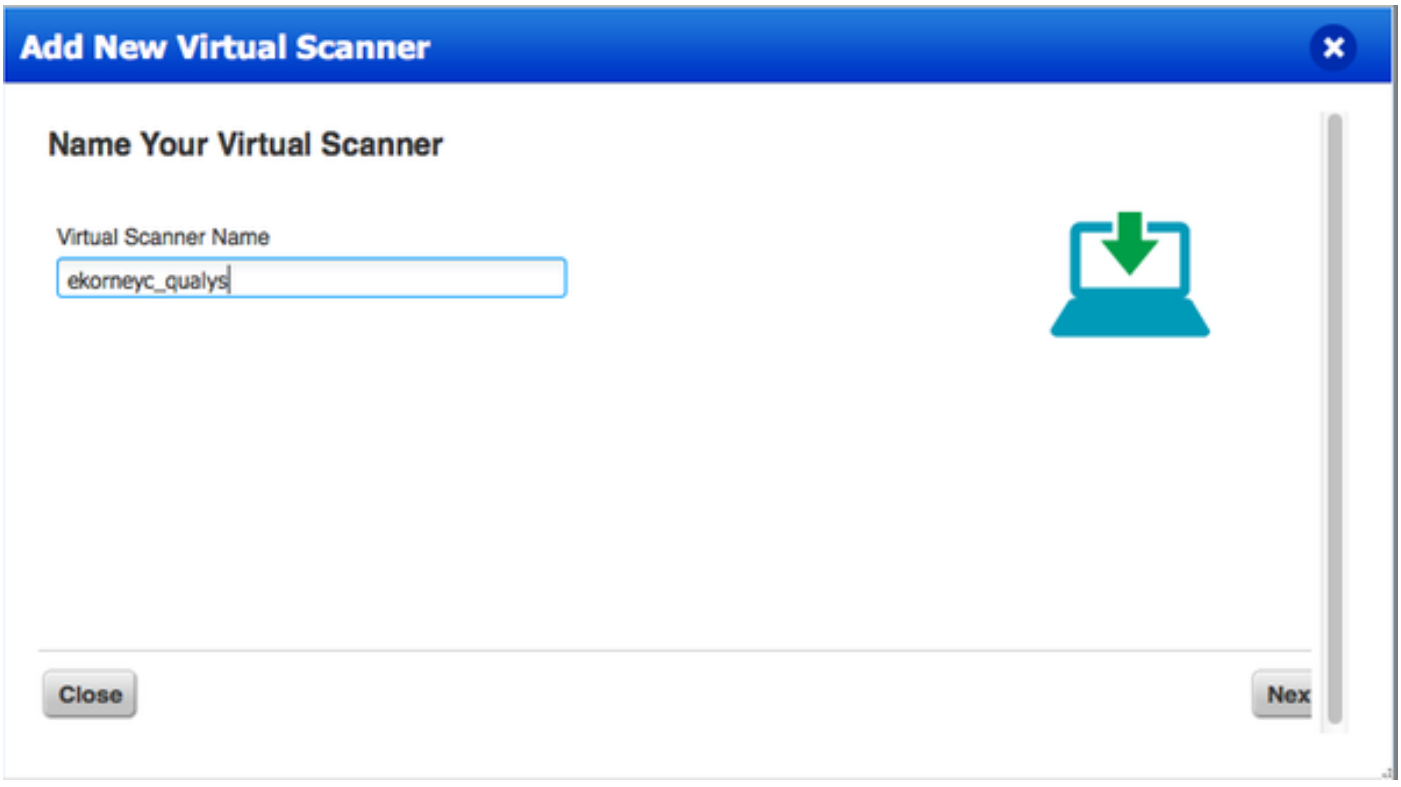
يمكن نشر الماسح الضوئي Qualys من ملف OVA. قم بتسجيل الدخول إلى Qualys cloud وانتقل إلى عمليات المسح > الأجهزة وحدد جديد > جهاز الماسح الضوئي الظاهري



حدد **تنزيل الصورة فقط** واختر التوزيع المناسب



للحصول على رمز التنشيط، يمكنك الانتقال إلى أجهزة الفحص > الأجهزة وتحديد جديد > جهاز الماسح الضوئي الظاهري وتحديد **صوري**



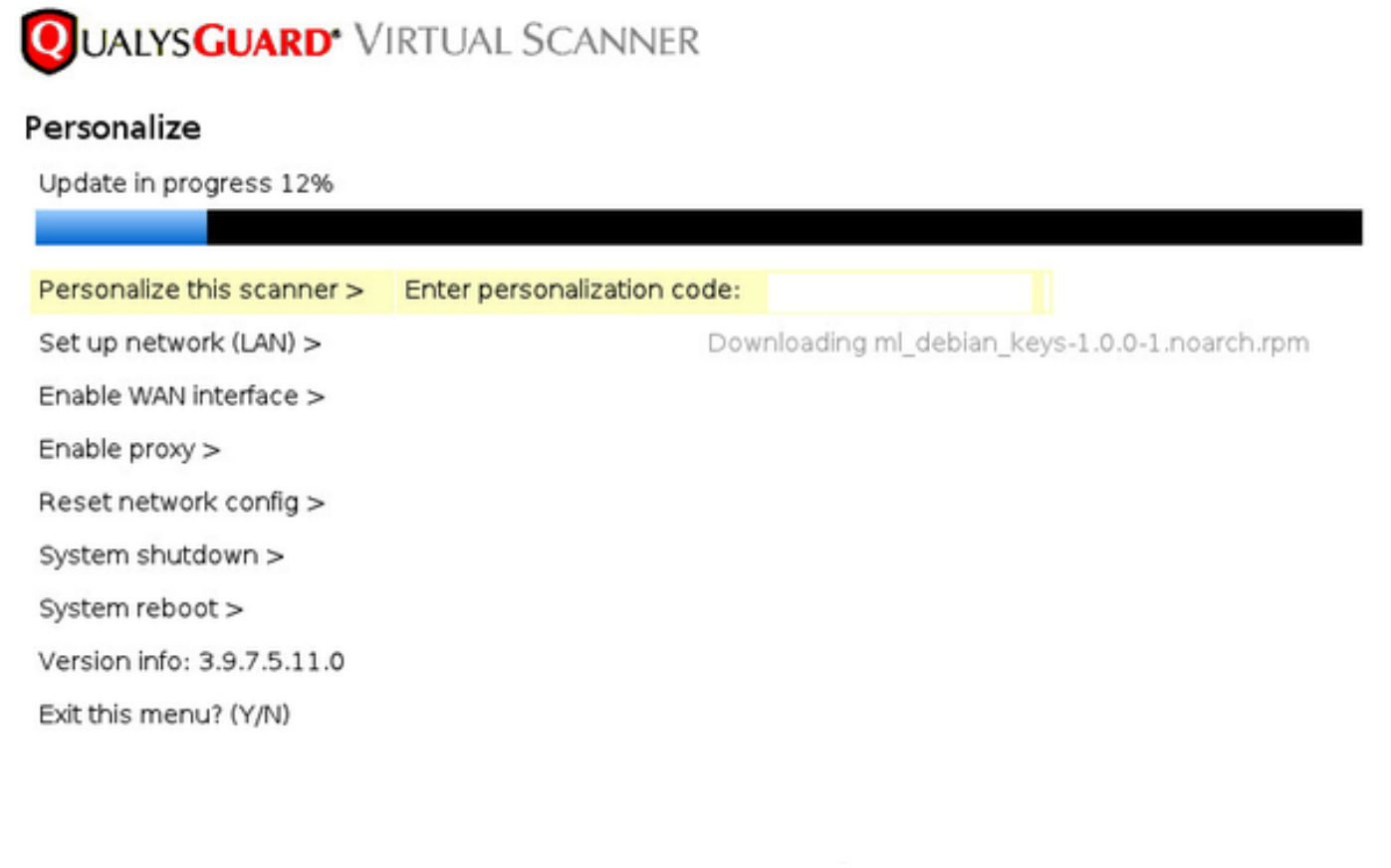
بعد إدخال اسم الماسح الضوئي، يتم منحك رمز التخويل الذي ستستخدمه لاحقا.

الخطوة 2. تكوين ماسح Qualys الضوئي

نشر OVA على النظام الأساسي للمحاكاة الافتراضية الذي تختاره. ما إن يتم، شكلت هذه عملية إعداد:

- إعداد الشبكة (LAN)
- إعدادات واجهة WAN (إذا كنت تستخدم واجهتين)
- إعدادات الوكيل (إذا كنت تستخدم الوكيل)
- تخصيص هذا الماسح الضوئي

بعد ذلك يتم توصيل الماسح الضوئي بوجود أحدث البرامج والتواقيع وتنزيلها.



للتحقق من اتصال الماسح الضوئي، يمكنك الانتقال إلى عمليات المسح الضوئي > الأجهزة.

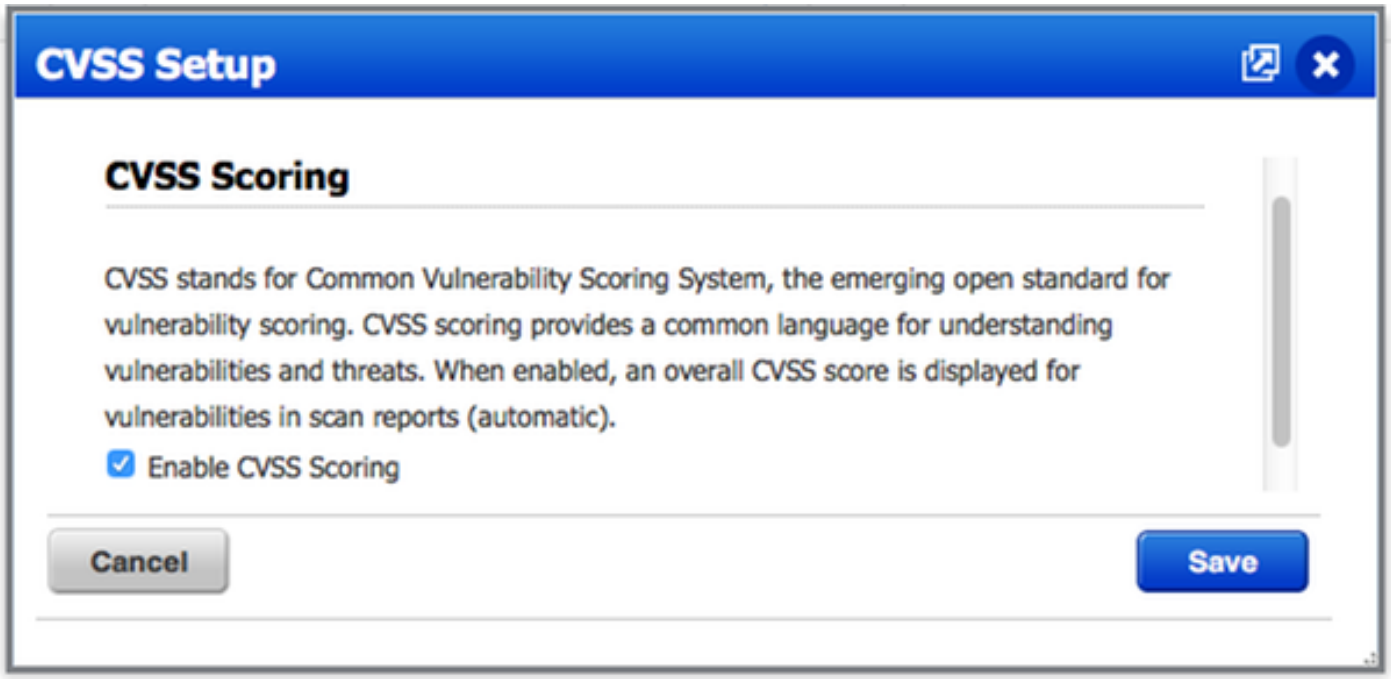
تشير علامة الربط الأخضر على اليسار إلى أن الماسح الضوئي جاهز، يمكنك أيضا رؤية LAN IP، WAN IP، إصدار الماسح الضوئي والتواقيع.

تكوين ISE

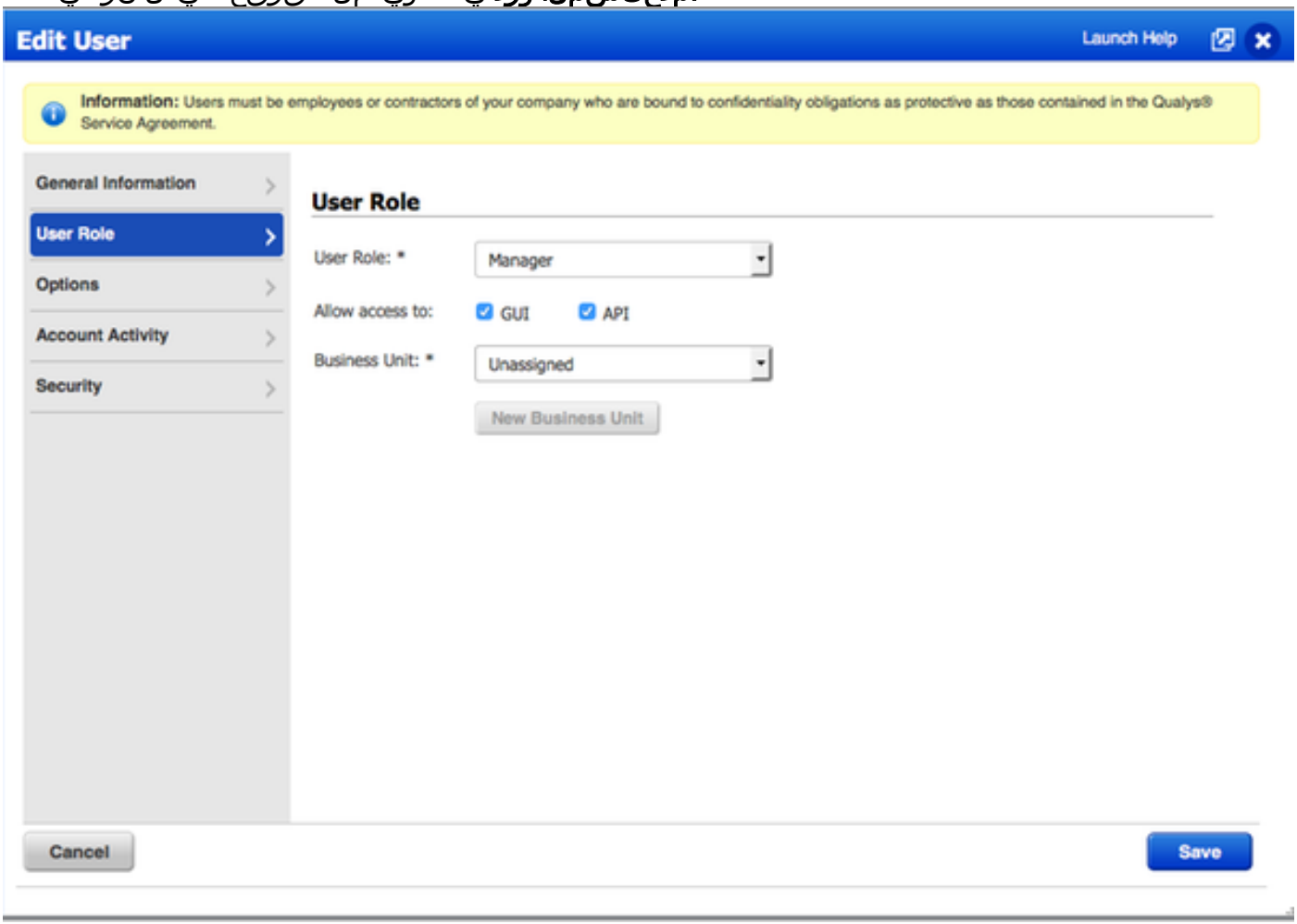
على الرغم من أنك قمت بتكوين Qualys Scan و Cloud، ال يزال يتعين عليك ضبط إعدادات السحابة للتأكد من أن التكامل مع ISE يعمل بشكل جيد. الحظ أنه يجب القيام بذلك قبل تكوين المحول من خالل واجهة المستخدم الرسومية (GUI)، حيث إن قاعدة المعارف التي تحتوي على نقاط CVSS يتم تنزيلها بعد تكوين المحول ألول مرة.

الخطوة 1. إعدادات Tune Qualys Cloud للتكامل مع ISE

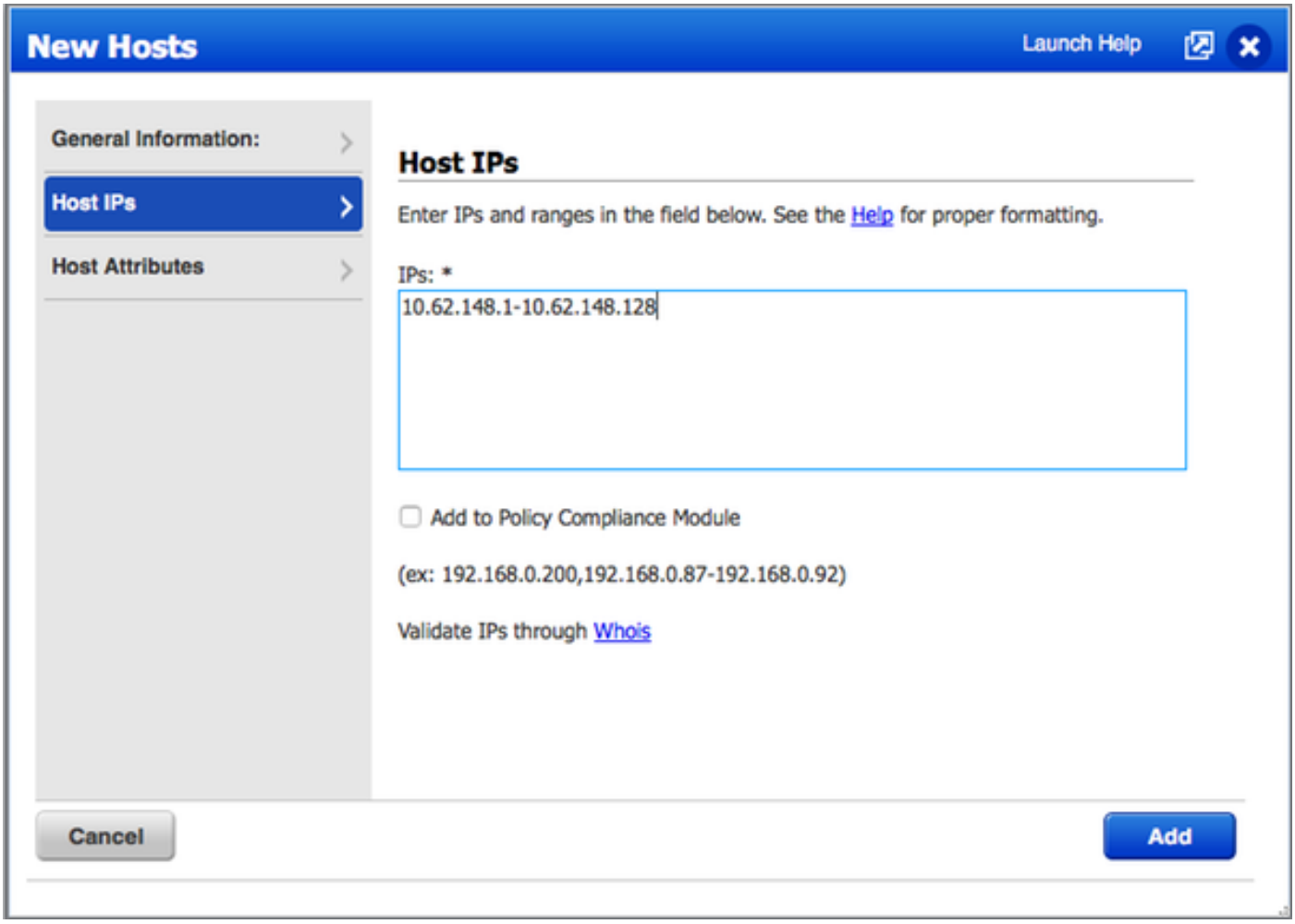
- قم بتمكين تسجيل نقاط CVSS في إدارة نقاط الضعف > التقارير > الإعداد > CVSS > تمكين تسجيل نقاط CVSS



- تأكد من أن مسوغات المستخدم المستخدمة في تكوين المحول لها امتيازات مدير. حدد المستخدم من الزاوية العلوية اليسرى وانقر على **ملف تعريف المستخدم**. يجب أن يكون لديك حقوق "المدير" في **دور المستخدم.**



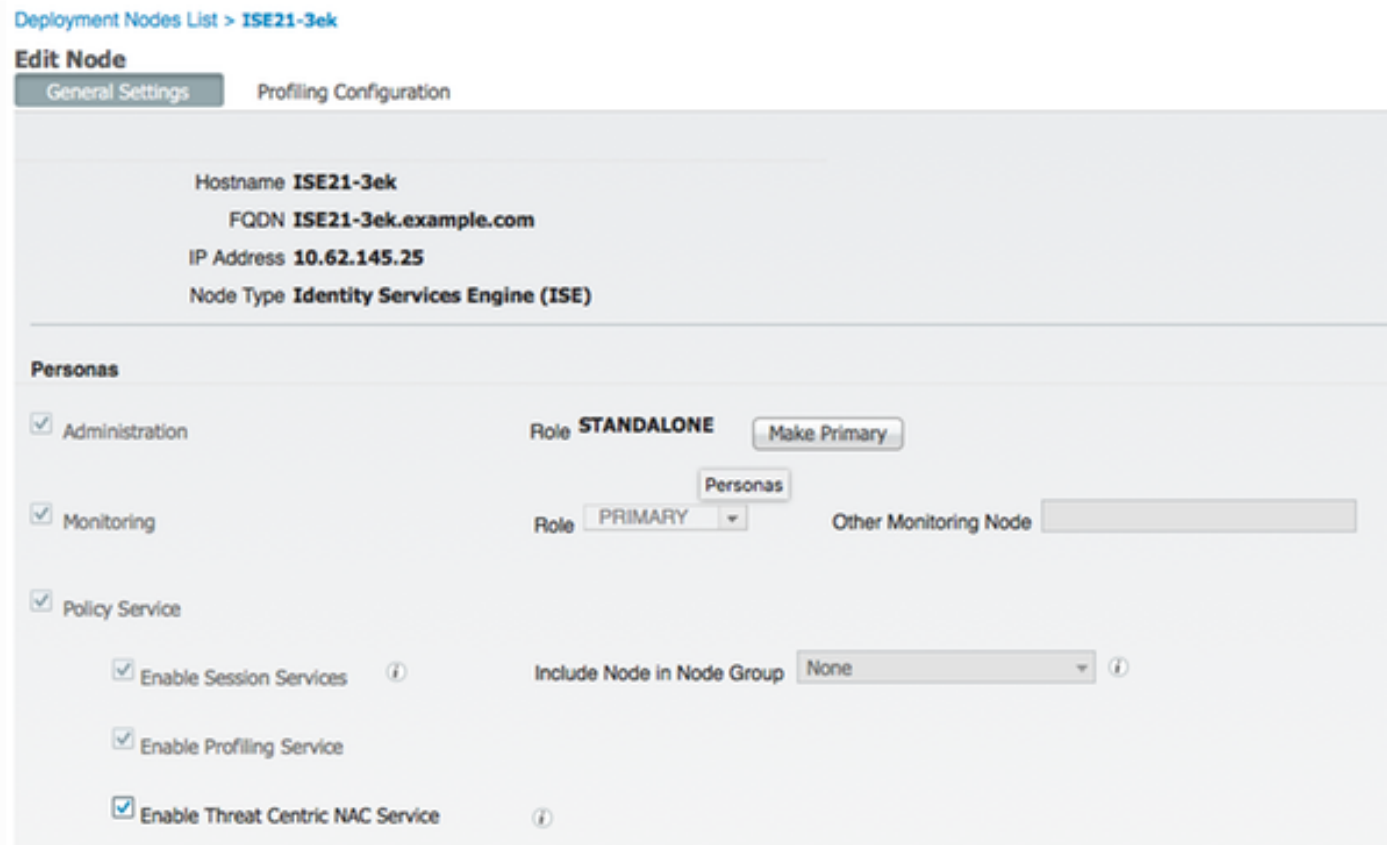
- تأكد من إضافة عناوين IP/الشبكات الفرعية لنقاط النهاية التي تتطلب تقييم قابلية التأثر إلى المردود عند إدارة الثغرات > الأصول > الأصول المضيفة > جديد > أجهزة IP المضيفة التي تم تعقبها



الخطوة 2. تمكين خدمات TC-NAC

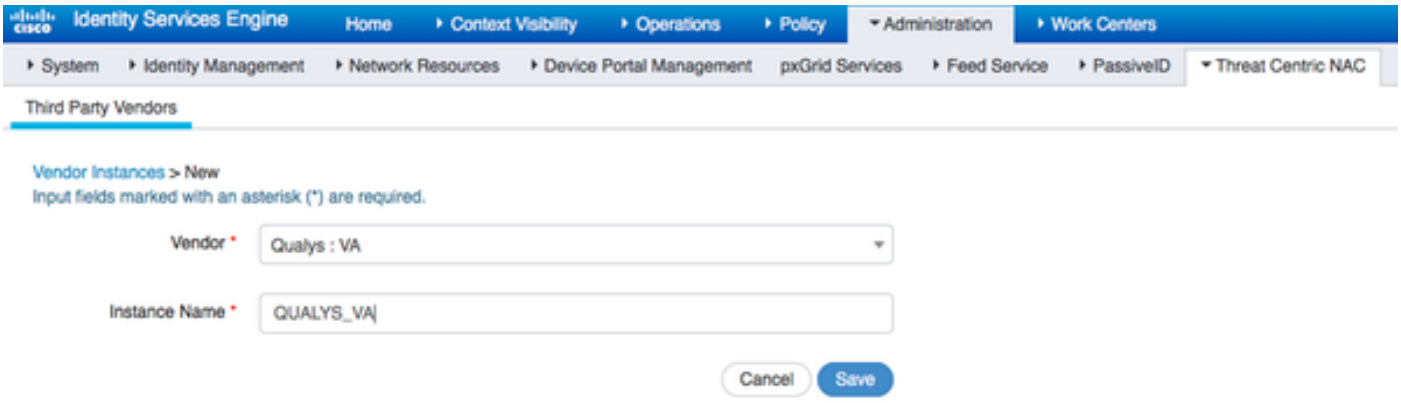
تمكين خدمات TC-NAC تحت الإدارة > النشر > عقدة التحرير. فحص **تمكين خدمة NAC التي ترتكز على التهديد** خانة إختيار.

ملاحظة: يمكن أن تكون هناك عقدة TC-NAC واحدة فقط لكل عملية نشر.

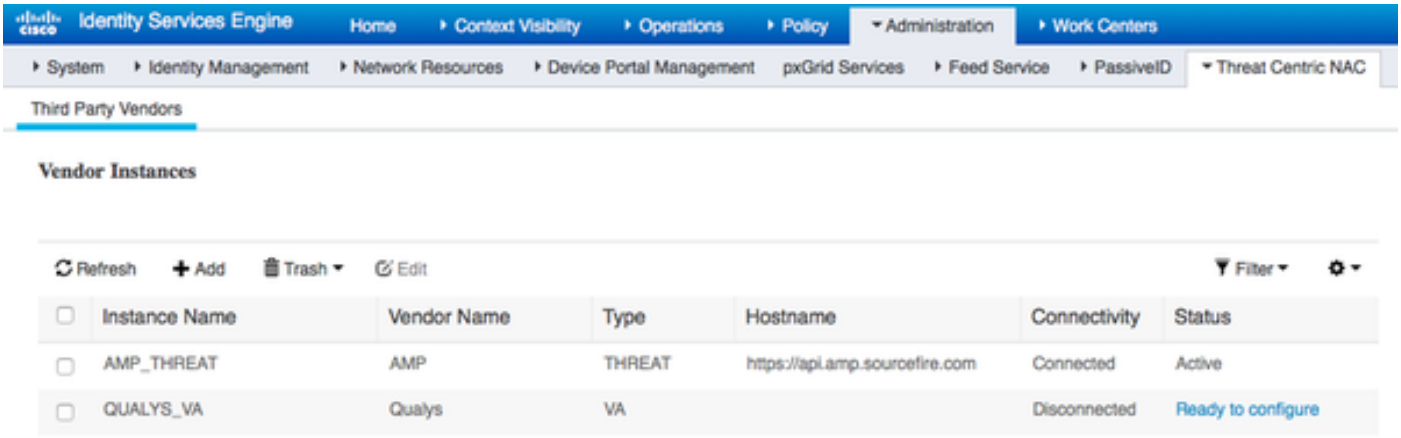


الخطوة 3. تكوين اتصال موفر Qualys بإطار عمل ISE VA

انتقل إلى الإدارة > NAC الذي يركز على التهديدات > موردي الجهات الخارجية > إضافة. انقر فوق **حفظ**.

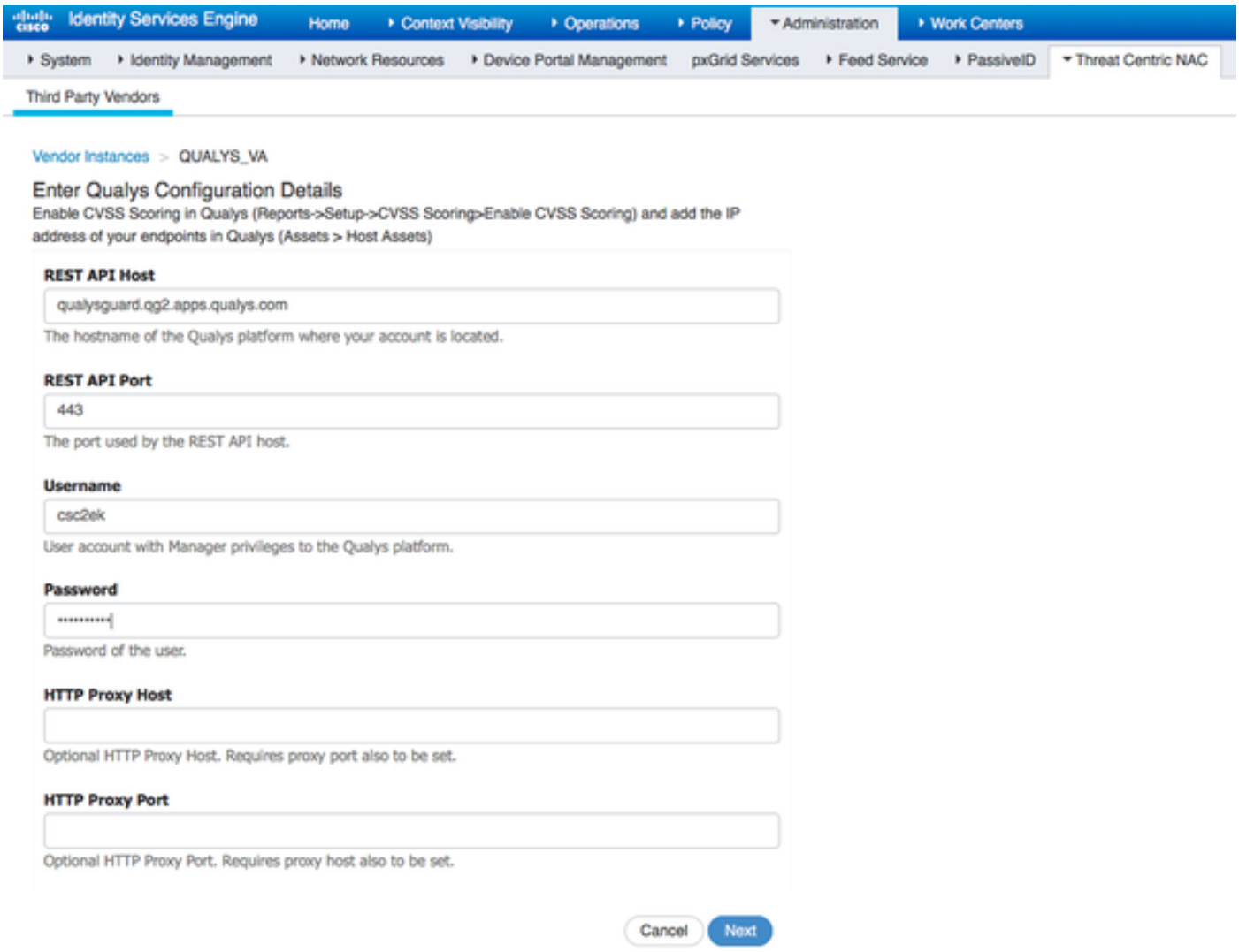


عندما تقوم بتهيئة اتصالات الموفر إلى **جاهز للتكوين** الحالة، انقر فوق **جاهز للتكوين** الخيار في الحالة.

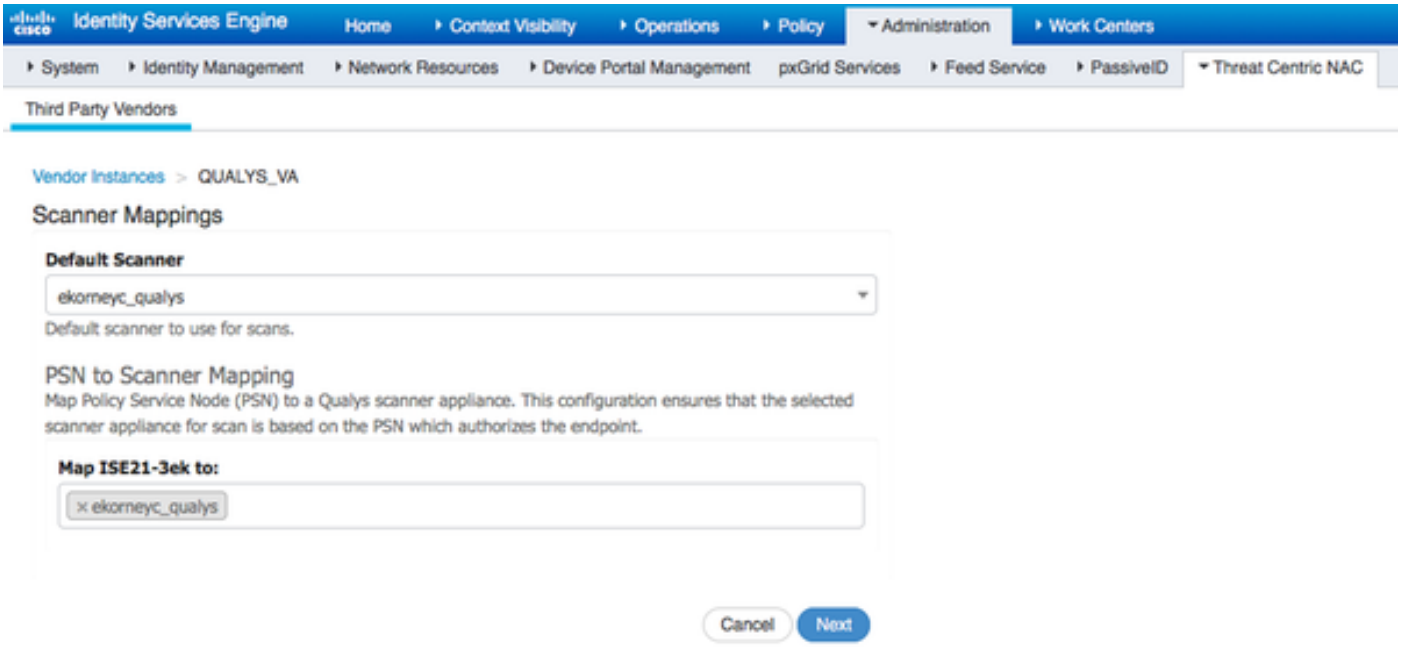


يجب أن يكون مضيف REST API وه المضيف الذي تستخدمه ل Qualys Cloud، حيث يوجد حسابك. في هذا المثال - qualysguard.qg2.apps.qualys.com

يجب أن يكون الحساب وه الذي يملك امتيازات Manager، انقر فوق **التالي**.

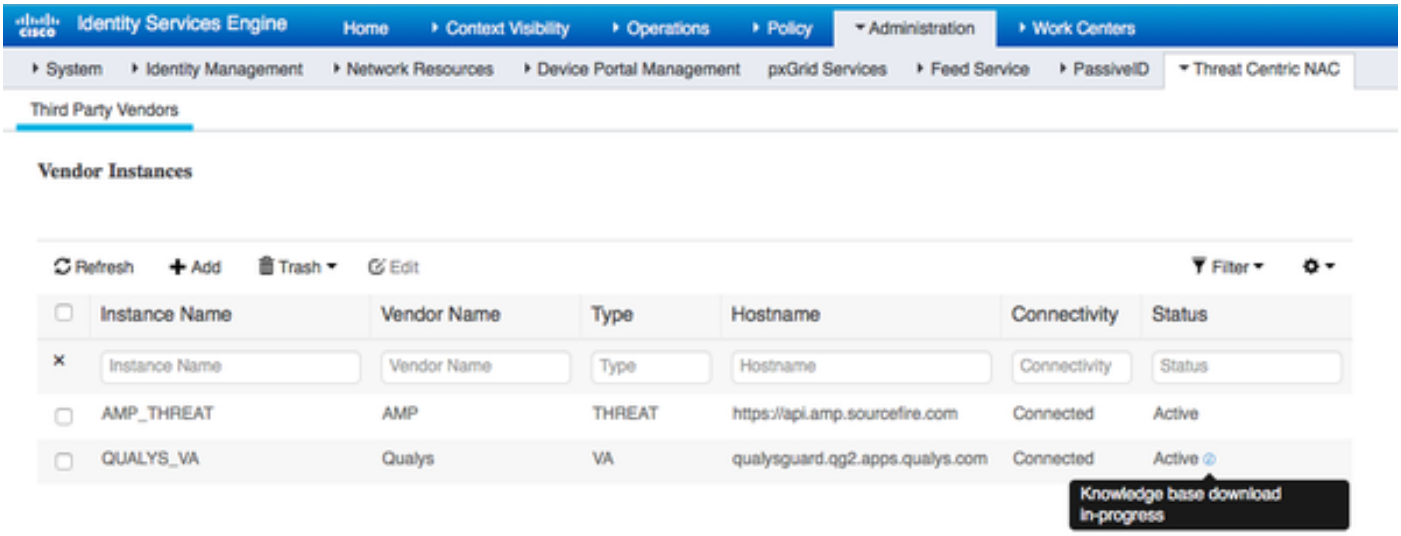


تقوم ISE بتنزيل المعلومات حول الماسحات الضوئية المتصلة بسحابة Qualys، يمكنك تكوين PSN إلى تخطيط الماسح الضوئي على هذه الصفحة. إنه يضمن انتقاء الماسح الضوئي بناء على PSN الذي يخول نقطة النهاية.



تم توثيق الإعدادات المتقدمة بشكل جيد في دليل مسؤول ISE 2.1، ويمكن العثور على الارتباط في قسم المراجع في هذا المستند. طقطقت فوق **بعد ذلك** و**إنجاز**. توضيح عمليات تحويل المثيل إلى الحالة **النشطة** وبدء تنزيل قاعدة المعارف.

ملاحظة: لا يمكن أن يكون هناك سوى مثيل Qualys واحد لكل عملية نشر.



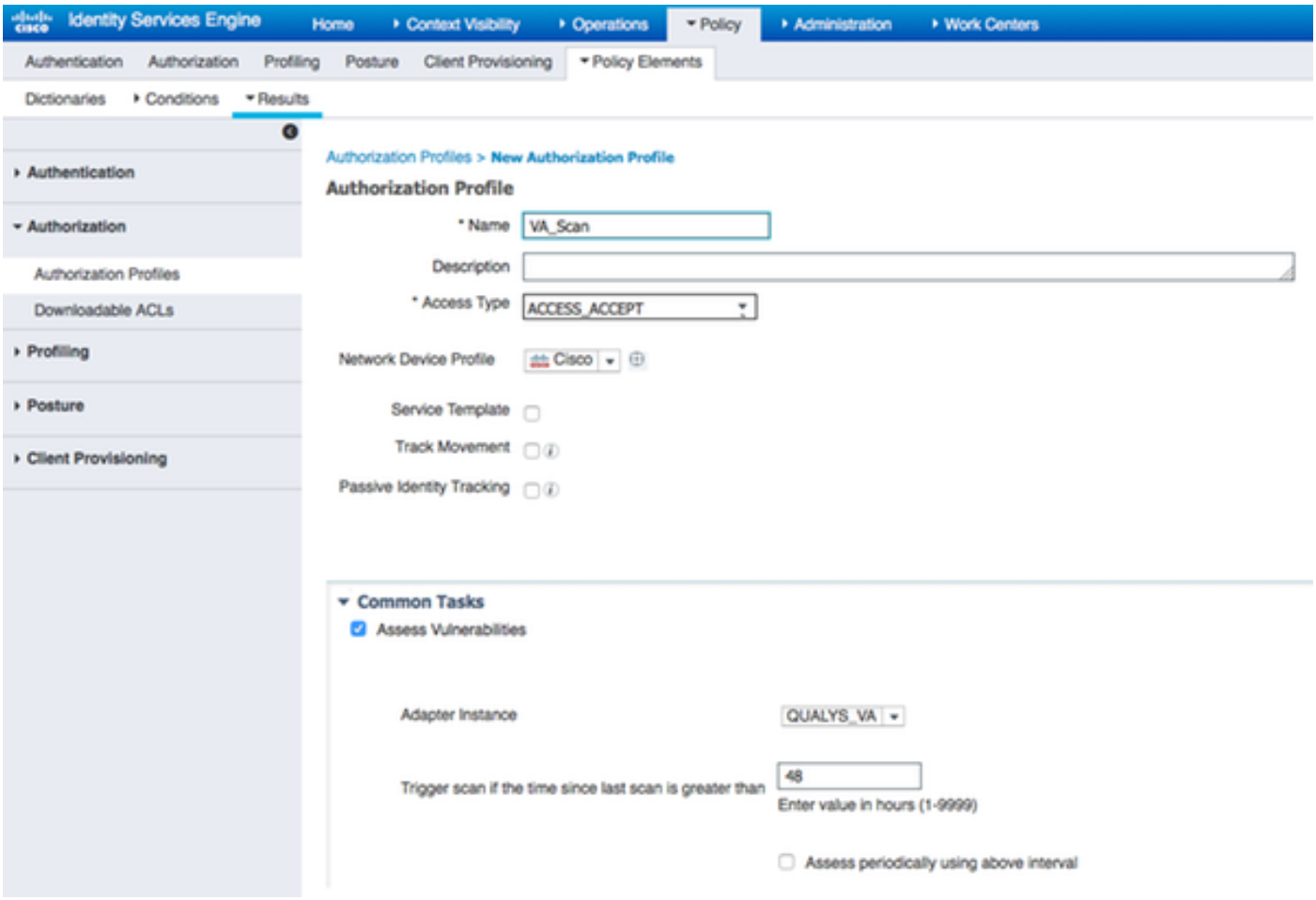
الخطوة 4. تكوين ملف تعريف التخويل لتشغيل مسح VA

انتقل إلى السياسة > عناصر السياسة > النتائج > التخويل > توصيفات 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=796440b7-09b5-4f3b-611-199fb81a4b99
```

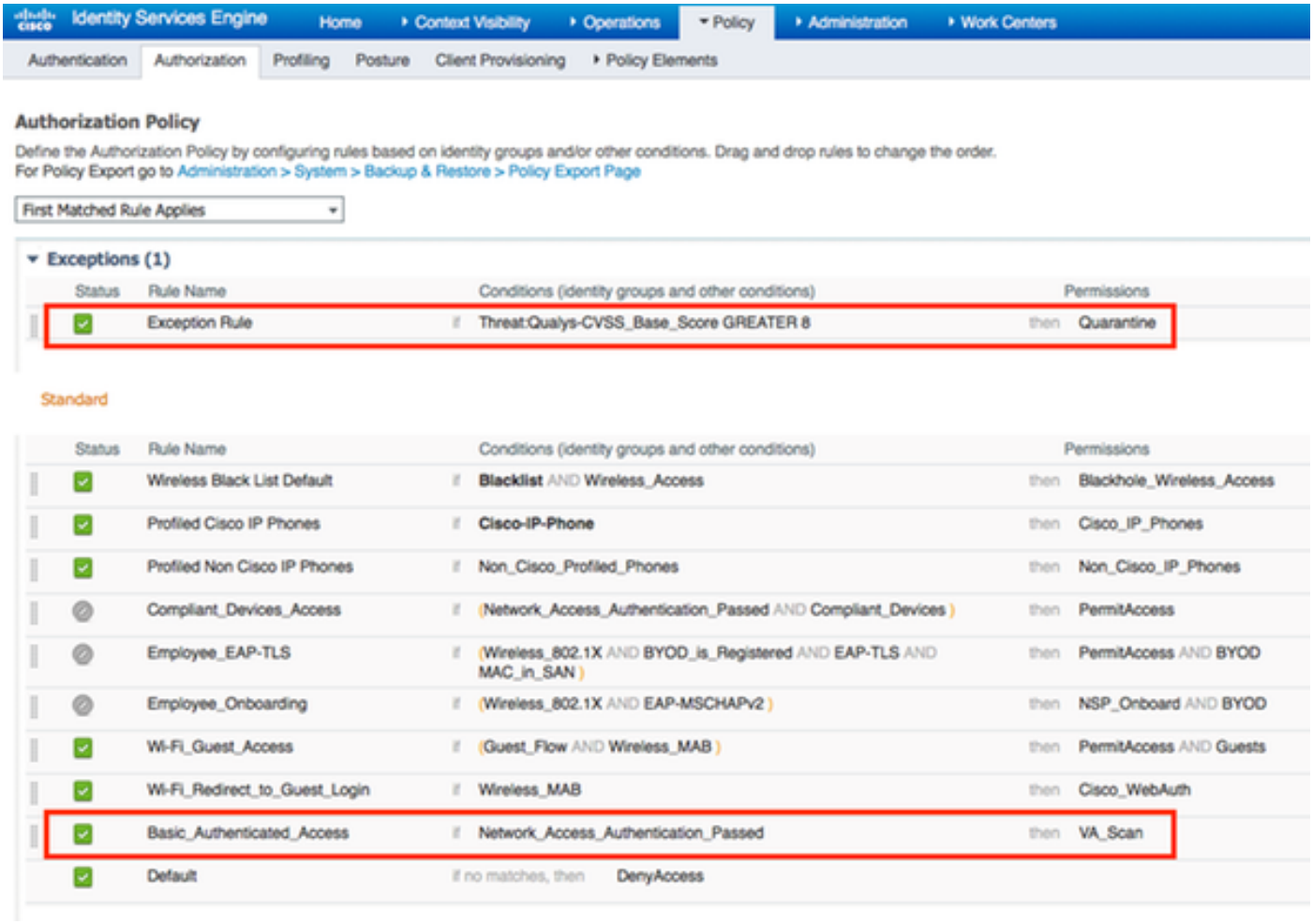
ويتم إرسالها إلى أجهزة الشبكة داخل حزمة قبول الوصول، على الرغم من أن الغرض الحقيقي منها هو إعلام عقدة MNT بضرورة تشغيل الفحص. يرشد MNT عقدة TC-NAC للاتصال بسحابة Qualys.



الخطوة 5. تكوين سياسات التخويل

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

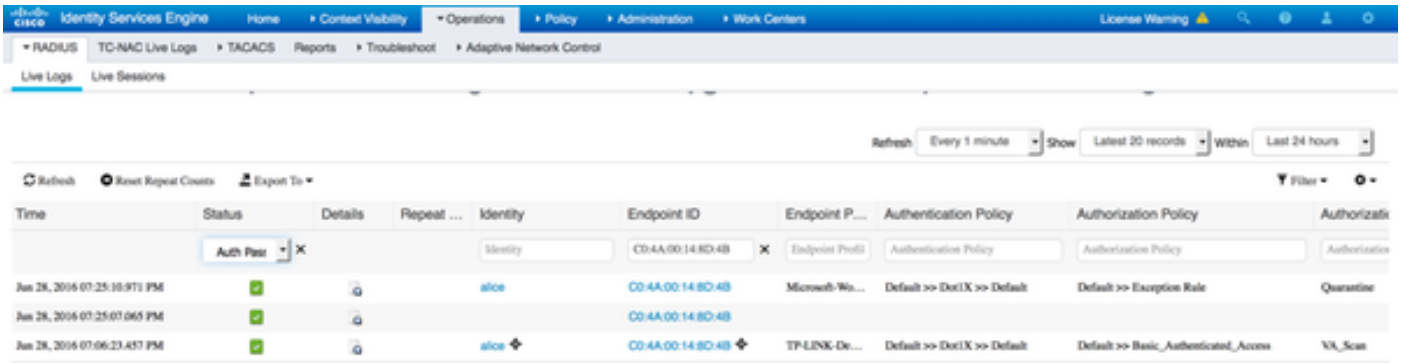
- إنشاء نهج اعتماد للأجهزة التي تم رفض حجر صحي عليها. انتقل إلى نهج > تخويل > نهج تخويل > إستثناءات وقم بإنشاء **قاعدة إستثناء**. انقر فوق شروط > إنشاء شرط جديد (خيار متقدم) > حدد سمة، انزلق لأسفل وحدد **تهديد**. قم بتوسيع سمة **التهديد** وحدد **Qualys-CVSS_BASE_SCORE**. قم بتغيير عامل التشغيل إلى **أكبر من** وقم بإدخال قيمة وفقا لنهج الأمان الخاص بك. يجب أن يعطي ملف تعريف تفويض **الحجر الصحي** وصولا محدودا للجهاز غير المحمي.



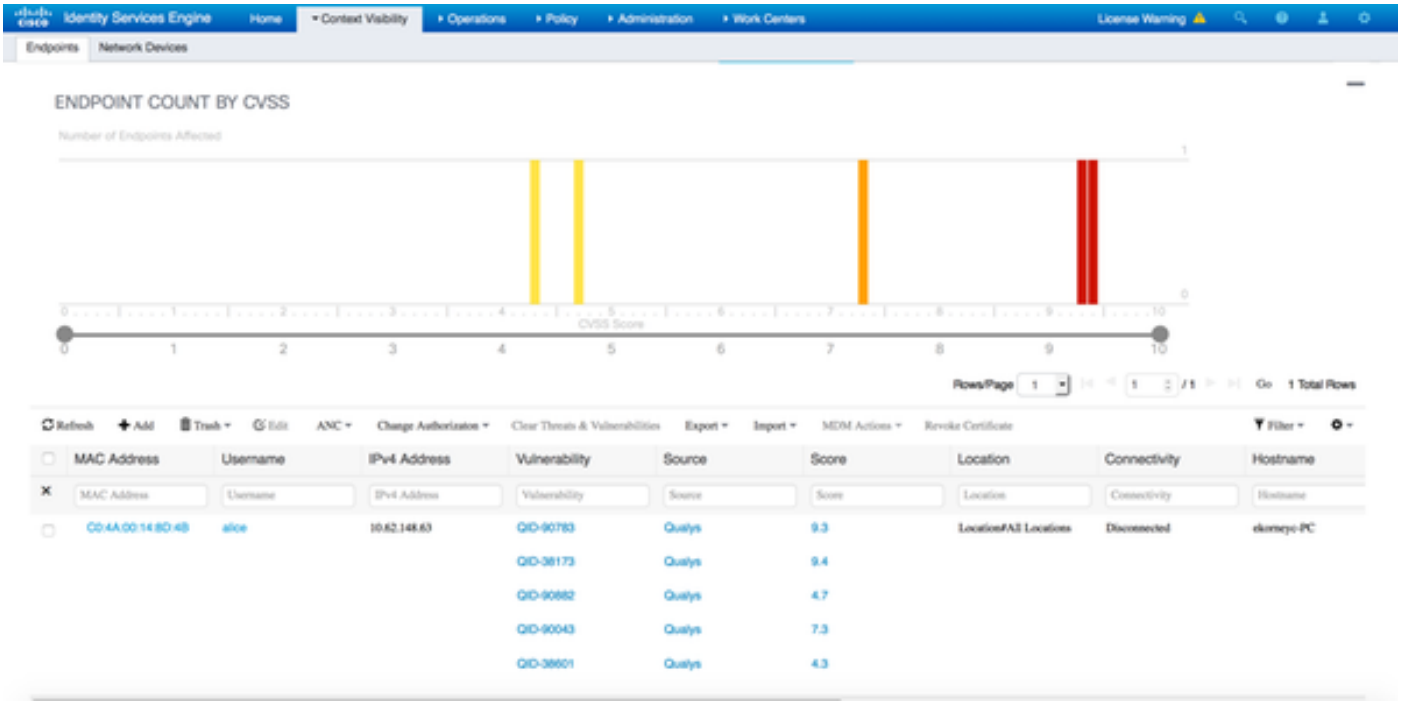
التحقق من الصحة

محرك خدمات الهوية

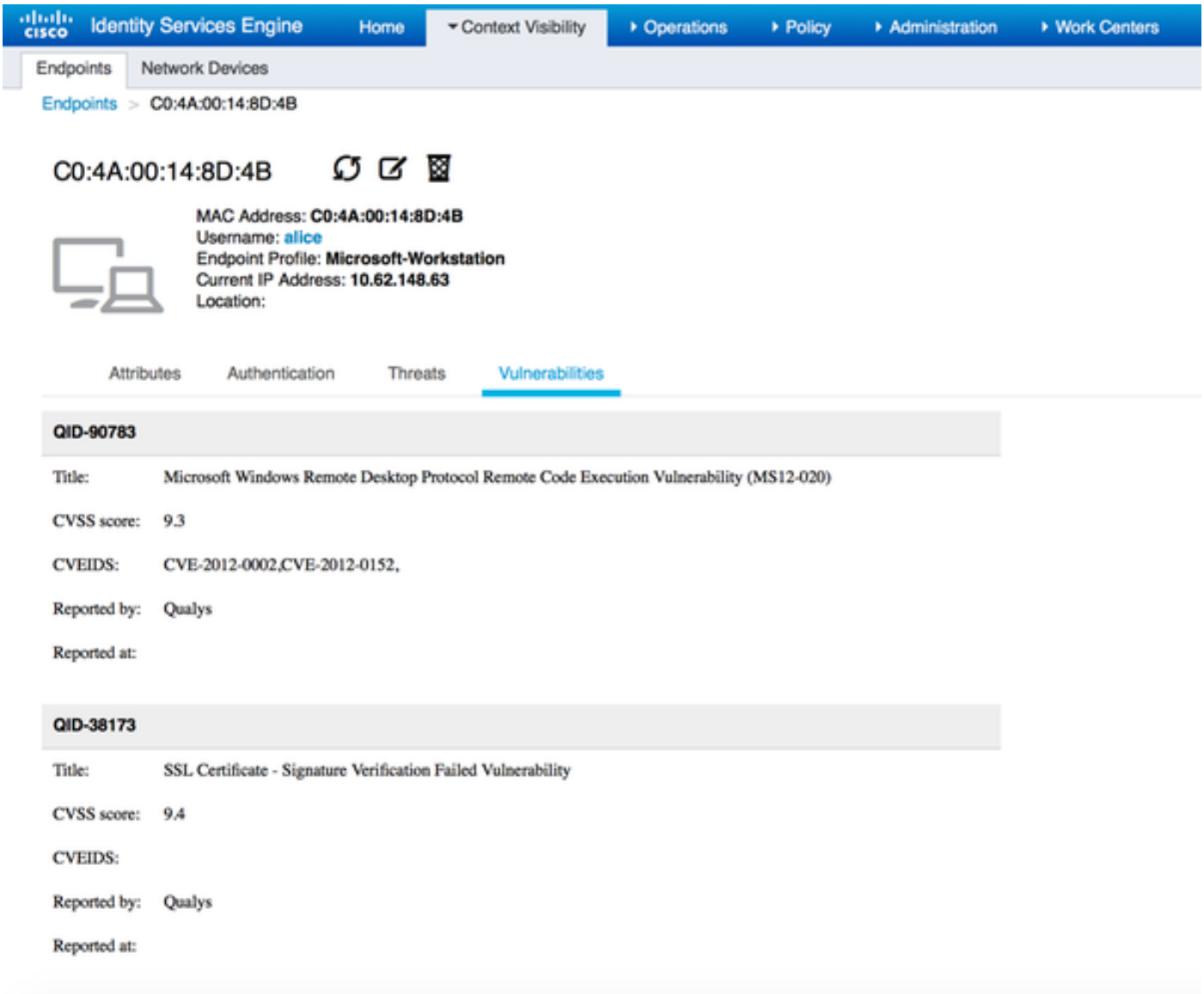
يقوم الاتصال الأول بتشغيل المسح الضوئي ل VA. عند انتهاء الفحص، يتم تشغيل إعادة مصادقة CoA لتطبيق نهج جديد في حالة مطابقته.



للتحقق من مكامن الضعف التي تم اكتشافها، انتقل إلى إمكانية رؤية السياق > نقاط النهاية. تحقق من نقاط الضعف لكل نقطة نهاية مع النقاط التي تم منحها من قبل Qualys.

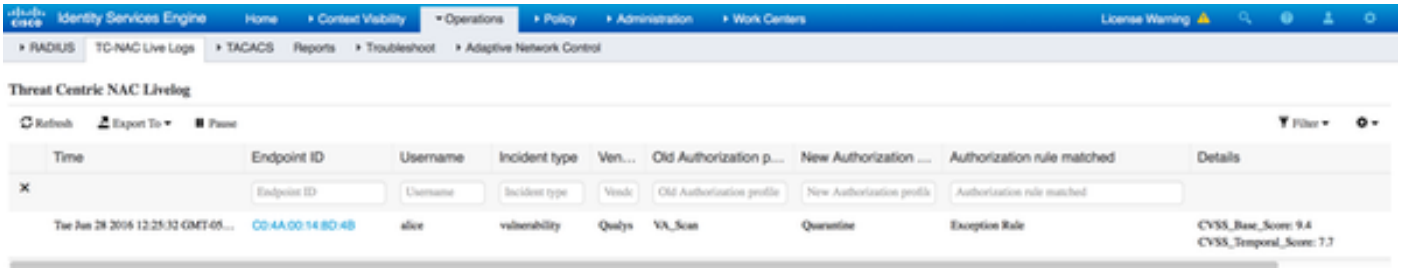


عند تحديد نقطة نهاية معينة، يظهر المزيد من التفاصيل حول كل نقطة ضعف، بما في ذلك **العنوان** و**CVEID**.



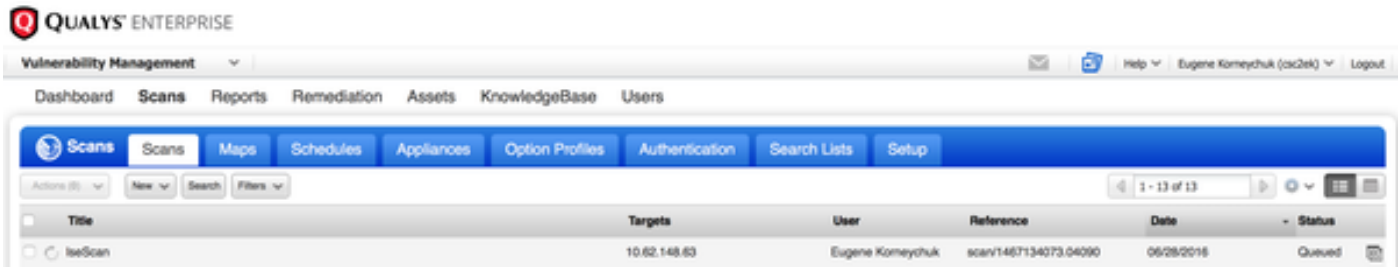
في العمليات > سجلات TC-NAC المباشرة، يمكنك رؤية سياسات التخويل القديمة مقابل الجديدة المطبقة والتفاصيل على CVSS_BASE_SCORE.

ملاحظة: يتم تنفيذ شروط التخويل استنادا إلى CVSS_BASE_SCORE، والتي تساوي أعلى نقاط الضعف التي تم الكشف عنها على نقطة النهاية.

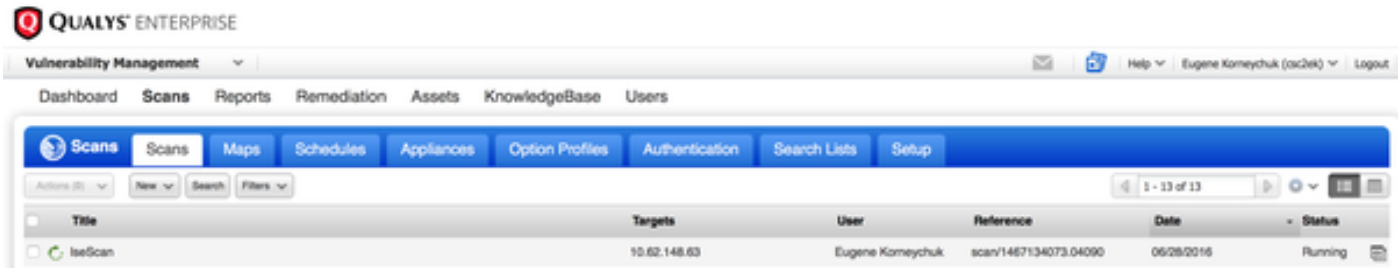


سحابة كوليس

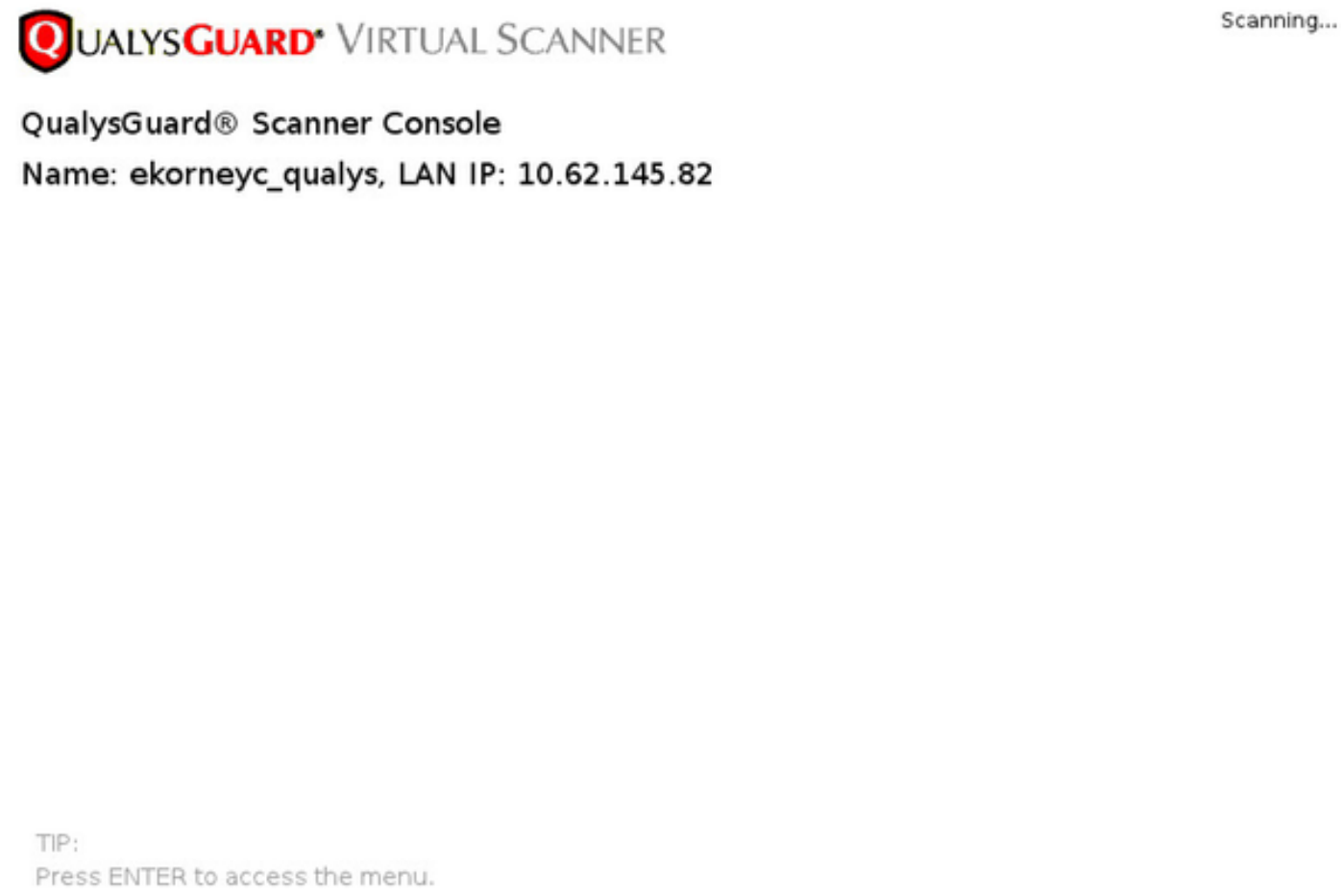
عندما يتم تشغيل المسح الضوئي ل VA بواسطة قوائم انتظار TC-NAC Qualys الخاصة بالمسح الضوئي، يمكن عرضه في عمليات المسح الضوئي > عمليات المسح



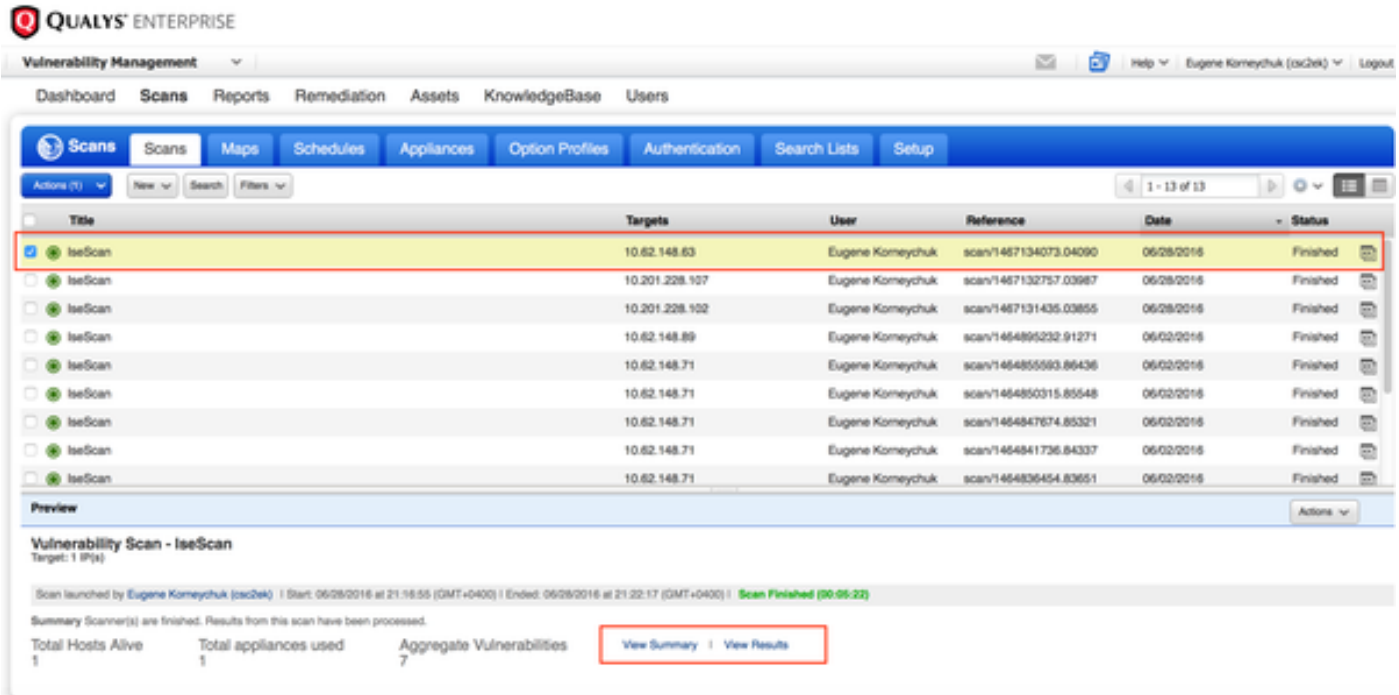
بعد ذلك ينتقل إلى التشغيل، مما يعني أن سحابة Qualys قد أصدرت تعليمات إلى ماسح Qualys لإجراء المسح الضوئي الفعلي



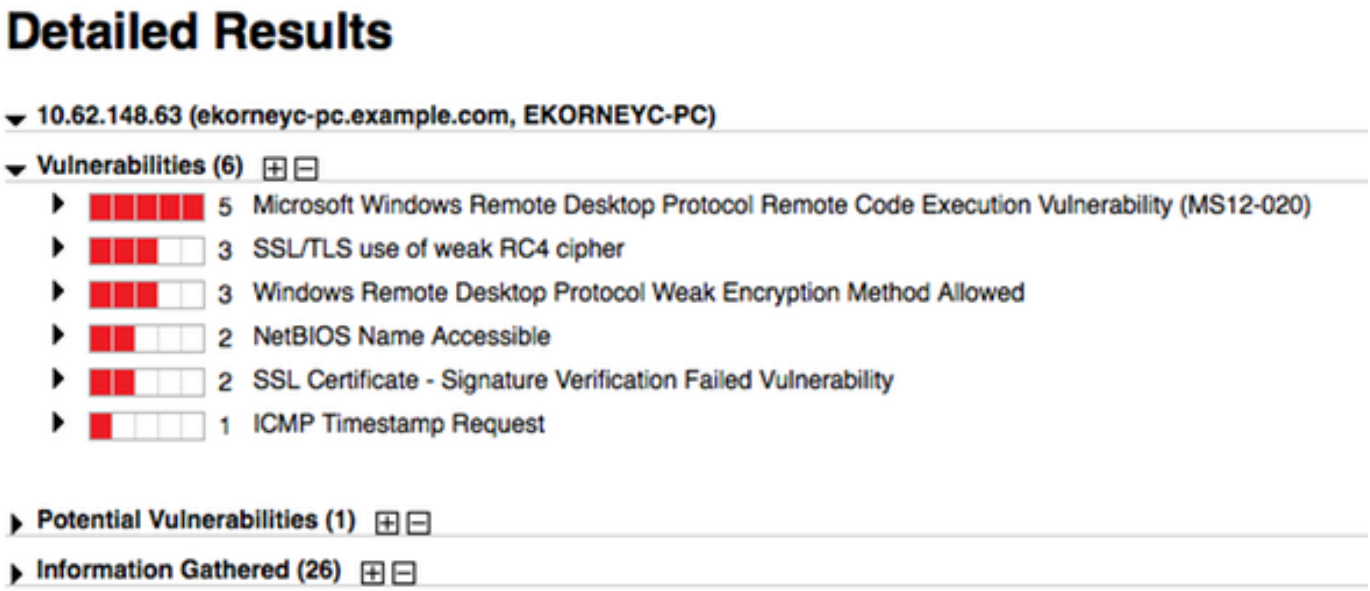
بينما يقوم الماسح الضوئي بإجراء المسح الضوئي، يجب أن ترى "المسح الضوئي..." تسجيل الدخول إلى الزاوية اليمنى العليا من Qualys Guard



بمجرد أن يتم الفحص، فإنه ينتقل إلى الحالة "منتهية". يمكنك عرض النتائج في عمليات مسح ضوئي > مسح ضوئي، حدد الفحص المطلوب وانقر فوق **عرض الملخص** أو **عرض النتائج**.



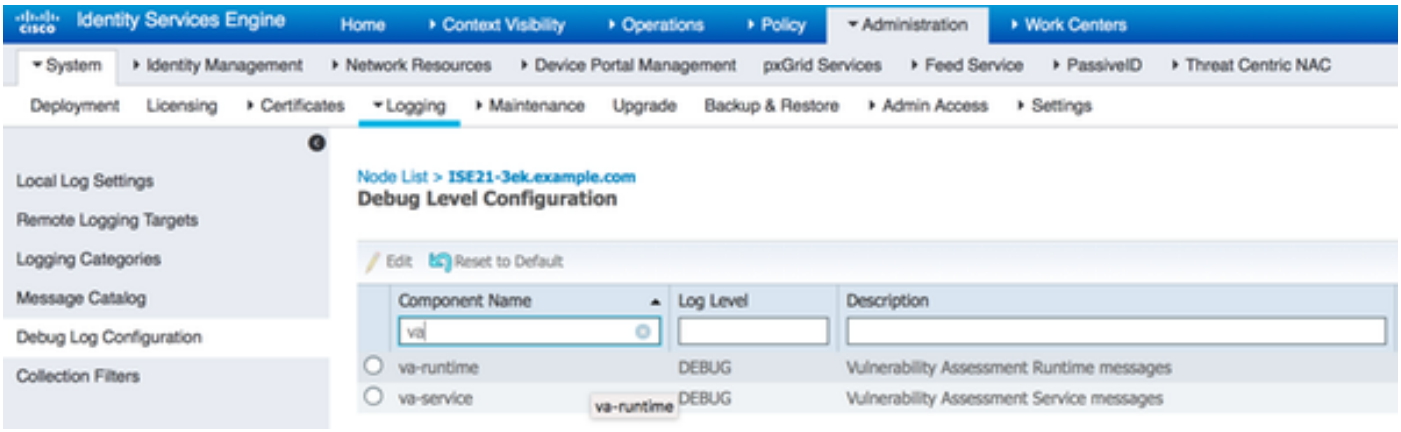
في التقرير نفسه يمكنك رؤية **النتائج التفصيلية**، حيث يتم عرض نقاط الضعف المكتشفة.



استكشاف الأخطاء وإصلاحها

تصحيح الأخطاء على ISE

لتمكين تصحيح الأخطاء على ISE الانتقال إلى الإدارة > النظام > التسجيل > تكوين سجل تصحيح الأخطاء، حدد عقدة TC-NAC وقم بتغيير مكون **مستوى السجل** va-runtime وva-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.

```
2016-06-28 19:06:30823   [Thread-70][] va.runtime.admin.mnt.EndpointFileReader -::::- VA: Read
Va Runtime.
[{"operationType":1"macAddress":"C0:4A:00:14:8D:4B""ondemandScanInterval":"48""isPeriodicScanEna
bled":false"periodicScanEnabledString":"0""vendorInstance":"79640b7-09b5-4f3b-611-
199fb8a4b99""psnHostName": 21-3ek""heartBeatTime":0"lastScanTime":0}]
2016-06-28 19:06:30824   [Thread-70][] va.runtime.admin.vaservice.VaServiceRemotingHandler -
::::- VA:     MNT:
```

```
{"operationType":1"macAddress":"c0:4a:00:14:8D:4B""ondemandScanInterval":"48""isPeriodicScanEnab
led":false"PeriodicScanScan4  String":"0""vendorInstance":"796440b7-09b5-4f3b-611-
199fb81a4b99""psnHostName":"ISE21-3ek""heartBeatTime":0"lastScanTime":0}
```

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

```
2016-06-28 19:25:02020 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::-     VaService:
[{"macAddress":"c0:4a:00:14:8d:4b""ipAddress":"10.62.148.63""lastScanTime":1476
:["{\"VulnerabilityId\":\"QID-90783\"\"cveIds\":\"CVE-2012-0002 CVE-2012-
0152\"\"cvssBaseScore\":\"9. 3\"\"cvssTemporaryScore\:\"7.\"\"VulnerabilityTitle\": "Windows
Remote Desktop Protocol Remote Execution Vulnerability (MS12-
020)\"\"VulnerabilityVendor\":\"Qualys\"}"{\"VulnerabilityId\":\"QID-
38173\"\"cveIds\"\"\"\"cvssBaseScore\":\"9. 4\"\"cvssTemporaryScore\":\"6.
9\"\"VulnerabilityTitle\":"SSL  -    \"
\"VulnerabilityVendor\":\"Qualys\"}""{\"VulnerabilityId\":\"QID-
90882\"\"cveIds\":\"\"\"cvssBaseScore\":\"4.
7\"\"cvssTemporaryScore\":\"4\"\"VulnerabilityTitle\":\"    Windows Remote Desktop
\"\"VulnerabilityVendor\"Qualys\"}""\"VulnerabilityID\"\"\": QID-
90043\"\"cveIds\":\"\"cvssBaseScore\":\"7. 3\"\"cvssTemporaryScore\":\"6.
3\"\"vulnerabilityTitle\":\"SMB    SMB
\"\"vulnerabilityVendor\":\"Qualys\"}"{\"vulnerabilityID\"\"QID-38601\"\"CVEid\": "CVE-2013-
2566CVE-2015-
2808\"\"cvssBaseScore\":\"4.3\"\"cvssTemporaryScore\":\"3.7\"\"VulnerabilityTitle\":\"SSL/TLS
RC4 \"\"VulnerabilityVendor\":\"Qualys\"}"]]]
2016-06-28 19:25:02127   [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -::::- VA:    db LastscanTime: 1467134394000
mac: c0:4a:00:14:8d:4b
2016-06-28 19:25:02268   [pool-311-thread-8][] va.runtime.admin.vaservice.VaAdminServiceContext
-:::- VA:  json    pri-lan
2016-06-28 19:25:02272   [pool-311-thread-8][] va.runtime.admin.vaservice.VaPanRemotingHandler -
::::::- VA:    : {C0:4a:00:14:8D:4B=[{"vulnerabilityId":"QID-90783""cveIds":"CVE-2012-02-0202
02CVE-2012-0152""cvssBaseScore":"9.3""cvssTemporaryScore":"7.7""vulnerabilityTitle":"Microsoft
Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)""vulnerabilityVendor":"Qualys"} {"vulnerabilityID:"QID-38173""cveIds":""CVSSbaseScore:":":
9.4""cvssTemporaryScore":"6.9""VulnerabilityTitle":" SSL -
""VulnerabilityVendor":"Qualys"} {"VulnerabilityId":"QID-
90882""cvssBaseScore":"4.7""cvssTemporaryScore":"4""VulnerabilityTitle":"
Windows""QualityVendor": ys"} {"vulnerabilityId":"QID-
90043""cveIds":""cvssBaseScore":"7.3""cvssTemporaryScore":"6.3""vulnerabilityTitle":"SMB
Signature Disabled  SMB Signature Not Required""vulnerabilityVendor":"Qualys"}
{"vulnerabilityID:"QID-38601""cveIds":"CVE-2013-223-23 66CVE-2015-
2808""cvssBaseScore":"4.3""cvssTemporaryScore":"3.7""vulnerabilityTitle":" SSL/TLS  RC4
""vulnerabilityVendor":"qualys"}]
```

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

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

تم إرسال طلب تقييم الضعف إلى المحول

```
2016-06-28 17:07:13200 DEBUG [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg : [{"systemMsg":"91019""isAutoInsertSelfAcsInstance":true"":["TC-
NAC.ServiceName""   " TC-NAC.Status" VA   ""TC-NAC.Details"" VA    ""TC-
NAC.MACAddress""C0:4a:00:14:8D:4B""TC-NAC.IPaddress""10.62.148.63""TC-
NAC.AdapterInstanceUid""79640B-003 9b5-4f3b-611-199fb81a4b99""TC-NAC.VendorName""Qualys""TC-
NAC.AdapterInstanceName""QUALYS_VA"]}]
```

يتحقق AdapterMessageListener كل 5 دقائق من حالة المسح الضوئي حتى ينتهي.

```
2016-06-28 17:09:43459   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-   :
{"AdapterInstanceName":"Qualys_VA""AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys""OperationMessageText":"           : 1        : 0          : 0"}
2016-06-28 17:14:43760 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-   :
{"AdapterInstanceName":"Qualys_VA""AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys""OperationMessageText":"           : 0        : 0          : 1"}
2016-06-28 17:19:43837   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-   :
{"AdapterInstanceName":"Qualys_VA""AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys""OperationMessageText":"           : 0        : 0          : 1"}
2016-06-28 17:24:43867   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-   :
{"AdapterInstanceName":"Qualys_VA""AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys""OperationMessageText":"           : 0        : 0          : 1"}
```

يحصل المحول على معرف فئة المورد (QID) وCVE ومعايير CVSS جنبا إلى جنب مع العلامات

```
2016-06-28 17:24:57556   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.adapterMessageListener -::::-   :
{"RequestedMacAddress":"C0:4a:00:14:8D:4B""scanStatus":"Assessment_SUCCESS""lastScanLong":146713
449 000"ipAddress":"10.62.148.63"" ":[{"VulnerabilityId":"QID-
38173""cvssBaseScore":"9.4""cvssTemporaryScore":"6.9""VulnerabilityTitle":" SSL -
""VulnerabilityVendor":"Qualys"}{"VulnerabilityID:"QID-90
43""cvssBaseScore":"7.3""cvssTemporaryScore":"6.3""vulnerabilityTitle":"SMB Signature Disabled
SMB Signature Not Required""vulnerabilityVendor":"Qualys"}{"vulnerabilityId":"QID-
90783""cveIds":"CVE-2012-002CVE-2012-012-512
2""cvssBaseScore":"9.3""cvssTemporaryScore":"7.7""vulnerabilityTitle":"Microsoft Windows Remote
Desktop Protocol Remote Execution Vulnerability (MS12-
020)""vulnerabilityVendor":"Qualys"}{"vulnerabilityId:"QID-38601""cveIds":"CVE-2013-2566CVE-
2015-22 08""cvssBaseScore":"4.3""cvssTemporaryScore":"3.7""vulnerabilityTitle":"SSL/TLS   RC4
""vulnerabilityVendor":"Qualys"}{"vulnerabilityId":"QID-
90882""cvssBaseScore":"4.7""cvssTimerScore":"4""VulnerabilityTitle":
""VulnerabilityVendor":"Qualys"}]}
2016-06-28  [SimpleAsyncTaskExecutor-2] [] cpm.va.service.processor.adapterMessageListener -
::::-      IRF  {"C0:4a:00:14:8d:4b":[{"
":{"CVSS_Base_Score":9.4"CVSS_Temporal_Score":7.7}"timestamp-4":1 67134394000"":"""":"Qualys"}]}
2016-06-28 17:25:01853 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg : [{"systemMsg":"91019""isAutoInsertSelfAcsInstance":true"":["TC-
NAC.ServiceName""   " TC-NAC.Status"VA  ""TC-NAC.Details""VA        : 5""TC-
NAC.MACAddress""C0:4a:00:14:8D:4B""TC-NAC.IPaddress""10.62.148.63""TC-
NAC.AdapterInstanceUid""796440B-0Address 9b5-4f3b-611-199fb81a4b99""TC-
NAC.VendorName""Qualys""TC-NAC.AdapterInstanceName""QUALYS_VA"]}]
```

المشكلات النموذجية

المسألة 1. يحصل ISE على تقرير الثغرات مع CVSS_BASE_SCORE من 0.0 و CVSS_TEMPORAL_SCORE من 0.0، بينما يحتوي تقرير Qualys Cloud على نقاط الضعف المكتشفة.

المشكلة:

أثناء التحقق من التقرير من Qualys Cloud يمكنك رؤية نقاط الضعف المكتشفة، ومع ذلك لا تظهر على ISE.

تم عرض تصحيح الأخطاء في catalyervice.log:

```
2016-06-02 08:30:10323  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.adapterMessageListener -::::-      IRF
{"c0:4a:00:15:75:c8":[{"Vulnerability":{"CVSS_Base_Score":0.0"CVSS_Temporal_Score":0.0}"stamp-
4":1 6485905000"title":" """:"Qualys"}]}
```

الحل:

السبب وراء كون درجة CVSS صفر هو إما أن ليس لها نقاط ضعف أو أن عالمة CVSS لم يتم تمكينها في Qualys Cloud قبل أن تقوم بتكوين المحول من الخلال UI. يتم تنزيل تكوين نقاط CVSS التي تحتوي على ميزة تسجيل نقاط CVSS التي تم تمكينها بعد إنشاء KnowledgeBase من قبل، حيث تم تمكين تسجيل نقاط CVSS. يجب عليك التأكد من تمكين تسجيل نقاط CVSS للمحول لأول مرة. يمكن القيام بذلك تحت إدارة نقاط الضعف > التقارير > الإعداد > CVSS > تمكين تسجيل نقاط CVSS

المسألة 2. لا يحصل ISE على نتائج من مجموعة Qualys Cloud، على الرغم من تطبيق نهج التخويل الصحيح.

المشكلة:

تمت مطابقة نهج التخويل المصحح، الذي يجب أن يؤدي إلى تشغيل فحص VA. بالرغم من هذه الحقيقة، لا يتم إجراء أي فحص.

تم عرض تصحيح الأخطاء في catalyervice.log:

```
2016-06-28 16:19:15401 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-    :
(:'[B@6da5e620([311])'MessageProperties [={} timestamp=null messageId=null userId=null
appId=null clusterId=null type=null correlationId=null   Null =Null =application/octet-stream
contentEncoding=null contentLength=0 deliveryMode=PERSISTENT expiration=null priority=0
redelivered=false receiveExchange=irf.topic.va-reports receiveRoutingKey= deliveryTag=9830
messageCount=0])
2016-06-28 16:19:15401   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::-    :
{"requestedMacAddress":"24:77:03:3d:CF:20""scanStatus":"scan_error""scanStatusMessage":"    :
          1904:      IP       ."lastScanTimeLong":0"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15771   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::::-      Macaddress:24:77:03:3d:CF:20
IP(DB): 10.201.228.102
2016-06-28 16:19:16336 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg : [{"systemMsg":"91008""isAutoInsertSelfAcsInstance":true"":["TC-
NAC.ServiceName""   " TC-NAC.Status"VA Failure""TC-NAC.Details""    :              1904:
IP       .""TC-NAC.MACAddress""24:77:03:3d:CF:20""TC-NAC.IPaddress""10.201.28.12" "TC-
NAC.AdapterInstanceUuid""79640b7-09b5-4f3b-611-199fb81a4b99""TC-NAC.VendorName""Qualys""TC-
NAC.AdapterInstanceName""QUALYS_VA"]}]
```

الحل:

يشير Qualys Cloud إلى أن عنوان IP الخاص بنقطة النهاية غير مؤهل للمسح الضوئي، الرجاء التأكد من إضافة عنوان IP لنقطة النهاية إلى إدارة الثغرات > الأصول > الأصول المضيفة > جديد > IP Track Host

المراجع

- دليل مسؤول محرك خدمات الهوية من Cisco، الإصدار 2.1
- الدعم التقني والمستندات - Cisco Systems
- الفيديو: ISE 2.1 مع Qualys

- توثيق Qualys

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).