تكوين دور TACACS المخصص ل Nexus 9k باستخدام ISE 3.2

المحتويات

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:

- Cisco Nexus 9000، ملف صورة NXOS هو: bootflash:///nxos.9.3.5.bin
- 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:

NX-OS من Cisco - TACACS+ الـ يتطلب أي ترخيص.

Cisco Identity Service Engine (محرك خدمة الهوية من Cisco) - بالنسبة لتثبيتات ISE الجديدة، يتوفر لديك ترخيص فترة تقييم لمدة 90 يوما لديه حق الوصول إلى جميع ميزات ISE، إذا لم يكن لديك ترخيص تقييمي، لاستخدام ميزة ISE TACACS، فأنت بحاجة إلى ترخيص مسؤول جهاز لعقدة خادم النهج التي تقوم بالمصادقة.

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

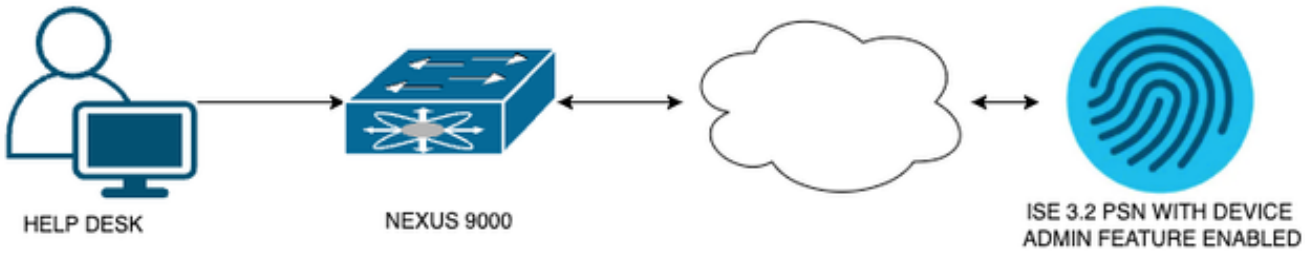
يمكن للمستخدم المعين بهذا الدور تنفيذ أستكشاف الأخطاء وإصلاحها الأساسية وإرجاع منافذ معينة.

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

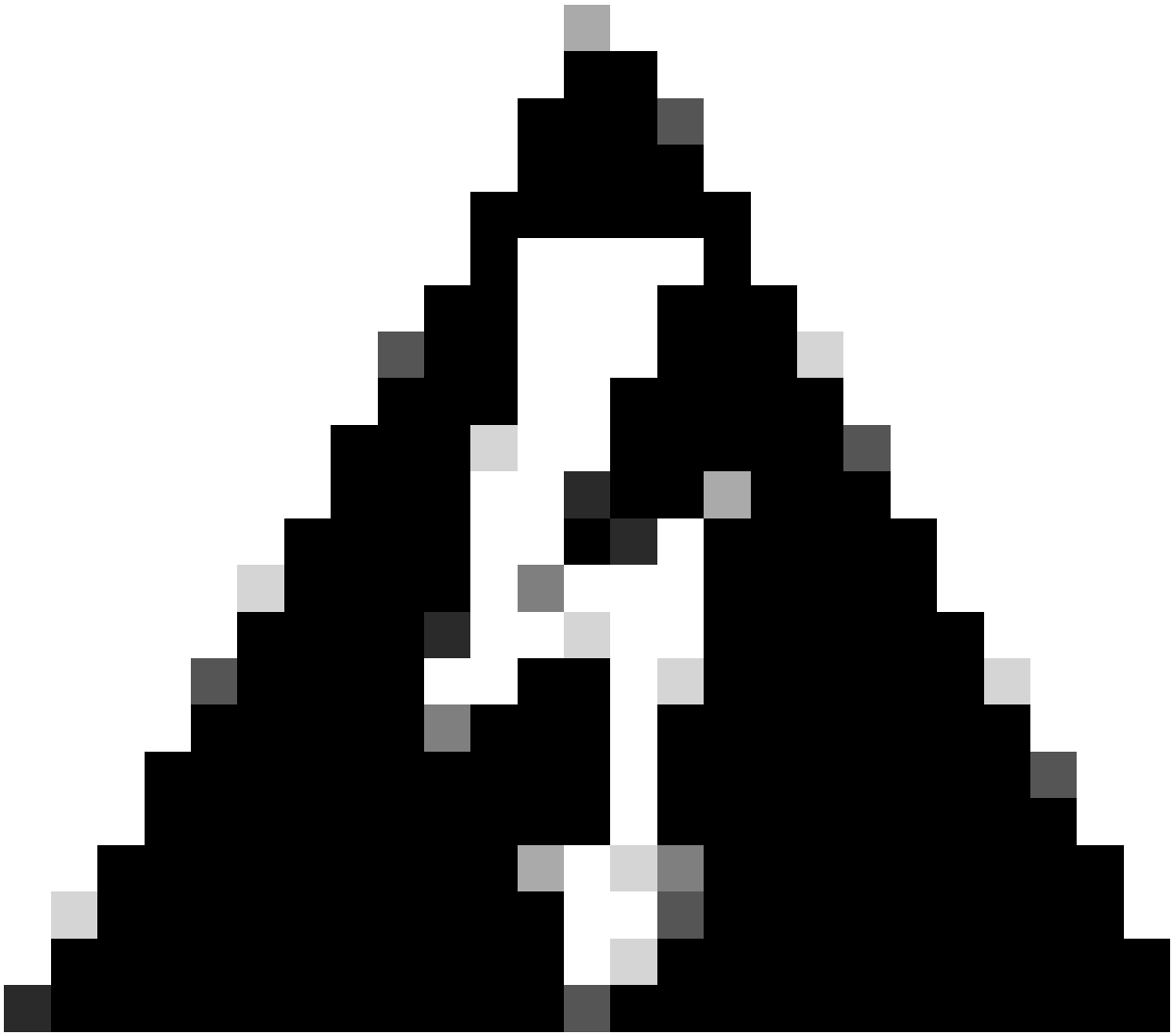
التكوين

الرسم التخطيطي للشبكة



الخطوة 1: تكوين Nexus 9000

1. تكوين 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.

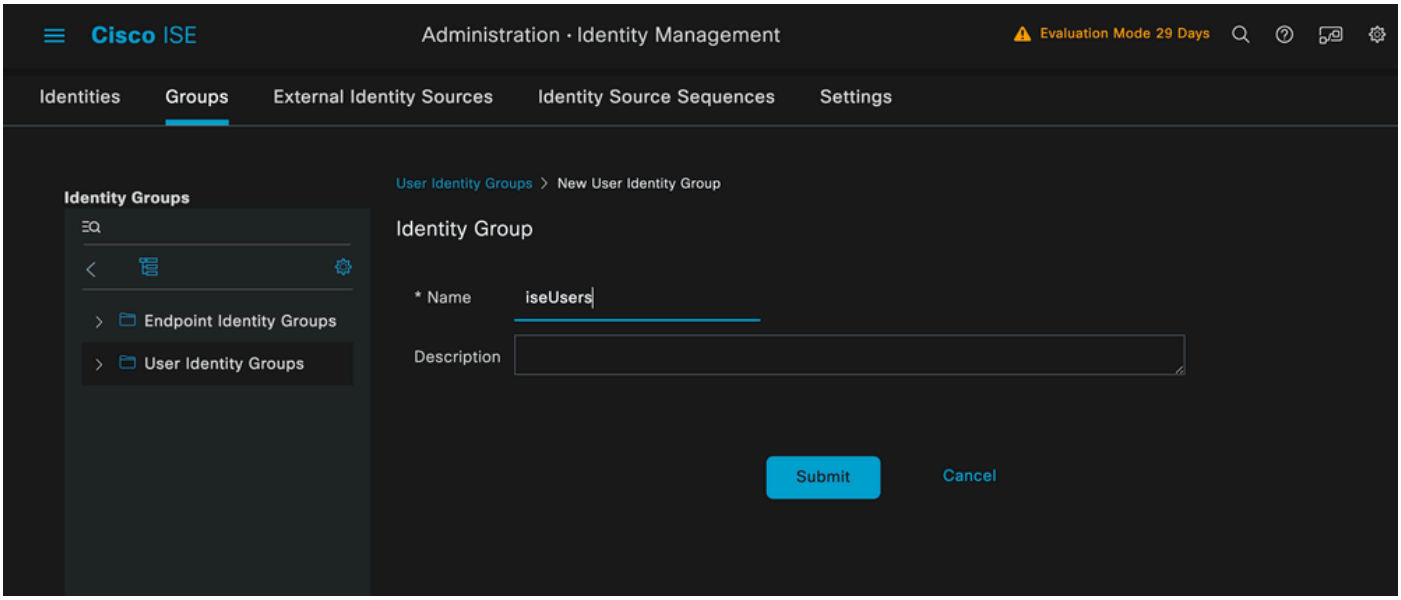
```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#   description Can perform basic Toubleshooting and bounce certain  ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# 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.

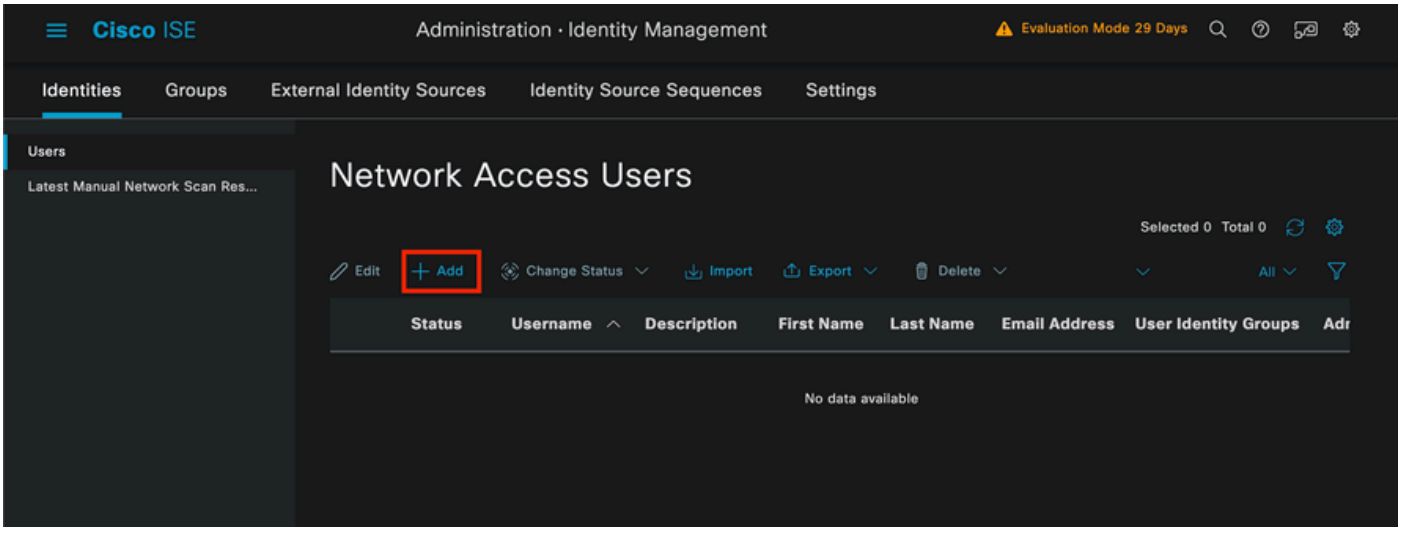


إنشاء مجموعة مستخدمين

انقر فوق الزر إرسال.

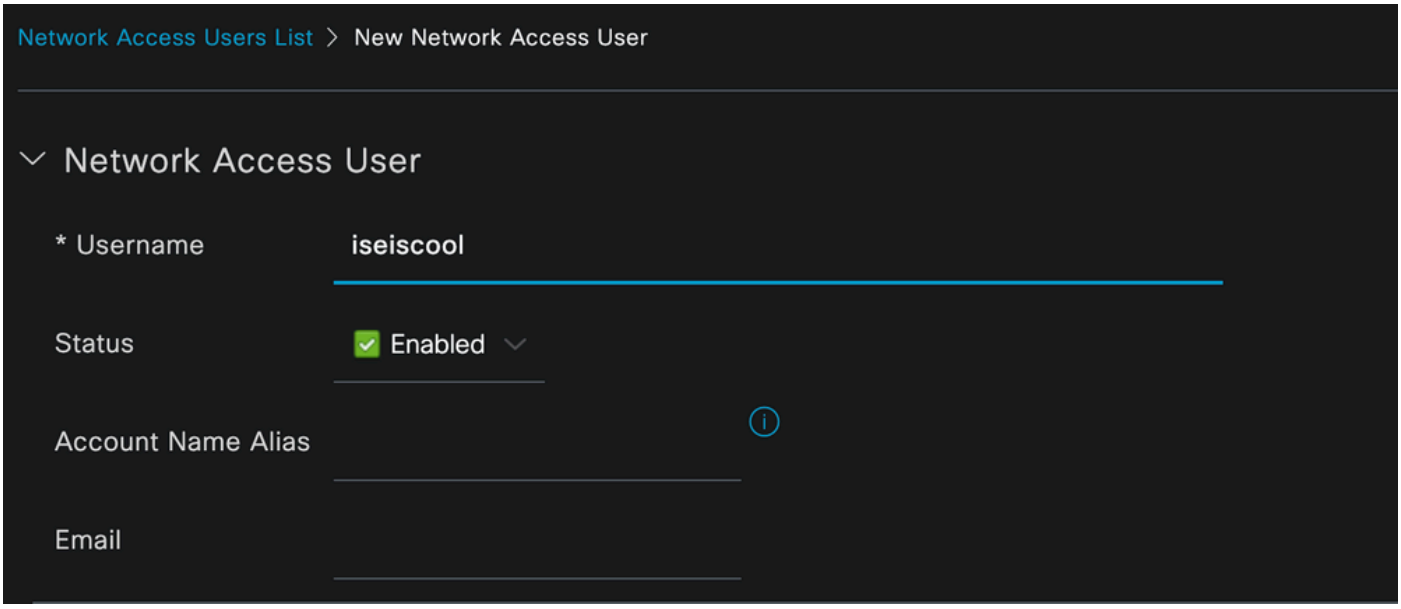
ثم انتقل إلى إدارة > إدارة الهوية > تعريف الهوية.

اضغط على الزر إضافة.



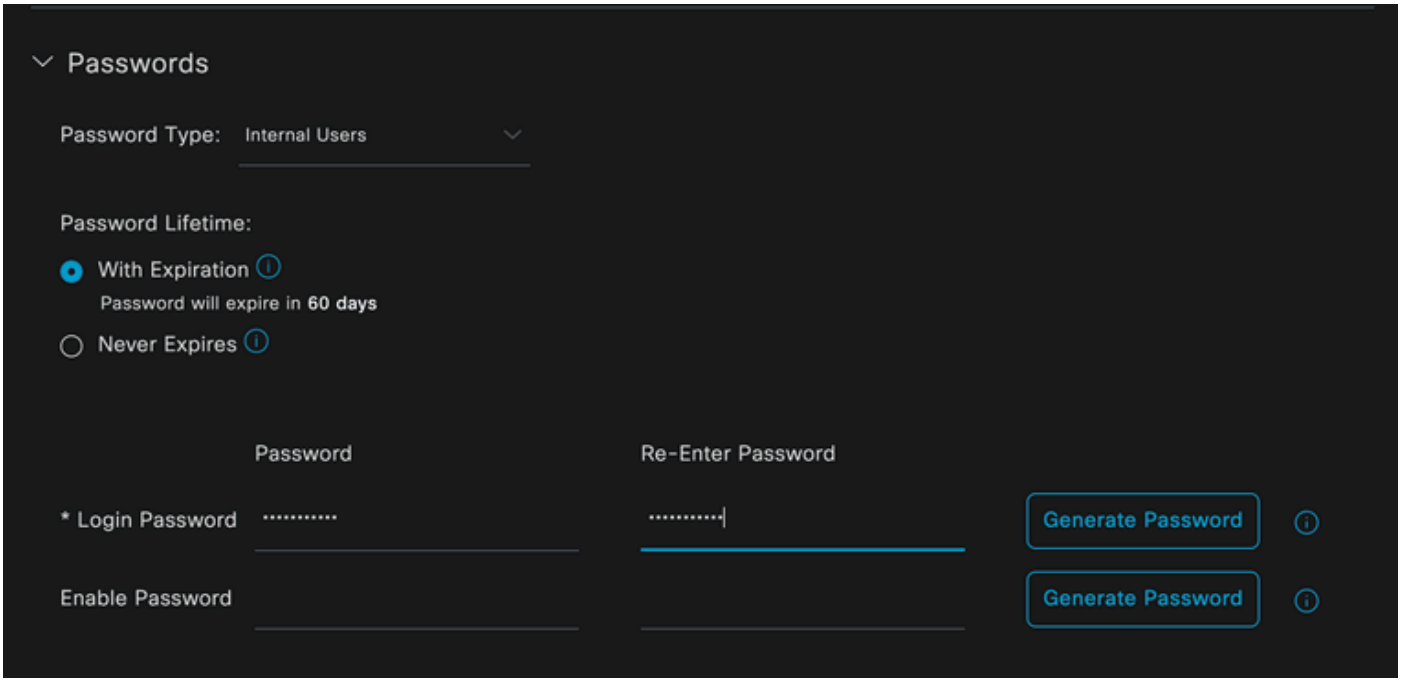
إنشاء المستخدم

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



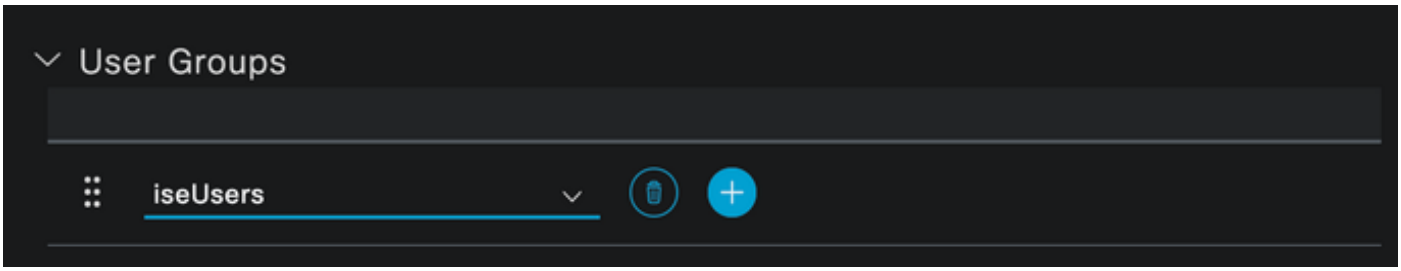
تسمية المستخدم وإنشاؤه

الخطوة التالية هي تعيين كلمة مرور إلى اسم المستخدم الذي تم إنشاؤه، VainillaISE97 وهو 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.

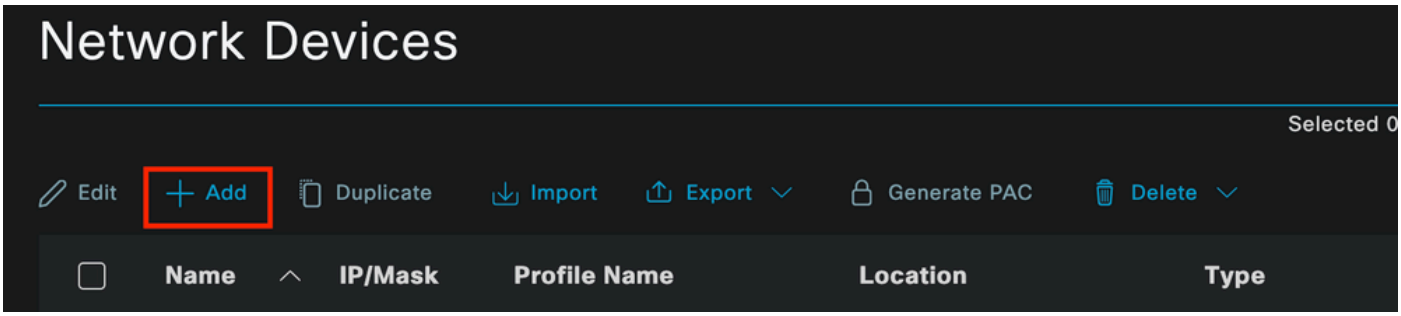


إحالة جماعية

2. تكوين جهاز الشبكة وإضافته.

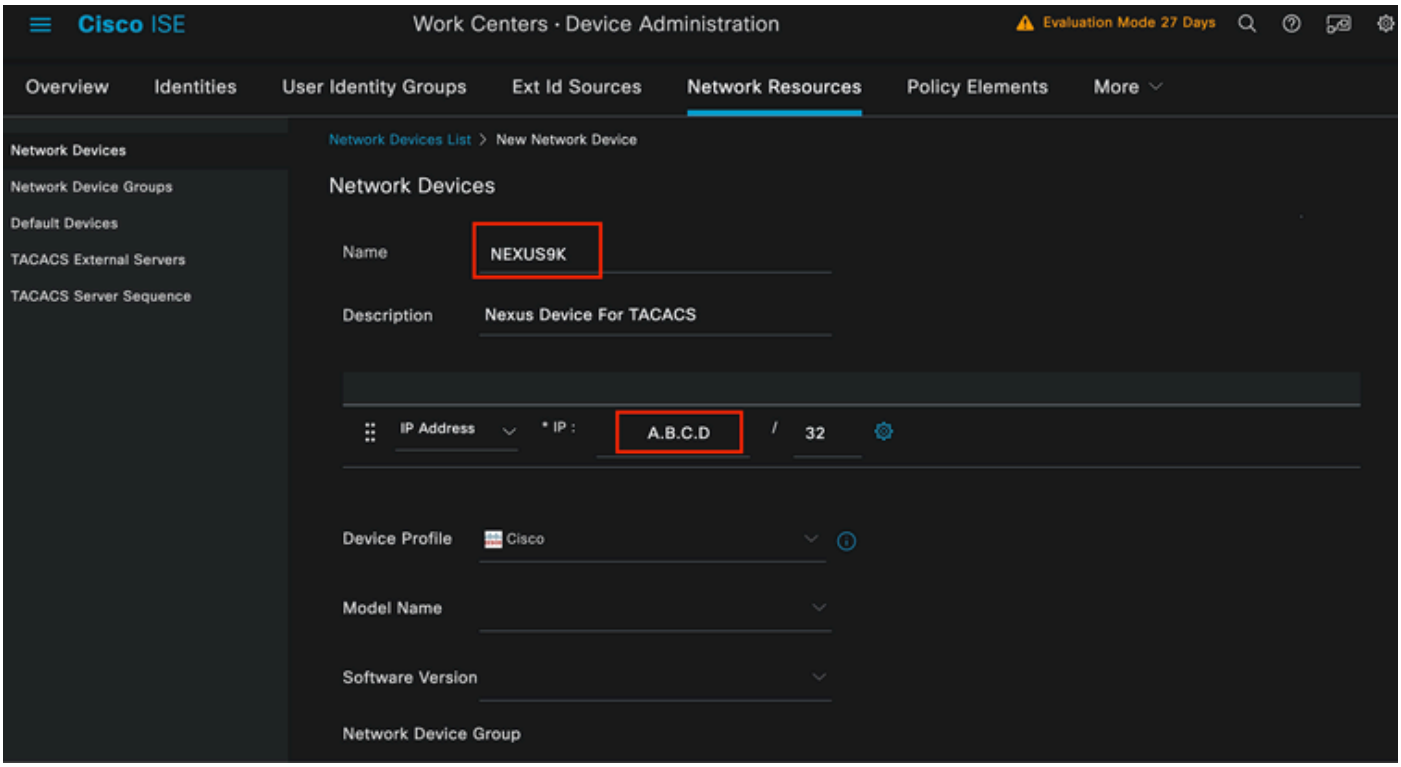
إضافة جهاز Nexus 9000 إلى إدارة ISE > موارد الشبكة > أجهزة الشبكة

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.

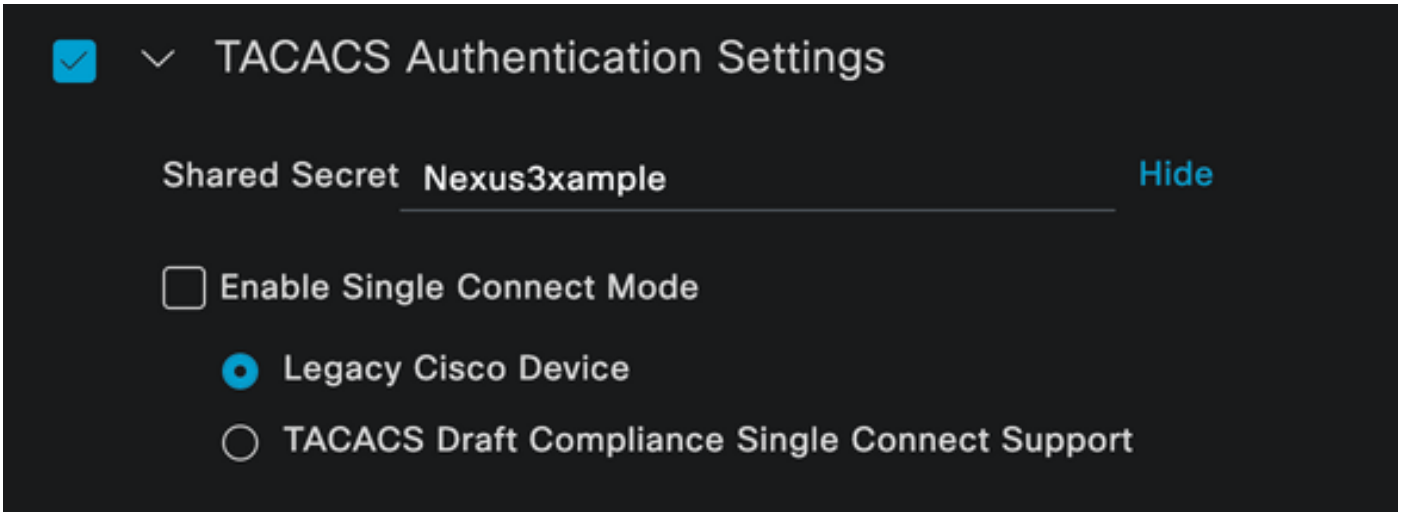


تكوين جهاز الشبكة

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 > نظام NAD > إعدادات مصادقة TACACS.

إضافة "السر المشترك" الذي أستخدمته ضمن تكوين NAD لهذا العرض التوضيحي، يتم إستخدام Nexus3xample في هذا العرض التوضيحي.

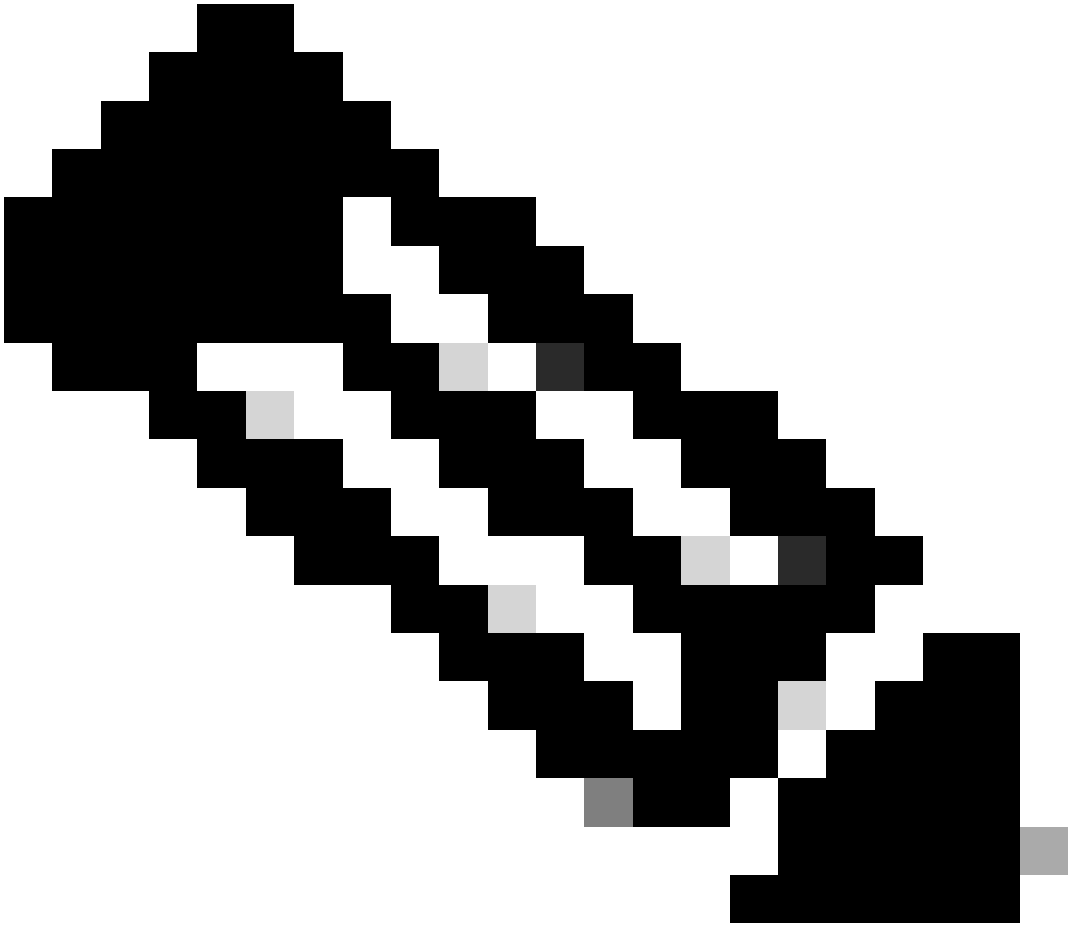


قسم تكوين *TACACS*

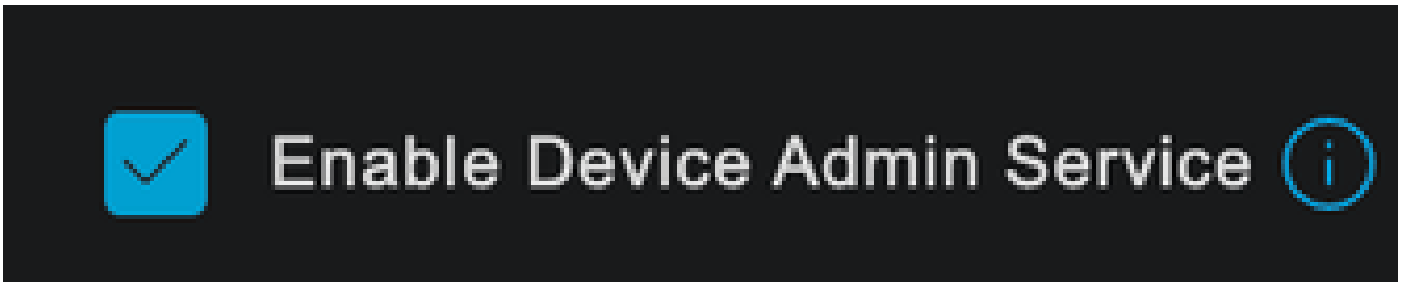
احفظ التغييرات بالنقر فوق الزر إرسال.

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.



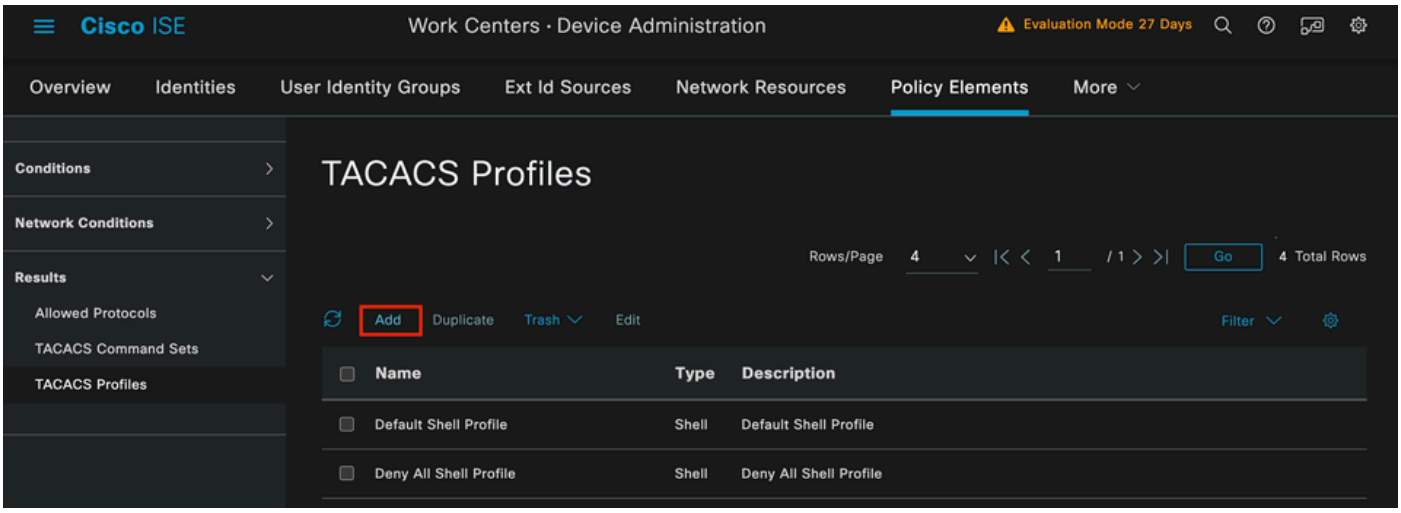
التحقق من ميزة إدارة جهاز PSN

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.

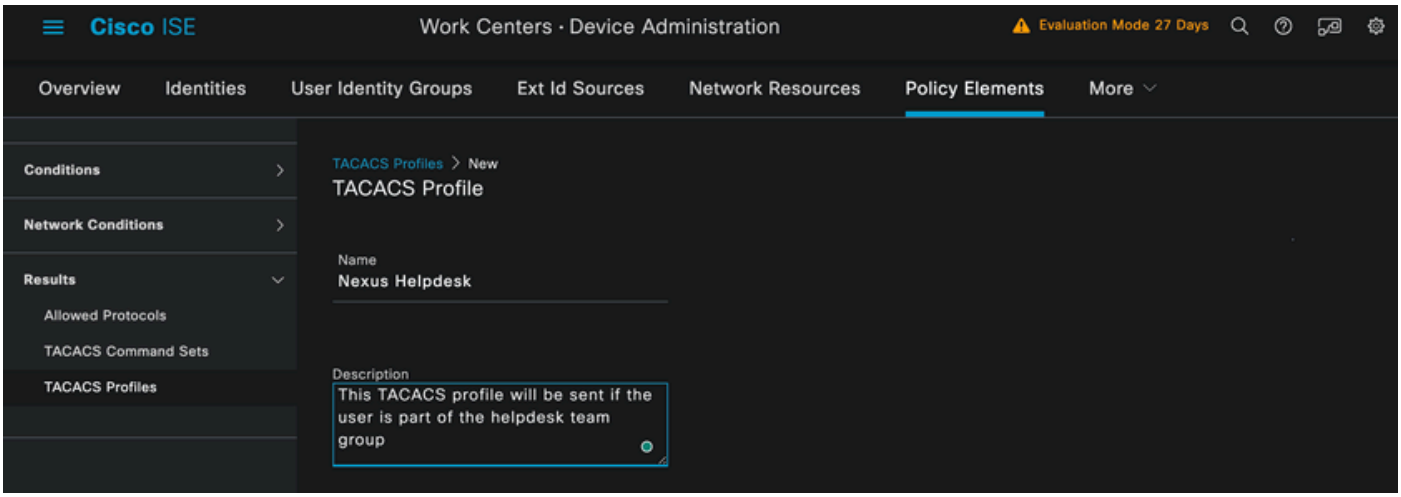
من قائمة ISE، انتقل إلى مراكز العمل > إدارة الأجهزة > عناصر السياسة > النتائج > ملفات

تعريف TACACS وانقر فوق الزر إضافة.



ملف تعريف *TACACS*

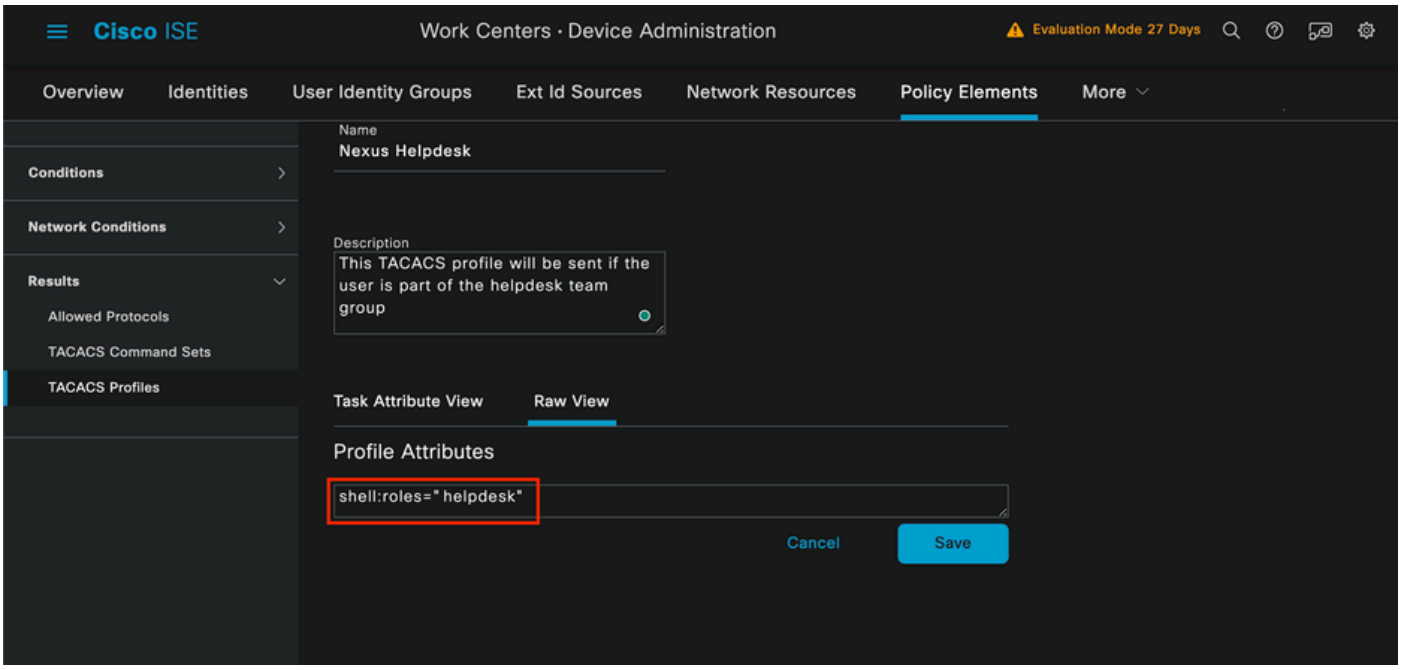
قم بتعيين اسم، ووصف إختياري.



تسمية ملف تعريف *TACACS*

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

وأدخل القيمة shell:roles="help desk".



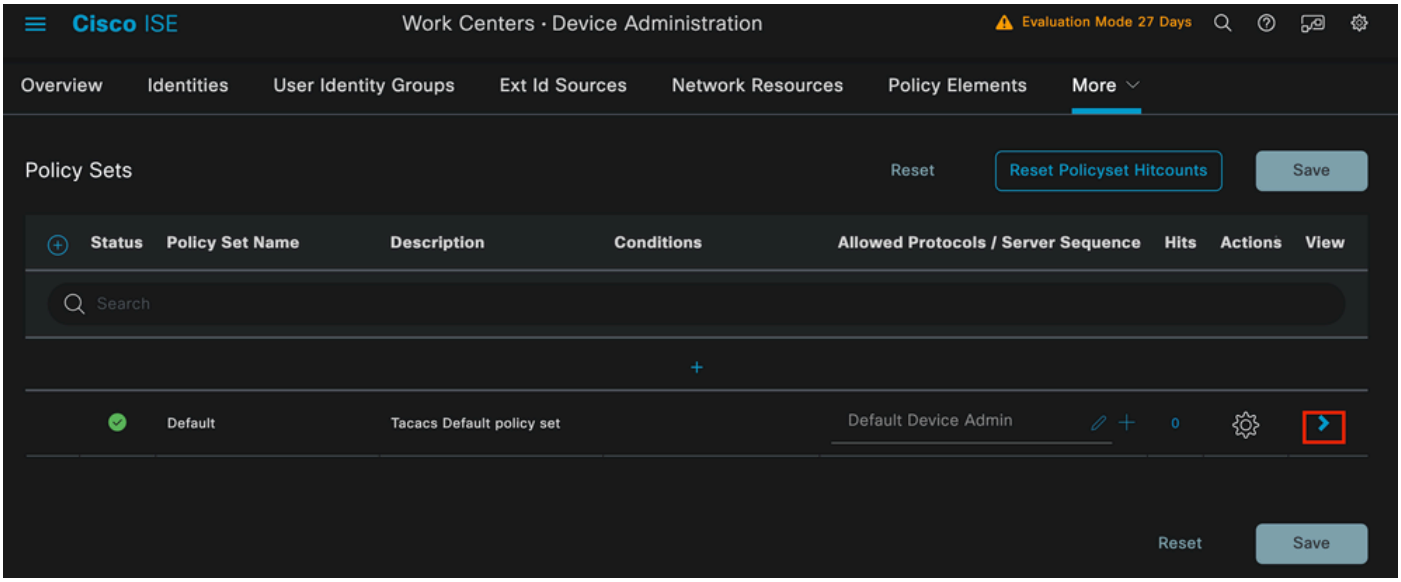
إضافة سمة ملف تعريف

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، بشروط لمطابقة سيناريوهات معينة.

انقر فوق السهم الموجود في نهاية الصف.

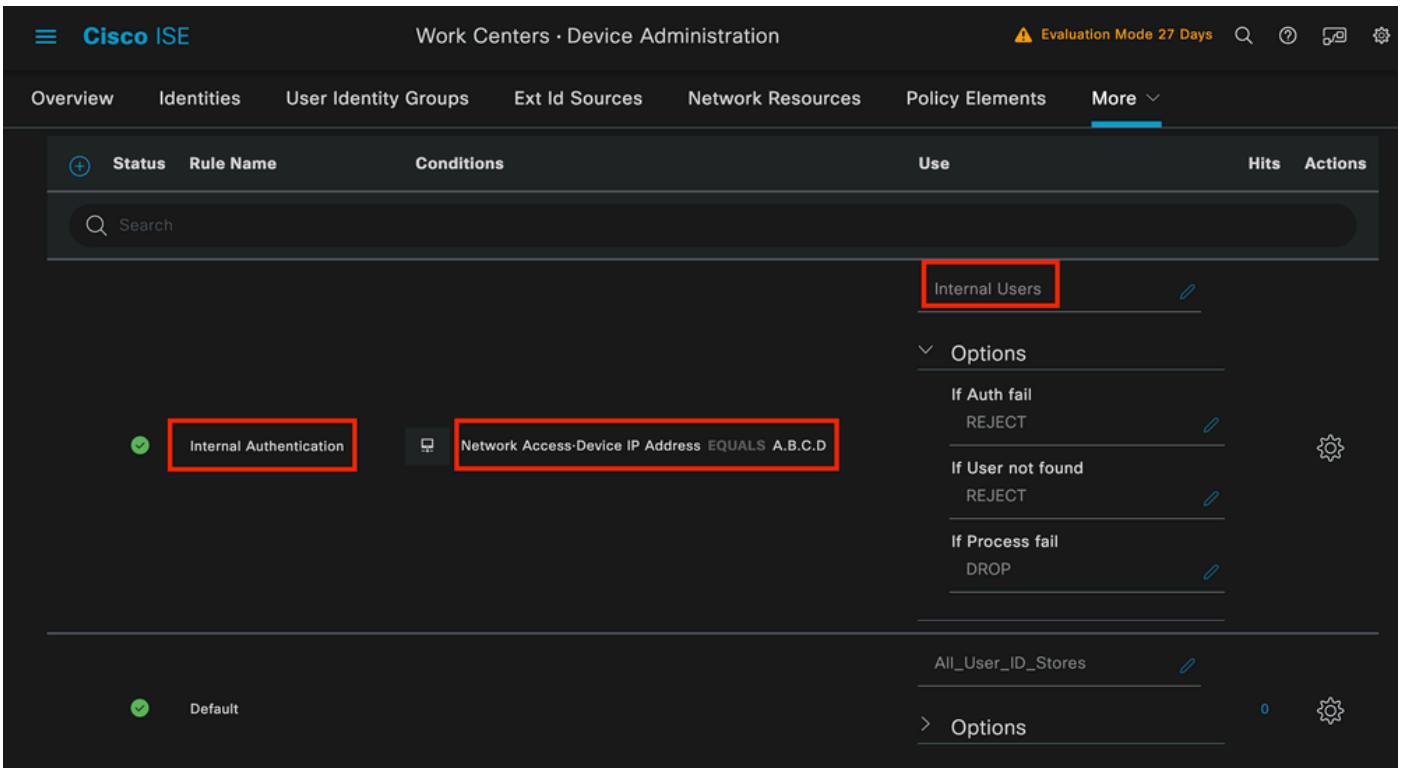


صفحة مجموعات نهج مسؤول الجهاز

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

انقر فوق أيقونة إضافة.

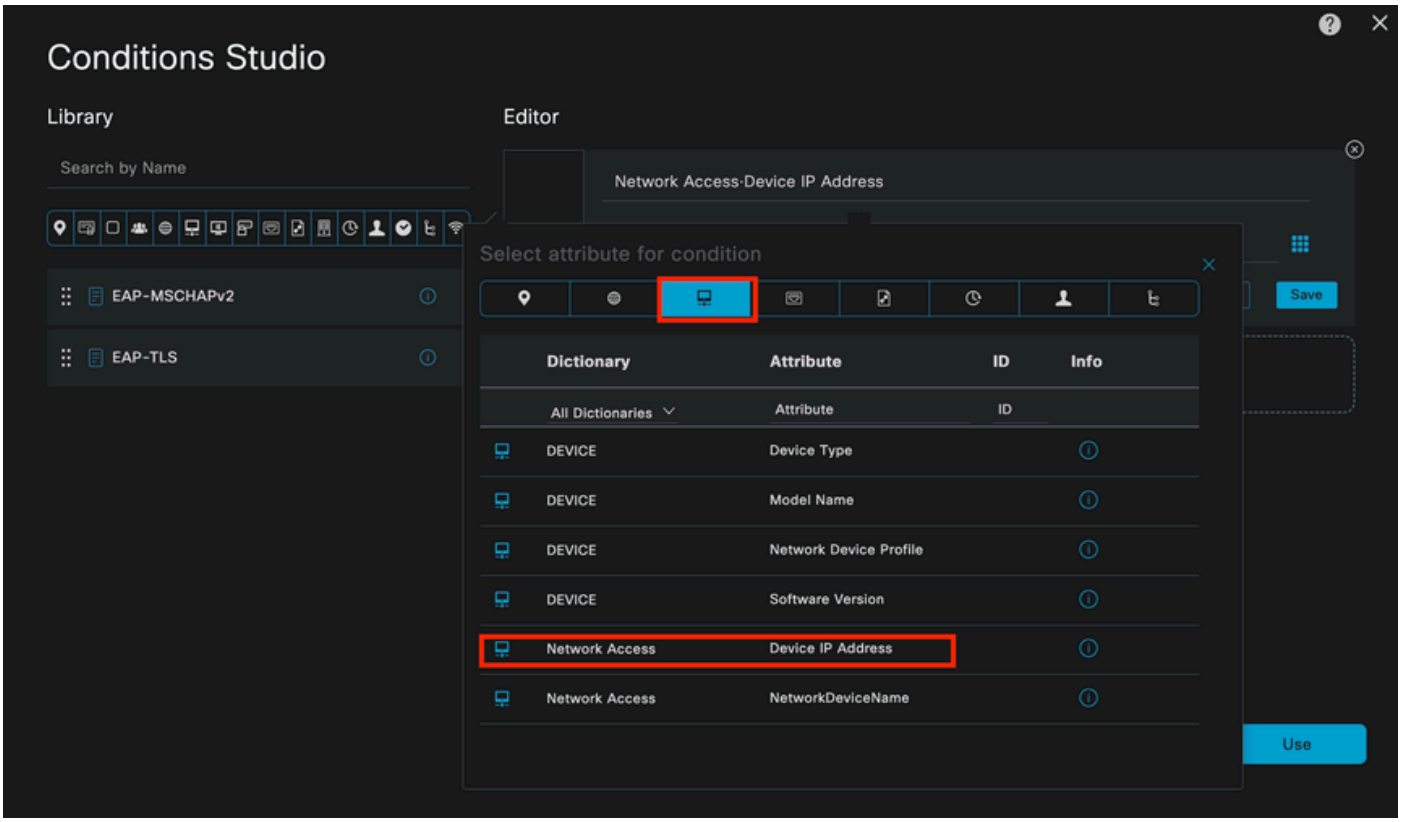
على مثال التكوين هذا، تكون قيمة الاسم هي المصادقة الداخلية والشرط المختار هو IP لجهاز الشبكة (Nexus) (يحل محل a.b.c.d.). يستخدم نهج المصادقة هذا مخزن هوية المستخدمين الداخلي.



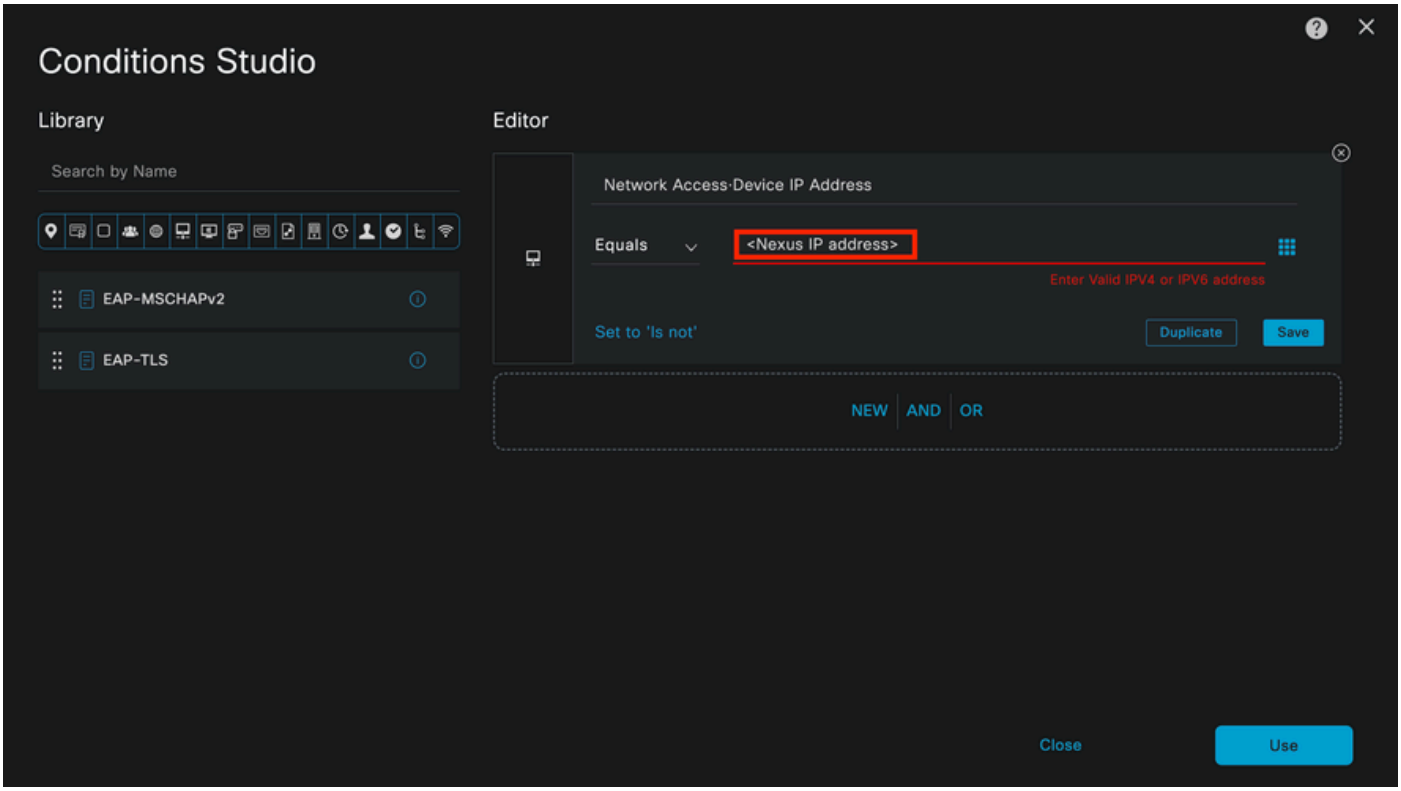
نهج المصادقة

فيما يلي كيفية تكوين الشرط.

حدد الوصول إلى الشبكة > سمة قاموس عنوان IP للجهاز.



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



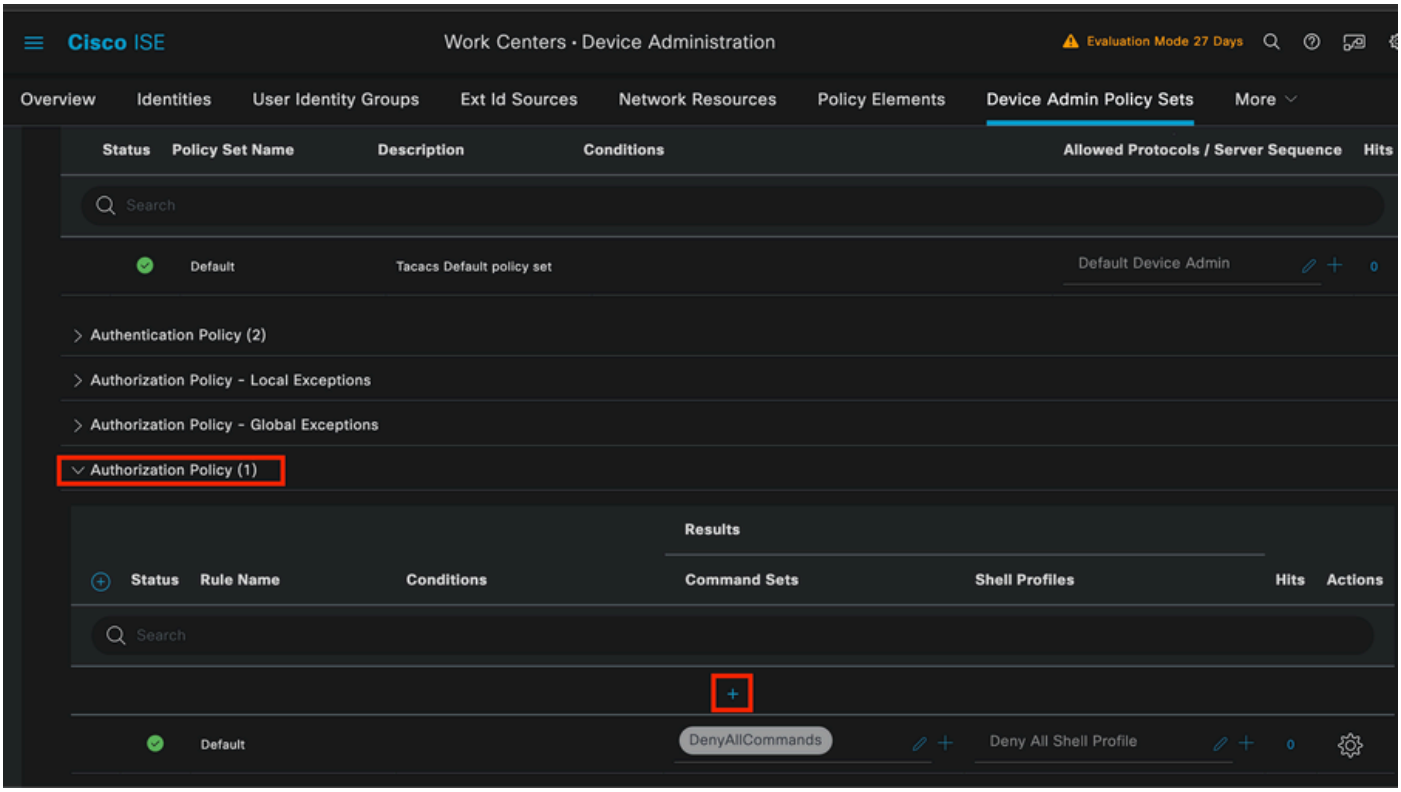
إضافة عامل تصفية *IP*

انقر فوق الزر إستخدام".

يتم الوصول إلى هذا الشرط فقط بواسطة جهاز Nexus الذي قمت بتكوينه، ومع ذلك، إذا كان الغرض هو تمكين هذا الشرط لكمية كبيرة من الأجهزة، فيجب مراعاة شرط مختلف.

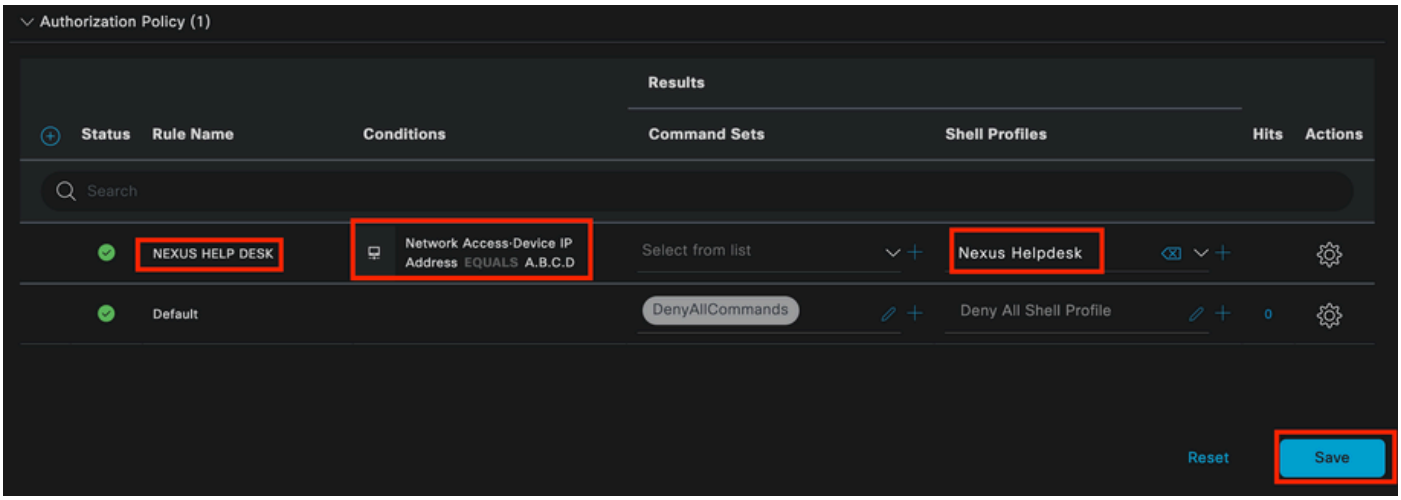
ثم انتقل إلى قسم نهج التخويل وقم بتوسيعه.

انقر على أيقونة + (زائد).



قسم نهج التخويل

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



أستوديو الشروط لنهج التخويل

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

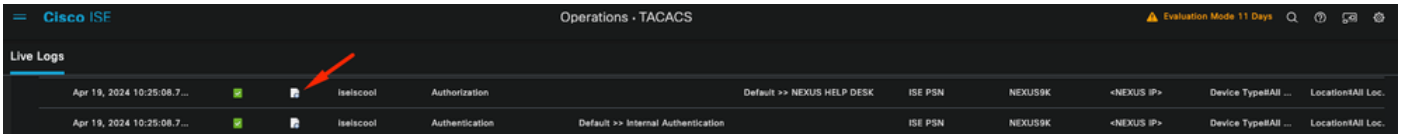
في عمود "ملفات تعريف Shell"، تم تحديد ملف التعريف الذي تم تكوينه قبل تحديد مكتب الدعم ل Nexus.

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، وقم بتعريف السجل الذي يطابق اسم المستخدم المستخدم، وانقر تفاصيل سجل التشغيل لحدث 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

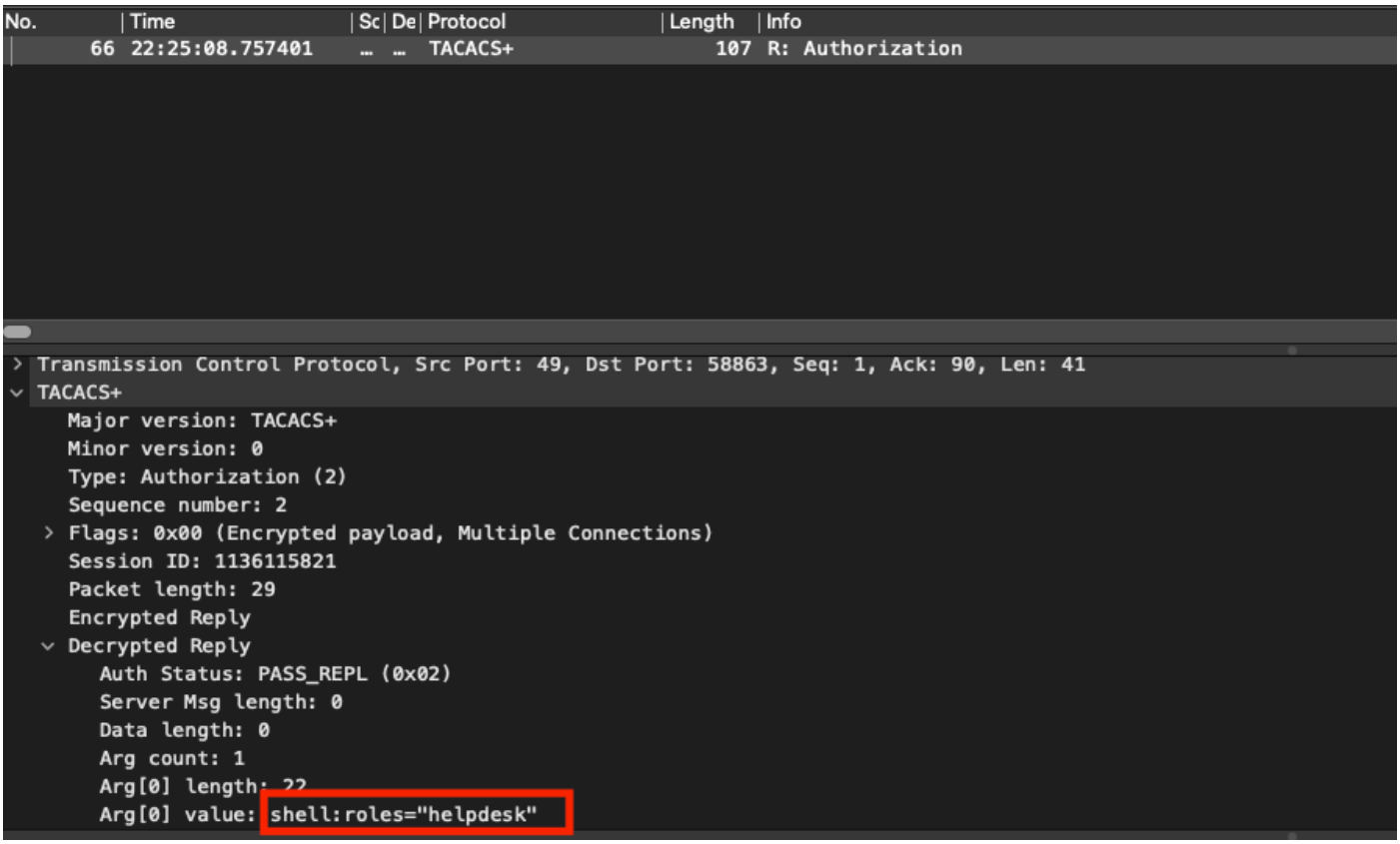
- تحقق من إمكانية الوصول إلى ISE من جهاز Nexus.Nexus9000# ping <ISE IP لديك>
  إختبار اتصال <ISE IP> (<ISE IP> 56 بايت بيانات)
  64 بايت من <ISE IP>: icmp_seq=0 ttl=59 time=1.22 مللي ثانية
  64 بايت من <ISE IP>: icmp_seq=1 ttl=59 وقت=0.739 مللي ثانية
  64 بايت من <ISE IP الخاص بك: icmp_seq=2 ttl=59 الوقت=0.686 مللي ثانية
  64 بايت من <ISE IP الخاص بك: icmp_seq=3 ttl=59 وقت=0.71 مللي ثانية
  64 بايت من <ISE IP>: icmp_seq=4 ttl=59 وقت=0.72 مللي ثانية
- دقق، أن فتح ميناء 49، بين ISE وجهاز Nexus.
  Nexus 9000# برنامج Telnet <Your ISE IP> 49
  يتم الآن محاولة <ISE IP> ...
  متصل ب <ISE IP الخاص بك> .
  حرف الهروب هو '^]'.
- 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 الى يستهلك 8421 opcode
2024 أبريل 19:50:44.199406 tacacs: process_implicit_cfs_session_start: إدخال...
2024 apr 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: إنهاء؛ نحن في حالة تعطيل التوزيع
2024 أبريل 19:50:44.199424 tacacs: process_aaa_tplus_request: الدخول لمعرف جلسة عمل المصادقة والتفويض والمحاسبة (AAA) 0
2024 APR 19 22:50:44.199438 tacacs: process_aaa_tplus_request:التحقق من حالة المنفذ mgmt0 مع servergroup IsePsnServers
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 apr 19 22:50:44.208027 tacacs: tacacs_global_config(4701): إستعادة قيمة الإرجاع لعملية تكوين البروتوكول العالمي:الناجح
2024 أبريل 19:50:44.208045 tacacs: tacacs_global_config(4716): req:num server 0
2024 apr 19 22:50:44.208054 tacacs: tacacs_global_config: req:num مجموعة 1
2024 apr 19 22:50:44.208062 tacacs: tacacs_global_config: req:num مهلة 5
2024 أبريل 19:50:44.208070 tacacs: tacacs_global_config: req:num deadtime 0
2024 apr 19 22:50:44.208078 tacacs: tacacs_global_config: req:num encryption_type 7
2024 أبريل 19:50:44.208086 tacacs: tacacs_global_config: إرجاع البيانات المكررة 0
2024 APR 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info في علم تم

aaa_req، ذلك تم إستخدام مجموعة الخوادم IsePsnServers
2024 أبريل 19:50:44.208108 tacacs: tacacs_servergroup_config: الدخول لمجموعة الخوادم، الفهرس 0
2024 apr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ لفهرس مجموعة خوادم البروتوكول:0 name:
2024 apr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 4048003 syserr2str = ال يوجد مفتاح PSS اذه
2024 apr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: إستدعاء pss2_getkey
2024 apr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ يحتوي على فهرس مجموعة خوادم البروتوكول:2 name:IsePsnServers
2024 apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: إستعادة قيمة الإرجاع العملية مجموعة البروتوكول:الناجح
2024 APR 19 22:50:44.208194 tacacs: tacacs_servergroup_config: إرجاع بيانات 0 لمجموعة خوادم البروتوكول:IsePsnServers
2024 APR 19 22:50:44.208210 tacacs: process_aaa_tplus_request: Group تم العثور على IsePsnServers. تم العثور على VRF المقابل افتراضي، المصدر-trf هو 0
2024 أبريل 19:50:44.208224 tacacs: process_aaa_tplus_request: التحقق من وجود mgmt0 vrf:management مقابل vrf:الافتراضي للمجموعة المطلوبة
2024 أبريل 19:50:44.208256 tacacs: process_aaa_tplus_request:mgmt_if 83886080
2024 apr 19 22:50:44.208272 tacacs: process_aaa_tplus_request:global_src_intf : 0، src_intf المحلي هو 0 و vrf_name هو الإعداد الافتراضي
2024 أبريل 19:50:44.208286 tacacs: create_tplus_req_state_machine(902): الدخول لمعرف جلسة عمل المصادقة والتفويض والمحاسبة (AAA) 0
2024 أبريل 19:50:44.208295 tacacs: عدد مرات إعادة المحاولة 0
2024 أبريل 19:50:44.208307 tacacs: init_tplus_req_state_machine: الدخول لمعرف جلسة عمل المصادقة والتفويض والمحاسبة (AAA) 0
2024 apr 19 22:50:44.208317 tacacs: init_tplus_req_state_machine(1298):tplus_ctx هو NULL يجب أن يكون في حالة المؤقت والاختبار
2024 APR 19 22:50:44.208327 tacacs: tacacs_servergroup_config: الدخول لمجموعة الخوادم IsePsnServers، الفهرس 0
2024 APR 19 22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ لفهرس مجموعة خوادم البروتوكول:0 name:IsePsnServers
2024 APR 19 22:50:44.208357 tacacs: find_tacacs_servergroup: الدخول لمجموعة الخوادم IsePsnServers
2024 apr 19 22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = ناجح
2024 APR 19 22:50:44.208382 tacacs: find_tacacs_servergroup: الخروج لمجموعة الخوادم IsePsnServers هو 2
2024 APR 19 22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ: find_tacacs_servergroup خطأ 0 لمجموعة خوادم البروتوكول IsePsnServers
2024 apr 19 22:50:44.208420 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = ناجح
2024 apr 19 22:50:44.208433 tacacs: tacacs_servergroup_config: GET_REQ يحتوي على فهرس مجموعة خوادم البروتوكول:2 name:IsePsnServers
2024 أبريل 19 22:52024 أبريل 19 22:52024 أبريل 19 22:5 2024 مايو
Nexus 9000#

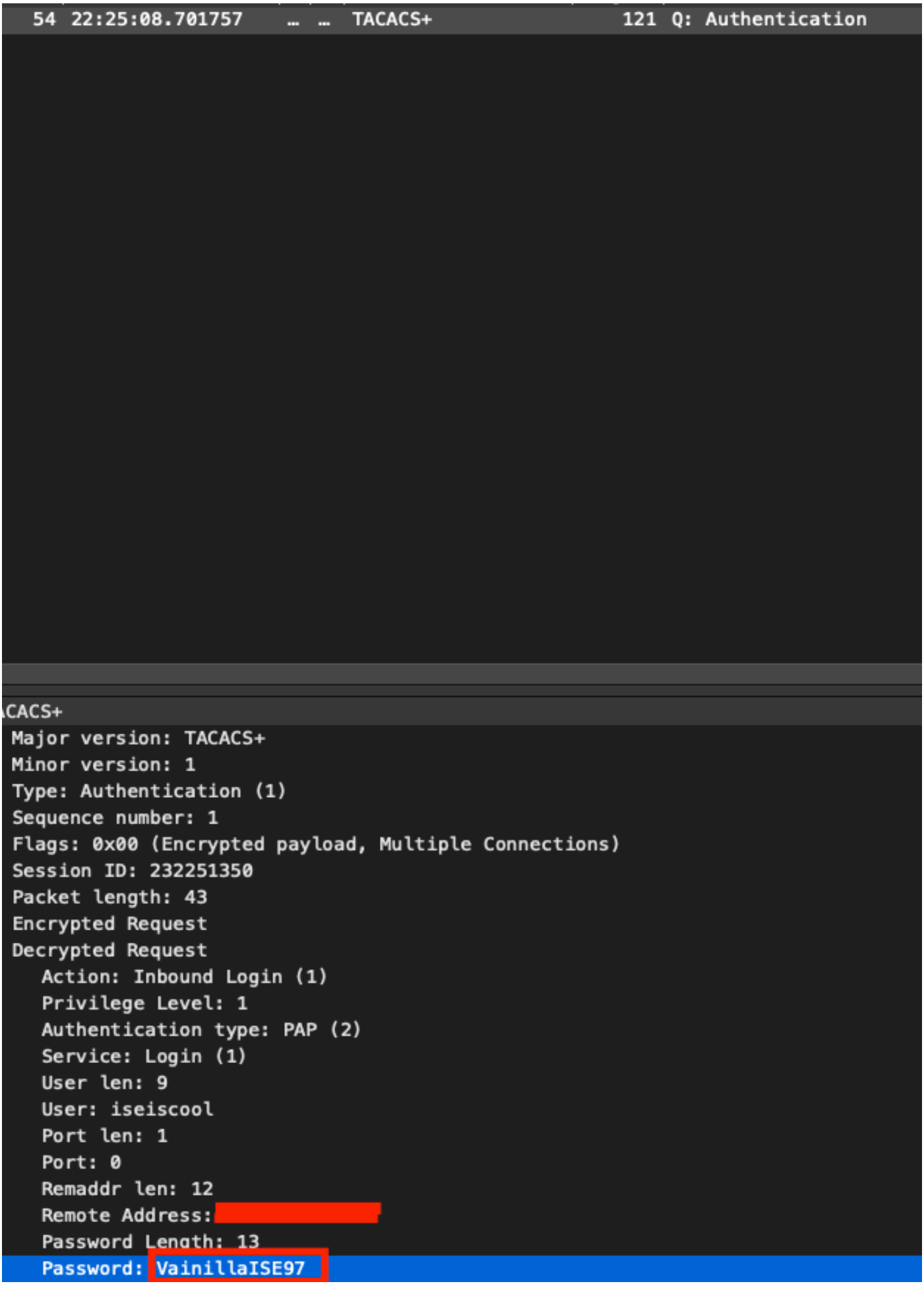
- قم بإجراء التقاط حزمة (لعرض تفاصيل الحزمة، يجب عليك تغيير تفضيلات

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 إيداع 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).