تكوين TACACS+ مع واجهة ISE Gigabit Ethernet 1

المحتويات

المقدمة

يصف هذا المستند تكوين ISE TACACS+ مع واجهة Gigabit Ethernet 1 حيث يعمل الموجه والمحول كأجهزة شبكة.

معلومات أساسية

يدعم Cisco ISE ما يصل إلى 6 واجهات Ethernet. والتي يمكن أن تكون لها سوى ثلاث سندات، سند 0، سند 1، وسند 2. والتي يمكنك تغيير الواجهات التي هي جزء من سند أو تغيير دور

الواجهة في سنن.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة على هذا موضوع:

- معرفة الشبكة الأساسية
- محرك خدمة الهوية من Cisco.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

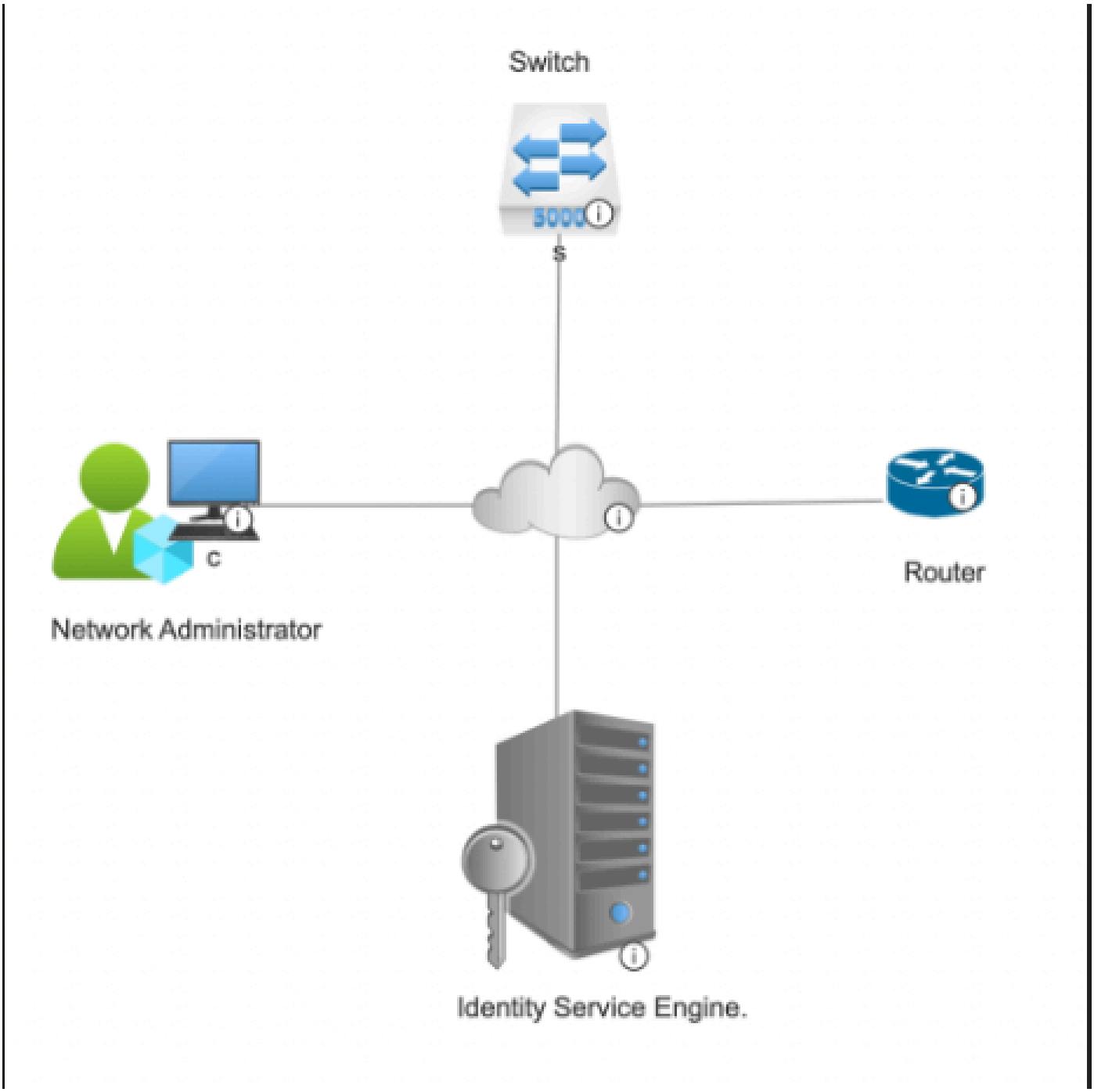
- Cisco Identity Service Engine v3.3
- برنامج Cisco IOS®، الإصدار 17.x
- المحول Cisco C9200 Switch.

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.

التكوين

الهدف من التكوين هو: قم بتكوين إثرنت جيجابت 1 من ISE لـ TACACS+ ومصادقة المحول والموجه باستخدام TACACS+ مع ISE كخادم مصادقة.

الرسم التخطيطي للشبكة



طوبولوجيا الشبكة

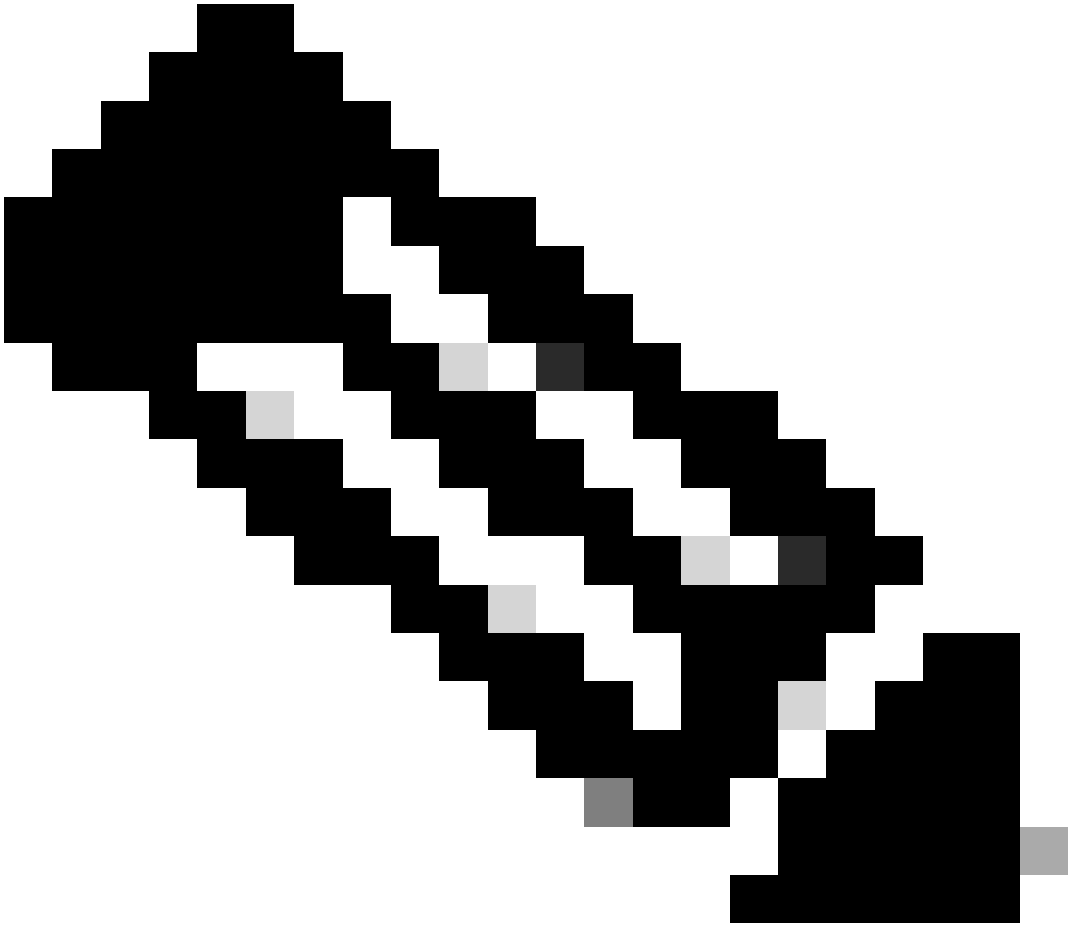
تكوين محرك خدمات الهوية ل TACACS+

تكوين عنوان IP لواجهة Gigabit Ethernet 1 في ISE

1. سجل الدخول إلى CLI الخاص بعقدة ISE PSN حيث يتم تمكين مسؤول الجهاز وتحقق من الواجهات المتاحة باستخدام الأمر show interface:

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 629139  bytes 226044590 (215.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 674817  bytes 100272799 (95.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 438392  bytes 363642766 (346.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 481076  bytes 369977760 (352.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1271564  bytes 203676256 (194.2 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 76672  bytes 116577841 (111.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 262  bytes 36180 (35.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 606 (606.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 2
        flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:8b:f8:5f  txqueuelen 1000  (Ethernet)
        RX packets 268  bytes 36228 (35.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 516 (516.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

التحقق من الواجهات في ISE



ملاحظة: في هذا التكوين، يتم تكوين ثلاث واجهات فقط في ISE، مع التركيز على واجهة Gigabit Ethernet 1. يمكن تطبيق الإجراء نفسه لتكوين عنوان IP لجميع الواجهات. وبشكل افتراضي، يدعم ISE ما يصل إلى ست واجهات Gigabit Ethernet.

---

2. من CLI الخاص بنفس عقدة PSN، قم بتعيين عنوان IP إلى واجهة Gigabit Ethernet 1 باستخدام هذه الأوامر:

hostnameofise#configure t

hostnameofise/admin(config)#interface gigabit إثرنيت 1

hostnameofise/admin(config-gigabitEthernet-1)# <ip address> <subnetMask> ٪ قد يؤدي تغيير عنوان IP إلى إعادة تشغيل خدمات ISE

هل تريد المتابعة مع تغيير عنوان IP؟

هل تريد المتابعة؟ [نعم، لا] نعم

3. يؤدي تنفيذ الخطوة 2 إلى إعادة تشغيل خدمات عقدة ISE. للتحقق من حالة خدمات ISE، قم بتشغيل الأمر show application status ise وتأكد من تشغيل حالة الخدمات وفقا لقطة الشاشة هذه:

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

التحقق من حالة خدمة ISE

4. تحقق من عنوان IP الخاص بواجهة Gig1 باستخدام الأمر show interface:

V

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

التحقق من عنوان IP لواجهة ISE Gig2 من CLI

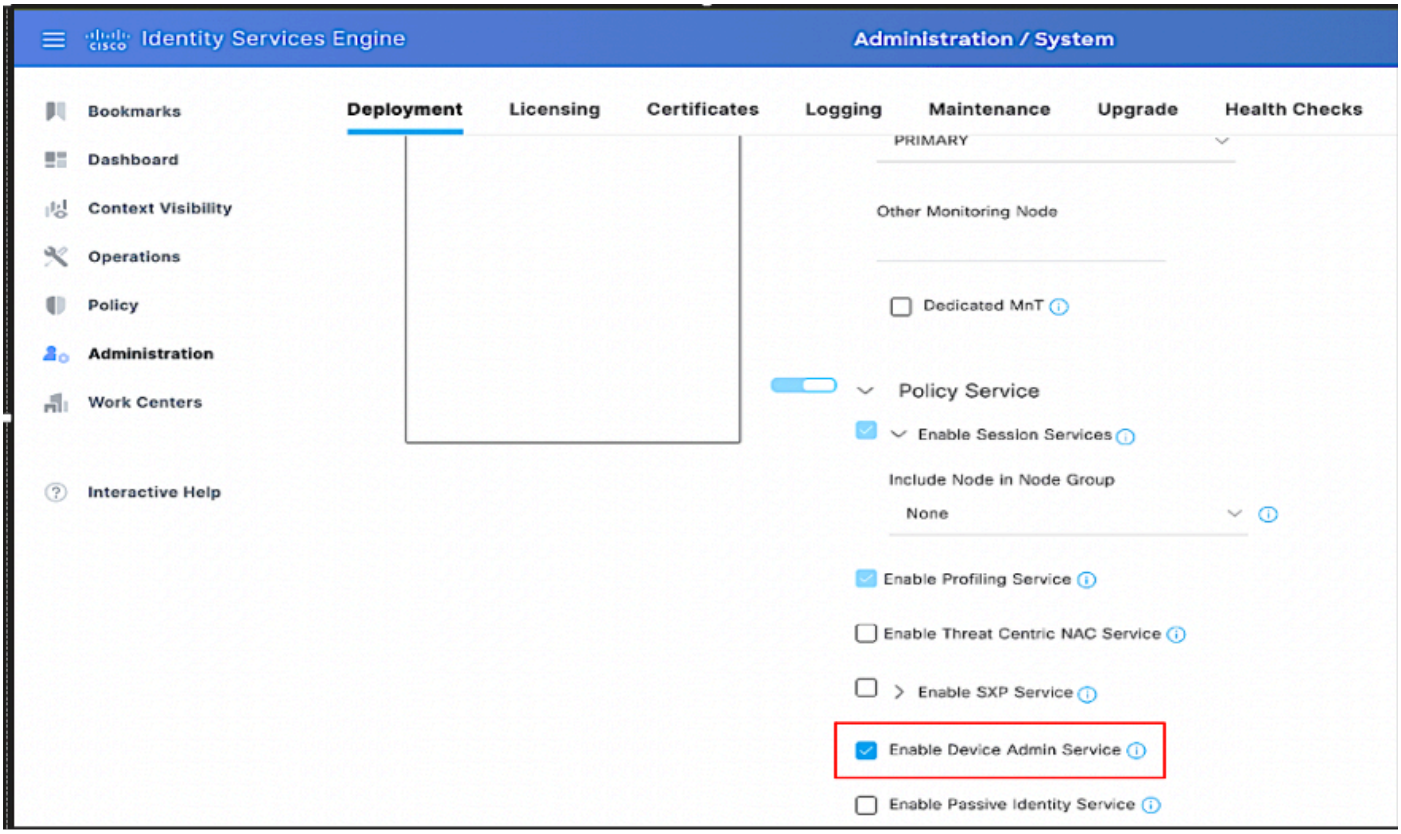
5.تحقق من السماح بالمنفذ 49 في عقدة ISE باستخدام show ports أمر | INC 49:

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

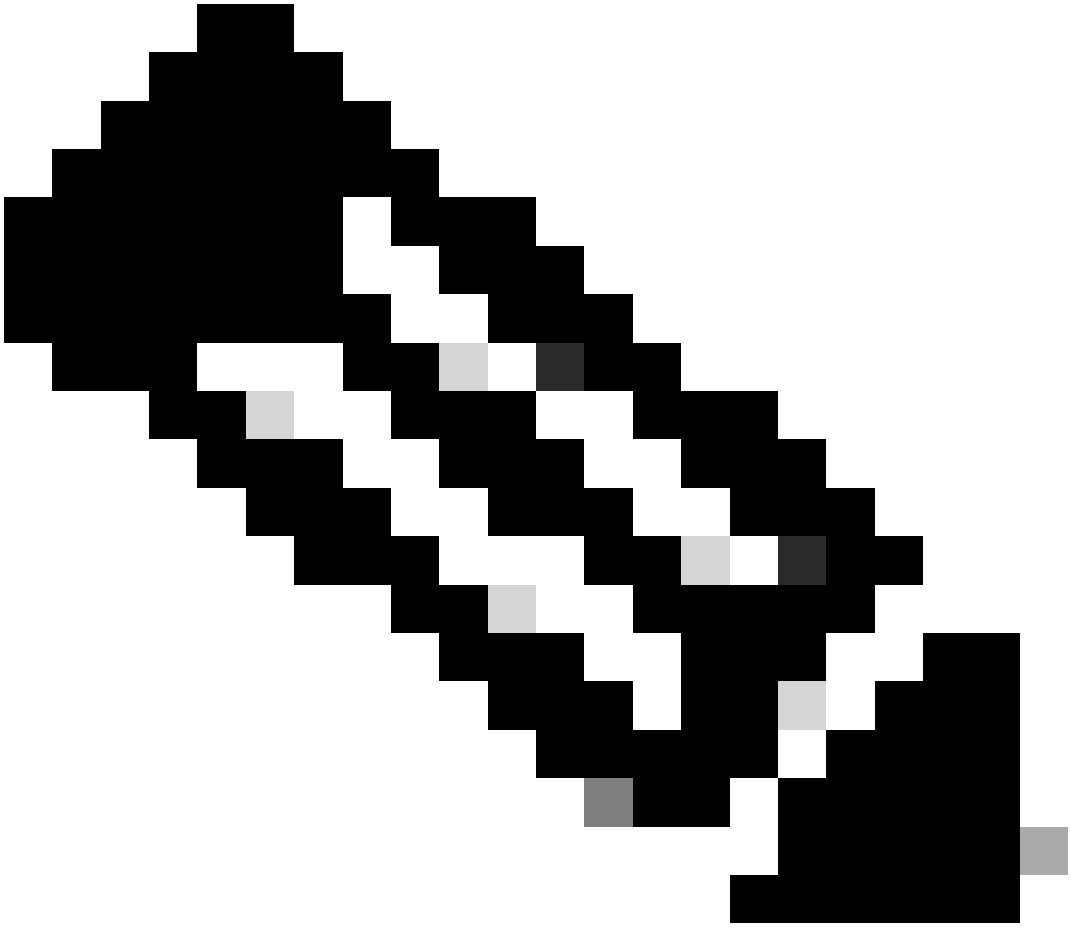
التحقق من بدل المنفذ 49 في ISE

تمكين إدارة الأجهزة في ISE

انتقل إلى واجهة المستخدم الرسومية (GUI) لـ ISE > الإدارة > النشر > تحديد عقدة PSN، ثم حدد تمكين خدمة إدارة الجهاز:



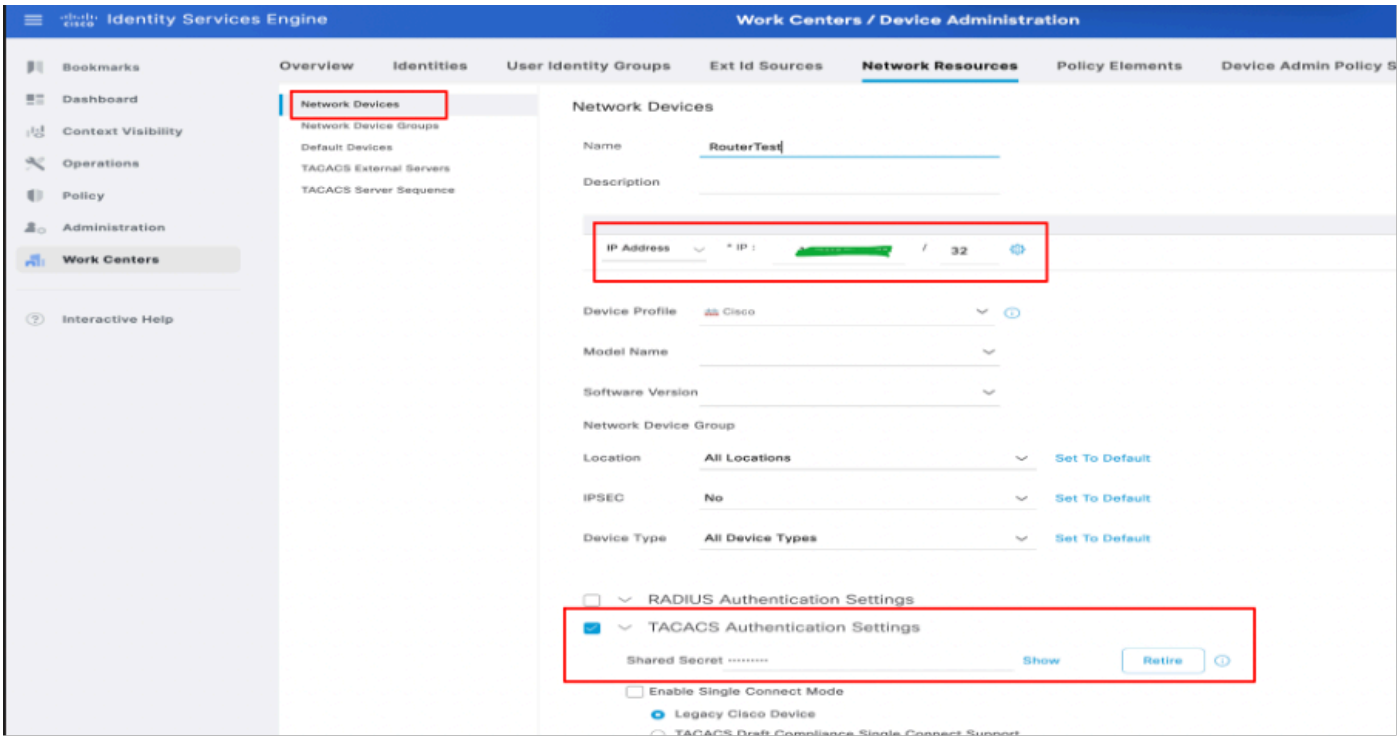
تمكين خدمة إدارة الأجهزة في ISE



ملاحظة: لتمكين خدمة إدارة الجهاز، يلزم وجود ترخيص إدارة الجهاز.

إضافة جهاز شبكة في ISE

1. انتقل إلى مركز العمل > إدارة الأجهزة > موارد الشبكة > أجهزة الشبكة. انقر فوق إضافة (Add). قم بتوفير الاسم وعنوان IP. حدد خانة الاختيار إعدادات مصادقة TACACS+ وقم بتوفير المفتاح السري المشترك.



تكوين جهاز الشبكة في ISE

2. اتبع الإجراء المذكور أعلاه لإضافة جميع أجهزة الشبكة المطلوبة لمصادقة TACACS.

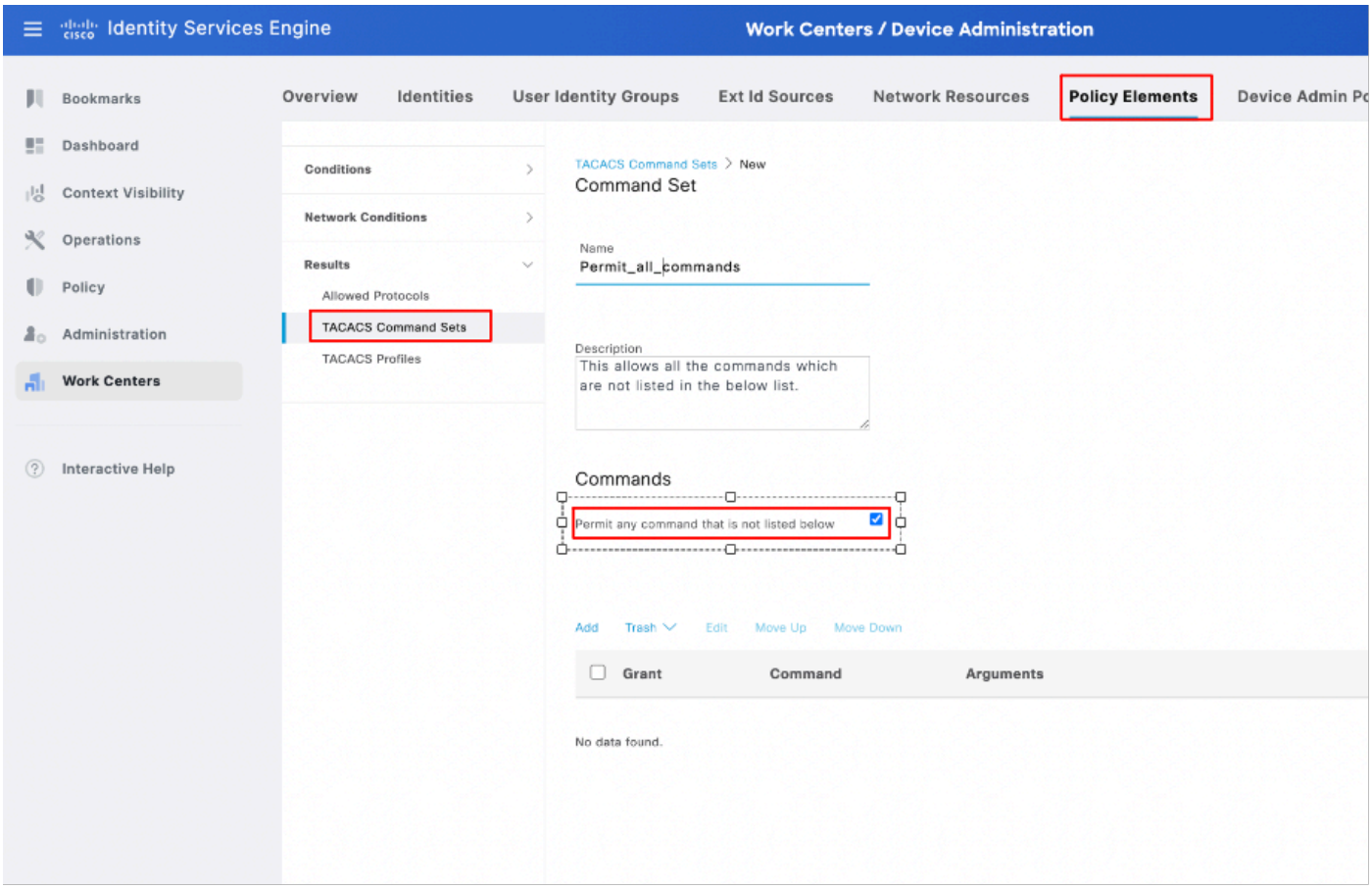
تكوين مجموعات أوامر TACACS+

تم تكوين مجموعتين من الأوامر لهذا العرض التوضيحي:

يتم تعيين ALLOWED_ALL_COMMANDS إلى مسؤول المستخدم ويسمح بجميع الأوامر على الجهاز.

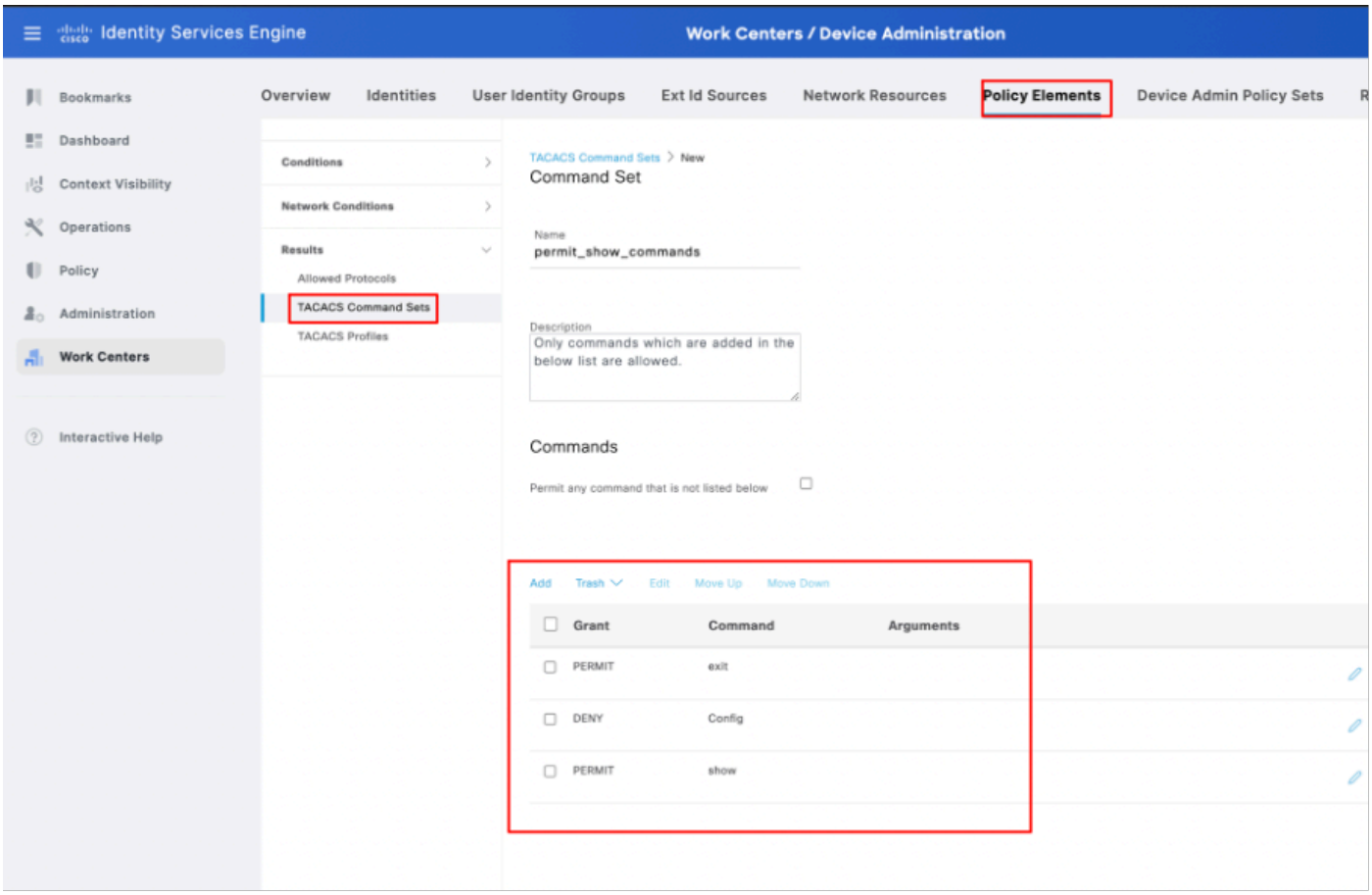
allow_show_commands، يتم تعيينه لمستخدم ويسمح بأوامر show فقط

1. انتقل إلى مراكز العمل > إدارة الأجهزة > نتائج السياسة > مجموعات أوامر TACACS. انقر إضافة. قم بتوفير الاسم PermitAllCommands، ثم أختر خانة الاختيار السماح بأي أمر غير المدرجة. انقر فوق إرسال.



تكوين مجموعات الأوامر في ISE

2. انتقل إلى مركز العمل > إدارة الأجهزة > نتائج السياسة > مجموعات أوامر TACACS. انقر فوق إضافة. قم بتوفير الاسم أذنعرض الأوامر، انقر فوق إضافة، ثم أخيرا، قم بالسماح بإظهار وإنهاء الأوامر. بشكل افتراضي، إذا تركت الوسيطات فارغة، يتم تضمين جميع الوسيطات. انقر فوق إرسال.

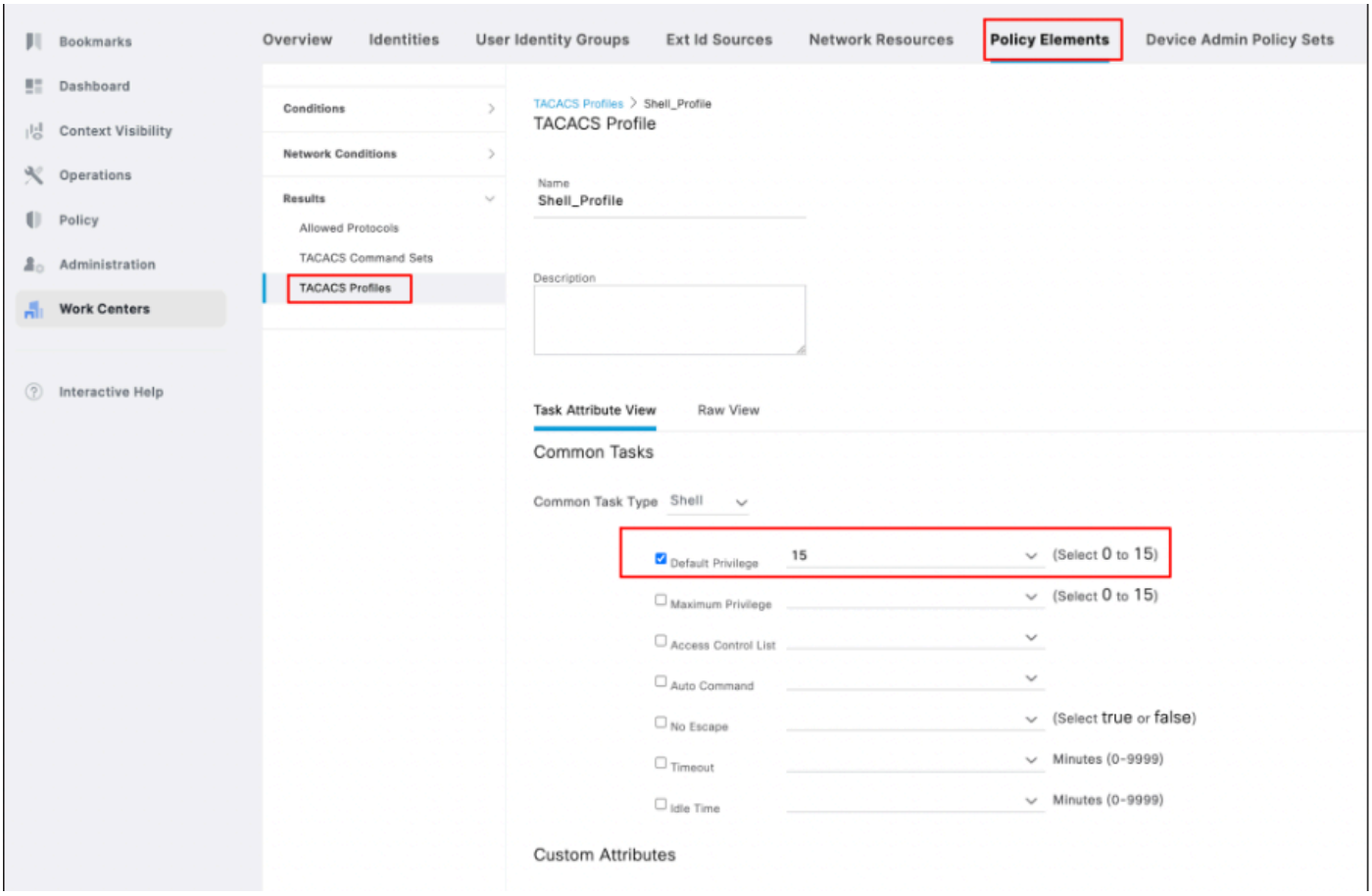


تكوين أوامر enable_show_commands في ISE

تكوين ملف تعريف TACACS+

يتم تكوين ملف تعريف TACACS+ واحد، ويتم تنفيذ تفويض الأوامر عبر مجموعات الأوامر.

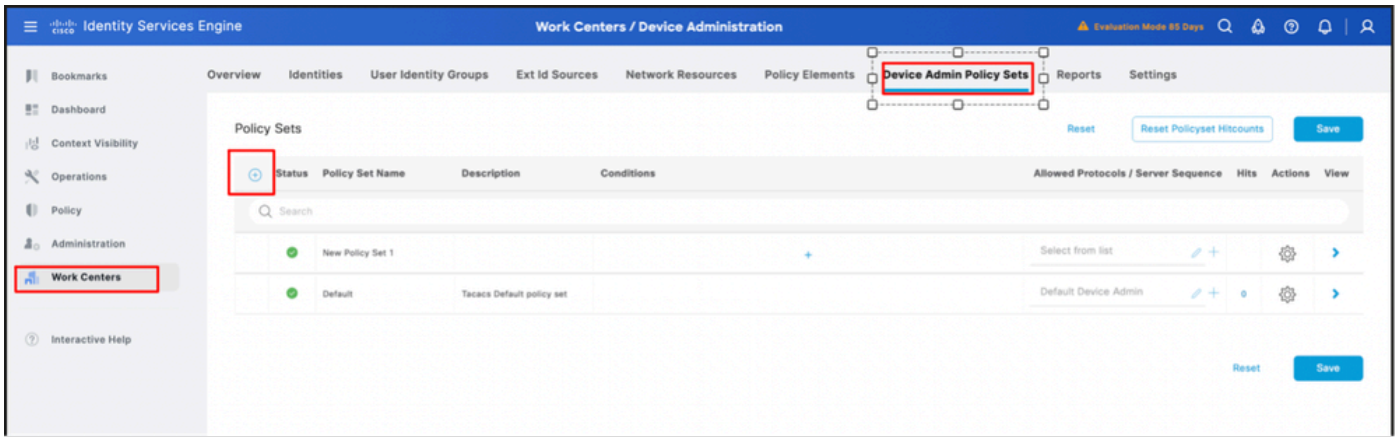
لتكوين ملف تعريف TACACS+، انتقل إلى مراكز العمل>إدارة الأجهزة>نتائج السياسة>ملفات تعريف TACACS. طقطقة يضيف، زودت اسم لملف تعريف Shell، عينت التقصير امتياز خانة الاختياري، وأدخل القيمة 15. أخيرا، طقطقة يسلم.



تكوين ملف تعريف TACACS في ISE

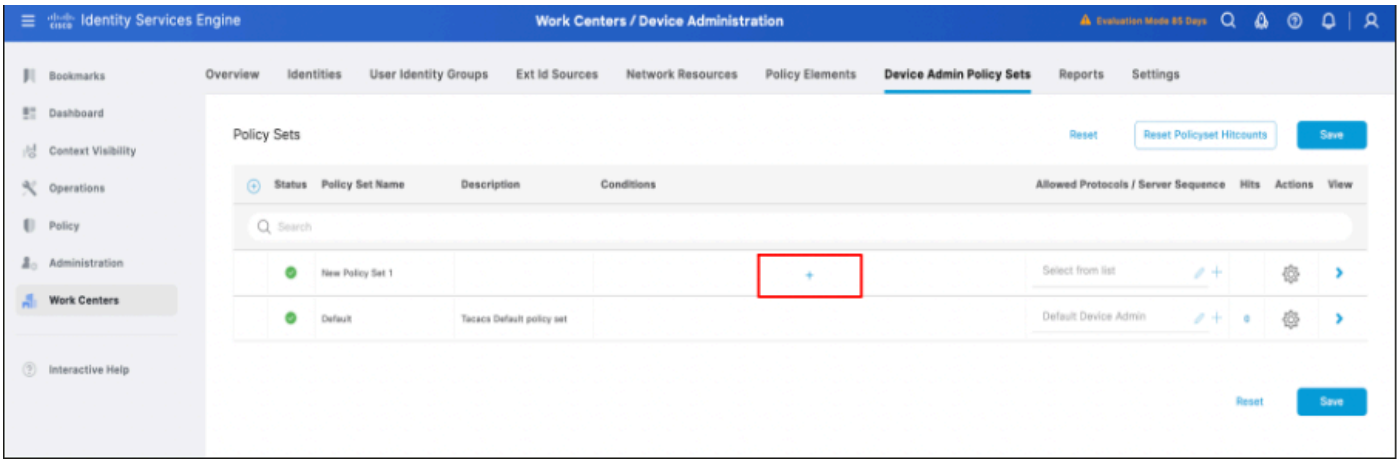
تكوين ملف تعريف مصادقة تفويض TACACS+

1. سجل الدخول إلى ISE pan GUI -> الإدارة -> مراكز العمل -> إدارة الجهاز -> مجموعات سياسات إدارة الجهاز. انقر على أيقونة + (زائد) لإنشاء سياسة جديدة. في هذه الحالة، يتم تسمية مجموعة النهج باسم مجموعة نهج جديدة 1.



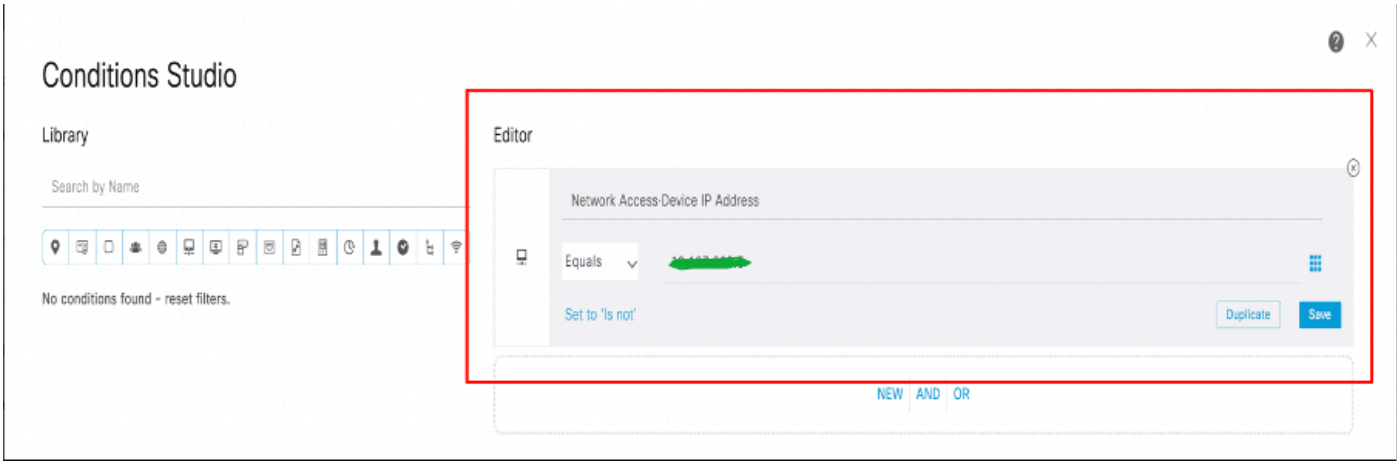
تكوين مجموعة النهج في ISE

2. قبل حفظ مجموعة النهج، يجب تكوين الشروط، كما هو موضح في لقطة الشاشة هذه. انقر فوق أيقونة + (زائد) لتكوين شروط مجموعة النهج.

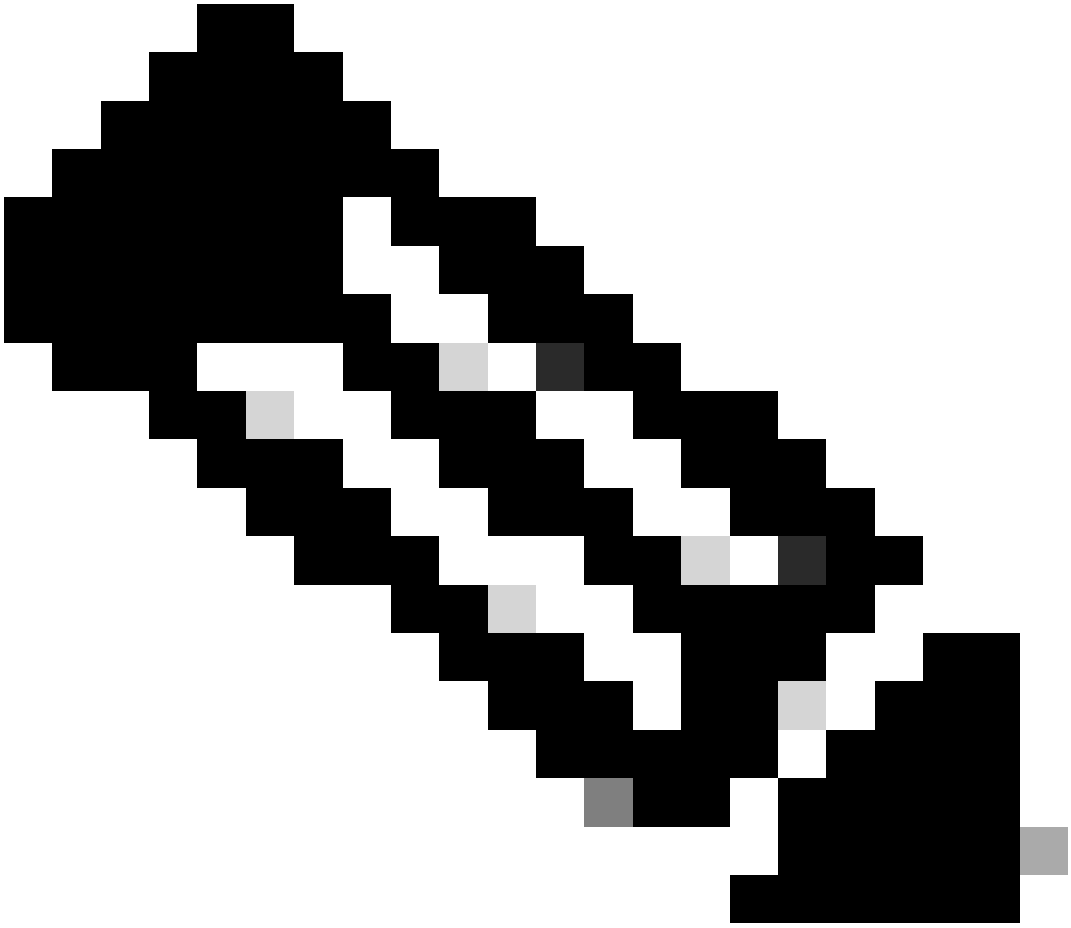


تكوين شروط مجموعة النهج في ISE

3. بعد النقر فوق رمز + (زائد) كما هو مذكور في الخطوة 2، يتم فتح مربع حوار Conditions Studio. هناك، قم بتكوين الشروط المطلوبة. قم بحفظ الشرط بالشروط الجديدة أو الموجودة، قم بالتمرير. طقطقة يستعمل.



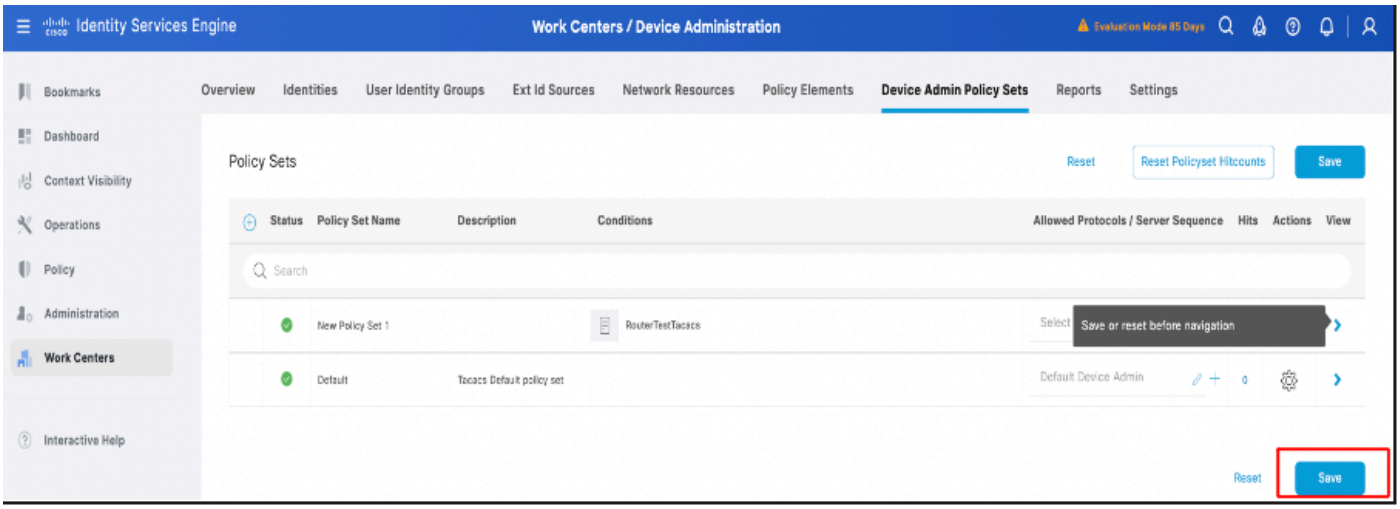
تكوين شروط مجموعة النهج في ISE



ملاحظة: لهذه الوثائق، تتطابق الشروط مع IP لجهاز الشبكة. ومع ذلك، يمكن أن تختلف الظروف حسب متطلبات النشر.

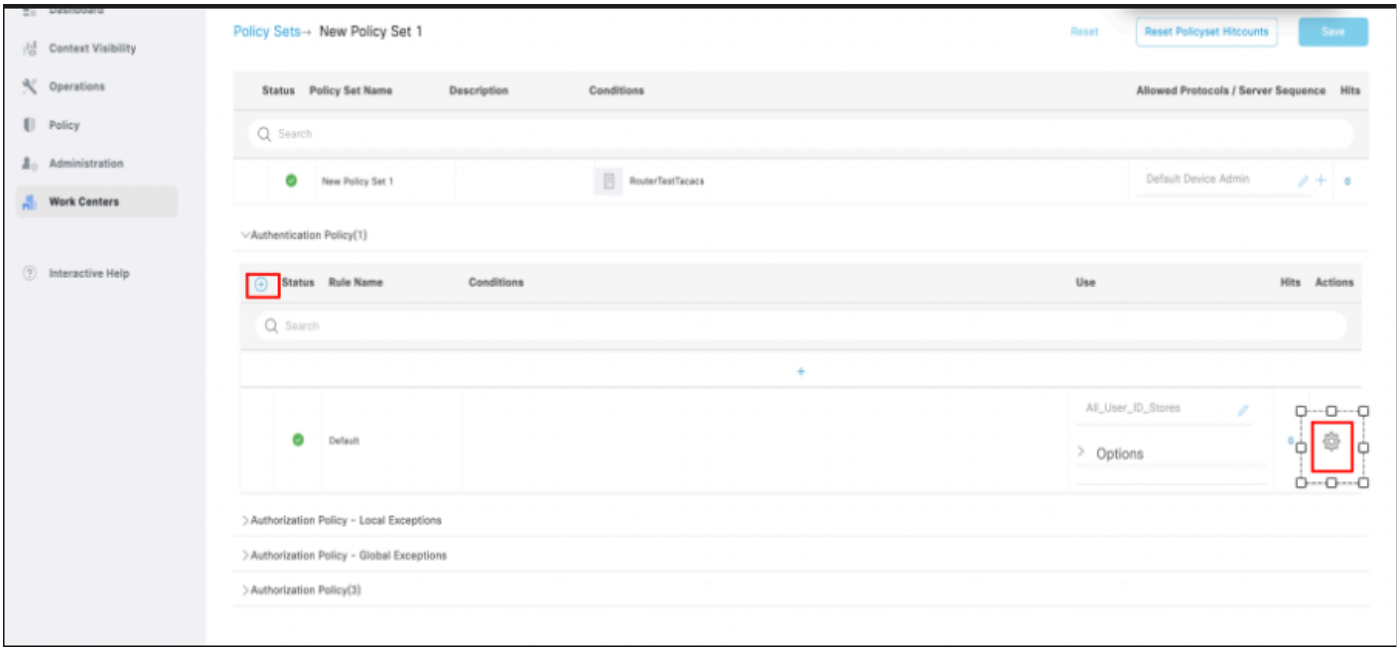
---

4. بعد تكوين الشروط وحفظها، قم بتكوين البروتوكولات المسموح بها كمسؤول جهاز افتراضي. احفظ مجموعة النهج التي تم إنشاؤها بالنقر فوق الخيار حفظ .

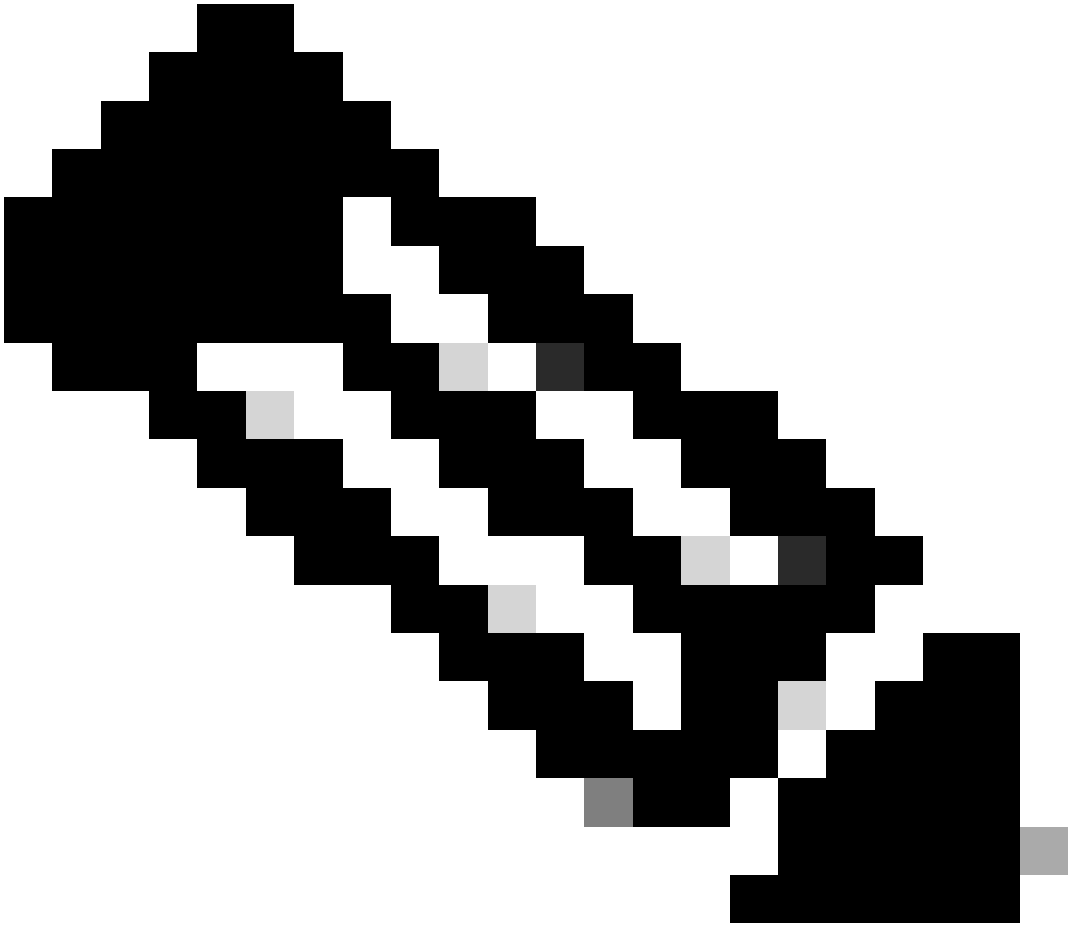


تأكيد تكوين مجموعة النهج.

5. توسيع مجموعة النهج الجديدة -> نهج المصادقة (1) -> إنشاء سياسة مصادقة جديدة بالنقر فوق رمز + (زائد) أو بالنقر فوق رمز العتاد، ثم إدراج صف جديد أعلاه.



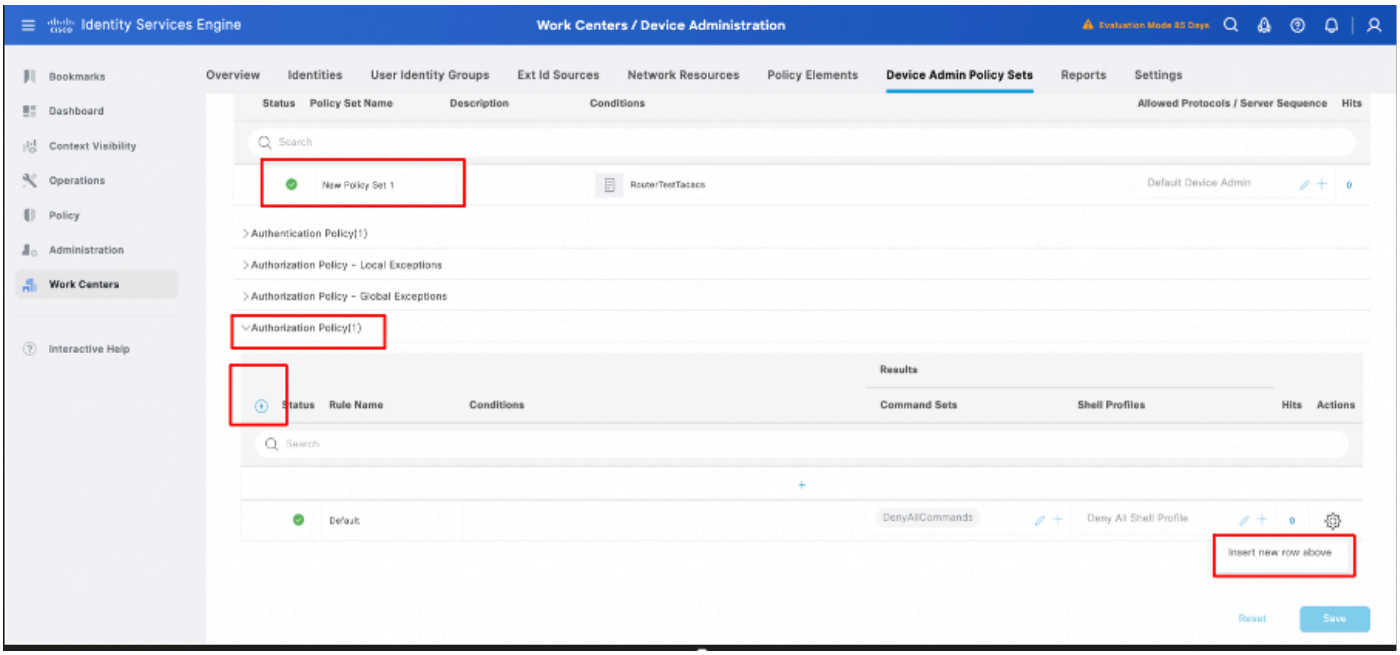
تكوين نهج المصادقة في مجموعة النهج.



ملاحظة: في هذا العرض، يتم إستخدام نهج المصادقة الافتراضي الذي تم تعيينه مع كافة_user_id_store. ومع ذلك، يمكن تخصيص إستخدام مخازن الهوية وفقا لمتطلبات النشر.

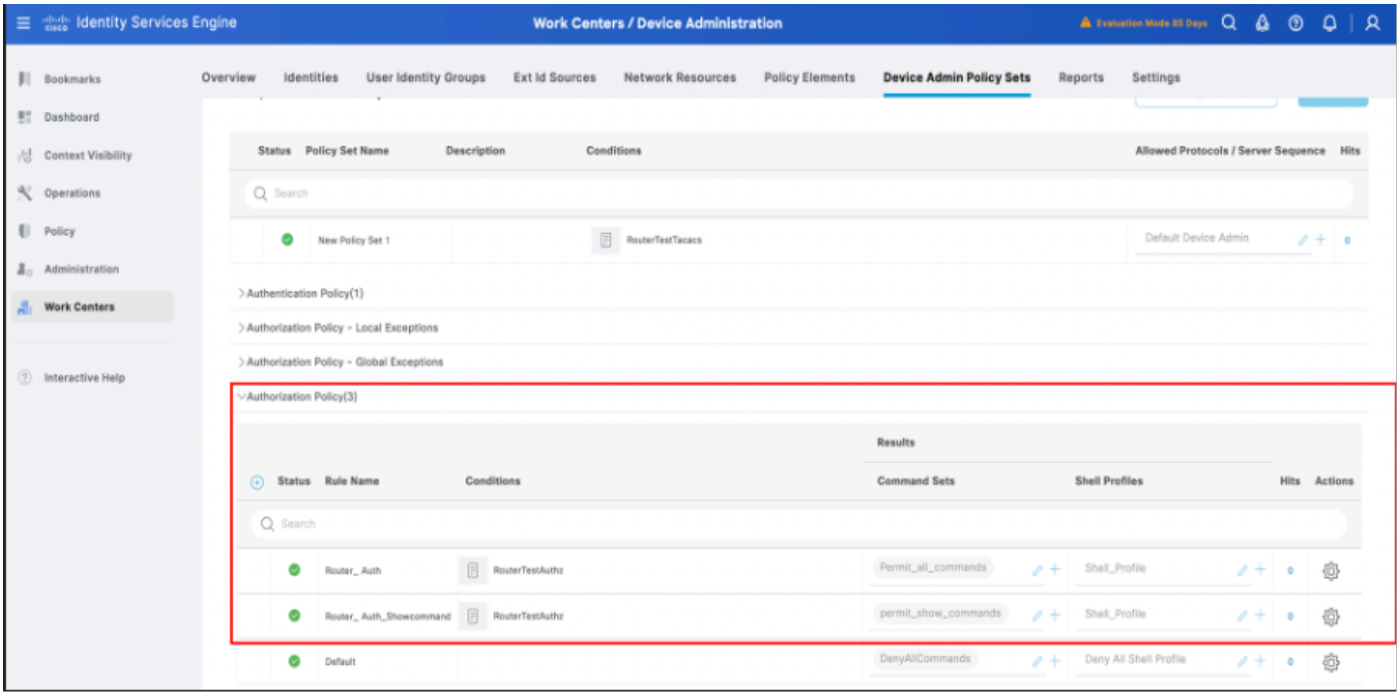
---

6. توسيع مجموعة السياسات الجديدة -> نهج التفويض (1). إما أن تنقر أيقونة + (زائد) أو أن تنقر أيقونة الترس. ثم، قم بإدراج صف جديد أعلاه لإنشاء نهج تخويل.

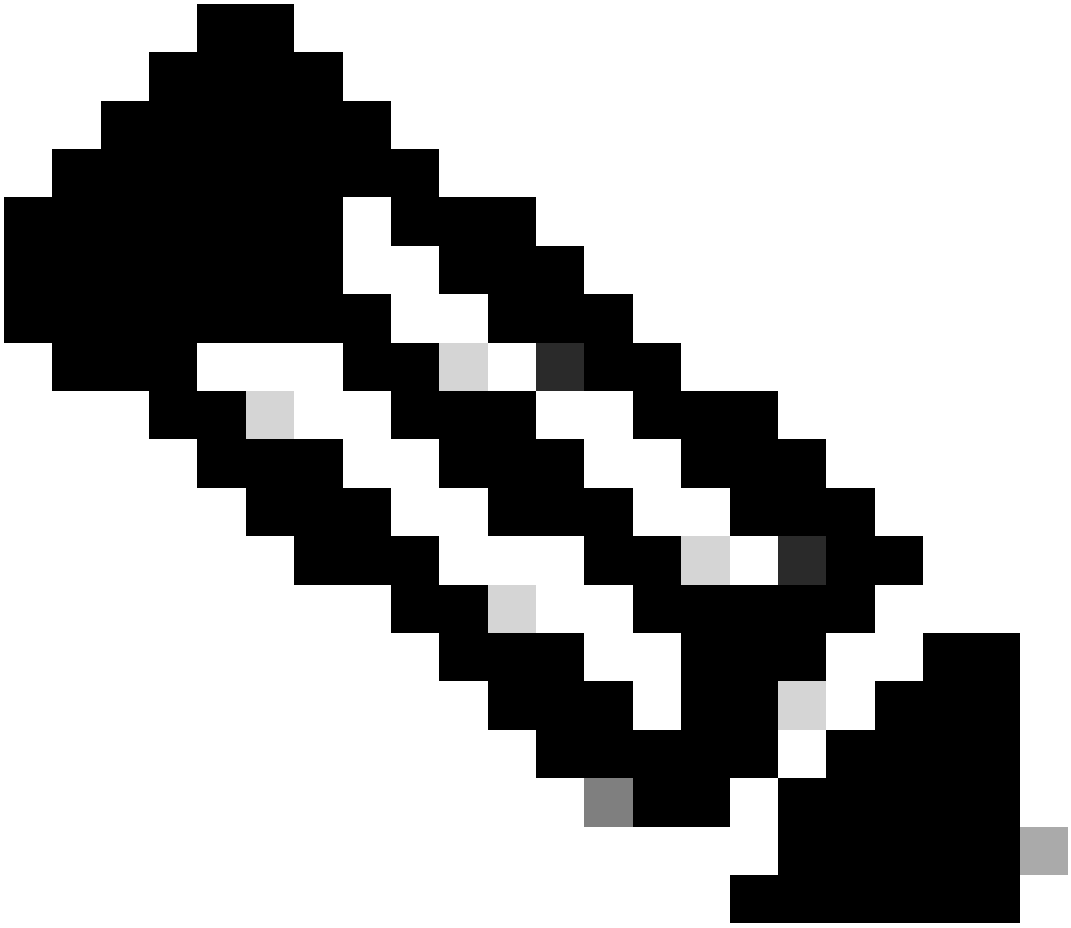


تكوين سياسة التخويل

7. قم بتكوين نهج التخويل بشروط ومجموعات أوامر وملف تعريف shell معين إلى سياسات التخويل.



إكمال تكوين نهج التخويل في ISE



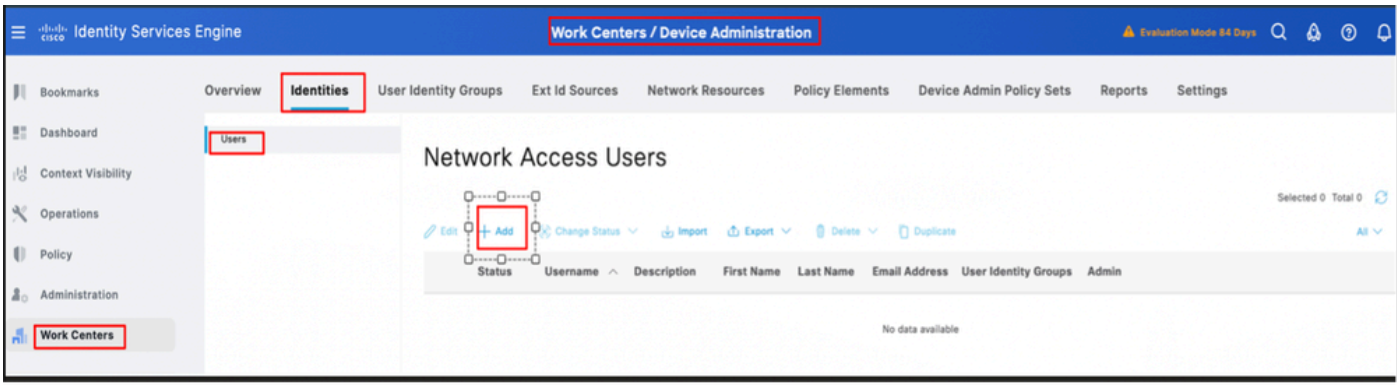
ملاحظة: يتم تكوين الشروط وفقا لبيئة المختبر ويمكن تكوينها وفقا لمتطلبات النشر.

---

8. اتبع الخطوات الست الأولى لتكوين مجموعات السياسات للمحول أو أي جهاز شبكة آخر يستخدم ل TACACS+.

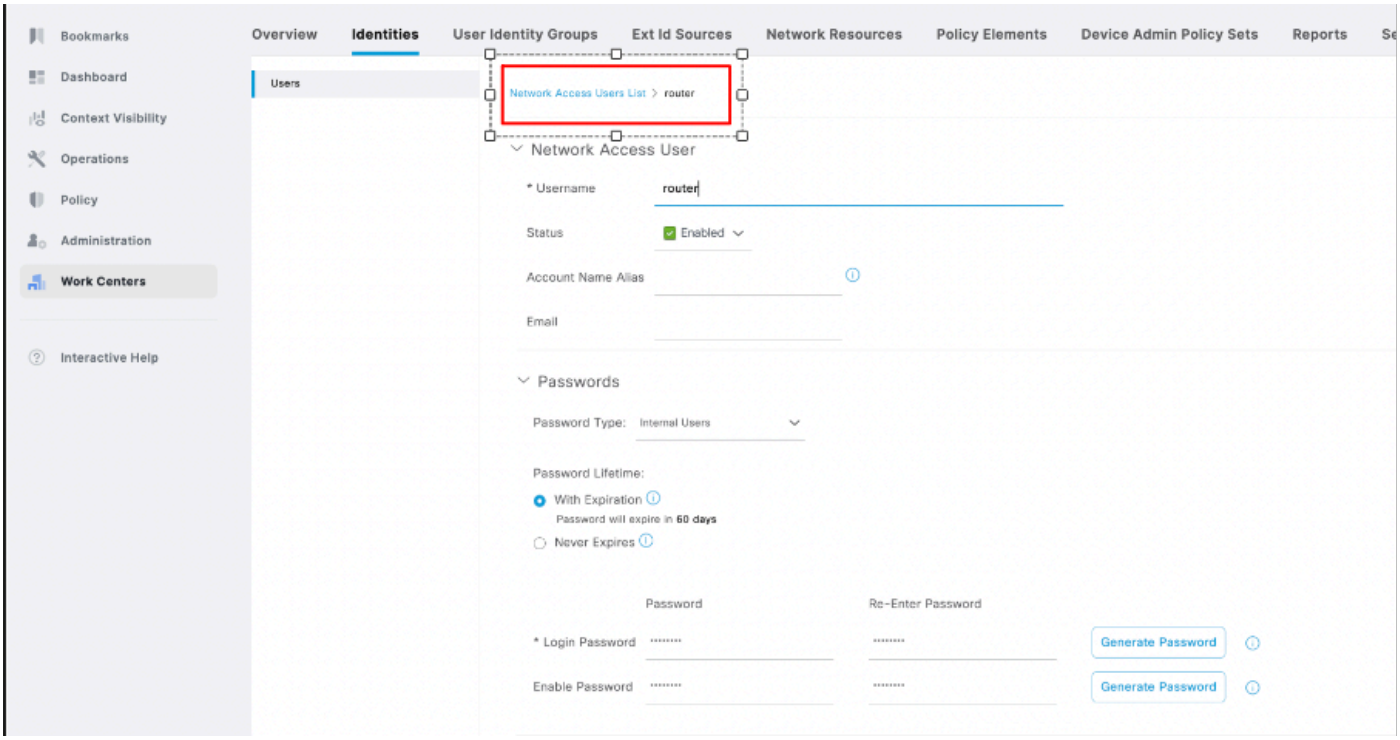
تكوين مستخدمي الوصول إلى الشبكة لمصادقة NAD TACACS في ISE

1. انتقل إلى مراكز العمل -> إدارة الأجهزة -> الهويات -> المستخدمون. انقر فوق أيقونة +(زائد) لإنشاء مستخدم جديد.



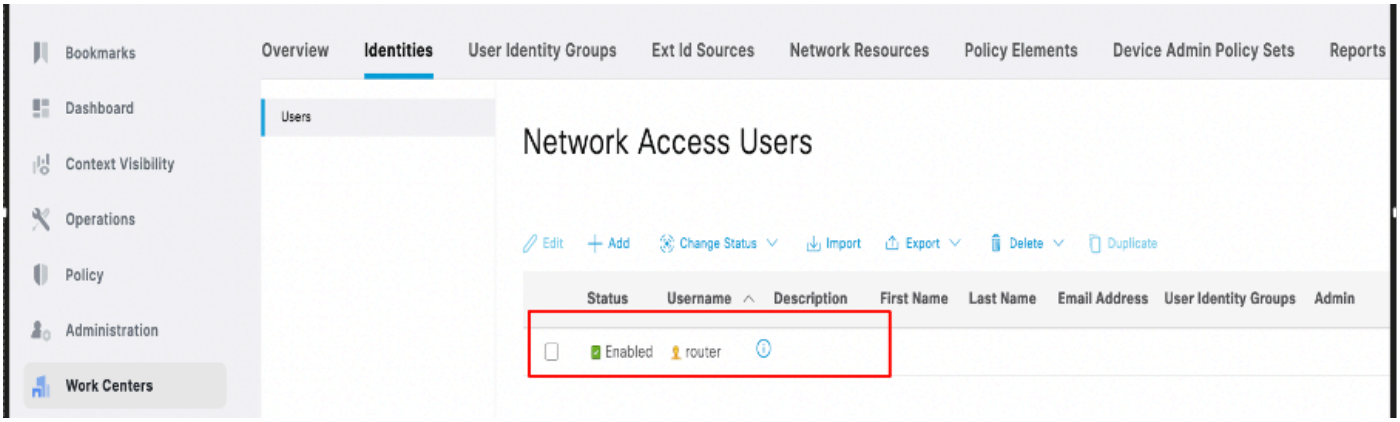
تكوين مستخدمي الوصول إلى الشبكة في ISE

2. قم بتوفير لتوسيع تفاصيل اسم المستخدم وكلمة المرور، وقم بتعيين المستخدم إلى مجموعة هوية المستخدم (إختياري)، ثم انقر فوق إرسال.



تكوين مستخدمي الوصول إلى الشبكة - متابعة

3. بعد إرسال تكوين اسم المستخدم في مراكز العمل -> الهويات -> المستخدمون -> مستخدمو الوصول إلى الشبكة ، يتم تكوين المستخدم وتمكينه بشكل مرئي.



تأكيد تكوين مستخدم الوصول إلى الشبكة.

تكوين موجه لـ TACACS+

تكوين موجه Cisco IOS لمصادقة TACACS+ وتخويل

1. قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة بالموجه وقم بتشغيل هذه الأوامر لتكوين TACACS في الموجه.

الأمر ASR1001-X(config)#aaa new-model — المطلوب لتمكين المصادقة والتفويض والمحاسبة (AAA) في NAD

ASR1001-X(config)#aaa session-id مشترك. —الأمر المطلوب لتمكين المصادقة والتفويض والمحاسبة (AAA) في NAD.

ASR1001-X(config)#aaa صحة هوية تسجيل الدخول المجموعة الافتراضية TACACS+ محلي

ASR1001-X(config)#aaa authorization exec default group tacacs+

ASR1001-X(config)#aaa تخويل شبكة قائمة1 مجموعة tacacs+

ASR1001-X(config)#tacacs server ise1

ASR1001-X(config-server-tacacs)#address ipV4 <عنوان IP الخاص بخادم TACACS > — عنوان ISE Interface G1 IP.

ASR1001-X(config-server-tacacs)# key xxxx

ASR1001-X(config)# aaa مجموعة لدان tacacs+ iseggroup

ASR1001-X(config-sg-tacacs+)#server name ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X(config)#exit

2. بعد حفظ تكوينات TACACS+ للموجه، تحقق من تكوين TACACS+ باستخدام الأمر show run aaa.

ASR1001-X#show ركض AAA

!

مجموعة AAA الافتراضية لتسجيل الدخول لمصادقة AAA المحلية

مجموعة مجموعات AAA الافتراضية لتفويض EXEC

مجموعة AAA لمجموعة أذون الشبكة 1

كلمة مرور مسؤول username 0 xxxxx

!

tacacs server ise1

عنوان IPv4 <عنوان IP لخادم TACACS>

المفتاح XXXXX

!

!

مجموعة AAA خادم tacacs+ iseggroup

اسم الخادم ise1

IP vrf Forwarding Mgmt-intf

ip tacacs source-interface GigabitEthernet1

!

!

!

aaa new-model

AAA جلسة-id مشترك

!

!

تكوين المحول لـ TACACS+

تكوين المحول لمصادقة TACACS+ والتفويض

1. login إلى الـ CLI من المفتاح وشغل هذه الأمر لـ يشكل TACACS في المفتاح.

C9200L-48P-4X#configure T

دخلت تشكيل أمر، واحد لكل خط. إنهاء بـ CNTL/Z.

C9200L-48P-4X(config)#aaa جديد-model. — الأمر المطلوب لتمكين المصادقة والتفويض والمحاسبة (AAA) في NAD

C9200L-48P-4X(config)#aaa session-id مشترك. — الأمر المطلوب لتمكين المصادقة والتفويض والمحاسبة (AAA) في NAD.

C9200L-48P-4X(config)#aaa صحة هوية تسجيل الدخول مجموعة افتراضية مجموعة ISGgroup محلي

C9200L-48P-4X(config)#aaa تخويل مجموعة افتراضية

C9200L-48P-4X(config)#aaa تخويل شبكة قائمة 1 مجموعة مجموعة

C9200L-48P-4X(config)#tacacs server ise1

c9200L-48P-4X(config-server-tacacs)#address ipV4 <عنوان TACACS server> — عنوان ISE Interface G1 IP.

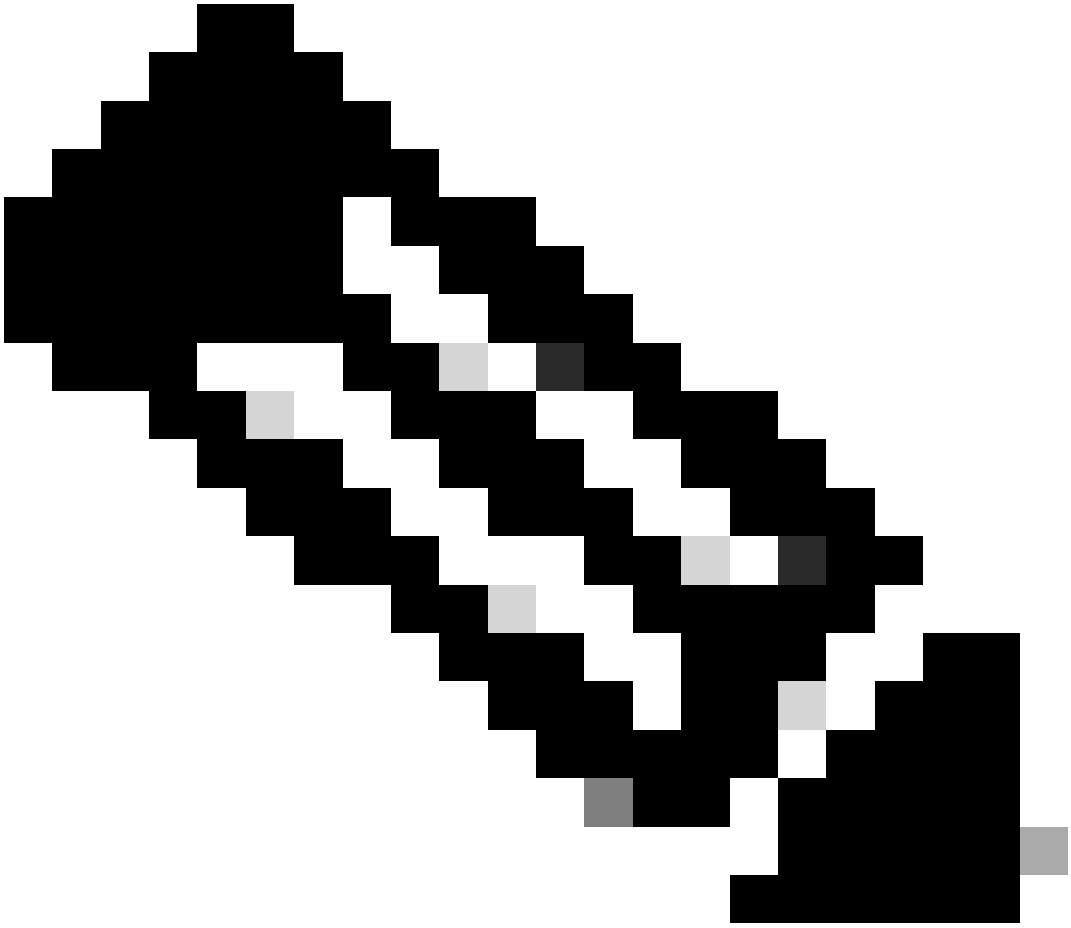
C9200L-48P-4X(config-server-tacacs)#key XXXX

C9200L-48P(config)#aaa مجموعة لدان tacacs+ iseggroup

C9200L-48P(config-sg-tacacs+)#server name ise1

C9200L-48P-4X(config)#exit

C9200L-48P-4X#wr mem



ملاحظة: في تكوين NAD TACACS+، TACACS+ هي المجموعة التي يمكن تخصيصها وفقا لمتطلبات النشر.

2. بعد حفظ تكوينات TACACS+ للمحول، تحقق من تكوين TACACS+ باستخدام الأمر show run aaa.

C9200L-48P#show يركض AAA

!

مجموعة AAA الافتراضية لتسجيل الدخول لمصادقة AAA المحلية

مجموعة مجموعات AAA الافتراضية لتفويض EXEC

مجموعة AAA لمجموعة أذون الشبكة 1

كلمة مرور مسؤول username 0 xxxx

!

!

tacacs server ise1

عنوان IPv4 <عنوان IP لخادم TACACS>

المفتاح XXXXX

!

!

مجموعة AAA خادم tacacs+ iseggroup

اسم الخادم ise1

!

!

!

aaa new-model

AAA جلسة-id مشترك

!

!

التحقق

التحقق من الموجه

من واجهة سطر الأوامر (CLI) الخاصة بالموجه، مصادقة القيمة ل TACACS+ مقابل ISE مع واجهة Gigabit Ethernet 1 باستخدام الأمر test aaa group tacacsgroupname username password new .

وفيما يلي نموذج للمخرجات من الموجه & ISE:

التحقق من المنفذ 49 من الموجه:

ASR1001-X#telnet ISE Gig 1 interface IP 49

يتم الآن محاولة إستخدام ISE GIg 1 interface IP، 49... فتح

الموجه ASR1001-X#test AAA Group Router XXXX جديد

إرسال كلمة المرور

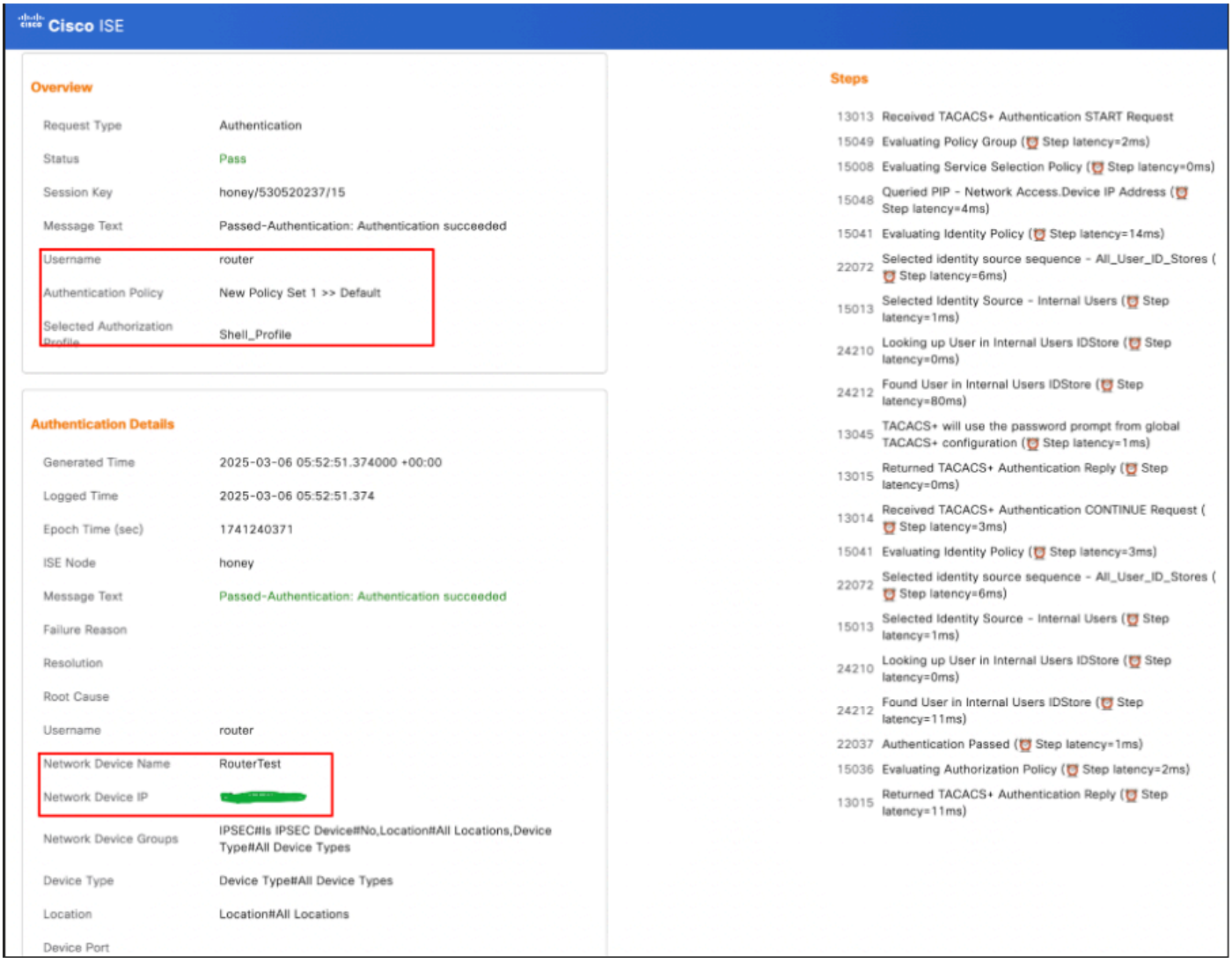
تمت مصادقة المستخدم بنجاح

سمات المستخدم

username 0 "مسجاج تخديد"

رسالة الدر 0 "كلمة المرور:"

للتحقق من ISE، سجل الدخول إلى واجهة المستخدم الرسومية -> العمليات -> سجلات TACACS المباشرة، ثم قم بالتصفية باستخدام موجه IP في حقل تفاصيل جهاز الشبكة.



TACACS Live Log من ISE - التحقق من الموجه.

التحقق من المحول

من واجهة سطر الأوامر (CLI) للمحول، تحقق من مصادقة TACACS+ مقابل ISE مع واجهة Gigabit Ethernet 1 باستخدام الأمر test aaa group tacacsgroupname password newn:

وفيما يلي نموذج للمخرجات من المحول و ISE.

التحقق من المنفذ 49 من المحول:

C9200L-48P# telnet ISE Gig1 Interface IP 49

يتم الآن محاولة إدخال ISE Gig1 interface IP، 49... فتح

المحول C9200L-48P#test AAA Group Switch XXXX جديد

إرسال كلمة المرور

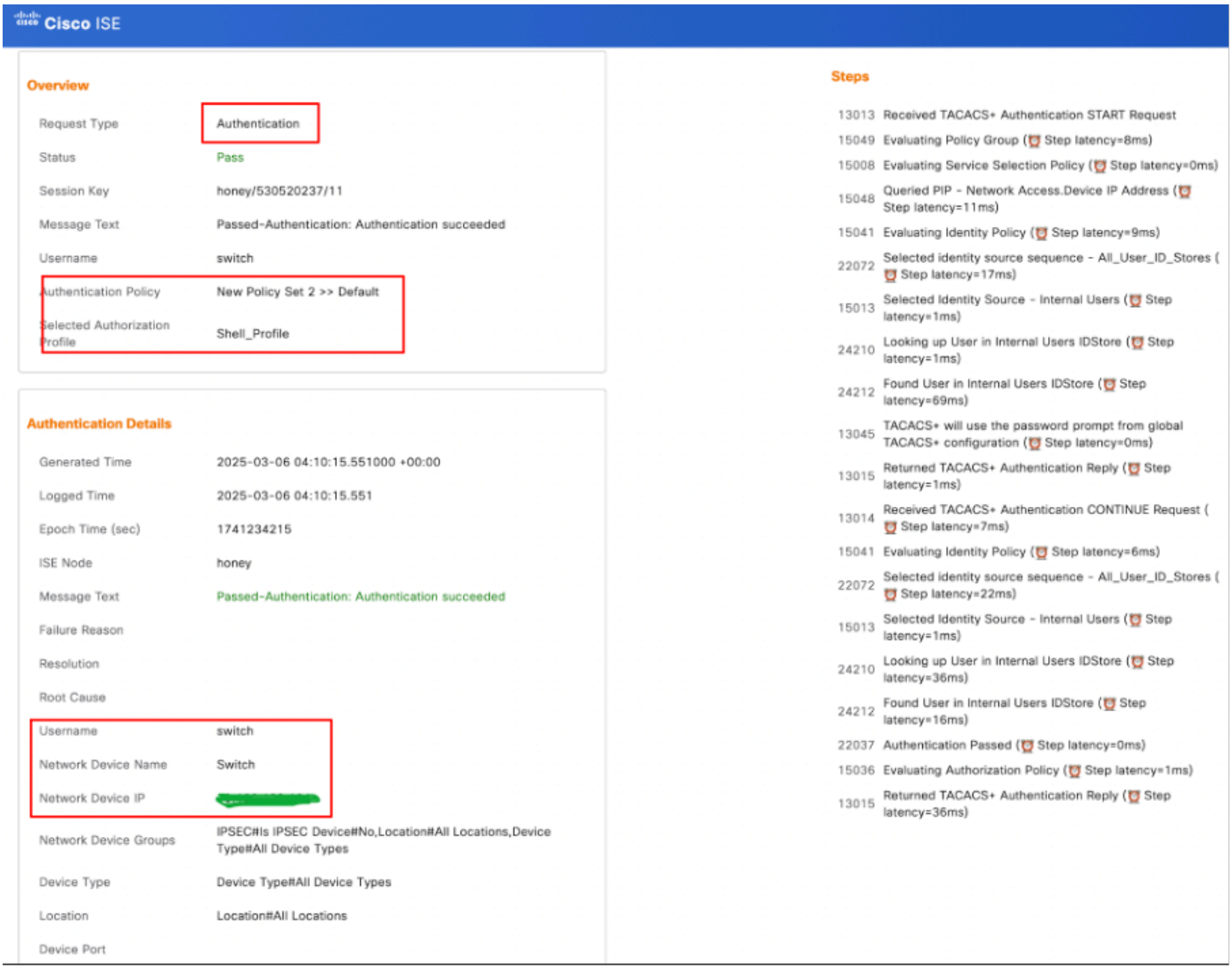
تمت مصادقة المستخدم بنجاح

سمات المستخدم

username 0 "مفتاح"

رسالة الرد 0 "كلمة المرور:"

للتحقق من ISE، سجل الدخول إلى واجهة المستخدم الرسومية -> العمليات -> سجلات TACACS المباشرة، ثم قم بالتصفية باستخدام مفتاح IP في حقل تفاصيل جهاز الشبكة.



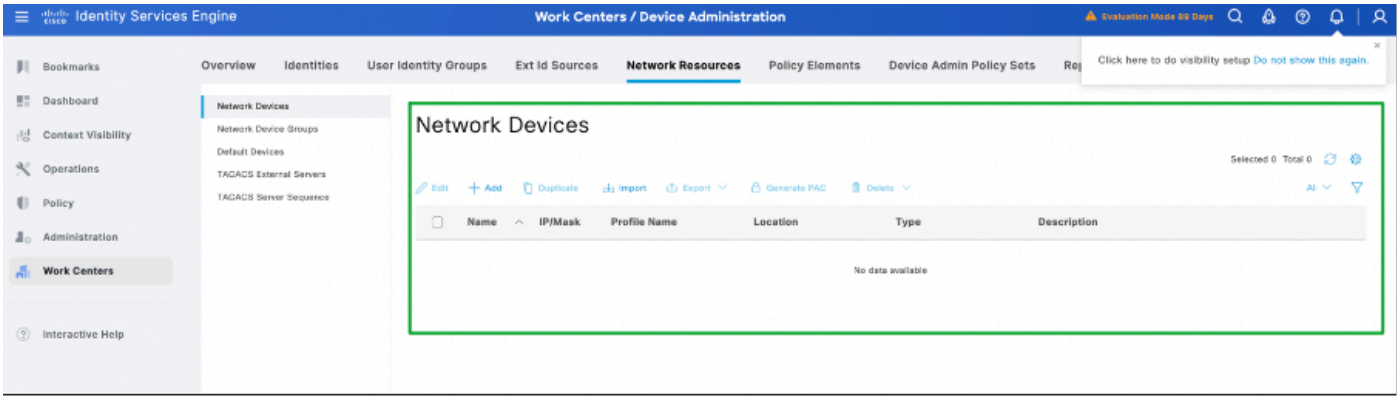
TACACS Live Log من ISE - التحقق من المحول.

استكشاف الأخطاء وإصلاحها

يناقش هذا القسم بعض القضايا المشتركة التي تم العثور عليها فيما يتعلق بمصادقة TACACS+.

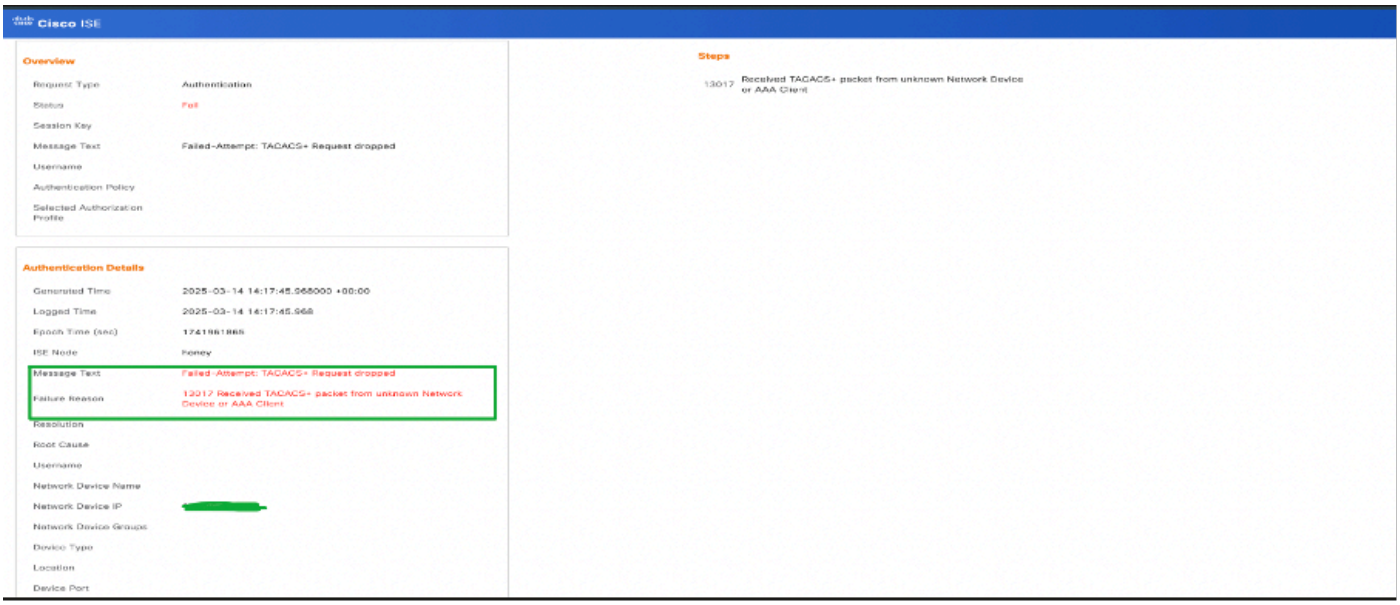
السيناريو 1: تفشل مصادقة TACACS+ مع الخطأ: حزمة TACACS+ المقفلة طراز 13017 من جهاز شبكة غير معروف أو عميل AAA".

يحدث هذا السيناريو عند عدم إضافة جهاز الشبكة كموارد شبكة في ISE. كما هو موضح في لقطة الشاشة هذه، لا تتم إضافة المحول في موارد الشبكة الخاصة ب ISE.



سيناريو أستكشاف الأخطاء وإصلاحها - لا تتم إضافة أجهزة الشبكة في ISE.

الآن، عندما تختبر المصادقة من المحول / جهاز الشبكة، تصل الحزمة إلى ISE كما هو متوقع. ومع ذلك، تفشل المصادقة مع حدوث الخطأ أخطأ : تلقى الطراز 13017 حزمة TACACS+ من جهاز شبكة غير معروف أو عميل AAA" كما هو موضح في لقطة الشاشة هذه:



سجلات TACACS المباشرة - فشل عند عدم إضافة جهاز الشبكة إلى ISE.

التحقق من جهاز الشبكة (المحول)

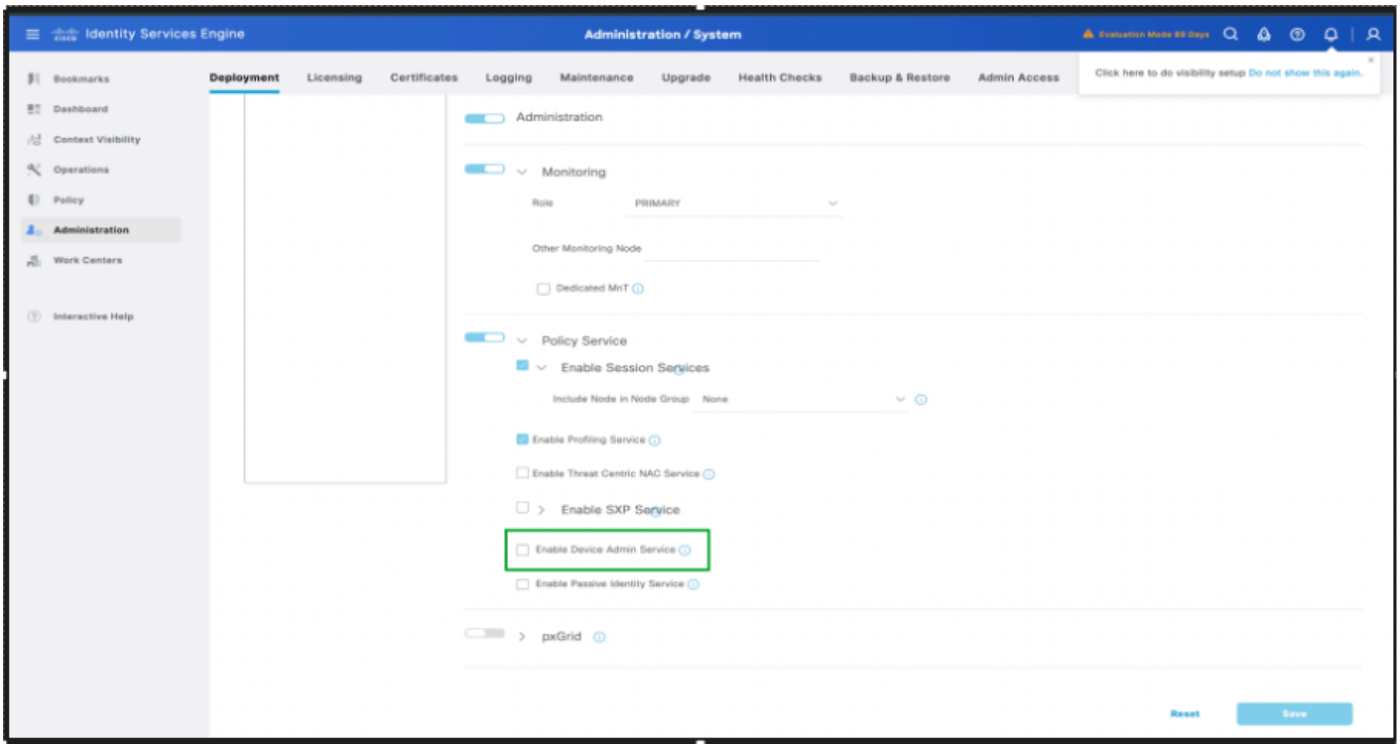
المحول #testAAA مجموعة مجموعة محول XXXXX جديد
تم رفض المستخدم

الحل: تحقق من إضافة المحول / الموجه / جهاز الشبكة كجهاز الشبكة في ISE. إذا لم تتم إضافة الجهاز، فقم بإضافة جهاز الشبكة إلى قائمة جهاز الشبكة الخاصة ب ISE.

السيناريو الثاني : يقوم ISE بإسقاط حزمة TACACS+ بصمت بدون أية معلومات.

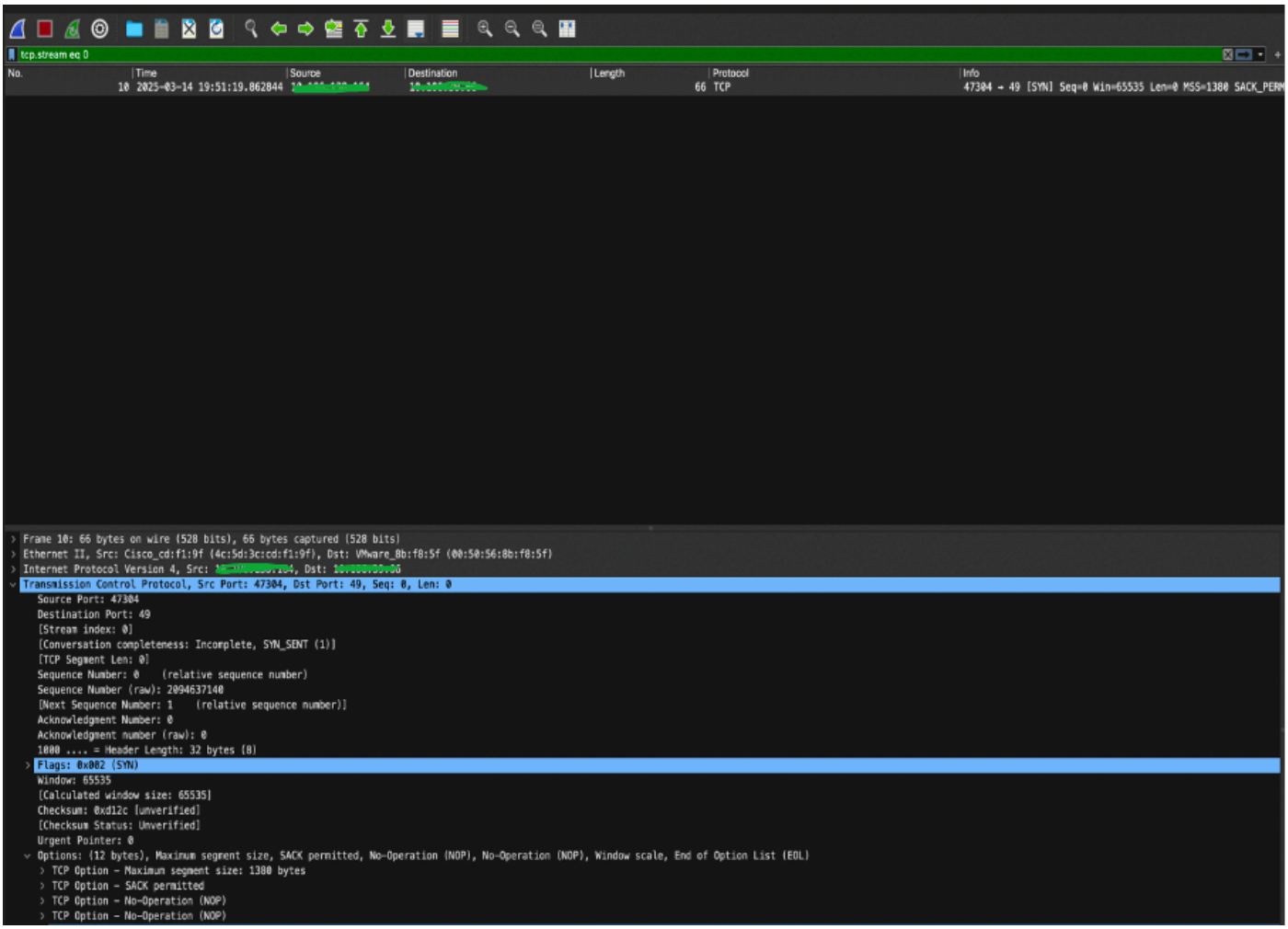
يحدث هذا السيناريو عندما يتم تعطيل خدمة إدارة الأجهزة في ISE. في هذا السيناريو، يقوم ISE بإسقاط الحزمة و الى يتم ملاحظة أي سجلات حية حتى على الرغم من أنه يتم بدء المصادقة من جهاز الشبكة الذي تتم إضافته إلى موارد الشبكة الخاصة ب ISE.

كما هو موضح في لقطة الشاشة هذه، تم تعطيل إدارة الأجهزة في ISE.



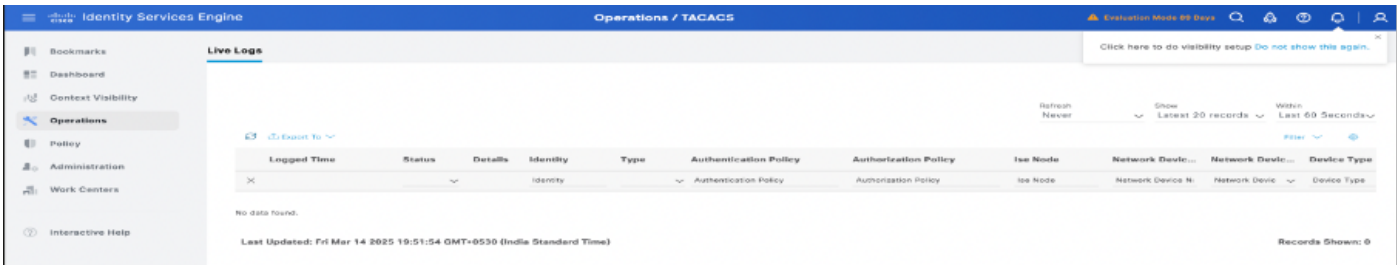
السيناريو، لم يتم تمكين إدارة الجهاز في ISE.

عندما يقوم المستخدم بتهيئة المصادقة من جهاز الشبكة، يقوم ISE بإسقاط الحزم دون أي معلومات في السجلات المباشرة و الى يستجيب ISE إلى حزمة Syn التي يتم إرسالها بواسطة جهاز الشبكة لإكمال عملية مصادقة TACACS. ارجع إلى لقطة الشاشة هذه:



ISE إسقاط الحزم بصمت أثناء TACACS

يظهر ISE ام من سجل حي أثناء المصادقة.



ال توجد سجلات مباشرة ل TACACS - التحقق من ISE

التحقق من جهاز الشبكة (المحول)

المحول#
المحول #testAAA مجموعة محول XXXX جديد
تم رفض المستخدم
المحول#
*14 مارس 13:54:28.144: ت+: الإصدار 192 (0xC0)، النوع 1، seq 1، التشفير 1، SC 0
*14 مارس 13:54:28.144: ت+: session_id 10158877 (0x9B031D)، dlen 14 (0xE)
*14 مارس 13:54:28.144: ت+: الكتابة:AUTHEN/START، priv_lvl:15 action:تسجيل الدخول ascii
*14 مارس 13:54:28.144: ت+: svc:Login user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0
*14 مارس 13:54:28.144: ت+: المستخدم: تبديل
*14 مارس 13:54:28.144: ت+: المنفذ:
*14 مارس 13:54:28.144: ت+: rem_addr:
*14 مارس 13:54:28.144: ت+: البيانات:
*14 مارس 13:54:28.144: ت+: انعاء الحزمة

الحل: تمكين إدارة الأجهزة في ISE.

المرجع

- استكشاف أخطاء مصادقة TACACS والحلها
- دليل مسؤول لمحرك خدمات الهوية من Cisco، الإصدار 3.3
- TACACS لمداخل VRF

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).