

ةيؤر ةيناك مإل Prime Infrastructure عم ISE جم د ةياهنلا ةطقن

تايوت حمللا

[ةمدقملا](#)

[ةيساسألا تابلطت ملا](#)

[تابلطت ملا](#)

[ةمدختسملا تانوك ملا](#)

[نيوكت ملا](#)

[ةكبشلا ليطيطخت ملا مسرلا](#)

[تانوكت ملا](#)

[لذب ملا نيوكت](#)

[Cisco Prime ل ةيساسألا ةينبلا نيوكت](#)

[ةياهنلا ةطقن نيوكت](#)

[ةحصلا نم ققحت ملا](#)

[ISE نم ققحت ملا](#)

[NAD نم ققحت ملا](#)

[Prime ل ةيساسألا ةينبلا نم ققحت ملا](#)

[اهالصل او عااخاللا فاشكتسا](#)

ةمدقملا

ةيؤرلا ةيناك مإل لىل لوصحلل Prime Infrastructure عم ISE جم د ةيفيك دنتسملا اذه حضوي
اهيلع قدصملا ةياهنلا طاقنل.

ةيساسألا تابلطت ملا

تابلطت ملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- ISE نم Cisco.
- Cisco Prime ل ةيساسألا ةينبلا.
- ISE لباقم ةقداصملا ةياهنلا طاقنل يكللس وأ يكللسال AAA قفدت.
- WLCs ةزهجأو تالوحملا لثم (ةكبشلا لىل لوصولا ةزهجأ) NADs لىل SNMP نيوكت.

ةمدختسملا تانوك ملا

ةيلاتلا ةيداملا تانوك ملا او جماربلا تارادصا لىل دنتسملا اذه يف ةدراولا تامولعملا دنتست:

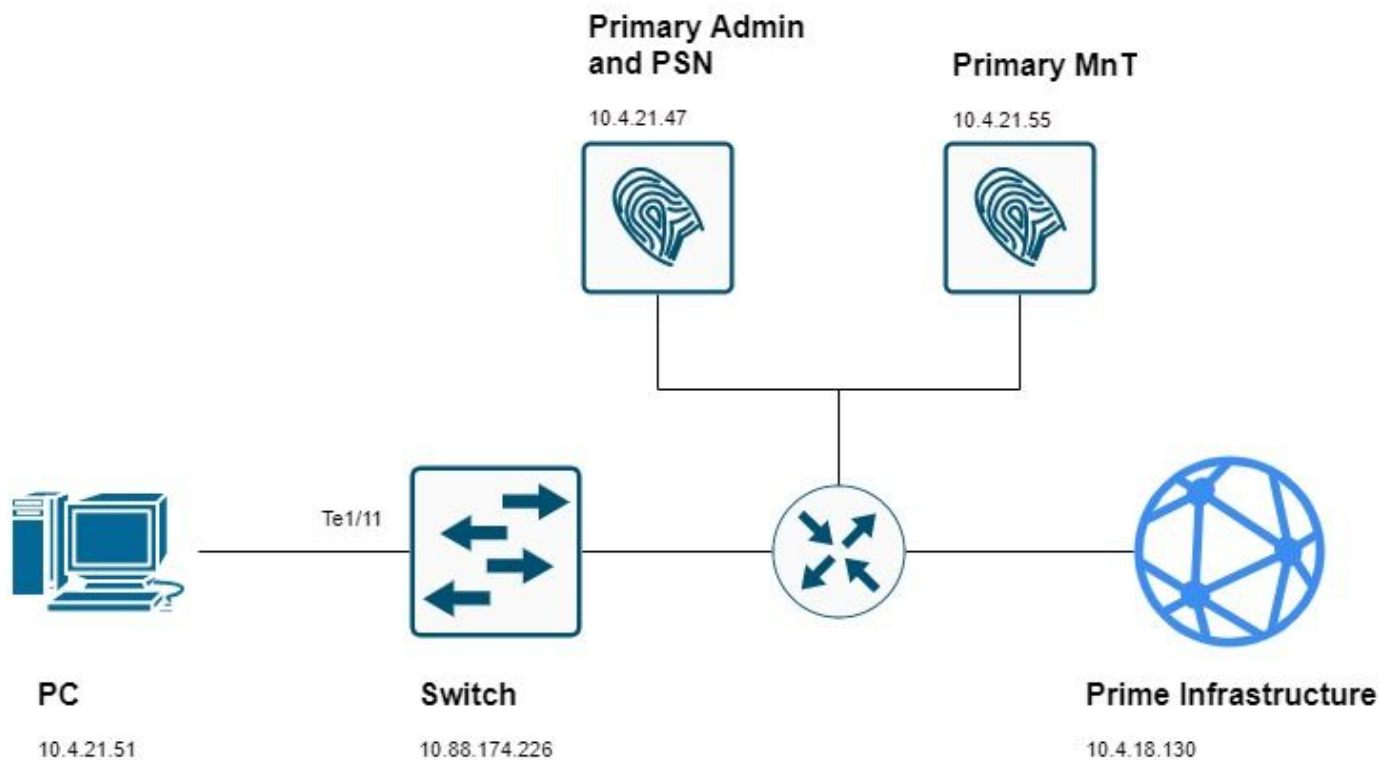
- ISE 3.1 رشن.
- Cisco Prime Infrastructure، رادصا لىل 3.8.

- Cisco IOS® 15. 5. جمانرب لغشي يذال C6816-X-LE
- Windows 10. زاھج

ةصاخ ةيلمعم ةئيې ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا (يضايرتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسُملا ةزهجالا عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكاتف ،ليغشتلا دي ق ككتبش

نيوكتلا

ةكبشلل يطيختلا مسرلا



تانيوكتلا

لدبملا نيوكت

تنأ ليلدلا اذه ي ف ISE لباقم AAA ةقداصل (NAD) ةكبشلا ىلإ لوصولا زاھج نيوكت 1. ليكشت اذه مدختست:

```

aaa new-model

radius server ise31
address ipv4 10.4.21.47 auth-port 1812 acct-port 1813
key Cisc0123

aaa server radius dynamic-author
client 10.4.21.47 server-key Cisc0123

aaa group server radius ISE
  
```

```
server name ise31
```

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
```

```
dot1x system-auth-control
```

2. لوجھال ي ف ةزهجال بقعت نيوكت:

```
device-tracking policy DT1
tracking enable
```

```
device-tracking tracking auto-source
```

3. هب زاهجال بقعت جهن قافراو dot1x ةقداصلم switchport نيوكتب مق:

```
interface TenGigabitEthernet1/11
device-tracking attach-policy DT1
authentication host-mode multi-domain
authentication order dot1x mab webauth
authentication priority dot1x mab webauth
authentication port-control auto
mab
dot1x pae authenticator
```

4. كب ةصاخلا تاكبشلل تابللطتم ةيبلتل SNMP تارابتخاو RO SNMP عمتجم نيوكتب مق (RW عمتجم نيوكت كنكمي، اي رايخا):

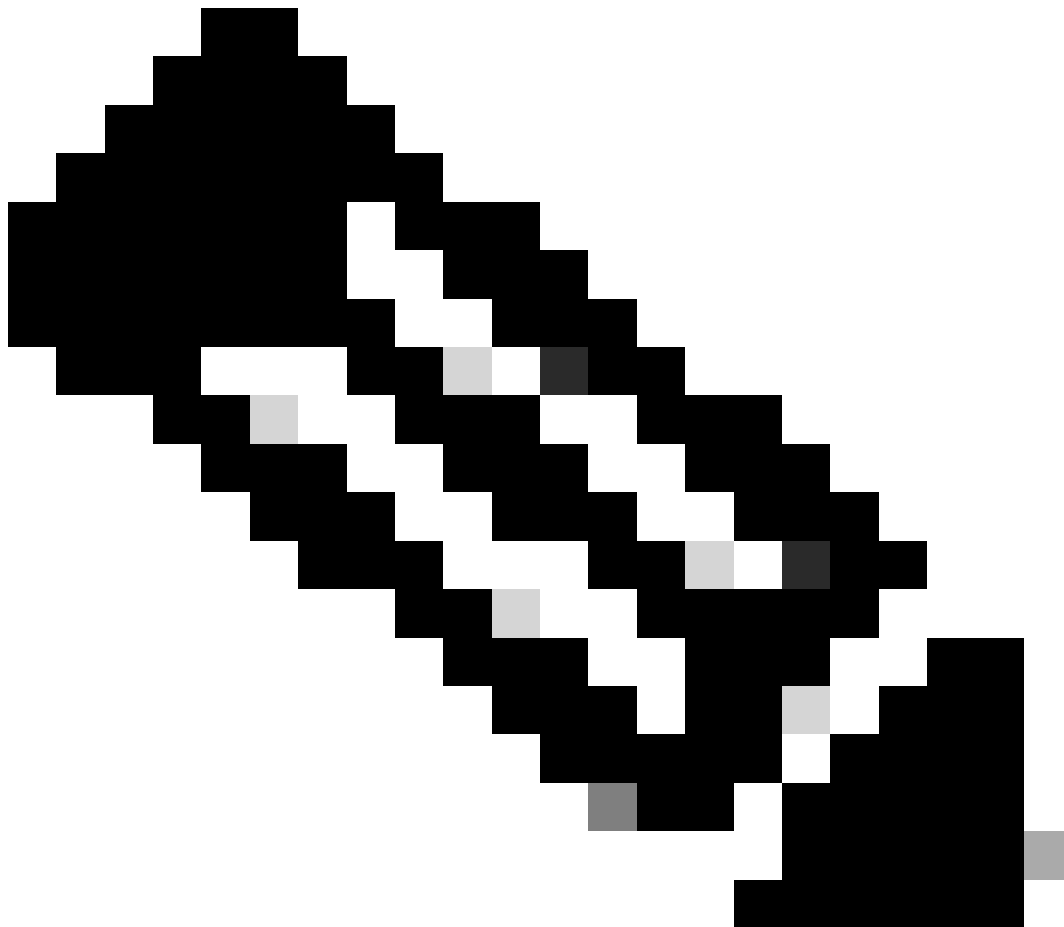
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server enable traps trustsec authz-file-error
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps port-security
snmp-server enable traps event-manager
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.4.18.130 version 2c public udp-port 161
```

5. زاهجال ةراد Prime ل نكمي ىتح SSH و Telnet لى لوصول نيوكتب مق:

```
username admin password 0 cisco!123
aaa authentication login default local

line vty 0 4
transport input ssh
login authentication default
```

هذه مداخلتساف ،دحاو NAD ىدل نكي مل اذا RSA. حاتفم رفوت مزلي ، SSH تالاصتال (يراي تخا). 6. هئاشنل تاوطخال

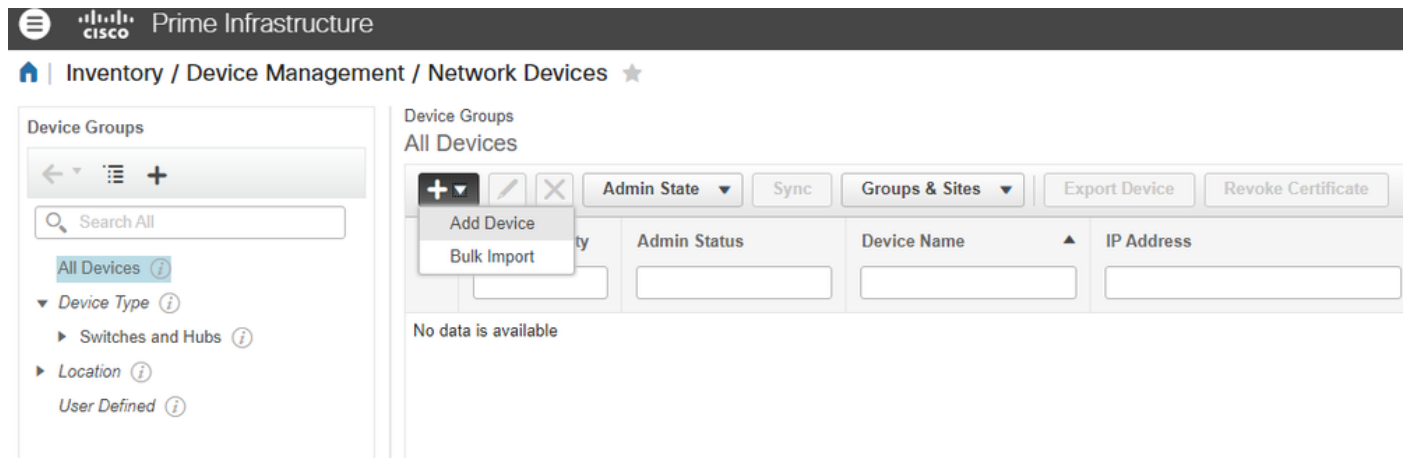


ناك اذا امم ققحت RSA. ءاشنل لبق هنيوكت مت لاجم ةزهجال ضعب بلطتت :ةظحالم
دوجومل لاجمل زواجتت ال شيحب هنيوكت مت لاجم زاهجال ىدل

```
ip domain-name cisco.com
crypto key generate rsa
```

Cisco Prime لةيساسألل ةينبلل نلوكل

ةفاضل > (+) دئازل ةمالع > ةكبشلل ةزهجل > ةزهجلال ةرادل > نوزلملل فل ةكبشلل زاهج ةفاضل. 7.
زاهج:



له نوزلملل لامكل دارمل ةلمازلللال لوقلل:

ةكللللل ةزهجللل ةبسنللل:

- DNS و IP امل: ماع
- SNMP: لولطم RO عململ
- Telnet/SSH: عضو EXEC نللملل

WLC لى ةبسنللل:

- DNS و IP امل: ماع
- SNMP: لولطم RO عململ

للالل cisco لمللللل نلأ دشرم اذهل:

ماع ماسق ط:

Add Device



* General ✓

* SNMP

Telnet/SSH

HTTP/HTTPS

Civic Location

* General Parameters

☒ IP Address 10.88.174.226

☐ DNS Name

License Level Full ?

Credential Profile --Select-- ?

Device Role --Select-- ?

Add to Group --Select-- ?

Add

Verify Credentials

Cancel

SNMP م س ق .ايناث

Add Device



* General ✓

* SNMP ✓

Telnet/SSH

HTTP/HTTPS

Civic Location

* SNMP Parameters

Version v2c

* SNMP Retries 2

* SNMP Timeout 10 (Secs)

* SNMP Port 161

* Read Community

* Confirm Read Community

Write Community

Confirm Write Community

Add

Verify Credentials

Cancel

Telnet/SSH مسق. اثلث

Edit Device

* General

* SNMP

Telnet/SSH

HTTP/HTTPS

Civic Location

Telnet/SSH Parameters

Protocol

SSH2

* CLI Port

22

* Timeout

60

(Secs)

Username

admin

Password

.....

Confirm Password

.....

Enable Password

.....

Confirm Enable Password

.....

* Note: Not providing Telnet/SSH credentials may result in partial collection of inventory data.

Update

Update & Sync

Verify Credentials

Cancel

امه ةومجم ال ؤلحو لوصول ةيناكم ا نأ نم دكأت ، ةبولطم ال لوقحو ال عي مج لامتك ا درجم ب 8. ي: لاوت ال لى لع نالمتكم ال او رضخ ال

Cisco Prime Infrastructure							
Inventory / Device Management / Network Devices							
Device Groups							
All Devices							
+ ✎ ✕ Admin State Sync Groups & Sites Export Device Revoke Certificate Show Quick Filter							
Reachability	Admin Status	Device Name	IP Address	DNS Name	Device Type	Last Inventory Collection Status	
☒	☒	Managed	MXC-TAC.M.07-6816-01.Iv...	10.88.174.226	10.88.174.226	Cisco Catalyst C6816-X-LE Fixe...	Completed

ISE عم Prime جم د 9.

ISE مداوخ > مداوخ > ةراد ا لى ل لقتنا ط.

لاقنتنا قوف رقنا م ث ISE مداوخ ةفاض ا دح ، ةلدسنم ال ةمئاق ال ي ف . ايناث

Cisco Prime Infrastructure							
Administration / Servers / ISE Servers							
None detected							
-- Select a command -- Go -- Select a command -- Add ISE Server Delete ISE Server(s)							

ظفح رقناو لوقحو ال لك ةئبعتب مق . اثلث



(نكم أن) ةيوناثلاو ةيساسأل ISE دقع لباقم لاصتالاءاشنإ بجي: ةظحالم
ةبقارم لل



حتف رخآ تلمعتسا عيظتسي تنأ نأ ريغ، 443 ىلإ ريصقت ءانيملا تتبث :ةظحالم
لېصوتلا سسؤي نأ ISE في ءانيم.


Prime Infrastructure

Administration / Servers / ISE Servers / Add ISE Server

Server Address

10.4.21.55

Port

443

Username

admin

Password

.....

Confirm Password

.....

HTTP Connection Timeout

30

(Max:300 secs)

Save

Cancel

(إم) رودل ضرع متي و هي إلو لوصولو نكمي هنأ مداخل ةلاح لوقت ISE. مداخل ةحفص إلو عجرا. اعبار [mnT] يونات وأ [mnT] ياساسأ وأ لقتسم:


Prime Infrastructure

Application Search

roy - ROOT-DOMAIN

Administration / Servers / ISE Servers

-- Select a command --

Go

	Server Address	Port	Retries	Version	Status	Role
☐	10.4.21.55	443	1	3.1.0.518	Reachable	Primary

ةياهنل ةطقن نيوك

نم إم كلذ قيقحت نكمي و. dot1x (RFC 3850) ةقداصم ءارجل ةياهنل ةطقن نيوك بجي 10. ماظن هجوم نم ةدافتسالا وأ Cisco نم (NAM) ةكبشلا إلو لوصولو ريديم نيوك لالخ هذه جارداب موقن ال ىتح نيوكتل اذهب ةقلعتمل ةلدأل نم ريثكلا كانه. يلصلأا ليغشتلا ليلدل اذه في تاوطخل

ةحصلال نم ققحتلا

ISE نم ققحتلا

حاجنب مدختسملا قداصتو NAD نم RADIUS بلط ISE ىقلتت

ةكبشلا ةزهجأ > ةكبشلا دراوم > ةرادا > ISE في RADIUS ل هنيوكتل و NAD ةفاضا مت

1. ةرشابم لمعلا تاسلج > RADIUS > تاي لمعلا ىلإ لقنتنا.

تامولعم ةكراشم متت. ةحفصلا هذه يف ةرشابم لمعلا مدختسم لمعلا ةسلج جاردنا نم دكأت Prime Infrastructure عم ةسلجلا.

Cisco ISE

Operations · RADIUS

Live Logs

Live Sessions

Refresh

Export To

Filter

Refresh

Every 1 minute

Show

Latest 20 records

Within

Last 24 hours

Initiated	Updated	Session Sta...	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Server	Auth M...	Authentication Prot
×				Endpoint ID	Identity		Endpoint Profile	Posture Statu	Security Grov	Server	Auth Meth	Authentication Protoco
Apr 14, 2022 08:04:54.72...	Apr 14, 2022 08:04:54.9...	Started	Show CoA Actions	A0:36:9F:89:67:EA	ivillega	10.4.21.51	Windows10-Workst...			ise-31	dot1x	PEAP (EAP-MSCHAPv2

Last Updated: Thu Apr 14 2022 13:04:40 GMT-0400 (Eastern Daylight Time)

Records Shown: 1

2. ةرشابم لتالسلج > RADIUS > تاي لمعلا يف لمعلا ةسلج فرع نم ققحت:

Cisco ISE

Operations - RADIUS

Live Logs

Live Sessions

Misconfigured Supplicants0

Misconfigured Network Devices0

RADIUS Drops0

Client Stopped Responding0

Repeat Counter0

Refresh

Reset Repeat Counts

Export To

Filter

Time	Status	Session ID	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	Event	IP Address	Network De...	Device Port
X				ivillega	x						IP Address		
Apr 14, 2022 08:04:54.9...		0A58AEE20000002F1E...	0	ivillega	A0:36:9F:89:67:EA	Windows1...	Default >>...	Default >>...	PermitAcc...	Session State is St...	10.4.21.51		TenGigabitEth...
Apr 14, 2022 08:04:54.7...		0A58AEE20000002F1E163DA0		ivillega	A0:36:9F:89:67:EA	Windows1...	Default >>...	Default >>...	PermitAcc...	Authentication suc...	10.4.21.51	DefaultNetwo...	TenGigabitEth...

Last Initiated: Thu Apr 14 2022 13:05:30 GMT-0400 (Eastern Daylight Time)Records Shown: 2

NAD نم ققحتلا

لمعلا ةسلج فرع عم لمعلا ةسلج فرع مقباطتي. NAD يف لمعلا ةسلج ليصافت عجار 3. يف ISE:

```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
Interface: TenGigabitEthernet1/11
MAC Address: a036.9fb9.67ea
IPv6 Address: Unknown
IPv4 Address: 10.4.21.51
User-Name: ivillega
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 0A58AEE20000002F1E163DA0
Acct Session ID: 0x00000023
Handle: 0xD9000001
Current Policy: POLICY_Te1/11
```

Method status list:
Method State

Authc Success

Prime لةيساسألةينبلانمققحتلا

MAC ناو نع ضرع متي .نيمدختسم لاو عالمعال > عبقارملا تاودأ > عاشلا ىلإ لقتنا 4. :ةياهنلا ةطقنل

Prime Infrastructure

Application Search

[Home](#) | [Monitor / Monitoring Tools / Clients and Users](#)

Troubleshoot

Test

Disable

Remove

More

Track Clients

Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name	Interface	Interfa...	VLAN	Protocol	Status	Association Time
	a0:36:9f:b9:67:ea	10.4.21.51	IPv4	ivillega		Intel C...	Unknown	MXC.TAC.M 0...	TenGigabit...		0	802.3	Disassoci...	Apr 06, 2022, 12:35:29 PM

5. SE: مداخل عامه و مدخست سمل لمع ةسلج لى صافت ىرتس ، اءقوف رقنلاب تمق اءا 5.

Prime Infrastructure

Monitor / Monitoring Tools / Clients and Users / a0:36:9f:b9:67:ea ☆

Test+ | Disa

Overview ISE Events Troubleshoot and Debug Location

Attributes

a0:36:9f:b9:67:ea MXC.TAC.M.07-6816-01.ivilega.com

Client Attributes

General		Session		Security	
User Name	ivilega ⓘ	Status	Disassociated	Authenticating ISE	ise-31
MAC Address	a0:36:9f:b9:67:ea	VLAN ID	0	Authentication Method	802.1X
IP Address	10.4.21.51	VLAN Name	Data Not Available	Auth Status	Authorization Succeeded
Vendor	Intel Corporate	Interface	TenGigabitEthernet1/11	Authorization Profile Name	PermitAccess ⓘ
Endpoint Type	Windows10-Workstation ⓘ	Interface Description	Data Not Available	Posture Status	Unknown
Hostname	Data Not Available	Switch Name	MXC.TAC.M.07-6816-01.ivil	TrustSec Security Group	Data Not Available
Media Type	Wired	Switch IP Address	Data Not Available	Audit Session ID	0A58AE2000000B00026CA4
CDP Device ID	Data Not Available	Wired Speed	1Gbps	Windows AD Domain	Data Not Available
Software Version	Data Not Available	On Network	No	EAP Type	Unknown
Model	Data Not Available				
UDI	Data Not Available				

Traffic

Last Accounting Time	Bytes Tx/Rx
2022-Apr-07, 22:48:21 UTC	0/0

6. **هياكل الطاقون لمعالجة شاحنات** ISE مساب ةامسم بيوبت ةمالع اضيأ كانه. هذه ISE نم شاحنات ل Prime Infrastructure هم دختست يذل ينمزل راطال دي دحت كنكمي. هذه

Authentication Records

Date	Status	Failure Reason	ISE
Apr 14, 2022 01:04 PM	Authentication Passed	None	ise-31
Apr 14, 2022 01:04 PM	Authentication Passed	None	ise-31

اهحال صاوا عا طخال فاشكتسا

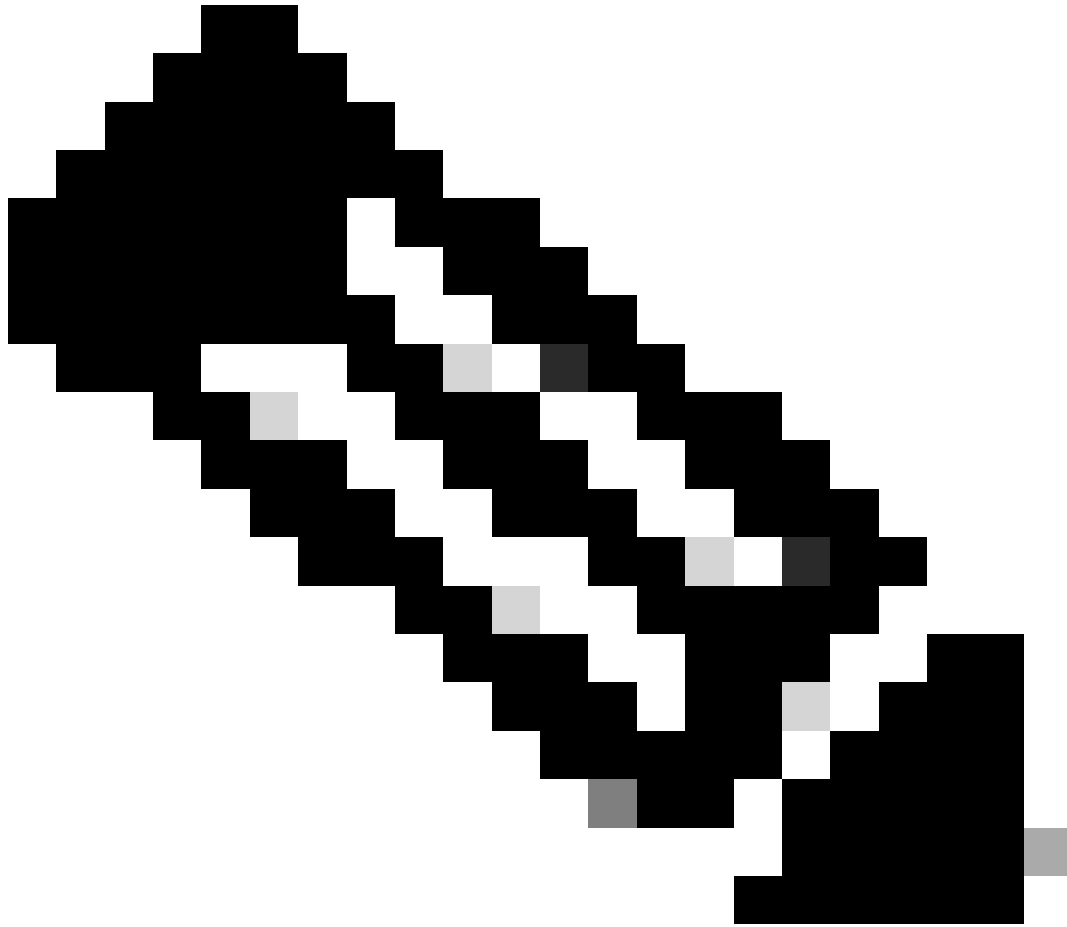
1. نكي مل اذا. لاصتال تارابتخإ مادختساب Prime Infrastructure و ISE نيب لاصتال رابتخإ. لاشكتسا عقوم ديدحتل PI و ISE نم اما عبتتال تاراسم مادختسا كنكمي ف، لاصتال كانه.

2. ذفنملا (ISE MnT) ةدقع ي ف 9 ةوطخال ي ف هنيوكت مت يذال ذفنملا حتف نم ققحت. (443 وه يضارفال):

```
ise-31-1/admin# show ports | include :443
tcp: 0.0.0.0:80, 0.0.0.0:19444, 0.0.0.0:19001, 0.0.0.0:443
```

حوتفملا ذفنملا هي دل ISE MnT نأ ينعي كلذ نإف، جارخال ي ف اجرم ذفنملا ناك اذا.

ذفنملا كلذ هي دل ISE MnT نأ ينعي اذهف، جردم ريغ ذفنملا ناك وأ جارخال كانه نكي مل اذا. قيرف ISE عم TAC ةلاح حتفا وأ ءانيم رخآ عم تلواح عيطتسي تنأ، ةلاحال هذه لثم ي ف. اقلغم حتفي مل ءانيملا امل صحتفي نأ.



ذفانملا حتفل ةقيرط دجوت الو، ذفانملا ضعب ال ISE MnT ةدقع مدختست ال :ةظحالم
ذفانملا عجرم مسق وأ ISE، تيبتت ليلد يف ةجرمدل ريغ ISE MnT ةدقع يف

ل ةيساسألآ ةينبل نم Telnet مادختساب 9 ةوطخل يف هنوكت مت يذلا ذفنملا ربتخا 3.
Prime:

```
prime-testcom/admin# telnet 10.4.21.55 port 443
Trying 10.4.21.55...
Connected to 10.4.21.55.
```

ا.حجان ناك رابتخالأ نأ ينعي اذهف ،<ISE MnT IP/FQDN> ب الصتم Telnet رابتخا جارخا ناك اذا

لشف ينعي كلذ نإف ،<ISE MnT IP/FQDN> ةلواحم يف اقلالاع Telnet رابتخا جارخا ناك اذا
عم وأ كيذل ةطيسولا ةكبشلا ةزهجأ يف ACL مئاوقب اطبترم اذه نوكي نأ نكمي .رابتخالأ
ةياملال رادج دعاوق

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا