إختبار ترخيص المنتج

المقدمة

يوضح هذا المستند كيفية تكوين دور Nexus مخصص ل TACACS عبر CLI (واجهة سطر الأوامر) على NK9.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- TACACS+
- ISE 3.2

المكونات المستخدمة

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

- bootflash:///nxos.9.3.5.bin :وه NXOS صورة ملف ،Cisco Nexus 9000
- Identity Service Engine، الإصدار 3.2

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

متطلبات الترخيص

لا يتطلب أي ترخيص خاص من Cisco - TACACS+ من NX-OS.

محرك خدمة الهوية من Cisco

بالنسبة لتثبيتات ISE الجديدة، يكون لديك فترة تقييم تبلغ 90 يوما لديه حق الوصول إلى جميع ميزات ISE، إذا لم يكن لديك ترخيص تقييمي، لاستخدام ميزة ISE، فأنت تحتاج إلى ترخيص مسؤول جهاز لعقدة خادم النهج التي تقوم بالمصادقة.

بعد أن يقوم مستخدم مكتب الدعم/الإدارة بالمصادقة على جهاز Nexus ISE بإرجاع دور Nexus Shell المطلوب.

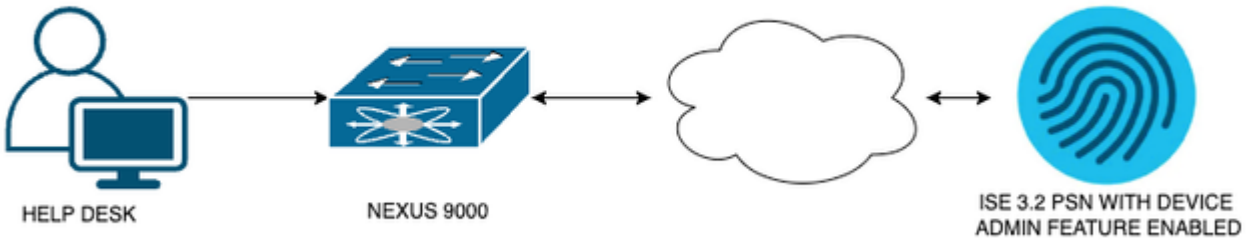
يمكن للمستخدم المعين بهذا الدور تنفيذ أستكشاف الأخطاء وإصلاحها الأساسية وإرجاع منافذ معينة.

يجب أن تكون جلسة عمل TACACS التي تحصل على دور Nexus قادرة على إستخدام الأوامر والإجراءات التالية وتشغيلها فقط:

- الوصول إلى تكوين وحدة طرفية للتنفيذ فقط مع إيقاف التشغيل وعدم إيقاف التشغيل للواجهات من 1/1-1/21 و 1/25-1/30
- بروتوكول النقل الآمن (ssh)
- SSH6
- telnet
- Telnet6
- traceroute
- traceroute6
- بينغ
- إختبار الاتصال 6
- تمكين

التكوين

الرسم التخطيطي للشبكة



الرسم التخطيطي لمكونات التدفق

الخطوة 1: تكوين Nexus 9000

1. تكوين المصادقة والتفويض والمحاسبة (AAA).

تحذير: بعد تمكين مصادقة TACACS، يتوقف جهاز Nexus عن إستخدام المصادقة المحلية ويبدأ في إستخدام المصادقة المستندة إلى خادم AAA.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+)# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

2. قم بتكوين الدور المخصص باستخدام المتطلبات المحددة.

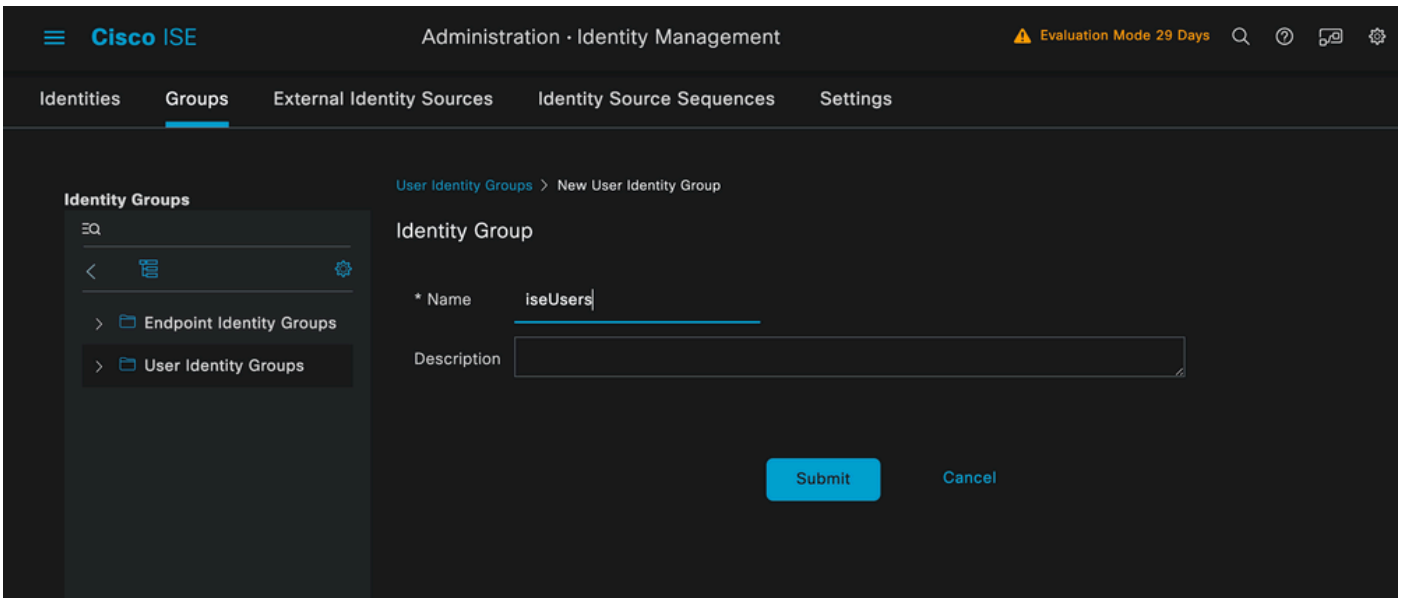
```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#   description Can perform basic Toubleshooting and bounce certain  ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown

vlan policy deny
interface policy deny

Nexus9000(config-role-interface)#     permit interface Ethernet1/1
Nexus9000(config-role-interface)#     permit interface Ethernet1/2
Nexus9000(config-role-interface)#     permit interface Ethernet1/3
Nexus9000(config-role-interface)#     permit interface Ethernet1/4
Nexus9000(config-role-interface)#     permit interface Ethernet1/5
Nexus9000(config-role-interface)#     permit interface Ethernet1/6
Nexus9000(config-role-interface)#     permit interface Ethernet1/7
Nexus9000(config-role-interface)#     permit interface Ethernet1/8
Nexus9000(config-role-interface)#     permit interface Ethernet1/8
Nexus9000(config-role-interface)#     permit interface Ethernet1/9
Nexus9000(config-role-interface)#     permit interface Ethernet1/10
Nexus9000(config-role-interface)#     permit interface Ethernet1/11
Nexus9000(config-role-interface)#     permit interface Ethernet1/12
Nexus9000(config-role-interface)#     permit interface Ethernet1/13
Nexus9000(config-role-interface)#     permit interface Ethernet1/14
Nexus9000(config-role-interface)#     permit interface Ethernet1/15
Nexus9000(config-role-interface)#     permit interface Ethernet1/16
Nexus9000(config-role-interface)#     permit interface Ethernet1/17
Nexus9000(config-role-interface)#     permit interface Ethernet1/18
Nexus9000(config-role-interface)#     permit interface Ethernet1/19
Nexus9000(config-role-interface)#     permit interface Ethernet1/20
Nexus9000(config-role-interface)#     permit interface Ethernet1/21
Nexus9000(config-role-interface)#     permit interface Ethernet1/22
Nexus9000(config-role-interface)#     permit interface Ethernet1/25
Nexus9000(config-role-interface)#     permit interface Ethernet1/26
Nexus9000(config-role-interface)#     permit interface Ethernet1/27
Nexus9000(config-role-interface)#     permit interface Ethernet1/28
Nexus9000(config-role-interface)#     permit interface Ethernet1/29
Nexus9000(config-role-interface)#     permit interface Ethernet1/30

Nexus9000# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...

Copy complete.
```

الخطوة 2. تكوين Identity Service Engine 3.2

1. قم بتكوين الهوية التي يتم إستخدامها أثناء جلسة عمل Nexus TACACS.

يتم إستخدام مصادقة ISE المحلية.

انتقل إلى علامة التبويب إدارة > إدارة الهوية > مجموعات" وقم بإنشاء المجموعة التي يجب أن يكون المستخدم جزءا منها، ومجموعة الهوية التي تم إنشاؤها لهذا العرض التوضيحي هي ISEusers.

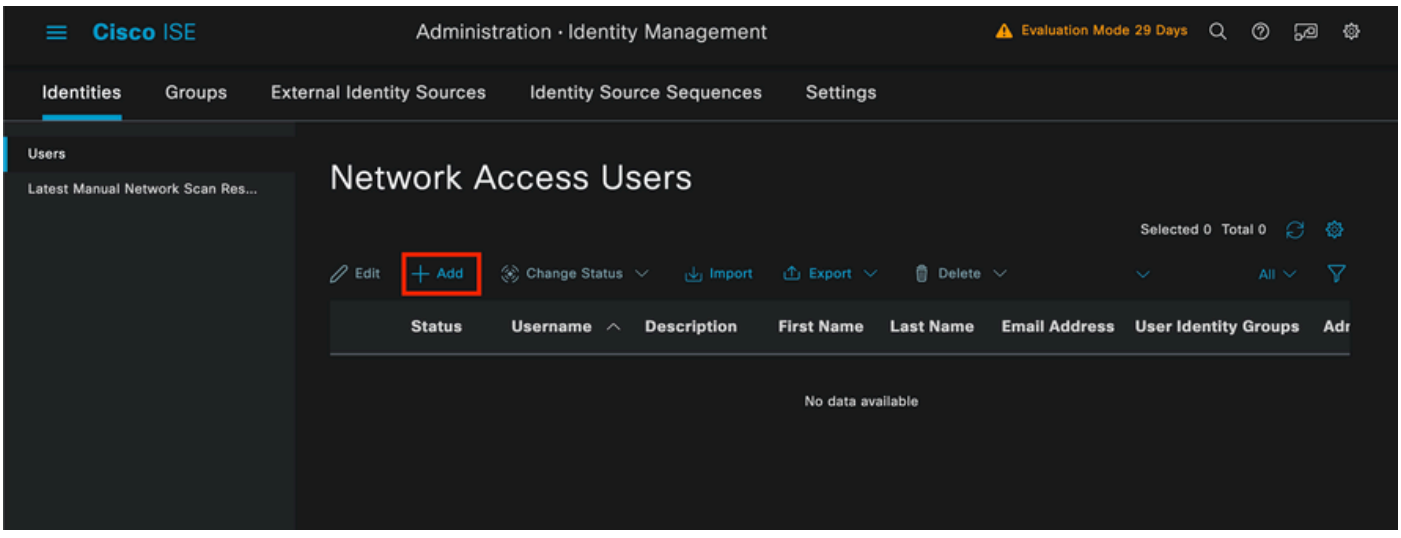


إنشاء مجموعة مستخدمين

انقر فوق الزر إرسال.

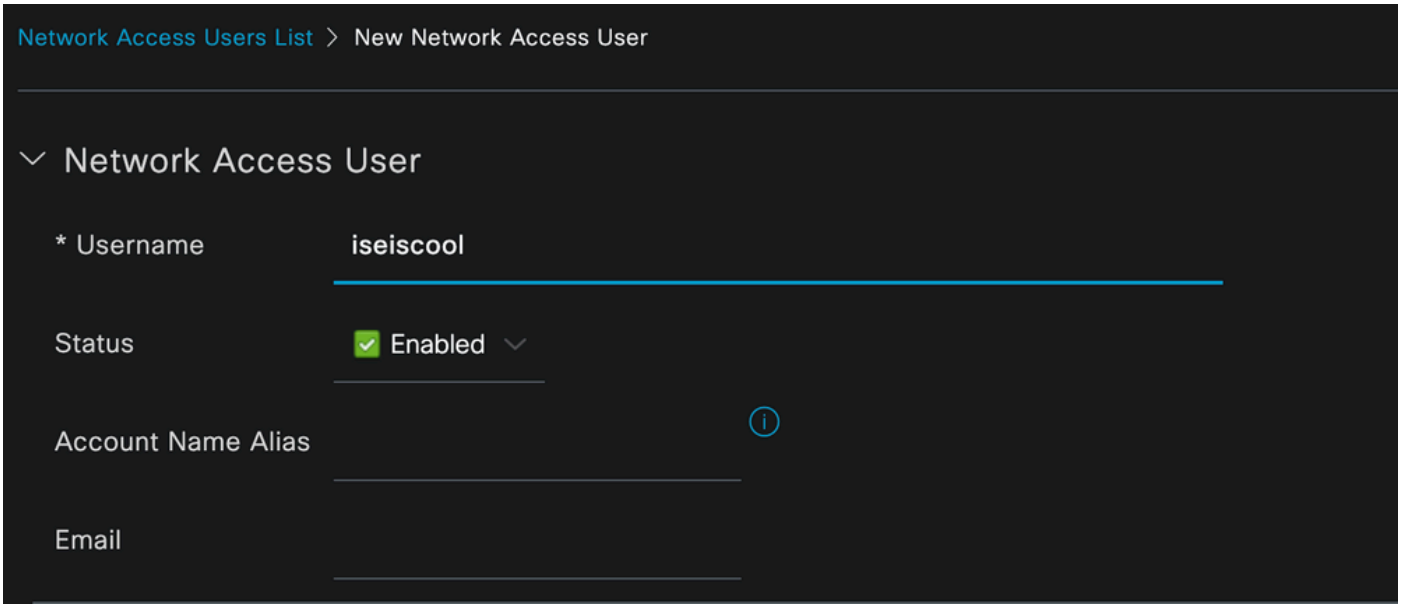
ثم انتقل إلى إدارة > إدارة الهوية > تبويب الهوية.

انقر فوق الزر إضافة.



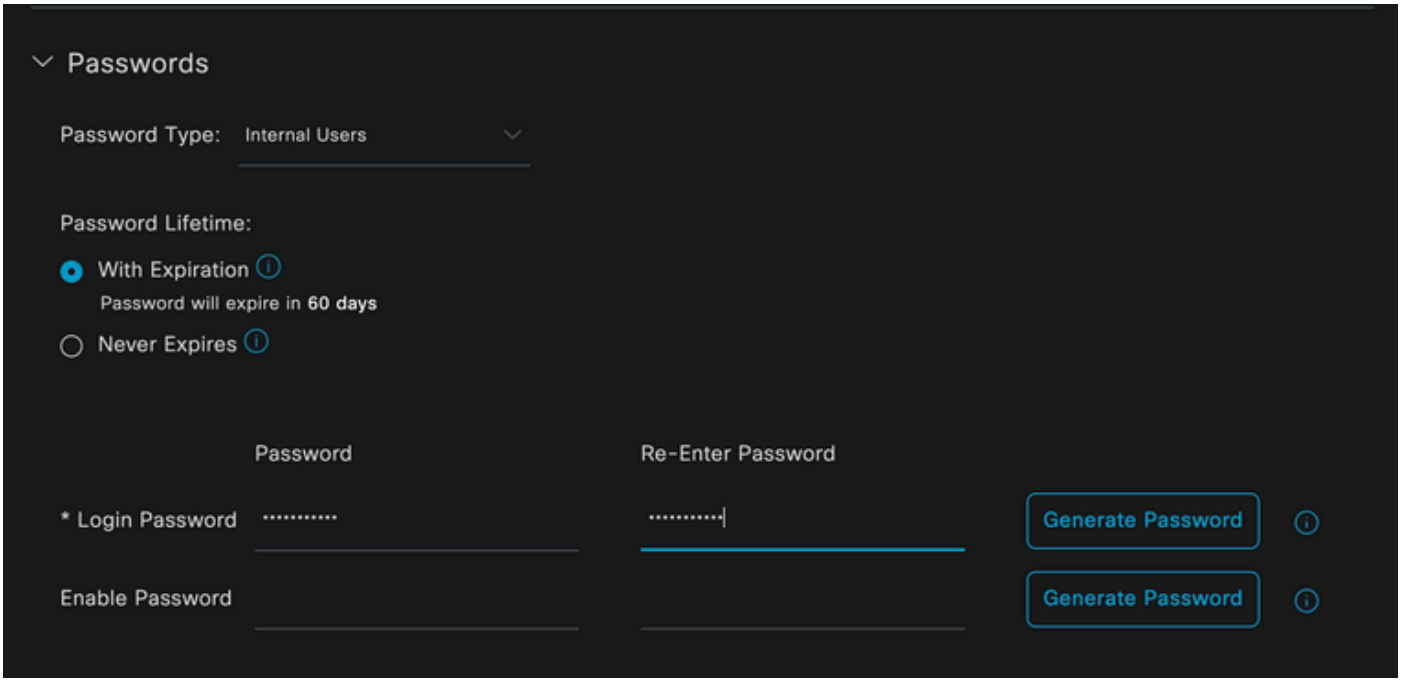
إنشاء المستخدم

كجزء من الحقول الإلزامية، ابدأ باسم المستخدم، يتم إستخدام اسم المستخدم iseiscool في هذا المثال.



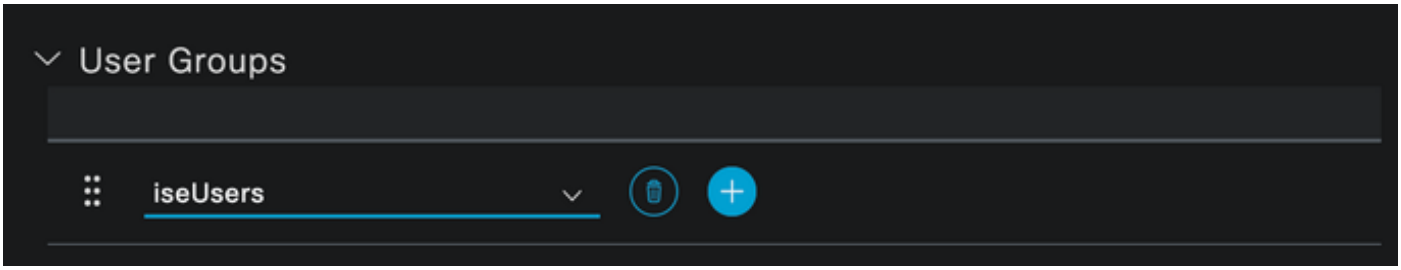
تسمية المستخدم وإنشاؤه

تتمثل الخطوة التالية في تعيين كلمة مرور لاسم المستخدم الذي تم إنشاؤه. VainillaISE97 هو كلمة المرور المستخدمة في هذا العرض التوضيحي.



تعيين كلمة المرور

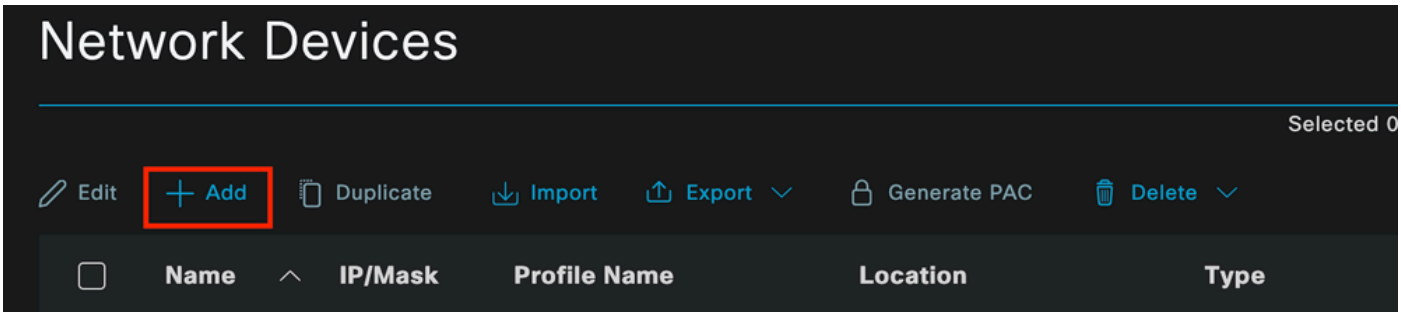
وأخيرا، قم بتعيين المستخدم إلى المجموعة التي تم إنشاؤها مسبقا، والتي هي في هذه الحالة ISEusers.



2. تكوين جهاز الشبكة وإضافته.

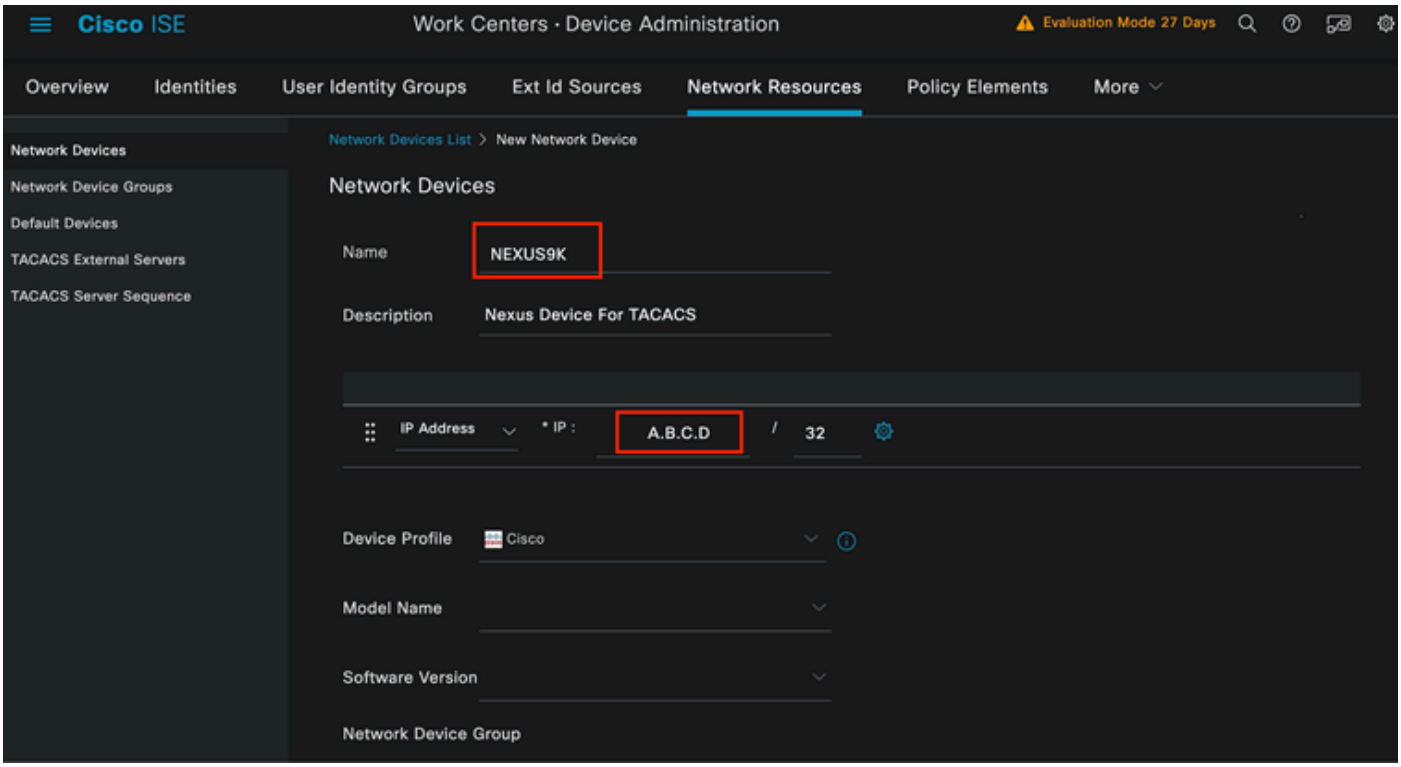
إضافة جهاز Nexus 9000 إلى إدارة ISE > موارد الشبكة > أجهزة الشبكة

انقر فوق الزر إضافة للبدء.



صفحة جهاز الوصول إلى الشبكة

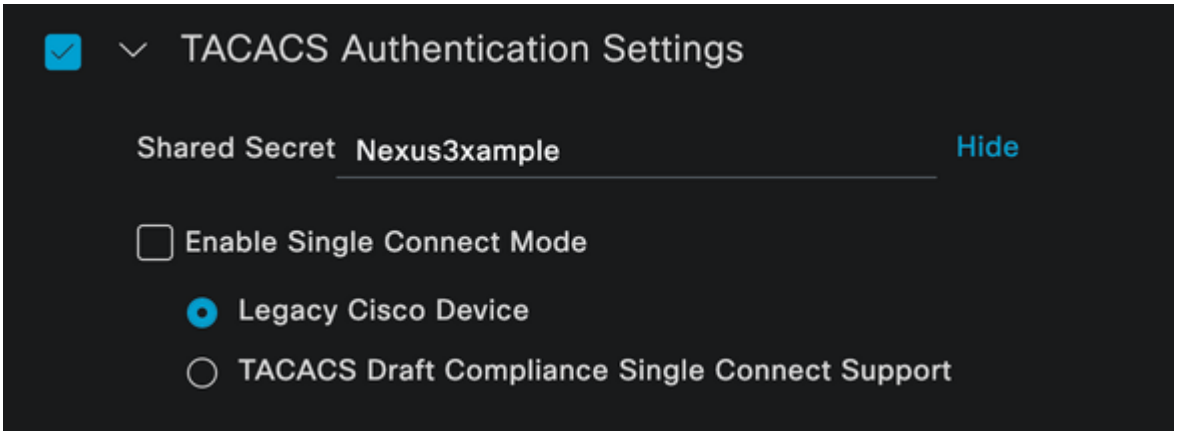
أدخل القيم إلى النموذج، وقم بتعيين اسم إلى NAD الذي تقوم بإنشائه، و IP والذي يتم من خلاله تعيين AND جهات الاتصال لمحادثة TACACS.



تكوين جهاز الشبكة

يمكن ترك الخيارات المنسدلة فارغة ويمكن حذفها، وتهدف هذه الخيارات إلى تصنيف NADs حسب الموقع ونوع الجهاز والإصدار، ثم تغيير تدفق المصادقة استنادا إلى عوامل التصفية هذه.

في الإدارة > موارد الشبكة > أجهزة الشبكة > NAD الخاص بك > إعدادات مصادقة TACACS، أضف السر المشترك الذي أستخدمته تحت تكوين NAD الخاص بك. يستخدم Nexus3xample في هذا العرض التوضيحي.



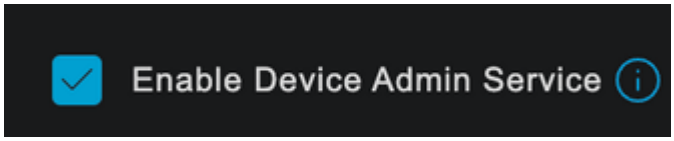
قسم تكوين *TACACS*

احفظ التغييرات بالنقر فوق الزر إرسال.

3. تكوين TACACS على ISE.

تحقق مرتين من أن PSN الذي قمت بتكوينه في Nexus 9k لديه الخيار Device Admin ممكن.

ملاحظة: لا يتسبب تمكين خدمة إدارة الجهاز في إعادة التشغيل على ISE.

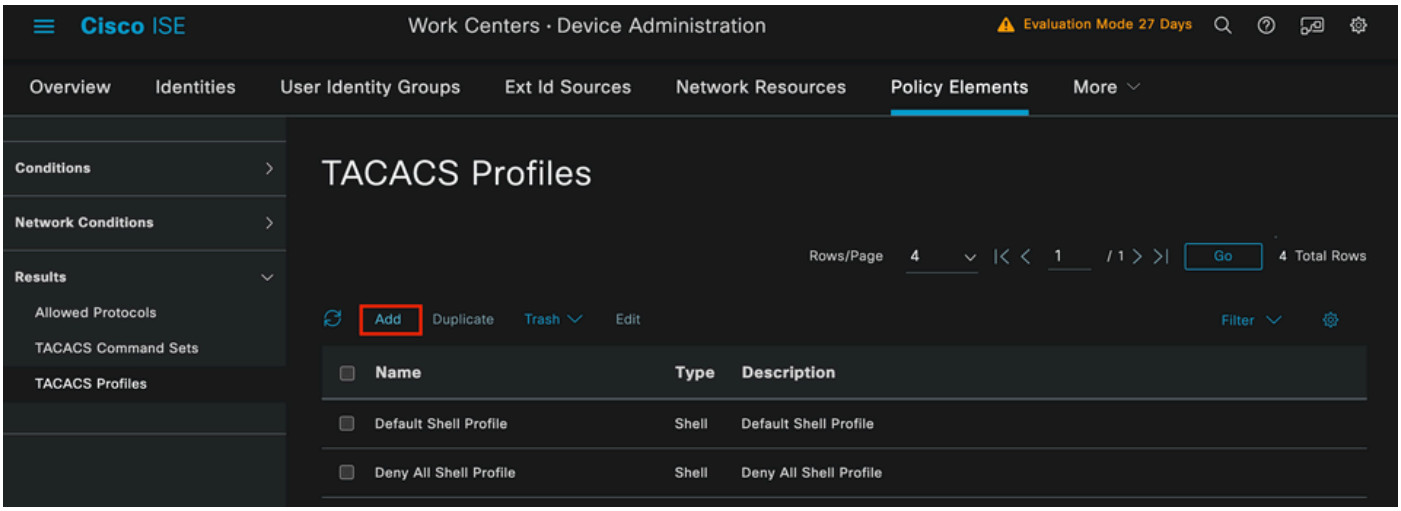


التحقق من ميزة إدارة جهاز PSN

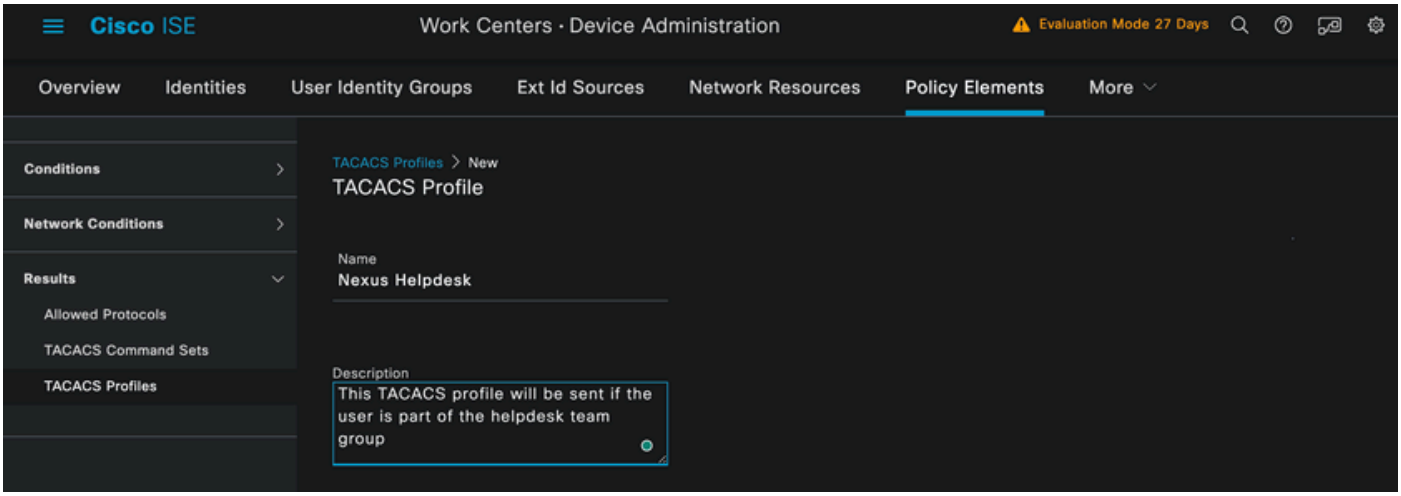
يمكن التحقق من هذا تحت إدارة قائمة ISE > النظام > النشر > PSN الخاص بك > قسم خادم السياسة > تمكين خدمات إدارة الجهاز.

- قم بإنشاء ملف تعريف TACACS، الذي يرجع مكتب مساعدة الدور إلى جهاز Nexus إذا نجحت المصادقة.

من قائمة ISE، انتقل إلى مركز العمل > إدارة الأجهزة > عناصر السياسة > النتائج > ملفات تعريف TACACS وانقر على زر إضافة.



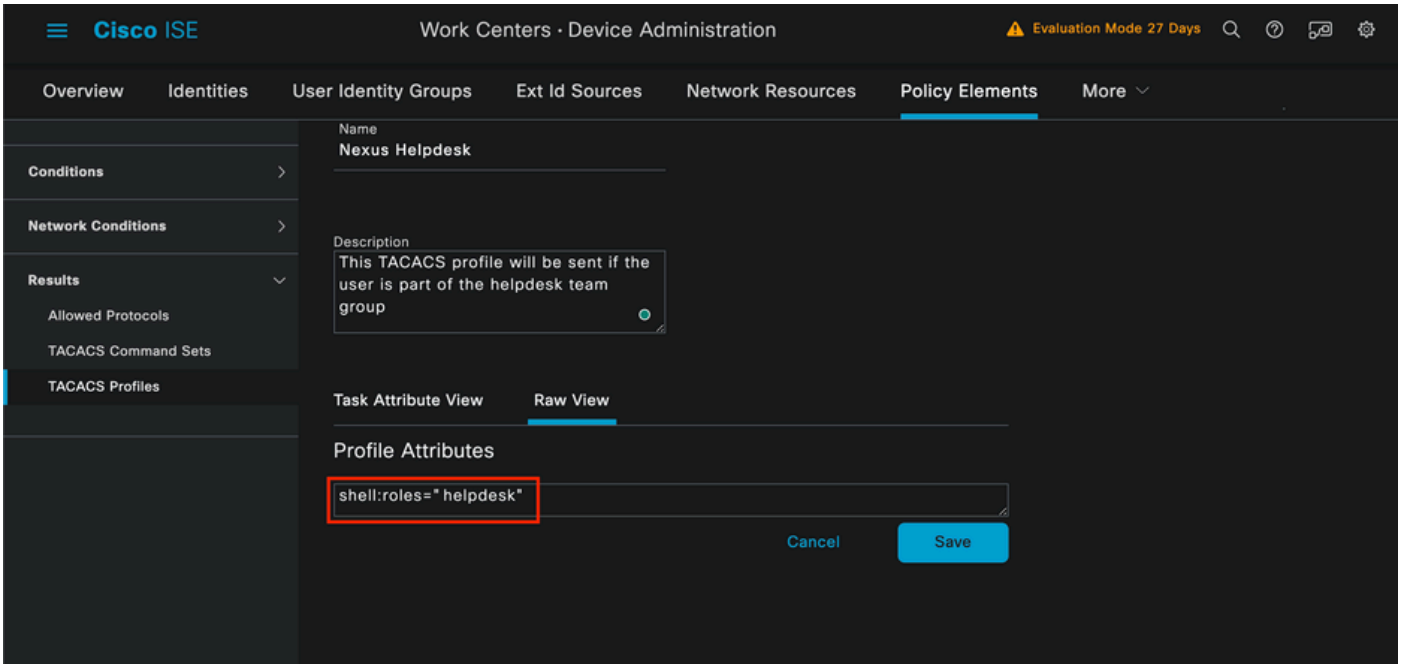
قم بتعيين اسم، ووصف إختياري.



تسمية ملف تعريف TACACS

قم بتجاهل قسم عرض سمة المهمة وانتقل إلى قسم العرض الأولي.

وأدخل القيمة shell:roles="help desk".



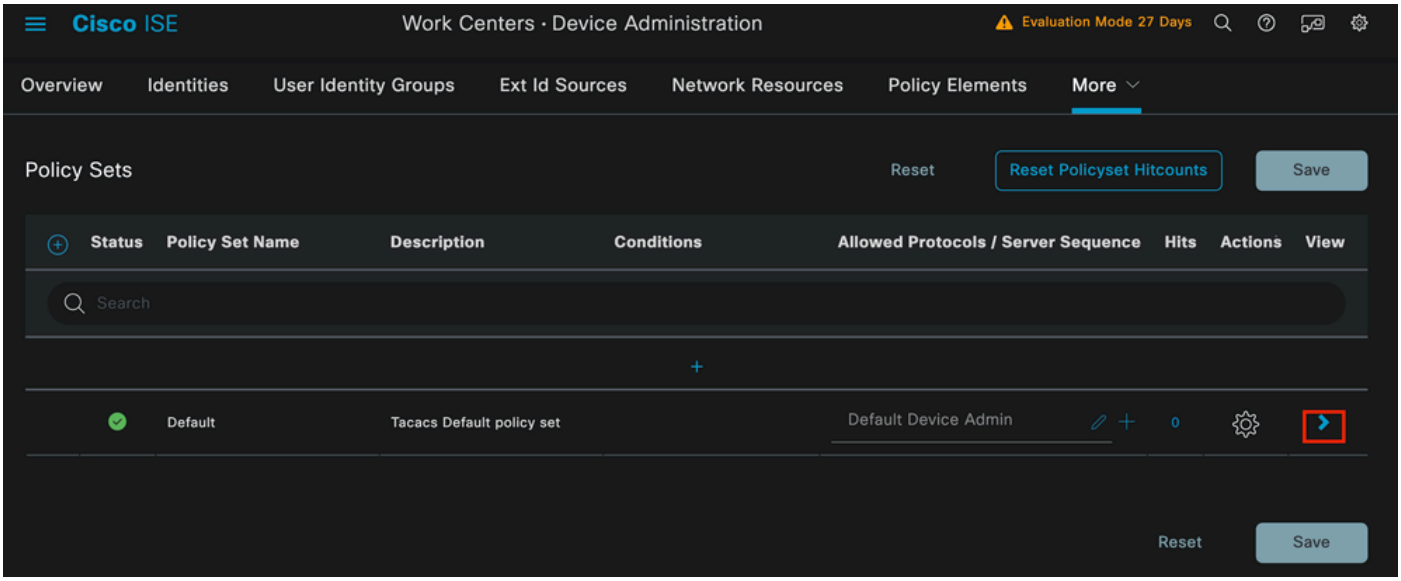
إضافة سمة ملف تعريف

قم بتكوين مجموعة النهج التي تتضمن نهج المصادقة ونهج التخويل.

في مركز عمل الوصول إلى قائمة ISE > إدارة الجهاز > مجموعات نهج إدارة الجهاز.

لأغراض العرض التوضيحي، يتم إستخدام مجموعة النهج الافتراضية. ومع ذلك، يمكن إنشاء مجموعة نهج أخرى، مع شروط لمطابقة سيناريوهات معينة.

انقر فوق السهم في نهاية الصف.

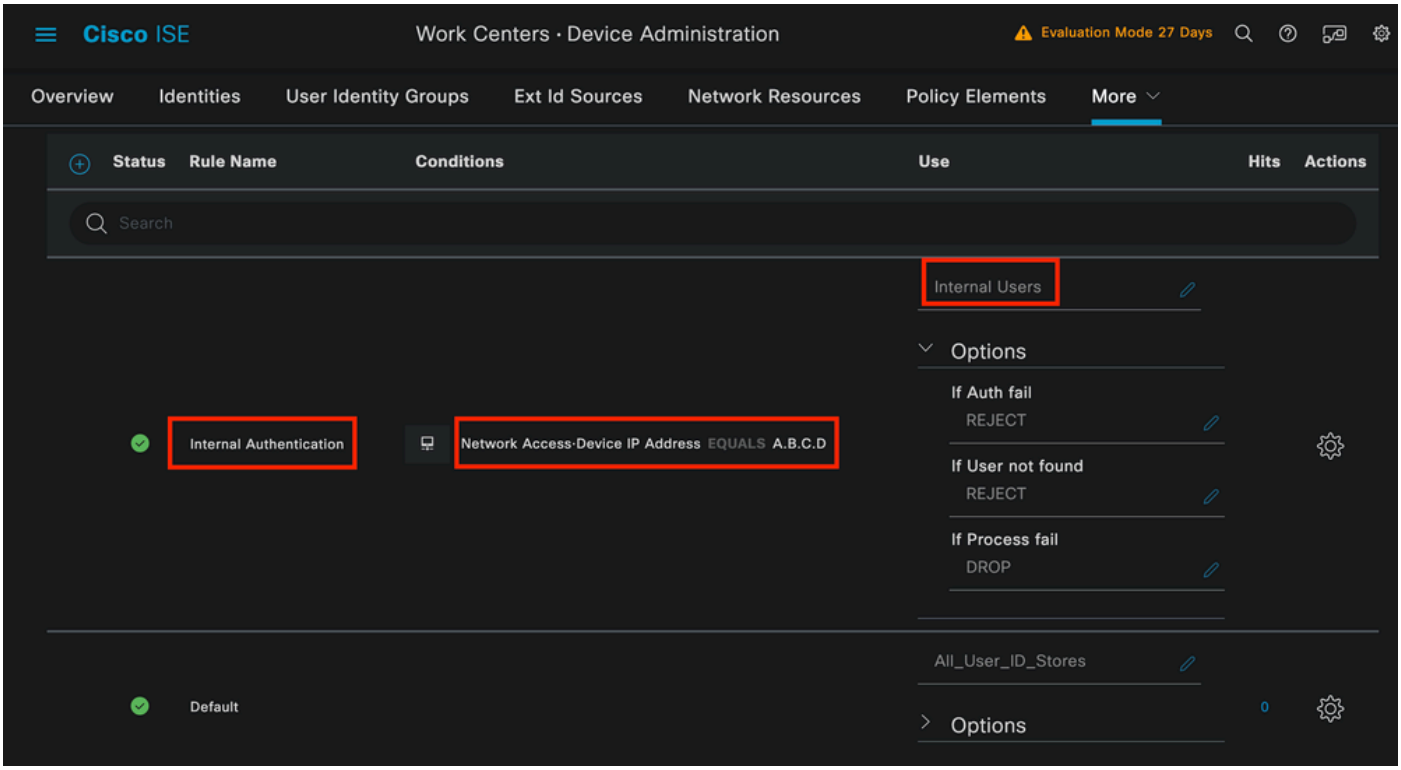


صفحة مجموعات نهج مسؤول الجهاز

بمجرد إدخال تكوين مجموعة السياسات وتخطيطه إلى أسفل وتوسيع قسم سياسة المصادقة.

انقر فوق أيقونة إضافة.

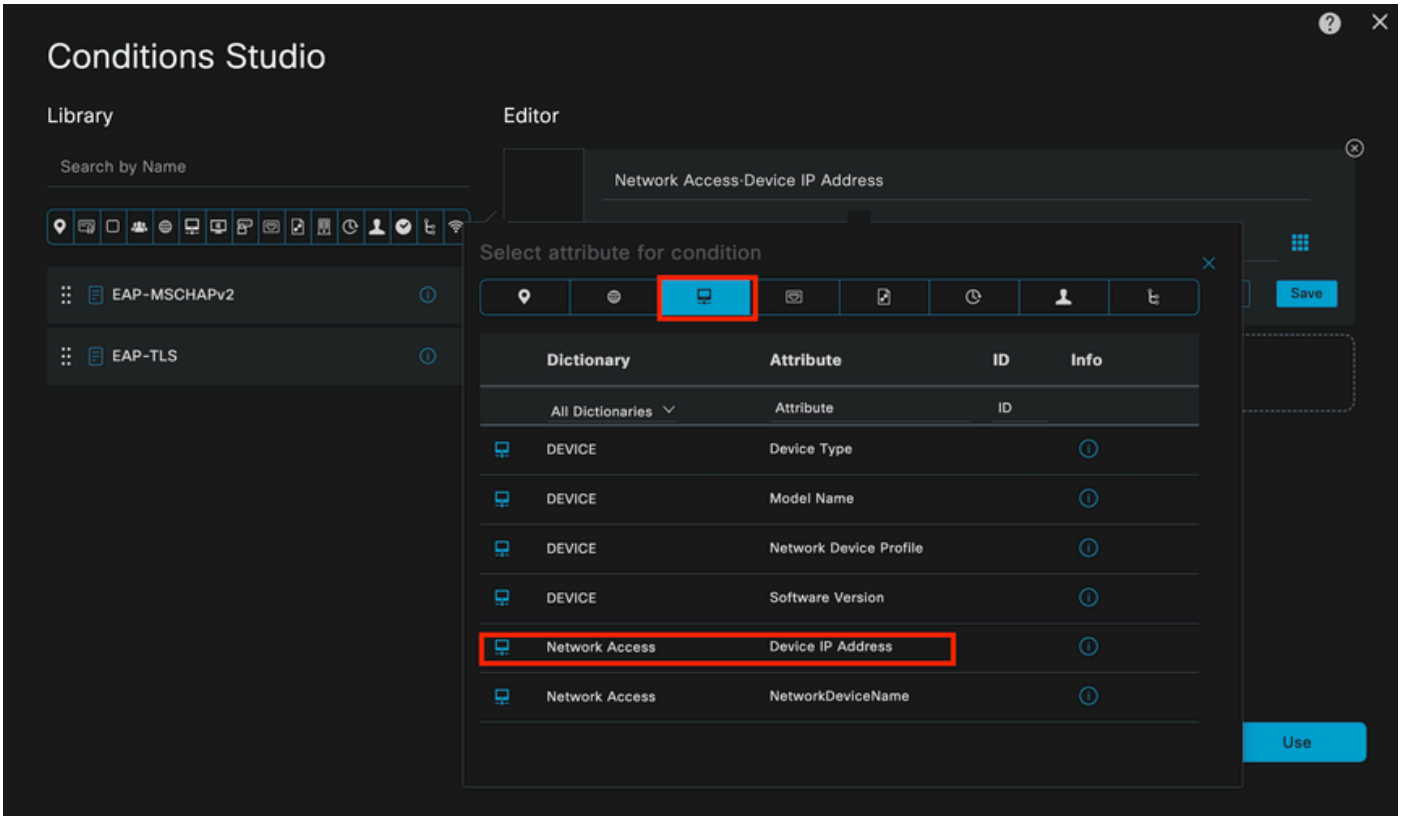
على مثال التكوين هذا، تكون قيمة الاسم هي المصادقة الداخلية والشرط المختار هو IP لجهاز الشبكة (Nexus) (يحل محل a.b.c.d.). يستخدم نهج المصادقة هذا مخزن هوية المستخدمين الداخلي.



نهج المصادقة

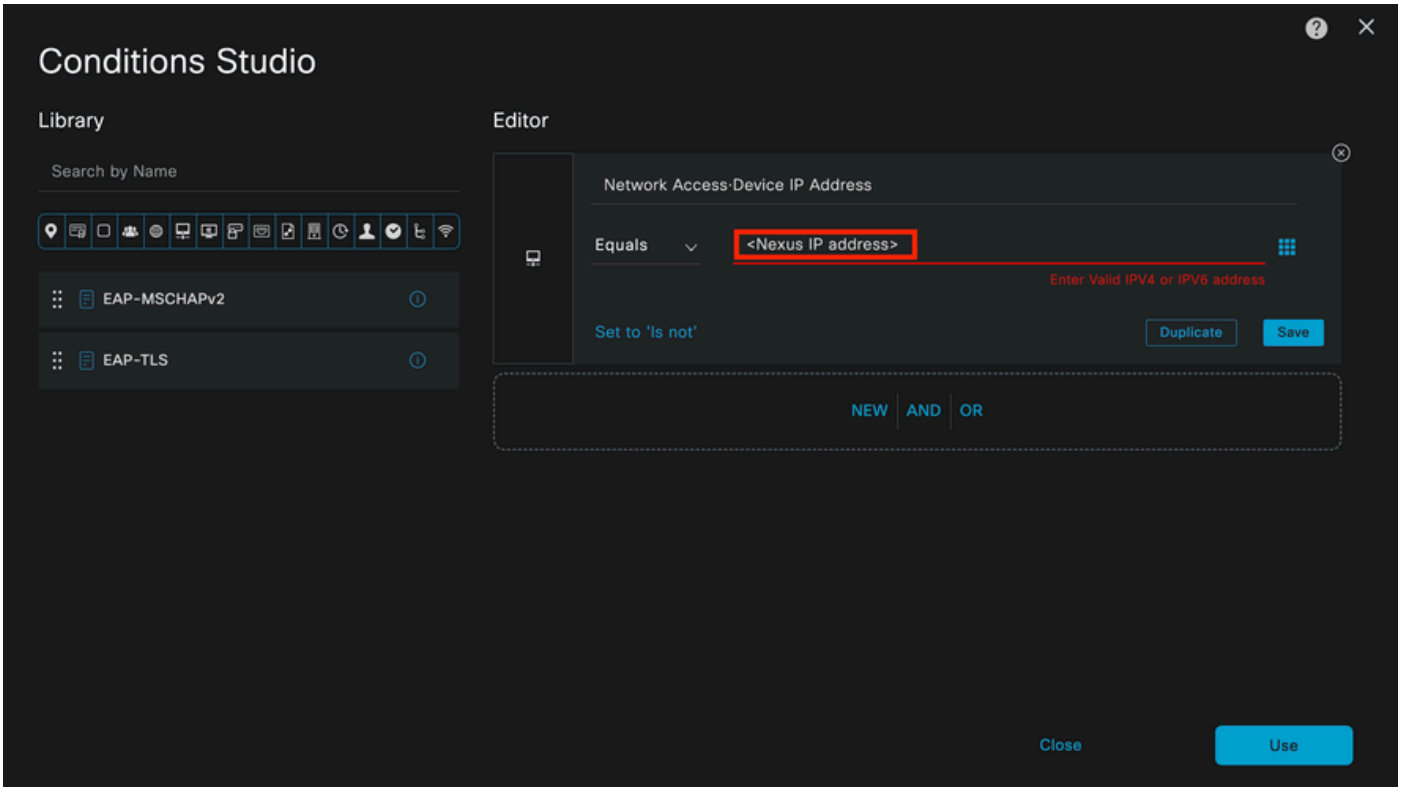
فيما يلي كيفية تكوين الشرط.

حدد الوصول إلى الشبكة > سمة قاموس عنوان IP للجهاز.



أستوديو الشروط لنهج المصادقة

استبدلت ال <Nexus IP عنوان> تعليق مع ال يصح IP.



إضافة عامل تصفية *IP*

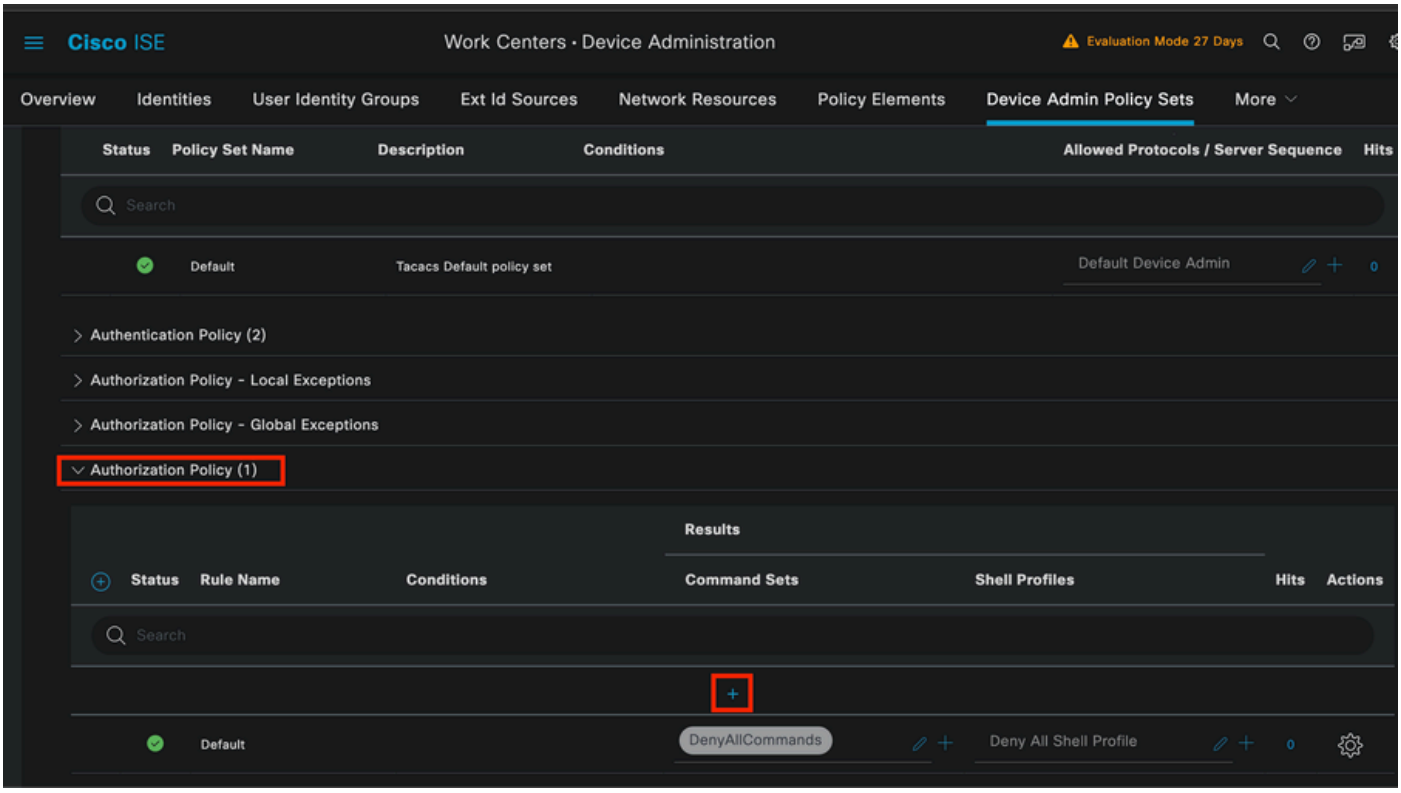
انقر فوق الزر إستخدام".

يتم الوصول إلى هذا الشرط فقط بواسطة جهاز Nexus الذي قمت بتكوينه. ومع ذلك، إذا كان

الغرض وه تمكين هذه الحالة لكمية كبيرة من الأجهزة، فعليك مراعاة شرط مختلف.

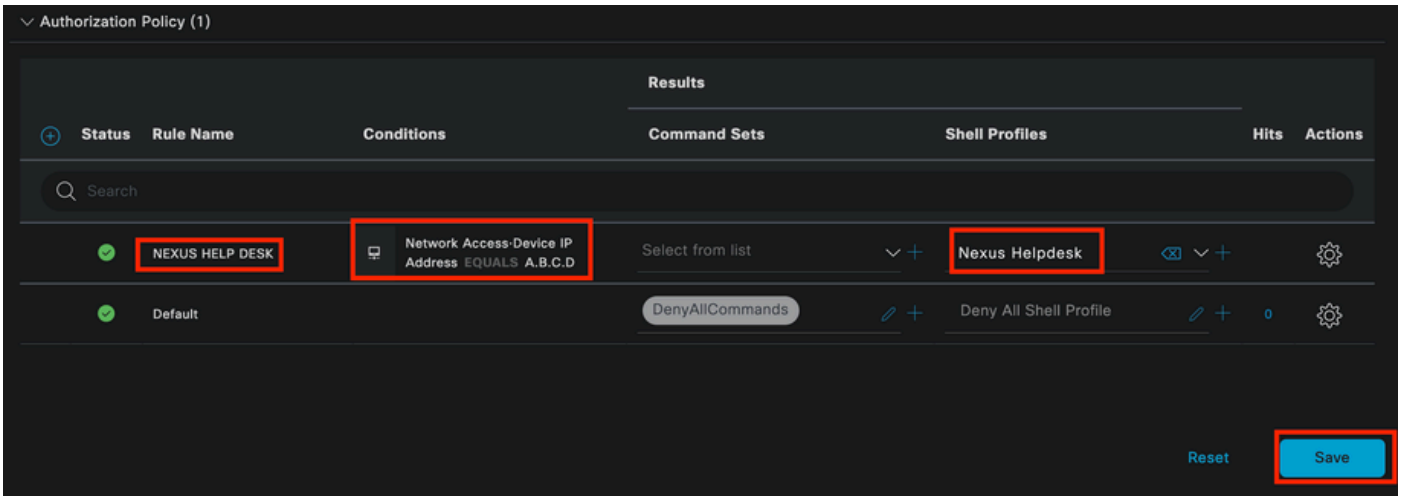
ثم انتقل إلى قسم نهج التخويل وقم بتوسيعه.

انقر على أيقونة + (زائد).



قسم نهج التخويل

في هذا المثال، تم إستخدام مكتب تعليمات Nexus كاسم لنهج التخويل.



أستوديو الشروط لنهج التخويل

يتم إستخدام نفس الشرط الذي تم تكوينه في نهج المصادقة لنهج التخويل.

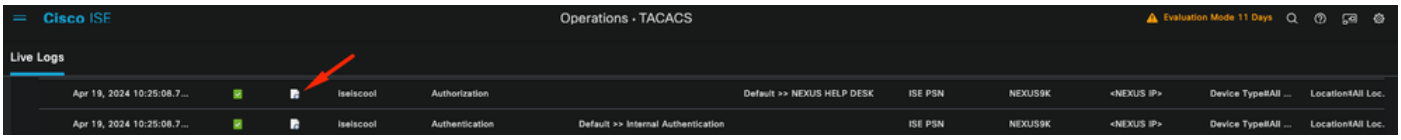
في عمود "ملفات تعريف Shell"، تم تحديد ملف التعريف الذي تم تكوينه قبل تحديد مكتب الدعم ل Nexus.

أخيرا، انقر زر حفظ.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

من واجهة المستخدم الرسومية (ISE)، انتقل إلى العمليات > TACACS > السجلات المباشرة. حدد السجل الذي يطابق اسم المستخدم المستخدم، وانقر فوق تفاصيل سجل Live الخاصة بحدث التفويض.



سجل Tacacs Live

وكجزء من التفاصيل التي يتضمنها هذا التقرير، يمكن العثور على قسم الاستجابة ، حيث يمكنك مشاهدة كيفية قيام ISE بإرجاع القيمة shell:roles="help desk"

Response	{Author-Reply-Status=PassRepl; AVPair=shell:roles=" helpdesk" ; }

الاستجابة لتفاصيل السجل النشط

على جهاز Nexus:

```
Nexus9000 login: iseiscool
   Password: VainillaISE97

                                    Nexus9000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
                    Nexus9000(config)# interface ethernet 1/23
                                  % Interface permission denied

                                       Nexus9000(config)# ?
                                interface  Configure interfaces
                    show        Show running system information
                                     end        Go to exec mode
                      exit       Exit from command interpreter

                             Nexus9000(config)# role name test
                              % Permission denied for the role

                                            Nexus9000(config)#

                          Nexus9000(config)# interface loopback 0
                                  % Interface permission denied

                                            Nexus9000(config)#
                                             Nexus9000# conf t

                        Nexus9000(config)# interface ethernet 1/5
```

```
Notice that only the commands allowed are listed.
                            Nexus9000(config-if)# ?

   no        Negate a command or set its defaults
      show      Show running system information
          shutdown  Enable/disable an interface
                       end       Go to exec mode
            exit      Exit from command interpreter

                               Nexus9000(config-if)# cdp
                          Nexus9000(config-if)# cdp enable
                          % Permission denied for the role
                                Nexus9000(config-if)#
```

استكشاف الأخطاء وإصلاحها

- تحقق من إمكانية الوصول إلى ISE من جهاز Nexus:

Nexus 9000# ping <ISE IP الخاص بك>
يتم إختبار اتصال <ISE IP> (<ISE IP الخاص بك> 56 بايت من البيانات

ةيناثلي ملل time=1.22 ttl=59 icmp_seq=0 : <ISE IP الخاص بك> من تاي باب 64
ةيناثلي ملل time=0.739 ttl=59 icmp_seq=1 : <ISE IP الخاص بك> من تاي باب 64
ةيناثلي ملل time=0.686 ttl=59 icmp_seq=2 : <ISE IP الخاص بك> من تاي باب 64
ةيناثلي ملل time=0.71 ttl=59 icmp_seq=3 : <ISE IP الخاص بك> من تاي باب 64
ةيناثلي ملل time=0.72 ttl=59 icmp_seq=4 : <ISE IP الخاص بك> من تاي باب 64

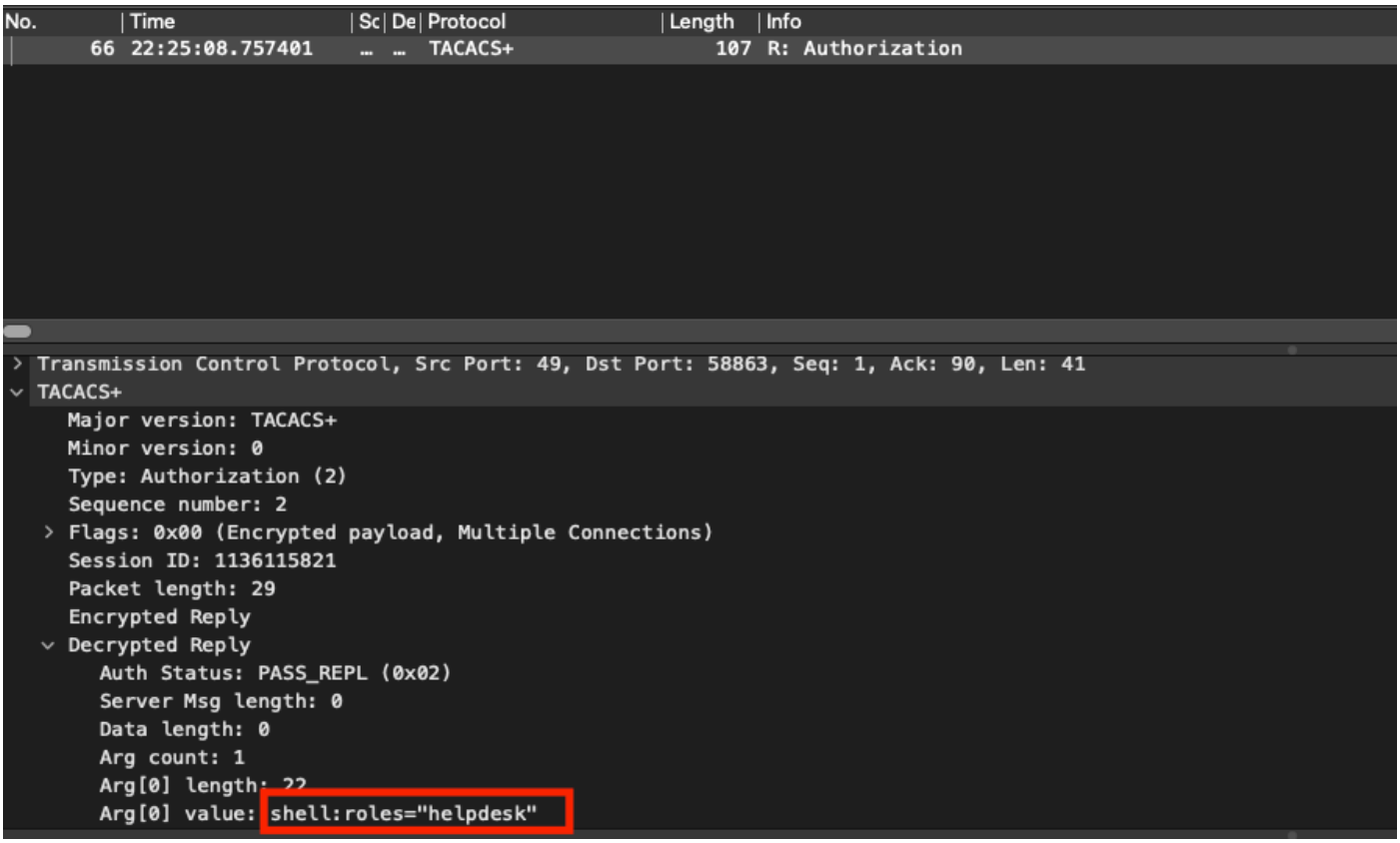
- :ةادأ nexus وال ISE نيب ،49 ءانيم حتف نأ ،تقد
49 <Your ISE IP> Telnet جمانرب #Nexus 9000
... <ISE IP> ةلواحم نآلا متي
. <ISE IP الخاص بك> ب لصتم
.'^]' وه بورهلا فرح

- :أستخدم تصحيح الأخطاء التالي

debug tacacs+ all
Nexus 9000#
Nexus 9000# 2024 apr 19 22:50:44.199329 tacacs: event_loop(): إستدعاء process_rd_fd_set
2024 أبريل 19:50:44.199355 tacacs: process_rd_fd_set: إستدعاء در الاتصال ل FD 6
2024 أبريل 19:50:44.199392 tacacs: FSRV ال يستهلك 8421 opcode
2024 أبريل 19:50:44.199406 tacacs: process_implicit_cfs_session_start: يتم الآن الدخول...
2024 أبريل 19:50:44.199414 tacacs: process_implicit_cfs_session_start: الخروج؛ نحن بحالة عدم القدرة على التوزيع
2024 أبريل 19:50:44.199424 tacacs: process_aaa_tplus_request: الدخول لمعرفة جلسة عمل AAA 0
2024 أبريل 19:50:44.199438 tacacs: process_aaa_tplus_request:التحقق من حالة المنفذ مجموعة الخوادم IsePsnServers باستخدام mgmt0
2024 أبريل 19:50:44.199451 tacacs: tacacs_global_config(4220): إدخال ...
2024 أبريل 19:50:44.199466 tacacs: tacacs_global_config(4577): get_req...
2024 أبريل 19:50:44.208027 tacacs: tacacs_global_config(4701): إستعادة قيمة الإرجاع الخاصة بعملية تكوين البروتوكول العام:النجاح
2024 أبريل 19:50:44.208045 tacacs: tacacs_global_config(4716): req:num لدان 0
2024 أبريل 19:50:44.208054 tacacs: tacacs_global_config: req:num مجموعة 1
2024 أبريل 19:50:44.208062 tacacs: tacacs_global_config: req:num مهلة 5
2024 أبريل 19:50:44.208070 tacacs: tacacs_global_config: req:num deadtime 0
2024 أبريل 19:50:44.208078 tacacs: tacacs_global_config: req:num encryption_type 7
2024 أبريل 19:50:44.208086 tacacs: tacacs_global_config: إرجاع ريتفافل 0
2024 أبريل 19:50:44.208098 tacacs: يتم تعميم process_aaa_tplus_request:group_info في IsePsnServers مجموعة الخوادم المستخدمة يتم لذلك ،aaa_req،
2024 أبريل 19:50:44.208108 tacacs: tacacs_servergroup_config: إدخال لمجموعة الخوادم،

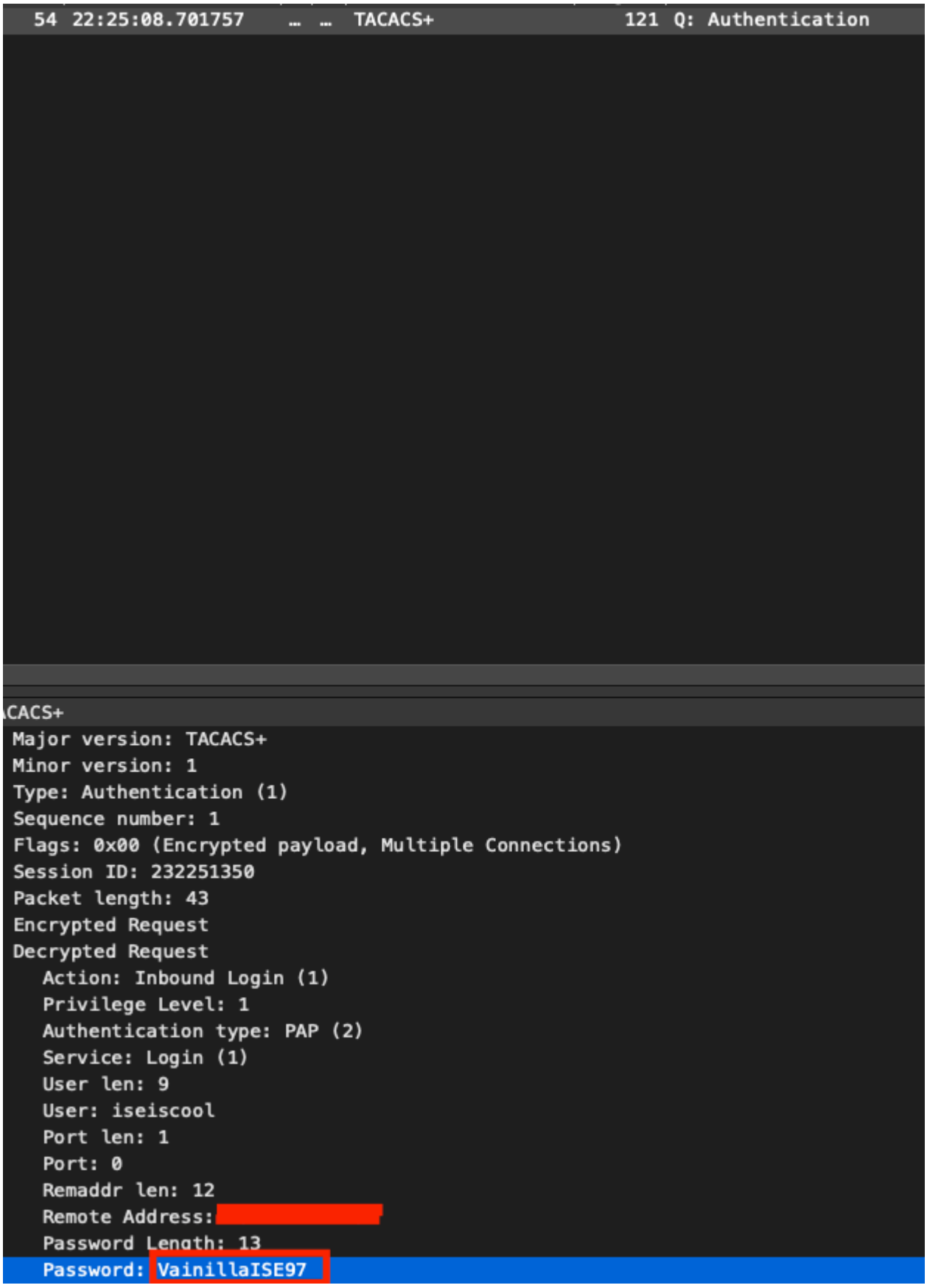
0 سرهفلا
ةعومجم سرهفل GetNext_REQ :tacacs_servergroup_config: 19:50:44.208117 tacacs: 2024 لريبمأ
:مسالا 0:لوكوتوربلا مداوخ
ال = syserr2str 4048003 = rcode :tacacs_pss2_move2key: 19:50:44.208148 tacacs: 2024 لريبمأ
اذه PSS حاتفم دجوي
pss2_getkey ب لاتصالا :tacacs_pss2_move2key: 19:50:44.208160 tacacs: 2024 لريبمأ
ىلع GetNext_REQ تحلص :tacacs_servergroup_config: 19:50:44.208171 tacacs: 2024 لريبمأ
فرهس مجموعة مداوخ البروتوكول:2 name:IsePsnServers
ةمئاقلا عيمجتسإ :tacacs_servergroup_config: 19:50:44.208184 tacacs: 2024 لريبمأ
عبعملية مجموعة البروتوكول:نجاح
ةعومجمل 0 ةمئاق عيجار عيجار :tacacs_servergroup_config: 19:50:44.208194 tacacs: 2024 لريبمأ
IsePsnServers:تالوكوتوربلا مداوخ
تم العثور على IsePsnServers :process_aaa_tplus_request: 19:50:44.208210 tacacs: 2024 لريبمأ
0 وه source-intf ،رييصقت وه قفاوتملا VRF .ةعومجملل
mgmt0 دوجو نم ققحتلا :process_aaa_tplus_request: 19:50:44.208224 tacacs: 2024 لريبمأ
ةبولطملا ةعومجملل يضارتفالا vrf:لباقم ةرادإلا vrf:
83886080 :process_aaa_tplus_request:mgmt_if 19:50:44.208256 tacacs: 2024 لريبمأ
src_intf ،0 :process_aaa_tplus_request:global_src_intf 19:50:44.208272 tacacs: 2024 لريبمأ
يضارتفالا وه vrf_name و 0 وه يلحملا
فرعملل لوخدلا :create_tplus_req_state_machine(902): 19:50:44.208286 tacacs: 2024 لريبمأ
0 AAA ةسلج عمل
0 ةلاحلا ةزهجأ ددع :tacacs: 19:50:44.208295 لريبمأ 2024
فرعملل لوخدلا :init_tplus_req_state_machine: 19:50:44.208307 tacacs: 2024 لريبمأ
0 AAA ةسلج عمل
بجيو NULL وه tplus_ctx):init_tplus_req_state_machine(1298): 19:50:44.208317 tacacs: 2024 لريبمأ
رابتخالاو فلؤملا ةلاح يف نوكي نأ
مداوخ ةعومجم ىلإ لوخدلا :tacacs_servergroup_config: 19:50:44.208327 tacacs: 2024 لريبمأ
0 سرهفلا ،IsePsnServers
ةعومجم سرهفل GET_REQ :tacacs_servergroup_config: 19:50:44.208339 tacacs: 2024 لريبمأ
name:IsePsnServers:0 لوكوتوربلا مداوخ
مداوخ ةعومجمل لوخدلا :find_tacacs_servergroup: 19:50:44.208357 tacacs: 2024 لريبمأ
ISEpsnServers
نجاح = syserr2str 0 = rcode :tacacs_pss2_move2key: 19:50:44.208372 tacacs: 2024 لريبمأ
مداوخ ةعومجمل جورخلا :find_tacacs_servergroup: 19:50:44.208382 tacacs: 2024 لريبمأ
2 وه IsePsnServers
أطخ :tacacs_servergroup_config: get_req: 19:50:44.208401 tacacs: 2024 لريبمأ
IsePsnServers تالوكوتوربلا مداوخ ةعومجمل 0 find_tacacs_servergroup
نجاح = syserr2str 0 = rcode :tacacs_pss2_move2key: 19:50:44.208420 tacacs: 2024 لريبمأ
سرهف ىلع GET_REQ تحلص :tacacs_servergroup_config: 19:50:44.208433 tacacs: 2024 لريبمأ
name:IsePsnServers:2 لوكوتوربلا مداوخ ةعومجم
22:5 19 لريبأ 2024 22:52024 19 لريبأ 2024 ريبمأ 2024
Nexus 9000#

- تنفيذ التقاط حزمة. (للاطلاع على تفاصيل الحزمة، يجب عليك تغيير تفضيلات Wireshark TACACS+، وتحديث المفتاح المشترك المستخدم من قبل Nexus و ISE.)



حزمة تفويض TACACS

- تحقق من أن المفتاح المشترك هو نفسه على جانب ISE و Nexus. يمكن أيضا إعادة هذه في Wireshark.



حزمة المصادقة

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).