

ISE Gigabit Ethernet ةهجاو عم TACACS+ نيوكت 1

تايوتحمل

[ةمدقملا](#)

[ةيساسأ تامولعم](#)

[ةيساسأ ل تاب ل ط ت م ل ا](#)

[تاب ل ط ت م ل ا](#)

[ةمدخت س م ل ا ت ا ن و ك م ل ا](#)

[ن ي و ك ت ل ا](#)

[ةك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[TACACS+ ل ةي و ل ا ت ا م د خ ك ر ح م ن ي و ك ت](#)

[ISE ي ف 1 Gigabit Ethernet ةهجاو ل IP ن ا و ن ع ن ي و ك ت](#)

[ISE ي ف ةز ه ج ا ل ا ة ر ا د ا ن ي ك م ت](#)

[ISE ي ف ةك ب ش ز ا ه ج ة ف ا ض ا](#)

[TACACS+ ر م ا و ا ت ا ع و م ح م ن ي و ك ت](#)

[TACACS+ ف ي ر ع ت ف ل م ن ي و ك ت](#)

[TACACS+ ض ي و ف ت ة ق د ا ص م ف ي ر ع ت ف ل م ن ي و ك ت](#)

[ISE ي ف NAD TACACS ة ق د ا ص م ل ة ك ب ش ل ل ا ل ل و ص و ل ا ي م د خ ت س م ن ي و ك ت](#)

[TACACS+ ل ه ج و م ن ي و ك ت](#)

[ل ي و خ ت و TACACS+ ة ق د ا ص م ل Cisco IOS ه ج و م ن ي و ك ت](#)

[TACACS+ ل ل و ح م ل ا ن ي و ك ت](#)

[ض ي و ف ت ل ا و TACACS+ ة ق د ا ص م ل ل و ح م ل ا ن ي و ك ت](#)

[ق ق ح ت ل ا](#)

[ه ج و م ل ا ت م ق ق ح ت ل ا](#)

[ل و ح م ل ا ت م ق ق ح ت ل ا](#)

[ا ه ج ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا](#)

[\(ل و ح م ل ا\) ة ك ب ش ل ل ا ز ا ه ج ت م ق ق ح ت ل ا](#)

[\(ل و ح م ل ا\) ة ك ب ش ل ل ا ز ا ه ج ت م ق ق ح ت ل ا](#)

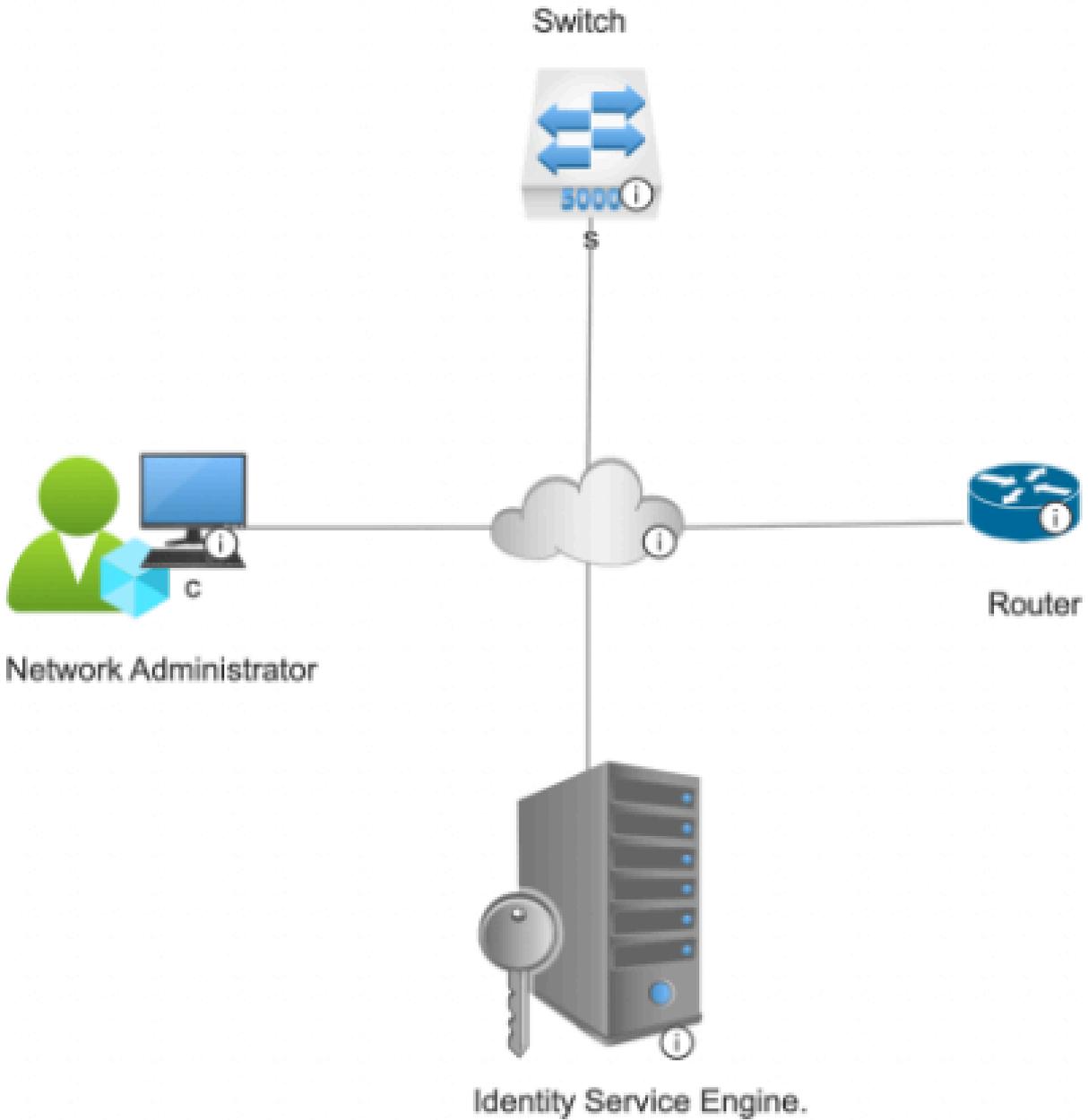
[ع ج ر م ل ا](#)

ةمدقملا

هجوملا لمعي شيح 1 Gigabit Ethernet ةهجاو عم TACACS+ ISE نيوكت دنت س م ل ا اذه فص ي ةك ب ش ةز ه ج ا ك ل و ح م ل ا و

ةيساسأ تامولعم

، تادنس ثالث يوس اهل نوكي نا نكمي الو. Ethernet تاهجاو 6 ل ل لص ي ام Cisco ISE م ع د ي رود ريغت و ا دنس نم عزج يه يتل تاهجاو ل ريغت مكنكمي الو. 2 دنسو، 1 دنس، 0 دنس



ةكبشلا ايجولوبوط

TACACS+ ل ةيوهلا تامدخ كرحم نيوكت

ISE ف 1 Gigabit Ethernet ةهجاول IP ناوع نيوكت

1. نم ققحت و زاهجلا لوؤسم نيكمتم تي شيح ISE PSN ةدقعب صاخلا CLI ل لوخدلا لچس.
show interface: رمألا مادختساب ةحاتملا تاهجاولا

```
honey/admin# show interface
```

```
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 100.255.255.1 netmask 255.255.255.0 broadcast 100.255.255.255  
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 100.255.255.2 netmask 255.255.255.0 broadcast 100.255.255.255  
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 100.255.255.15 netmask 255.255.255.0 broadcast 100.255.255.255  
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
```

ىلع زيكرتلا عم، ISE، يف طقف تاهجاو ثالث نيوكت متي، نيوكتلا اذه يف: ةظحالم
عيمجل IP ناوع نيوكتل هسفن ءارجلا قيبطت نكمي. 1. Gigabit Ethernet ةهجاو
Gigabit Ethernet تاهجاو تسىل لصي ام ISE معدى، يضارتفا لكشبو. تاهجاولا

2. Gigabit Ethernet ةهجاو لىل IP ناوع نيويعب مق، PSN ةدقع سفنب صاخلا CLI نم.
رمأوالا هذه مادختساب:

```
hostnameofise#configure t
```

```
hostnameofise/admin(config)#interface gigabit 1
```

```
hostnameofise/admin(config-gigabitEthernet-1)# <ip address> <subnetMask> %  
ريغت ي دؤي دق %  
ISE تامدخ ليغشت ةداع لىل IP ناوع
```

IP ناوع ريغت عم ةعباتملا ديرت له

معن [ال، معن]؟ ةعباتملا ديرت له

3. ISE، تامدخ ةلاح نم ققحتلل ISE ةدقع تامدخ ليغشت ةداع|ىل| 2 ةوطخال ذيفنت يدؤي. مق ةطوقل اقفو تامدخال ةلاح ليغشت نم دكأتو show application status ise رمالا ليغشتب هذه ةشاشلا:

```
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

ISE ةمدخ ةلاح نم ققحتلا

4. show interface رمالا مادختساب Gig1 ةهجاوب صاخلا IP ناووع نم ققحت:

v

```

honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 192.254.2.3 netmask 255.255.255.0 broadcast 192.254.2.255
  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 192.254.1 netmask 255.255.255.0 broadcast 192.254.1.255
  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 192.254.256 netmask 255.255.255.0 broadcast 192.254.256.255
  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 192.254.257 netmask 255.255.255.0 broadcast 192.254.257.255
  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

```

CLI نم ISE Gig2 ةه اول IP ناونع نم ققحتال

5. INC 49 | رمأ show ports مادختساب ISE ةدقع يف 49 ذفنم لابل حامس لال نم ققحت.

```

honey/admin#show ports | include 49
tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, 192.254.256:49, 192.254.257:49,

```

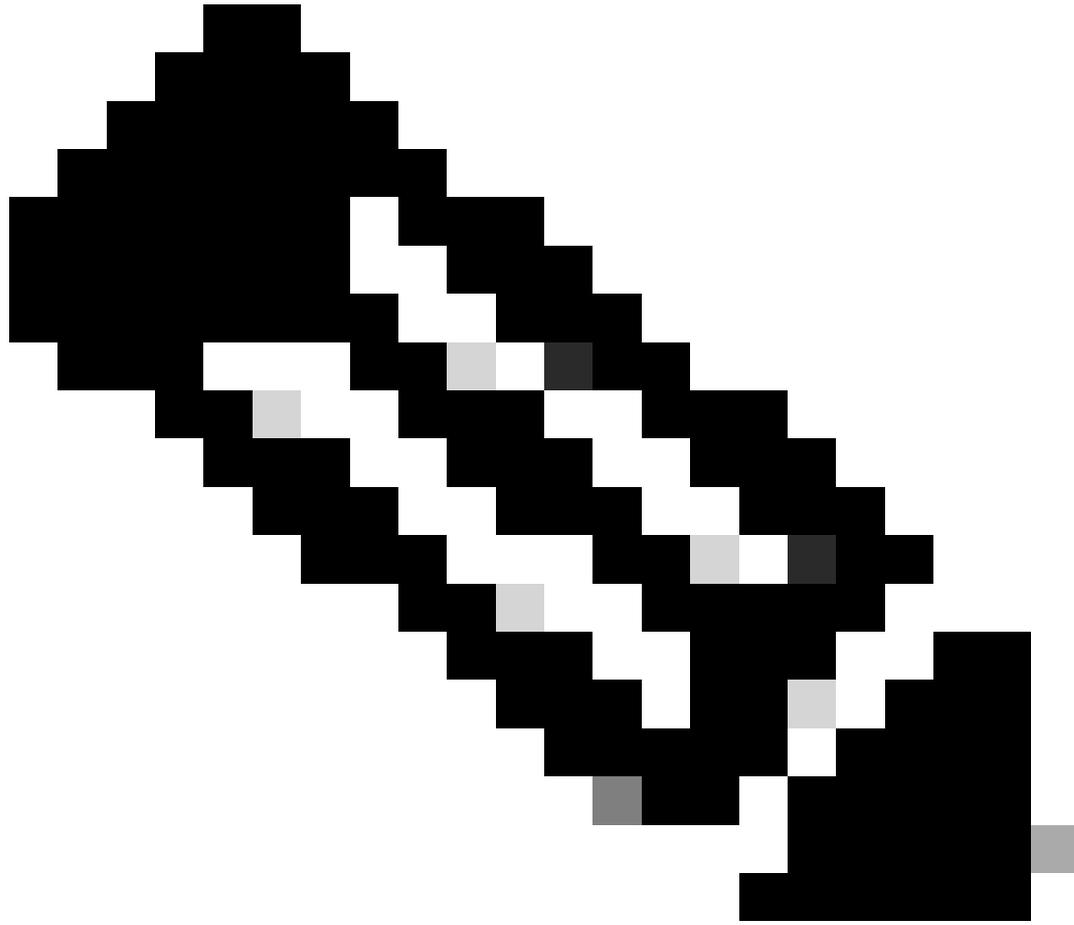
ISE يف 49 ذفنم لابل لذب نم ققحتال

ISE في ةزهجألا ةرادإ نيكمم

م، PSN ةدق ع ديحت > رشنلا > ةرادإلا > ISE ل (GUI) ةيموسرلا مدختسمل ةهجاو ل لقتنا
زاهجلا ةرادإ ةمدخ نيكمم ددح:

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System page. The page is divided into several tabs: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, and Health Checks. The 'Policy Service' section is expanded, showing a list of services that can be enabled or disabled. The 'Enable Device Admin Service' option is checked and highlighted with a red box. Other services listed include 'Enable Session Services', 'Enable Profiling Service', 'Enable Threat Centric NAC Service', 'Enable SXP Service', and 'Enable Passive Identity Service'. The 'Policy Service' section also includes a toggle switch and a dropdown menu for 'Include Node in Node Group'.

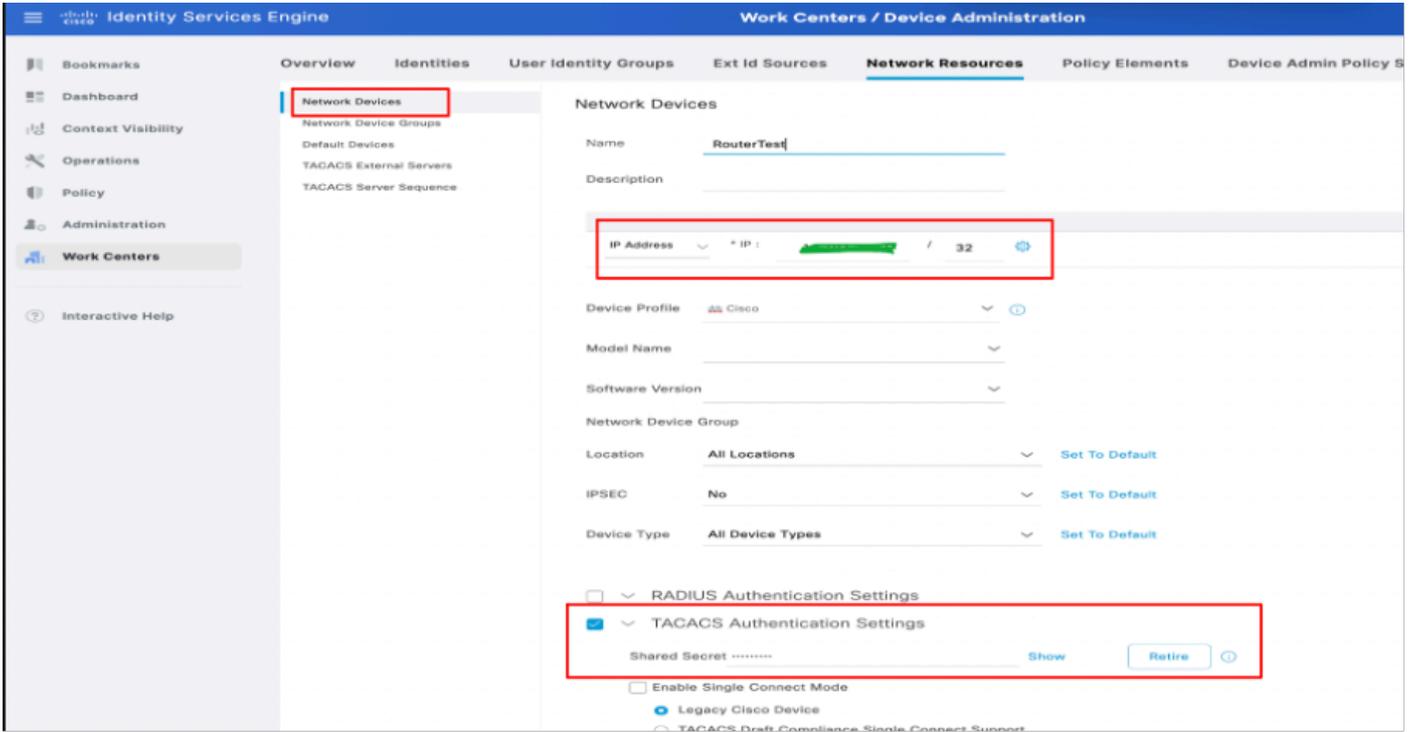
ISE في ةزهجألا ةرادإ ةمدخ نيكمم



زاهجلا ةرادا صيخرت دوجو مزلي ،زاهجلا ةرادا ةمدخ نيكم تل :ةظحالم

ISE في ةكبش زاهج ةفاضإ

ةفاضإ قوف رقنا .ةكبشلا ةزهجأ > ةكبشلا دراوم > ةزهجألا ةرادا > لمعلل زكارم ىلا لقتنا 1.
مقو TACACS+ ةقداصم تادادعإ رايخال ةناخ ددح .IP ناونعو مسالا ريفوتب مق .(Add)
كرتشمالا يرسلالات فملا ريفوتب



ISE في ةكبشال زاهاج نيوكت

2. TACACS ةقداصل ةبولطمال ةكبشال ةزهجأ عيمج ةفاضال هالعأ روكذمال ءارجال عبتا.

TACACS+ رماوأتاعومجم نيوكت

يحيضوتال ضرعال اذهل رماوالا نم نيوتاعومجم نيوكت مت

ىلع رماوالا عيمجب حمسيو مدختسمل لوؤسم الى ALLOWED_ALL_COMMANDS نيوتاعمت متي زاهاجال.

طقف show رماوآب حمسيو مدختسمل هنيوتاعمت متي، allow_show_commands،

1. رقنا TACACS رماوأتاعومجم > ةسايسال جئاتن > ةزهجال ةرادا > لمعال زكارم الى لقتنا. رماوآب حامسال رايتخالال ةناخ رتخأ مت، PermitAllCommands مرسالا ريفوتب مق. ةفاضال لاسرا قوف رقنا. ةجرذمال ريغ.

Identity Services Engine Work Centers / Device Administration

Policy Elements

TACACS Command Sets > New Command Set

Name: permit_show_commands

Description: Only commands which are added in the below list are allowed.

Commands

Permit any command that is not listed below

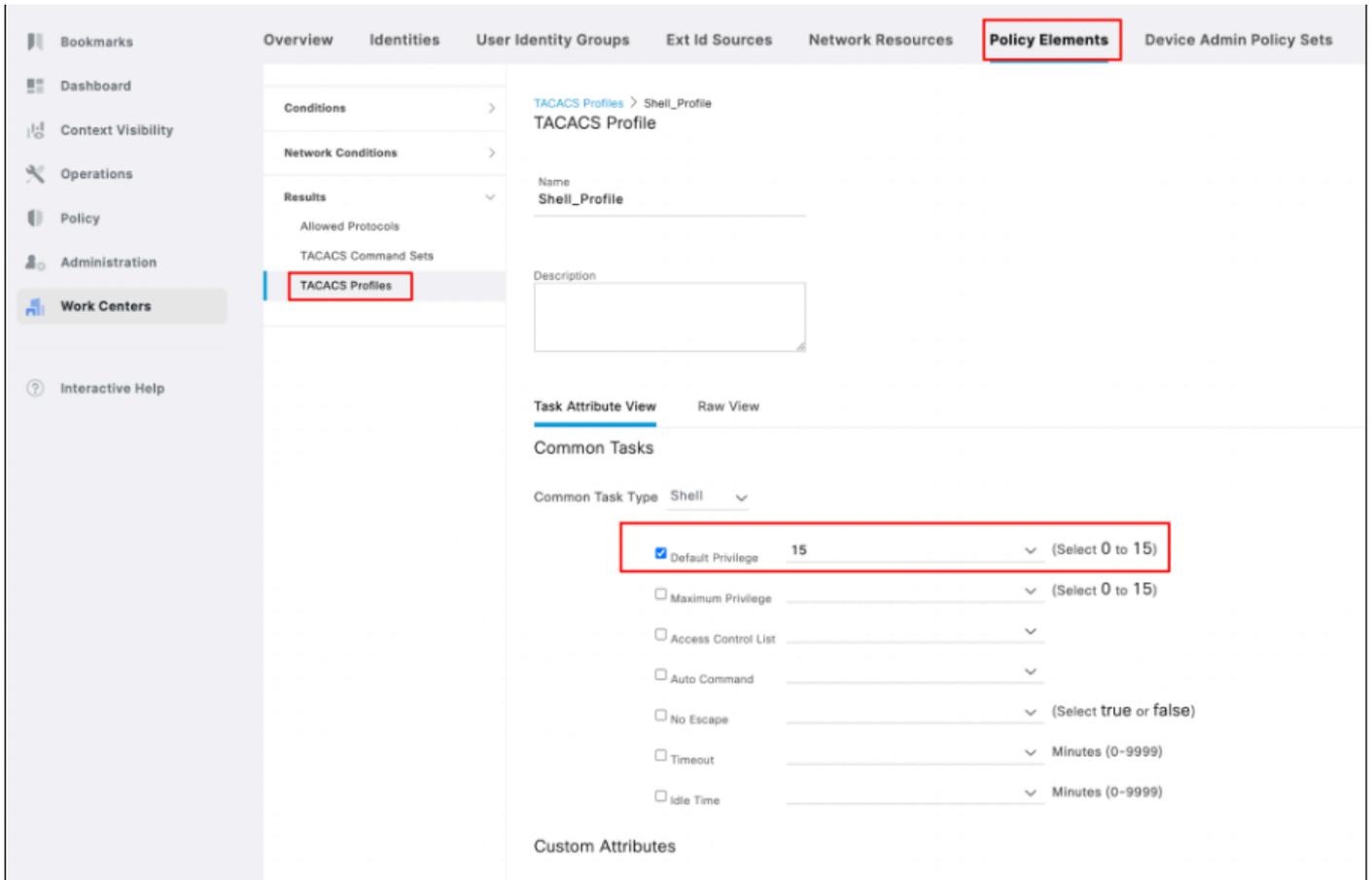
Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	exit
<input type="checkbox"/>	DENY	Config
<input type="checkbox"/>	PERMIT	show

ISE في enable_show_commands رم او نيوكت

TACACS+ في رعت فلم نيوكت

رم او ال تا عوم جم ربع رم او ال ضي وفت ذي فنت متي و، دحاو TACACS+ في رعت فلم نيوكت متي

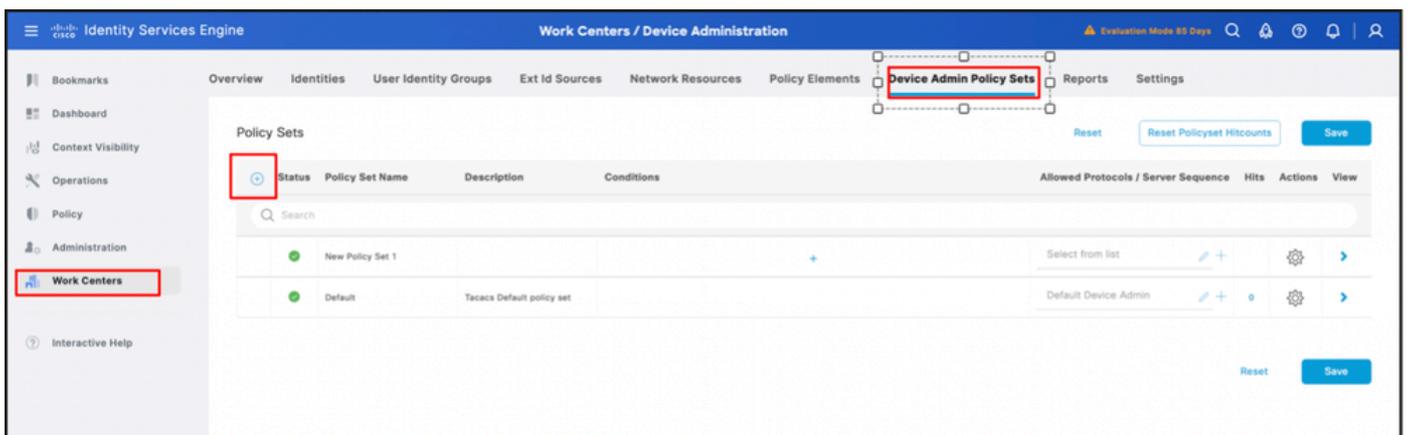
جئاتن >زه جال ادراد ا لم عل زكارم الى لقتنا ، TACACS+ في رعت فلم نيوكت ل
 تنيع Shell في رعت فلم ل مسا تدوز ، في ضي ة ققط . TACACS في رعت تا فلم > سايس ل
 ملسي ة ققط ، اريخا 15 ة مقي ل ل خ داو ، رايت خال ا ن اخ زايت ما ري صقت ل



ISE في TACACS فيرعت فلم نيوكت

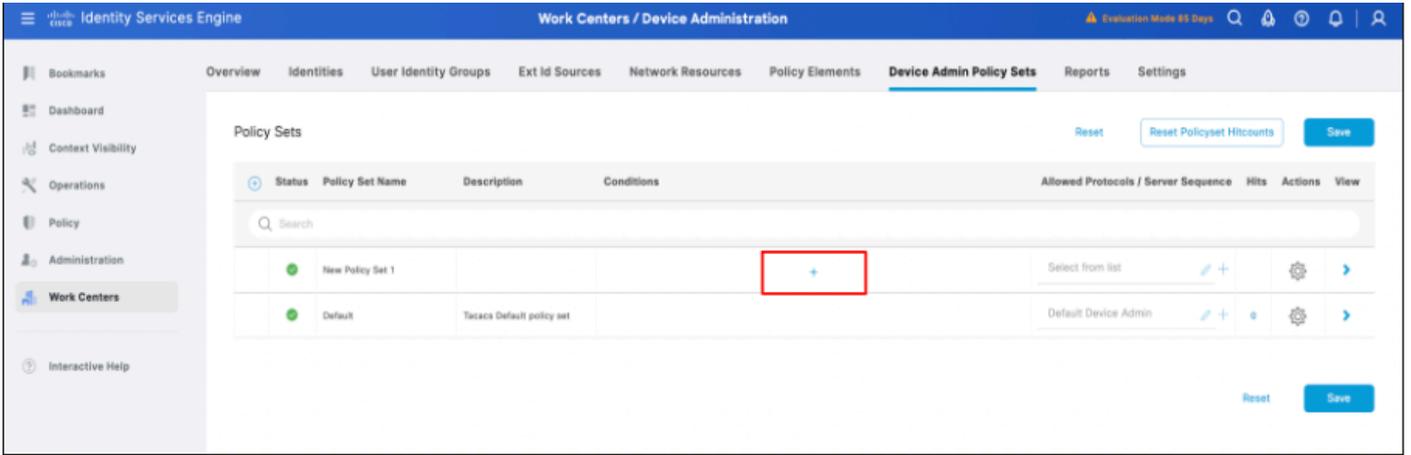
TACACS+ ضيوفت ةقداصم فيرعت فلم نيوكت

1. تاسايس تاعومجم -> زاهجال ةرادا -> لمعال زكارم -> ةرادال -> ISE pan GUI لى لوخدلا لچس 1. ةيمست متي، ةلحال هذه في. ةديج ةسايس ءاشنال (دئاز) + ةنوقيا لىل رقنا. زاهجال ةرادا 1. ةديج جهن ةعومجم مساب جهنلا ةعومجم



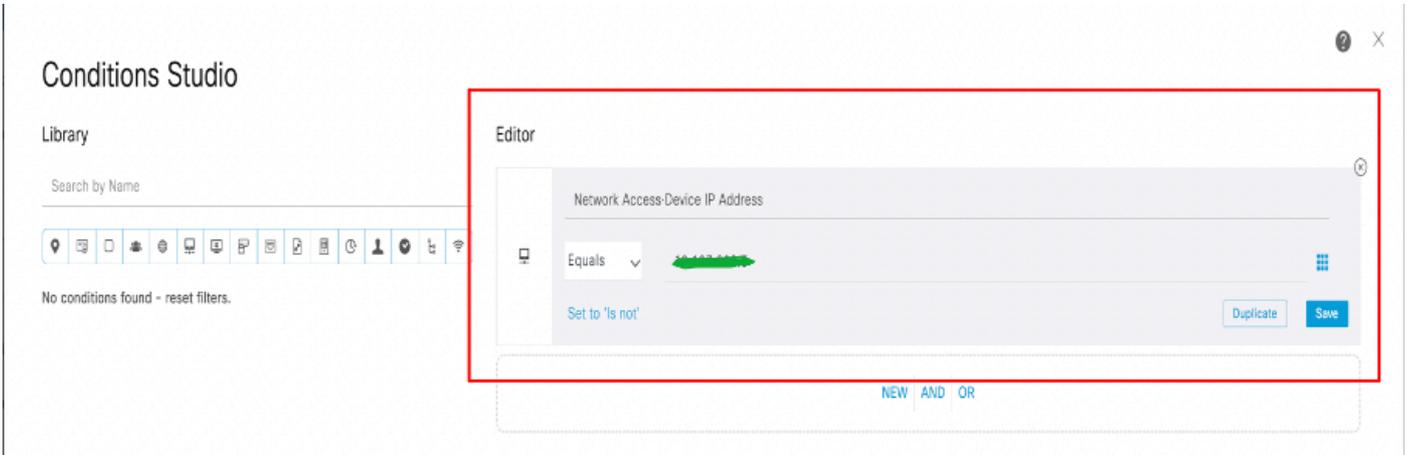
ISE في جهنلا ةعومجم نيوكت

2. هذه ةشاشلا ةطول في حضورم وه امك، طورشال نيوكت بچي، جهنلا ةعومجم ظفح لبق 2. رقنا. جهنلا ةعومجم طورش نيوكتل (دئاز) + ةنوقيا قوف

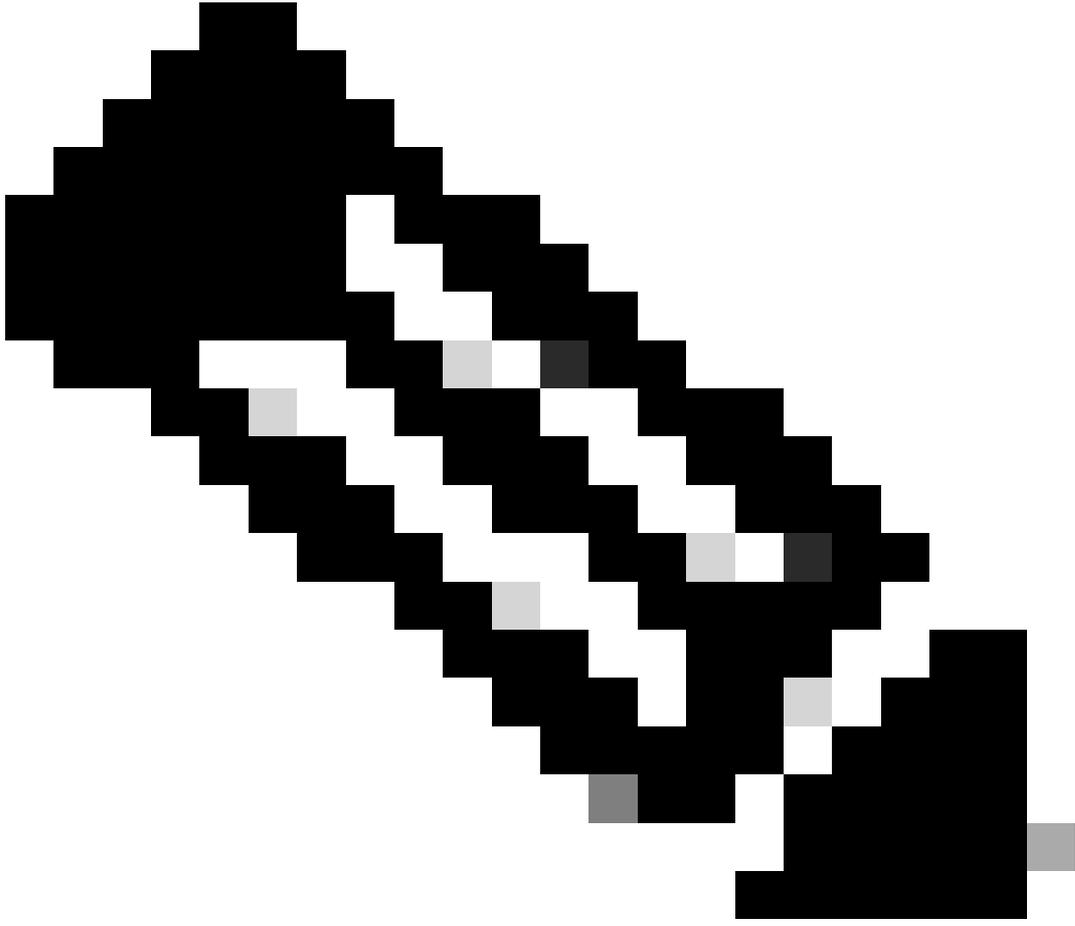


ISE في جهنلا ةعومجم طورش نيوكت

3. Conditions راجح عبرم حتف متي، 2 ةوطخلال في روكذم وه امك (دئاز) + زمرقوف رقنلا دعب. Studio. وأ ةديجال طورشلاب طرشلال ظفح مق. ةبولطلال طورشلال نيوكتب مق، كانه. لمعتسي ةقطق. ريرمتلاب مق، ةدوجوملا

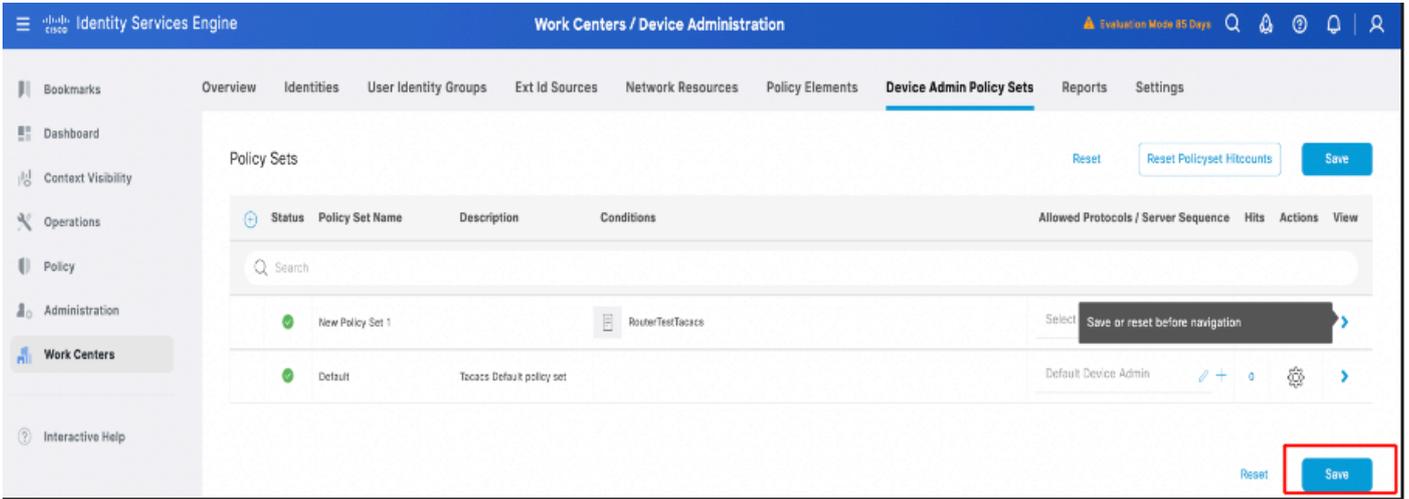


ISE في جهنلا ةعومجم طورش نيوكت



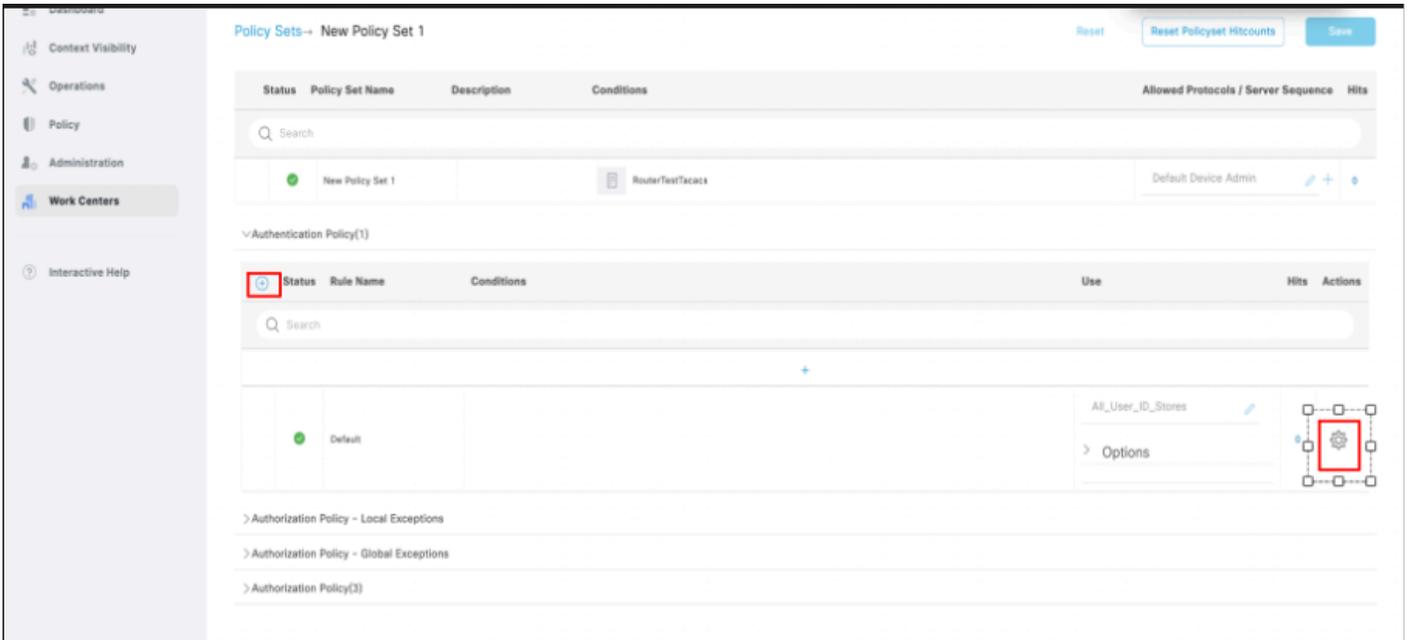
نأ نكمي، كلذ عمو. ةكبشلا زاهج ل IP عم طورشلا قباطت، قئاثولا هذهل: ةظحالم
رشنلا تابلطتم بسح فورظلا فلتخت.

زاهج لوؤسمك اهب حومسملال تالوكوتوربلال نيوكتب مق، اهظفحو طورشلا نيوكت دعب 4.
. ظفح راixelال قوف رقلابل اهؤاشنإ مت يتللا جهنلال ةعومجم ظفحا. يضارتفا

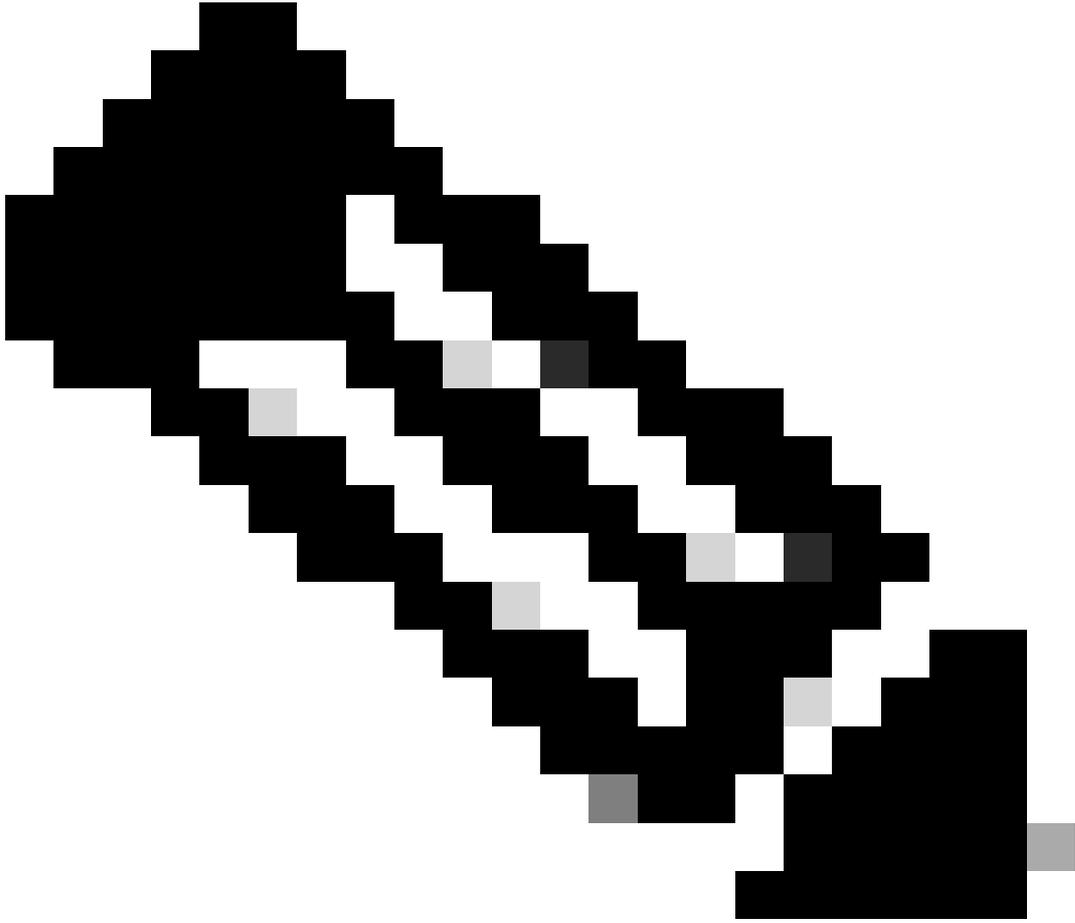


جەنلە عومجەم نەيوكت ديكأت

ەديج ەق داصم ەسايس عاشن | -> (1) ەق داصم لاجەن -> ەديجال جەنلە عومجەم عيسوت 5. ەال عأ ديدج فص جاردا م ث ، دات ع ل زمر قوف رقن ل اب وأ (دئان) + زمر قوف رقن ل اب

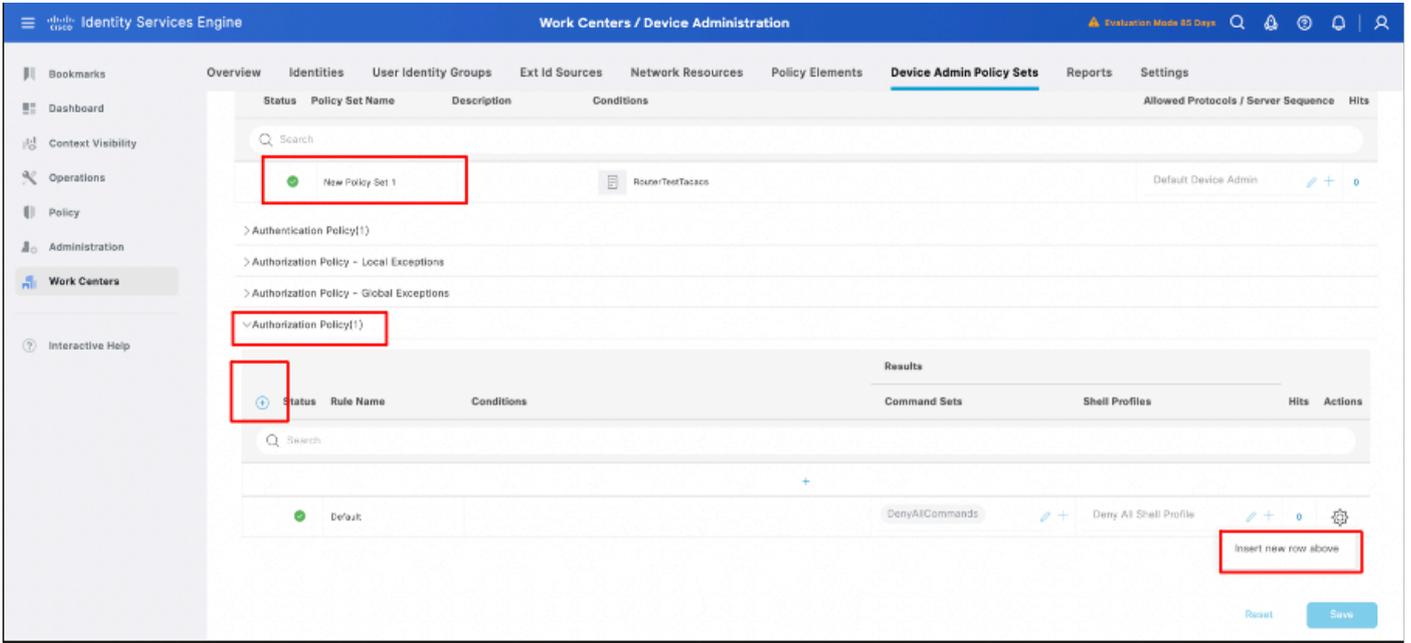


جەنلە عومجەم ي ەق داصم لاجەن نەيوكت



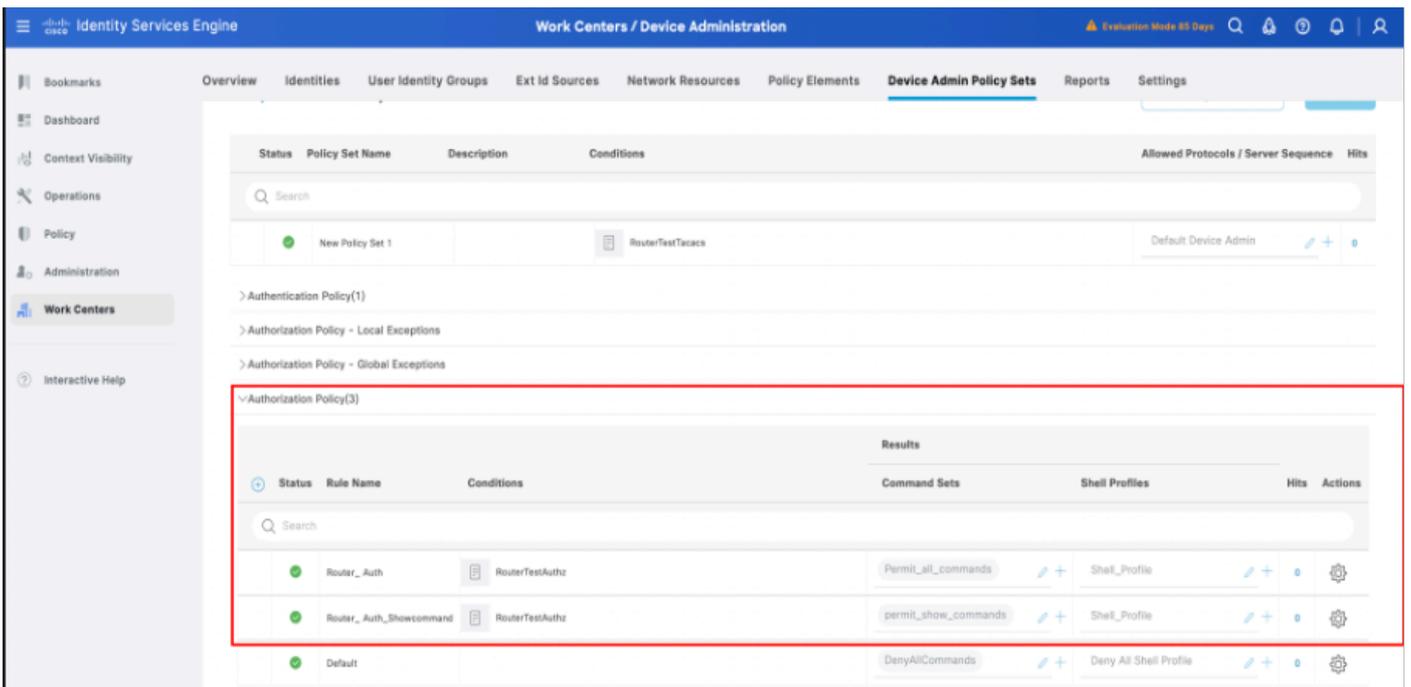
هنيي عت مت يذلا ي ضارت فالالة قداصل مال جهن مادختسا متي ، ضرعلا اذه ي ف :ةظحال م
اق فوة يوهلا نزاخم مادختسا صي صخت نكمي ، كلذ عمو .user_id_store_ة فاك عم
رشنلا تاب ل ط ت مل .

نأ وأ (دئاز) + ةنوقيأ رقت نأ أم (1) ضيوفتلا جهن -> ةدي دجال تاسايسلا ةومجم عيسوت 6.
ليوخت جهن عاشنال هالعأ ديدج فص جارداب مق ، مث .سرتلا ةنوقيأ رقت

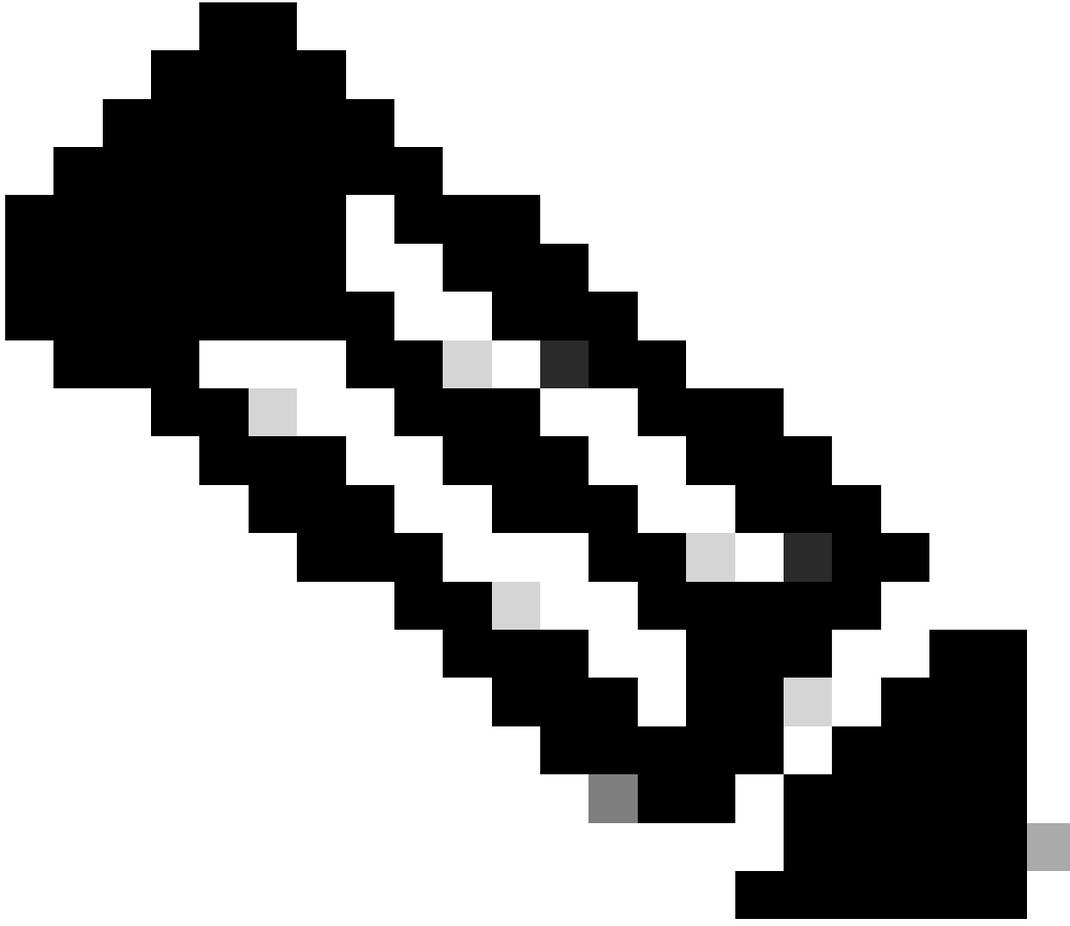


ليوختلا ةسايس نيوكت

7. تاسايس لىا ني عم shell فيرعت فلم ورم او اعمومجم و طورشب ليوختلا جهن نيوكت ب مق .
ليوختلا.



ISE في ليوختلا جهن نيوكت لامك

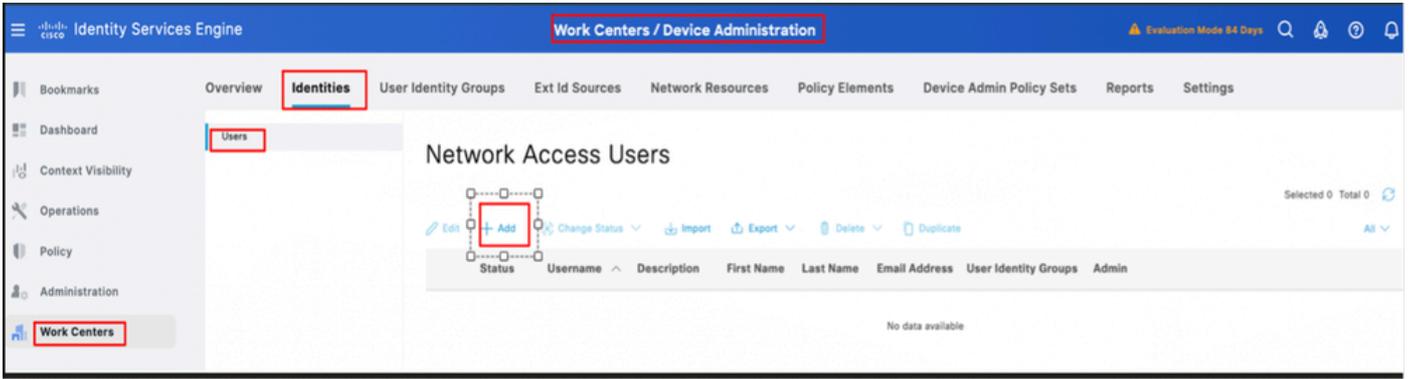


اقف واه نيوكت نكمي ورب تخملا ةئيبلا اق فو طورشلا نيوكت متي: ةظحالم
رشنلا تابلطتمل

رخآ ةكبش زاهج يأ وأ لوحملل تاسايسلا تاعومجم نيوكتل يلوألا تسلا تاوطخل عبتا 8.
TACACS+ ل مدختسي

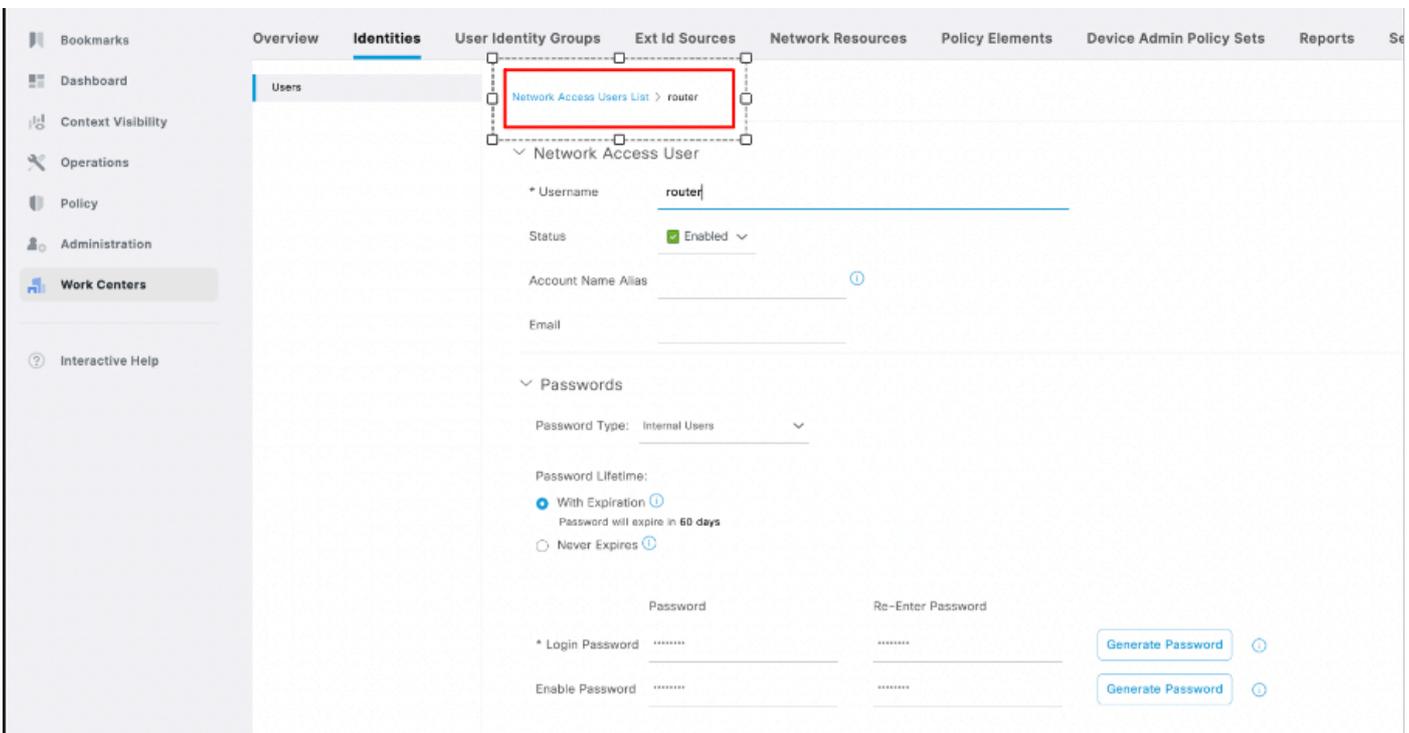
ISE ف NAD TACACS ةقداصل ةكبشلا يلا لوصولي مدختسم نيوكت

ةنوقيأ قوف رقنا. نومدختسملا -> تايوهلا -> ةزهجالا ةرادا -> لمعلل زكارم يلا لقتنا 1.
ديدج مدختسم ءاشنل (دئاز) +



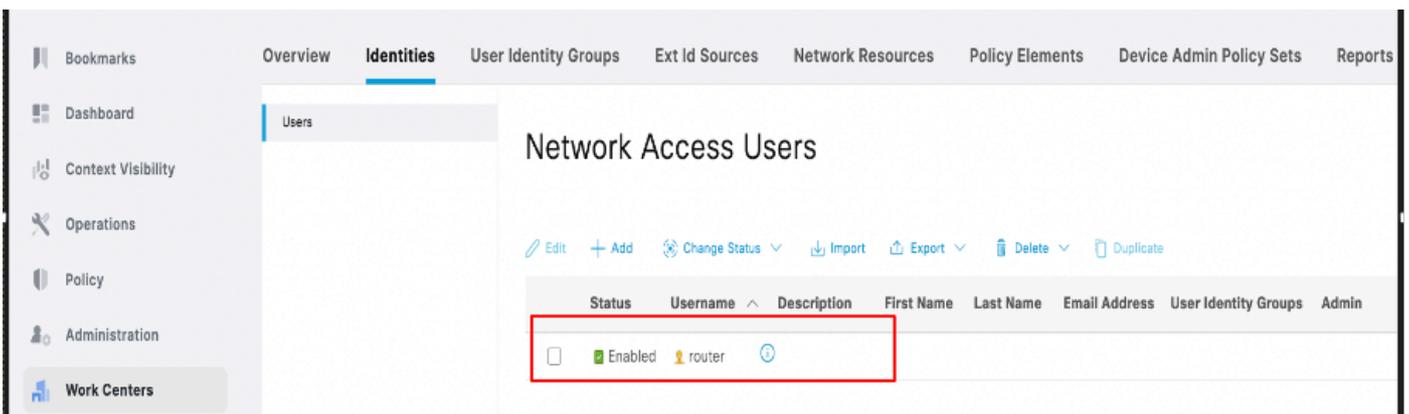
ISE في ةكبشال لى لوصولي مدختم نيوكت

مدختم اسمال نييغب مقو، رورمال ةمكلو مدختم اسمال مسا لي صافات عيسوتل ريفوتب مق 2. لاسرا قوف رونا م (يرايخا) مدختم اسمال ةيوه ةعومجم لى



ةعباتم - ةكبشال لى لوصولي مدختم نيوكت

-> نومدختم اسمال -> تايوهال -> لمعال زكارم في مدختم اسمال مسا نيوكت لاسرا دعب 3. يئرملك شبهنكي متو مدختم اسمال نيوكت متي، ةكبشال لى لوصولو ومدختم اسم



TACACS+ ل هجوم نيوكت

ليوختو TACACS+ ةقداصلم ل Cisco IOS هجوم نيوكت

1. هذه ليغشتب مقو هجوملاب ةصاخلا (CLI) رماوألارطس ةهجاو لىل لوخدلا ليجستب مق .
هجوملا في TACACS نيوكتل رماوألار

ضيوفتلاو ةقداصلم ل نيكمتل بولطم ل — ASR1001-X(config)#aaa new-model رمالا
NAD في (AAA) ةبساحملاو

ضيوفتلاو ةقداصلم ل نيكمتل بولطم ل رمالا — ASR1001-X(config)#aaa session-id .
NAD في (AAA) ةبساحملاو

ليححم TACACS+ ةيضارتفالا ةعومجم ل لوخدلا ليجستب ةيوه ةحص ASR1001-X(config)#aaa

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

ASR1001-X(config)#aaa tacacs+ ةعومجم 1 ةمئاق ةكبش ليوخت

ASR1001-X(config)#tacacs server ise1

ASR1001-X(config-server-tacacs)#address ipv4 < IP ناوع > TACACS مداخل صاخلا IP ناوع — ISE
Interface G1 IP.

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

ASR1001-X(config)# aaa tacacs+ isegroup لدان ةعومجم

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. show رمالا مادختساب TACACS+ نيوكت نم ققحت، هجوم ل TACACS+ تانيوكت ظفح دعب .
run aaa.

ASR1001-X#show AAA ضكري

!

ةيحلحم ل AAA ةقداصلم ل لوخدلا ليجستل ةيضارتفالا AAA ةعومجم

EXEC ضيوفتلا ةيضارتفالا AAA تاعومجم ةعومجم

1 ةكبش ل نودأ ةعومجم ل AAA ةعومجم

username 0 xxxxx لوؤسم رورم ةم لك

!

tacacs server ise1

<TACACS مداخل IP ناوع> IPv4 ناوع

XXXXX حاتفم ل

!

!

tacacs+ iseggroup مداخل AAA ةعومجم

ise1 مداخل مسا

IP vrf Forwarding Mgmt-intf

ip tacacs source-interface GigabitEthernet1

!

!

!

aaa new-model

كرتشم id-ةس ل AAA

!

!

TACACS+ ل لوجم ل نيوكت

ضيوفت ل او TACACS+ ةقداصم ل لوجم ل نيوكت

1. حاتفم ل ف TACACS لكشي ل رمأ اذه لغش وحاتفم ل نم CLI ل لى ل

C9200L-48P-4X#configure T

CNTL/Z. ب اهان. طخ ل لك دحاو، رمأ ل لكشت تلخد

ضيوفت ل او ةقداصم ل نيوكم تل بولطم ل رمأ ل — C9200L-48P-4X(config)#aaa دي- model. NAD ف (AAA) ةبسا حم ل او

اهصيصخت نكمي يتالاعومجم لايه TACACS+، TACACS+ نايوكت يف: عظهارالم
رشنللابلطتمل اقفو.

show رمألما ادختساب TACACS+ نايوكت نم ققحت، لوجملل TACACS+ تانيوكت ظفح دعب 2.
run aaa.

C9200L-48P#show AAA ضكري

!

ةي لجم ل AAA ةقداصم ل لوخدلا ليحستل ةيضارتفال AAA عومجم

EXEC ضيوفتل ةيضارتفال AAA تاعومجم عومجم

1 ةكبشلل نوذاعومجم ل AAA عومجم

username 0 xxxx لوؤسم رورم ةملك

!

!

tacacs server ise1

<TACACS مداخل IP ناوع> IPv4 ناوع

XXXXX حاتفملا

!

!

tacacs+ iseggroup مداخل AAA ةومجم

ise1 مداخل مسا

!

!

!

aaa new-model

كرتشم id-ةسلج AAA

!

!

ققحتلا

هجوملا نم ققحتلا

ةهجاوعم ISE لباقم TACACS+ لةميقللة قداصم ،هجوملاب ةصاخلا (CLI) رماوالا رطسة هجاو نم
Gigabit Ethernet 1 مادلما test aaa group tacacsgroupname username password new .

ISE: & هجوملا نم تاجرخلل جذومن يلي امي فو

هجوملا نم 49 ذفنملا نم ققحتلا

ASR1001-X#telnet ISE Gig 1 interface IP 49

حتف ... 49, ISE Gig 1 interface IP, مادلما ةلواحم نالا متي

ديج ASR1001-X#test AAA Group Router XXXX هجوملا

رورملا ةملك لاسرا

حاجب مدخت سمل ا قداصم تم

مدخت سمل تامس

username 0 "دخت حاجسم"

"رورملا م لك" 0 درلا قلاسر

تالجمس -> تايلمعل -> ةيموسرلا مدخت سمل ا هجاو يلا لوخدلا لجمس، ISE نم ققحتلل
ةكبشلا زاهج ليصافت ل قح ي ف IP هجوم مادختساب ةيفصتلاب مق م ث، ةرشابملا TACACS

The screenshot displays the Cisco ISE interface for a TACACS+ authentication log. It is divided into three main sections: Overview, Authentication Details, and Steps.

Overview:

- Request Type: Authentication
- Status: Pass
- Session Key: honey/530520237/15
- Message Text: Passed-Authentication: Authentication succeeded
- Username: router
- Authentication Policy: New Policy Set 1 >> Default
- Selected Authorization Profile: Shell_Profile

Authentication Details:

- Generated Time: 2025-03-06 05:52:51.374000 +00:00
- Logged Time: 2025-03-06 05:52:51.374
- Epoch Time (sec): 1741240371
- ISE Node: honey
- Message Text: Passed-Authentication: Authentication succeeded
- Failure Reason: (empty)
- Resolution: (empty)
- Root Cause: (empty)
- Username: router
- Network Device Name: RouterTest
- Network Device IP: (redacted)
- Network Device Groups: IPSEC#Is IPSEC Device#No.Location#All Locations,Device Type#All Device Types
- Device Type: Device Type#All Device Types
- Location: Location#All Locations
- Device Port: (empty)

Steps:

- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group (Step latency=2ms)
- 15008 Evaluating Service Selection Policy (Step latency=0ms)
- 15048 Queried PIP - Network Access.Device IP Address (Step latency=4ms)
- 15041 Evaluating Identity Policy (Step latency=14ms)
- 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=6ms)
- 15013 Selected Identity Source - Internal Users (Step latency=1ms)
- 24210 Looking up User in Internal Users IDStore (Step latency=0ms)
- 24212 Found User in Internal Users IDStore (Step latency=80ms)
- 13045 TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=1ms)
- 13015 Returned TACACS+ Authentication Reply (Step latency=0ms)
- 13014 Received TACACS+ Authentication CONTINUE Request (Step latency=3ms)
- 15041 Evaluating Identity Policy (Step latency=3ms)
- 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=6ms)
- 15013 Selected Identity Source - Internal Users (Step latency=1ms)
- 24210 Looking up User in Internal Users IDStore (Step latency=0ms)
- 24212 Found User in Internal Users IDStore (Step latency=11ms)
- 22037 Authentication Passed (Step latency=1ms)
- 15036 Evaluating Authorization Policy (Step latency=2ms)
- 13015 Returned TACACS+ Authentication Reply (Step latency=11ms)

هجوملا نم ققحتلل - ISE نم TACACS Live Log

لوجملا نم ققحتلل

Gigabit Ethernet 1 هجاو عم ISE لباقم TACACS+ ةقداصم نم ققحت، لوجملا (CLI) رم اوألا رطس هجاو نم
test aaa group tacacs groupname password newn: رمال مادختساب

ISE. و لوجملا نم تاجرملا جذومن يلي امي و

لوجملا نم 49 ذف نملا نم ققحتلل:

C9200L-48P# telnet ISE Gig1 Interface IP 49

حتف 49... ISE Gig1 interface IP، ؤلواحم نآلآ متي

ديج C9200L-48P#test AAA Group Switch XXXX لوجمل

رورملا ؤمكل لاسرا

حاجنب مدختسمل ؤقداصم تمت

مدختسمل تامس

username 0 "حاتفم"

:"رورملا ؤمكل" 0 درلا ؤلاسرا

تالجمس -> تايلمعل -> ؤيموسرلا مدختسمل ؤهجاو لي لوجدل لجمس، ISE نم ققحتلل زاهج لي صافات ل قح في IP حاتم مادختساب ؤيفصتلاب مق م، ؤرشابم TACACS ؤكبشلل.

The screenshot displays the Cisco ISE interface for a TACACS+ authentication log. The 'Overview' section shows a successful authentication for user 'switch' using policy 'New Policy Set 2 >> Default'. The 'Authentication Details' section provides a timestamp of 2025-03-06 04:10:15.551000 and lists various fields like 'Network Device Name' (Switch) and 'Network Device IP' (redacted). The 'Steps' section on the right provides a detailed sequence of events, including 'Received TACACS+ Authentication START Request', 'Evaluating Policy Group', 'Selected identity source sequence', and 'Authentication Passed'.

Request Type	Authentication
Status	Pass
Session Key	honey/530520237/11
Message Text	Passed-Authentication: Authentication succeeded
Username	switch
Authentication Policy	New Policy Set 2 >> Default
Selected Authorization Profile	Shell_Profile

Generated Time	2025-03-06 04:10:15.551000 +00:00
Logged Time	2025-03-06 04:10:15.551
Epoch Time (sec)	1741234215
ISE Node	honey
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	switch
Network Device Name	Switch
Network Device IP	[REDACTED]
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	

Step	Description
13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group (Step latency=8ms)
15008	Evaluating Service Selection Policy (Step latency=0ms)
15048	Queried PIP - Network Access.Device IP Address (Step latency=11ms)
15041	Evaluating Identity Policy (Step latency=9ms)
22072	Selected identity source sequence - All_User_ID_Stores (Step latency=17ms)
15013	Selected Identity Source - Internal Users (Step latency=1ms)
24210	Looking up User in Internal Users IDStore (Step latency=1ms)
24212	Found User in Internal Users IDStore (Step latency=69ms)
13045	TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms)
13015	Returned TACACS+ Authentication Reply (Step latency=1ms)
13014	Received TACACS+ Authentication CONTINUE Request (Step latency=7ms)
15041	Evaluating Identity Policy (Step latency=6ms)
22072	Selected identity source sequence - All_User_ID_Stores (Step latency=22ms)
15013	Selected Identity Source - Internal Users (Step latency=1ms)
24210	Looking up User in Internal Users IDStore (Step latency=36ms)
24212	Found User in Internal Users IDStore (Step latency=16ms)
22037	Authentication Passed (Step latency=0ms)
15036	Evaluating Authorization Policy (Step latency=1ms)
13015	Returned TACACS+ Authentication Reply (Step latency=36ms)

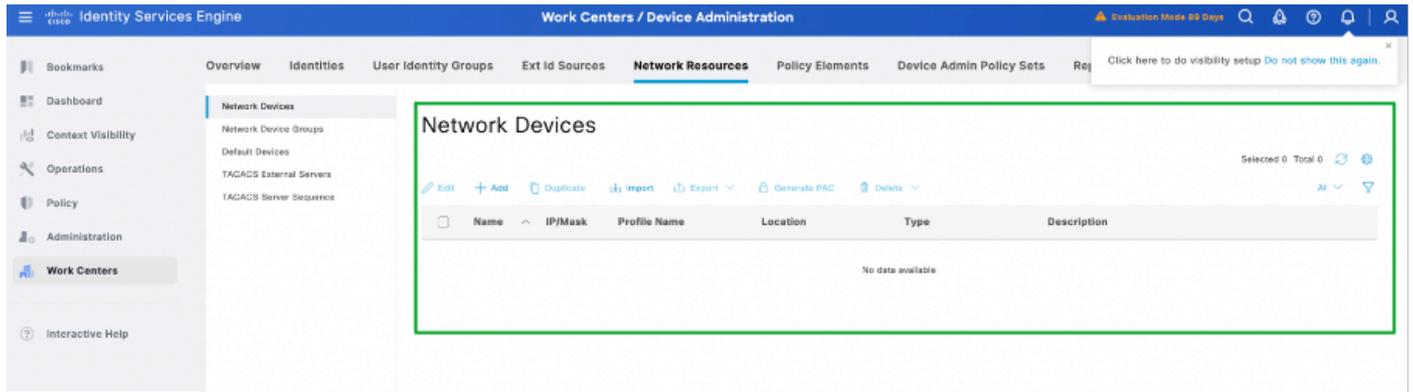
لوجمل نم ققحتلل - ISE نم TACACS Live Log.

اهحال صاوا عا طخال فاشكتسا

قلعتي اميف اهيلع روثعلل مت يتلا فكرتشملا اياضقلا ضع ب مسقلا اذه شقاني
TACACS+ ةقداصم ب.

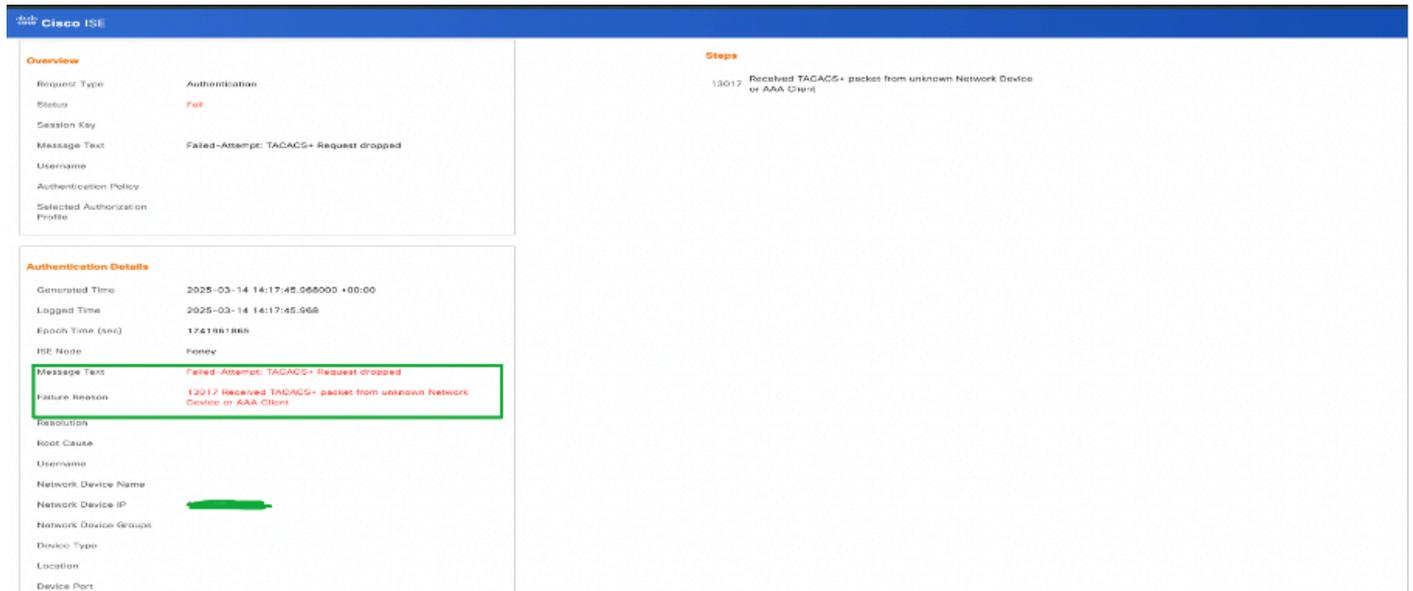
نم 13017 زارط ةلقملا TACACS+ ةمزح: أطخال عم TACACS+ ةقداصم لشفت 1: ويراني سل
"AAA" ليمع وأ فورعم ريغ ةكبش زاهج.

يف حضورم وه امك. ISE يف ةكبش دراومك ةكبشلا زاهج ةفاضل مدع دنع ويراني سل اذه ثدحي
ISE ب ةصاخلا ةكبشلا دراوم يف لوحملا ةفاضل متت ال، هذه ةشاشلا ةطلق.



ISE يف ةكبشلا ةزهج ةفاضل متت ال - اهحال صاوا عا طخال فاشكتسا ويراني سل.

عقوتم وه امك ISE لىل ةمزلال لصت، ةكبشلا زاهج / لوحملا نم ةقداصملا ربتخت ام دنع، نآلا
زاهج نم TACACS+ ةمزح 13017 زارطلا يقلت: أطخال ثودح عم ةقداصملا لشفت، كلذ عم و
هذه ةشاشلا ةطلق يف حضورم وه امك "AAA" ليمع وأ فورعم ريغ ةكبش:



ISE لىل ةكبشلا زاهج ةفاضل مدع دنع لشف - ةرشابملا TACACS تالچس.

لوحملا) ةكبشلا زاهج نم ققحتلا

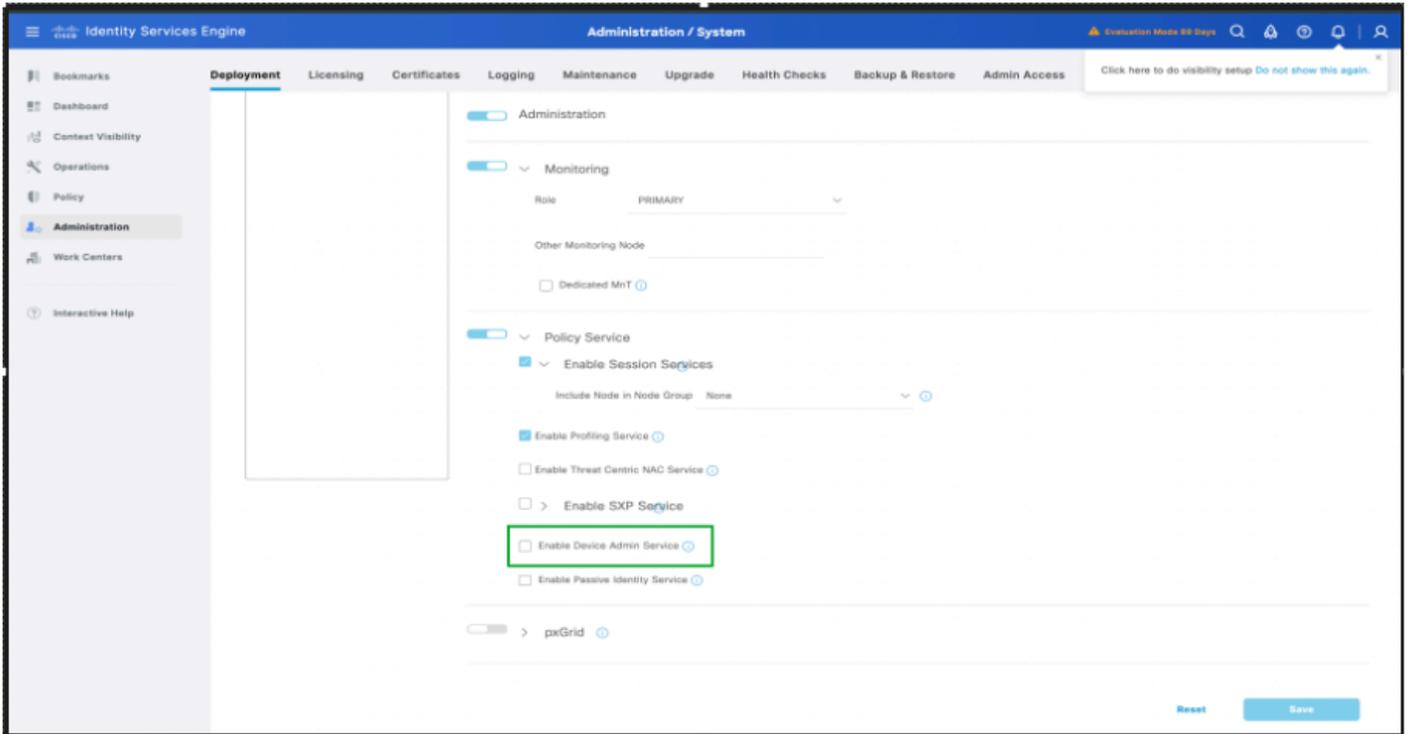
ديج XXXXX لوحم ةومجم ةومجم #testAAA لوحملا
مدختسملا صفر مت

متم مل اذا ISE. يف ةكبشلا زاهك ةكبشلا زاهج / هجوملا / لوجملا ةفاضل نم ققحت :لحل
ISE. ب ةصاخلا ةكبشلا زاهج ةمئاق ىل ةكبشلا زاهج ةفاضل مقف ،زاهجلا ةفاضل

تامولعم ةيأ نودب تمصب TACACS+ ةمزح طاقسإب ISE موقى : يناتللا ويرانيسللا

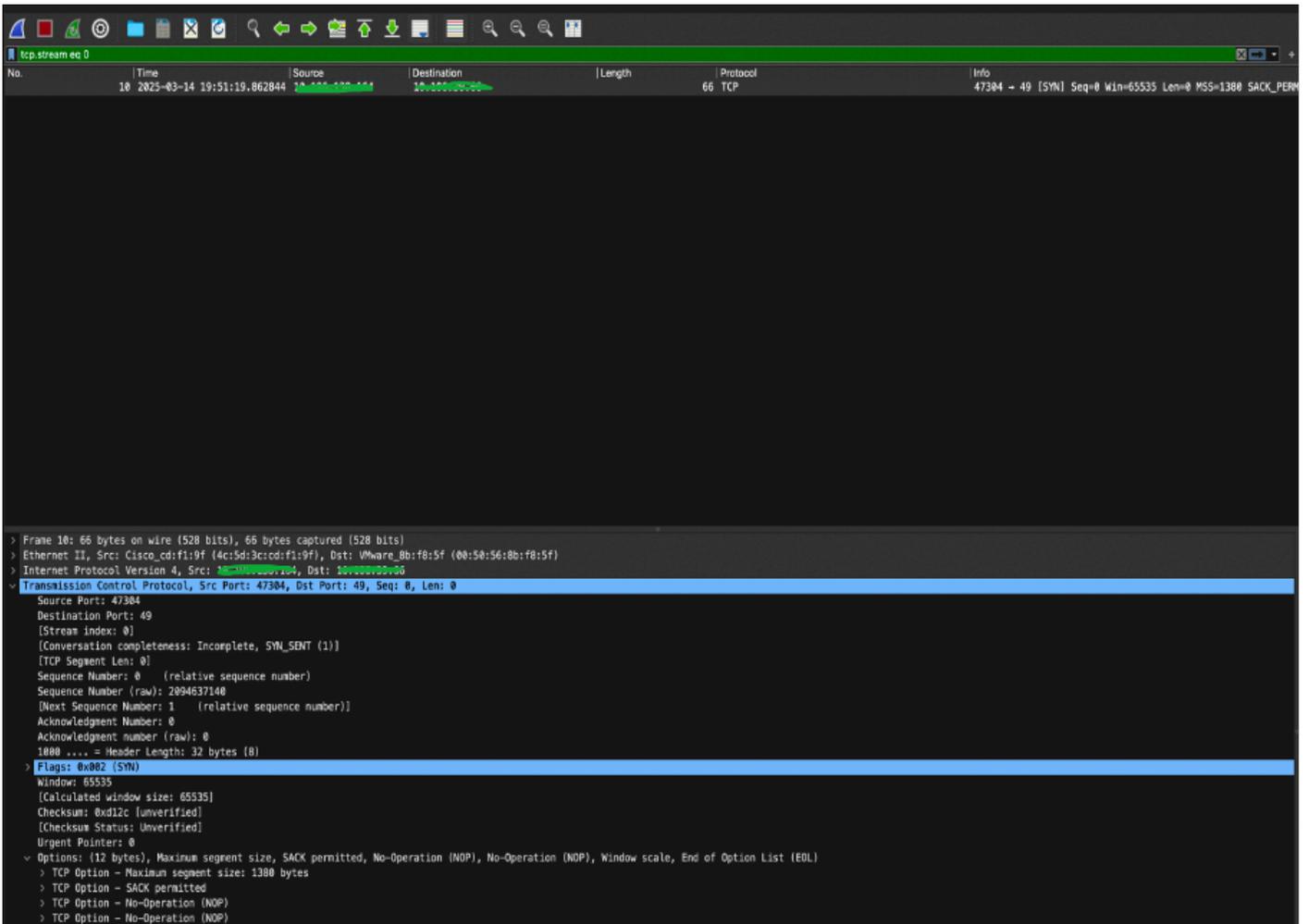
موقى ،ويرانيسللا اذه يف ISE. يف ةزهجال ةرادل ةمدخ لىطعت متي ام دنع ويرانيسللا اذه ثدحي
ءدب متي هنا نم مغرلا ىلع ةيح تالچس يأ ةظحالم متي الو ةمزحلا طاقسإب ISE
ISE. ب ةصاخلا ةكبشلا دراوم ىل هتفاضل متت يذلا ةكبشلا زاهج نم ةقداصملا

ISE. يف ةزهجال ةرادل لىطعت مت ،هذه ةشاشلا ةطقل يف حضوم وه امك



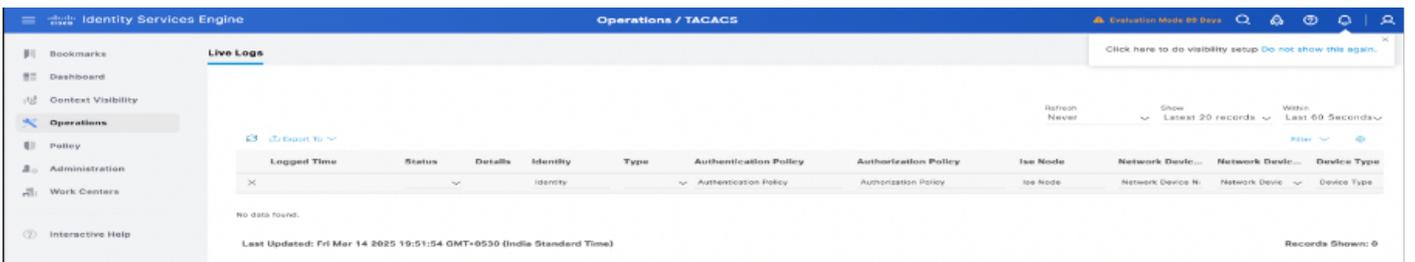
ISE. يف زاهجلا ةرادل نيكم مت متي مل ،ويرانيسللا

يأ نود مزحلا طاقسإب ISE موقى ،ةكبشلا زاهج نم ةقداصملا ةئيهتب مدختسملا موقى ام دنع
طساوب اهلاسرا متي يتلا Syn ةمزح ىل ISE بيحتسي الو ةرشابملا تالچسلا يف تامولعم
هذه ةشاشلا ةطقل ىل عجرا. TACACS. ةقداصم ةيلمع لامكإل ةكبشلا زاهج



ISE TACACS انثاء تم صب مزحل طاقس |

ةقداصم ال انثاء يح لجس نم ام ISE رهظي



ال ISE نم ققحت ال - TACACS ل ةرشابم تالجس دجوت ال

(لوحمل ال) ةكبش ال زاخ نم ققحت ال

#لوحمل

ديج XXXX لوحم ةومجم #testAAA لوحمل

مدختسم ال صفر مت

#لوحمل

*14 سرام 13:54:28.144: ت+: رادص ال 192 (0xC0)، عون ال 1، seq 1، ريفش ال 1، SC 0

*14 سرام 13:54:28.144: ت+: session_id 10158877 (0x9B031D)، clen 14 (0xE)

*14 سرام 13:54:28.144: ت+: ةباتك ال: AUTHEN/START، priv_lm:15 action: لجس ت: ascii

*14 سرام 13:54:28.144: ت+: svc: Login user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0

*14 سرام 13:54:28.144: ت+: مديبت: مدختسم ال

*14 سرام 13:54:28.144: ت+: ذفنم ال:

*14 سرام 13:54:28.144: ت+: rem_addr:

*14 سرام 13:54:28.144: ت+: تاناي ال:

*14 سرام 13:54:28.144: ت+: ةمزحل ال اهان:

ISE ف ةزهجألا ةرادإ نيكمت :لحل

عجرملا

- [اهالص او TACACS ةقداصم عاڤخأ فاشكتسأ](#)
- [3.3 رادصلالا، Cisco نم ةي وهلا تامدخ كرحم لوؤسم ليلد](#)
- [TACACS مداوخل VRF](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انء عيچ ي ف ني مدختسمل معد يوتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال م يچري. ةصاغل مه تلبل
Cisco ي لخت. فرتحم مچرت م اهم دقي ي تلل ةي فارتحال ةمچرتل عم لالحل وه
ىل إأمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقد نع اهتيل وئس م Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل