

Nexus زاھج ىلع TLS 1.3 ربع TACACS+ نيوكت ISE مادختساب

تايوتحمل

[عمدقملا](#)

[عماع قرظن](#)

[لىلدلا اذه مادختسا](#)

[قيساسلا تابلاطت ملا](#)

[تابلاطت ملا](#)

[عمدختسملا تانوك ملا](#)

[صيخرت ملا](#)

[زاھجلا لوؤسملا ISE نيوكت](#)

[TACACS+ مداخ عمداصملا عداھشلا عيقوت بلاط عاشن](#)

[TACACS+ مداخ عمداصملا رنجلال قدصملا عجرملا عداھش ليمحت](#)

[ISE ب \(CSR\) عقوملا عداھشلا عيقوت بلاط طبر](#)

[نيكمت TLS 1.3](#)

[ISE ىلع عزھجالا قرادا نيكمت](#)

[TLS ربع TACACS نيكمت](#)

[ككشللا عزھجا تاغومجمو ككشللا عزھجا](#)

[ConfigureIdentity رجاتم](#)

[TACACS+ قبط فيرعت تافل م نيوكت](#)

[NX-OS قرادا](#)

[NX-OS عمدعاسم بتكم](#)

[زاھجلا لوؤسم جهن تاغومجم نيوكت](#)

[TLS ربع TACACS+ ل Cisco NX-OS نيوكت](#)

[TACACS+ مداخ نيوكت](#)

[TrustPoint نيوكت](#)

[TACACS+ TLS نيوكت](#)

[AAA نيوكت](#)

[اھجالصا و NX-OS ىلا مدختسملا لوصو عاطخا فاشكتسا و رابتخا](#)

[ققحتلا](#)

[اھجالصا و عاطخال فاشكتسا](#)

عمدقملا

مداخك Cisco نم (ISE) ةيولال تامدخ كرحم عم TLS ربع TACACS+ ل الاثم دنتسملا اذه فصى ليمعك NX-OS زاھجو.

عماع قرظن

ةيفرطال ةطحملال إلال لوصولال مكحت ةدحو إلال لوخدلال ةبقارم ماظن لوكوتورب حيتي ةكبشلال إلال لوصولال مداوخو تاهجوملل زاهجلل ةيزكرمل ةرادلال ةيناكم [RFC8907] (TACACS+) تامدخ رفوي وهو. رثكأ وأ دحاو TACACS+ مداخ لالخنم ةكبشلال ةلصتلمال ىرخألال ةزهجالاو ةزهجالا ةرادا مادختسا تالاحل اصيصخ ةممصملا (AAA) ةبساحملاو ضيوفتلاو ةقداصملا

لقن ةقبط لالخدلال لالخنم لوكوتوربال نيسحت ىلع [RFC8446] TLS 1.3 ربع TACACS+ لمعي ةهازنلاو ةيرسلال لماكتلا اذه نمضي. ةيساسحلل ةديش تانايبلا ةيامح ىلع لمعي امم، ةنمأ م. مداوخلالو TACACS+ ءالمع نيب ةكبشلال رورم ةكرحو لالصلال ةقداصملاو

ليلدللا اذه مادختسا

ةكبشلال ةزهجالا يرادلل لوصولال ةرادا نم ISE نيكمتل نيئزج ىلإ ةطشنألا ليلدللا اذه مسقي Cisco NX-OS نم NX-OS ىلإ ةدنتسمل

- زاهجلال لوؤسمل ISE نيوكت - 1 ءزجل
- TLS ربع TACACS+ ل Cisco NX-OS ليغشت ماظن نيوكت - 2 ءزجل

ةيساسألا تابلطتملا

تابلطتملا

TLS ربع TACACS+ نيوكتل ةيساسألا تابلطتملا:

- عيقوتل TLS ربع TACACS+ لبق نم ةمدختسملل ةداهشلا عيقوتل (CA) قدصم عجرم ةكبشلال ةزهجالو ISE تاداهش.
- (CA) ةداهشلا حنم ةهج نم رزجلل ةداهشلا.
- ءامسألا ح اهنكميو DNS ىلإ لوصولال ةيناكل ىلع ISE و ةكبشلال ةزهجالو يوتحت فيضملا.

ةمدختسملل تانوكمل

هاندا ةيداملل تانوكمل او جماربال تارادصل ىلإ دنتسملل اذه في ةدراولل تامولعملل دنتست

- ISE VMware، رادصلال 3. 4 Patch 2. يرهاظلال زاهجل
- Nexus 9000 switch model C9364D-GX2A، Cisco NX-OS، رادصلال 10.5(3t).

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجالا نم دنتسملل اذه في ةدراولل تامولعملل ءاشنإ مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسملل اذه في ةمدختسملل ةزهجالا عيمجتأ دب رمأ يأل لمحتحملل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك كبش

صيخرتلا

في. ةسايسلا ةمدخ ةدقع ىلع TACACS+ تامدخ مادختساب ةزهجالا ةرادا صيخرت كل حمسي تامدخ مادختساب ةزهجالا ةرادا صيخرت كل حمسي، رفوتلا ةيلاع (HA) ةلقتسم رشن ةيلمع HA. جوز في ةدحاو ةسايس ةمدخ ةدقع ىلع TACACS+

زاهجال ل وؤس مل ISE نيوكت

TACACS+ مداخ ة قداصل مل ة داهشل عي قوت بل ط عاشنإ

ة موعدم لا تا ضرعت سمل دحأ مادختساب بيولا ىلع ISE ة رادإ ة باب ىلإ لوخدلا لجس 1. ة ووطخل

ىل وائل ة ووطخل لثمتت. تامدخل ايمجل ايتاذ ة عقوم ة داهش ISE مدختسي، يضارتفا لكشبو (CA) قداصل عجرمل لبق نم ه عي قوتل (CSR) ة داهش عي قوت بل ط عاشنإ يف

تاداهشل > ماظنلل > ة رادإل ىلإ لقتنا 2. ة ووطخل



Your Evaluation license expires in 83 days. You will

Vulnerability

Administration

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings

Identity Management

Identities

Groups

External Identity Sources

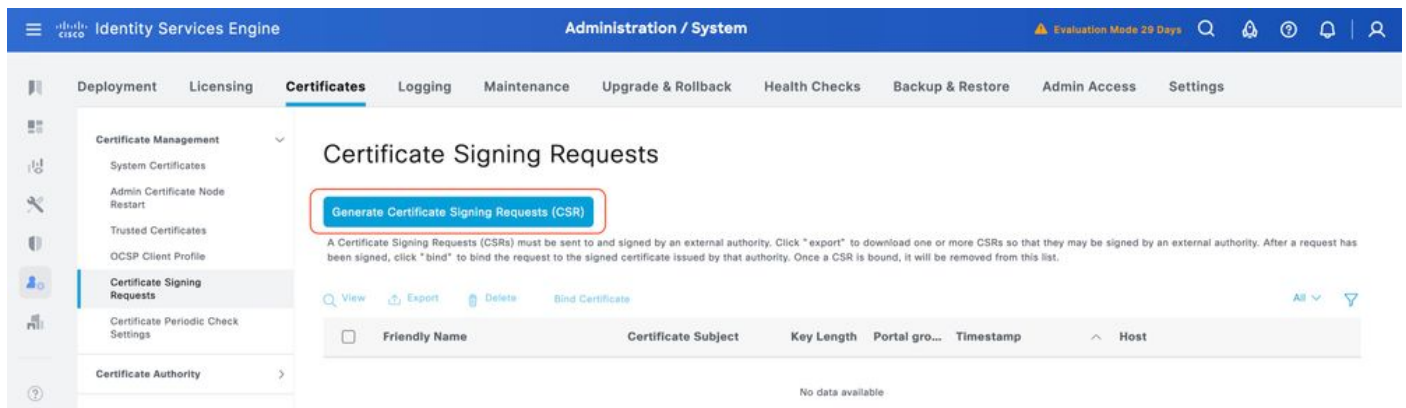
Identity Source Sequences

Settings

Feed Service

Profiler

3. عوطخلا



مادختسالا في TACACS ددح 4. ةوطخل

Usage

Certificate(s) will be used for **TACACS** ▼

Allow Wildcard Certificates ☐ ?

اهل TACACS+ نيكمت مت ي التال PSN تاكبش ددح 5. ةوطخل

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

ةبسانملا تامولعملاب عوضوملا لوقح ألما 6. ةوطخل

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

Country (C)
US

(SAN) ليدب ال عوضوم ال مسا تحت IP ناو نعو DNS مسا فضا 7. ةوطخل

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	-	+	
⋮	IP Address	✓	10.225.253.209	-	+	①

ري دصت م ث عاشن ا قوف رقا 8. ةوطخل



(CA) صيخرتل ةئيه نم ةعقوم (CRT) ةداهشل ىلع لوصحلل كنكمي ،نآل

TACACS+ مداخل ةقداصل رذل قداصل عجرم ةداهش ليمحت

ىلع رقنا ،نومضم صيخرتل تحت .تاداهشل > ماظنل > ةرادلإ ىلإ لقتنا .1 ةوطخل داريتسإ

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	Ent
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Ent
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Ent
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 2016	Sun, 9 Aug 20...	Ent
☐	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...	Ent
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Ent

ةداهش عيقتو بلط تعقويتل (CA) قداصل عجرم نع ةرداصل ةداهشل دح .2 ةوطخل ISE نمض ةقداصل ةقثل راخي نكمتم نم دكأت .كب صاخل (CSR) TACACS

Import a new Certificate into the Certificate Store

* Certificate File **Examinar...** ISE SVSLab CA.crt

Friendly Name

Trusted For:

- ☒ Trust for authentication within ISE
- ☐ Trust for client authentication and Syslog
 - ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPSec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit

Cancel

اهب قوٹومل تاداهشل نمض نأل ةداهشل رهظت نأ بجي .لاسرا ىلع رقنا

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Trusted Certificates

For disaster recovery it is recommended to export and backup all your trusted certificates.

Edit Import Export Delete View show internal CA certificates

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2025	Enz
☐	Default self-signed server certificate	Endpoints Infrastructure	02 36 30 F4 6...	ISE2.tmo.svs.com	ISE2.tmo.svs.com	Fri, 11 Jul 2025	Sun, 11 Jul 2025	Enz
☐	DigiCert Global Root CA	Cisco Services	08 3B E0 56 9...	DigiCert Global R...	DigiCert Global R...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enz
☐	DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6 ...	DigiCert Global R...	DigiCert Global R...	Thu, 1 Aug 2013	Fri, 15 Jan 20...	Enz
☐	DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26 ...	DigiCert High Ass...	DigiCert High Ass...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enz
☐	DigiCert SHA2 High Assurance Server ...	Endpoints Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 Hi...	DigiCert High Ass...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	Enz

ISE ب (CSR) عقوقم ةداهشل عي قوت بلط طبر

ISE. ىلع ةعقوقم ةداهشل تي بثت كنكمي ،(CSR) ةداهشل عي قوت بلط عي قوت درجم

TACACS دح ،ةداهشل عي قوت تابلط تحت .تاداهشل > ماظنل > ةرادإل ىلإ لقتنا . 1 ةوطخل ةداهشل طبر قوف رقناو ةقباسل ةوطخل ي ف مؤاشنإ مت يذل CSR

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings

Certificate Signing Requests

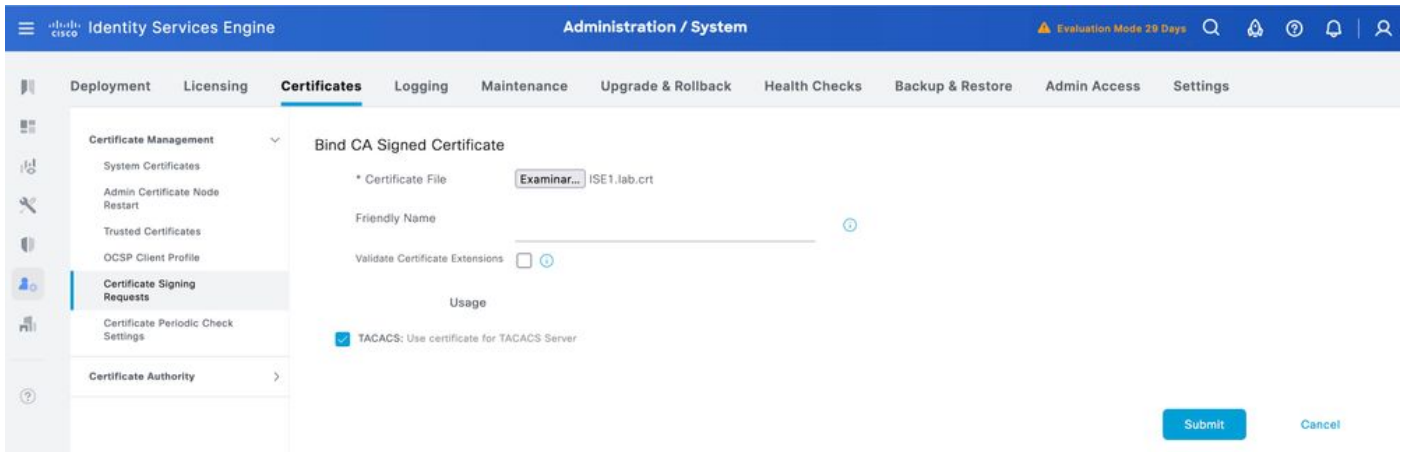
Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

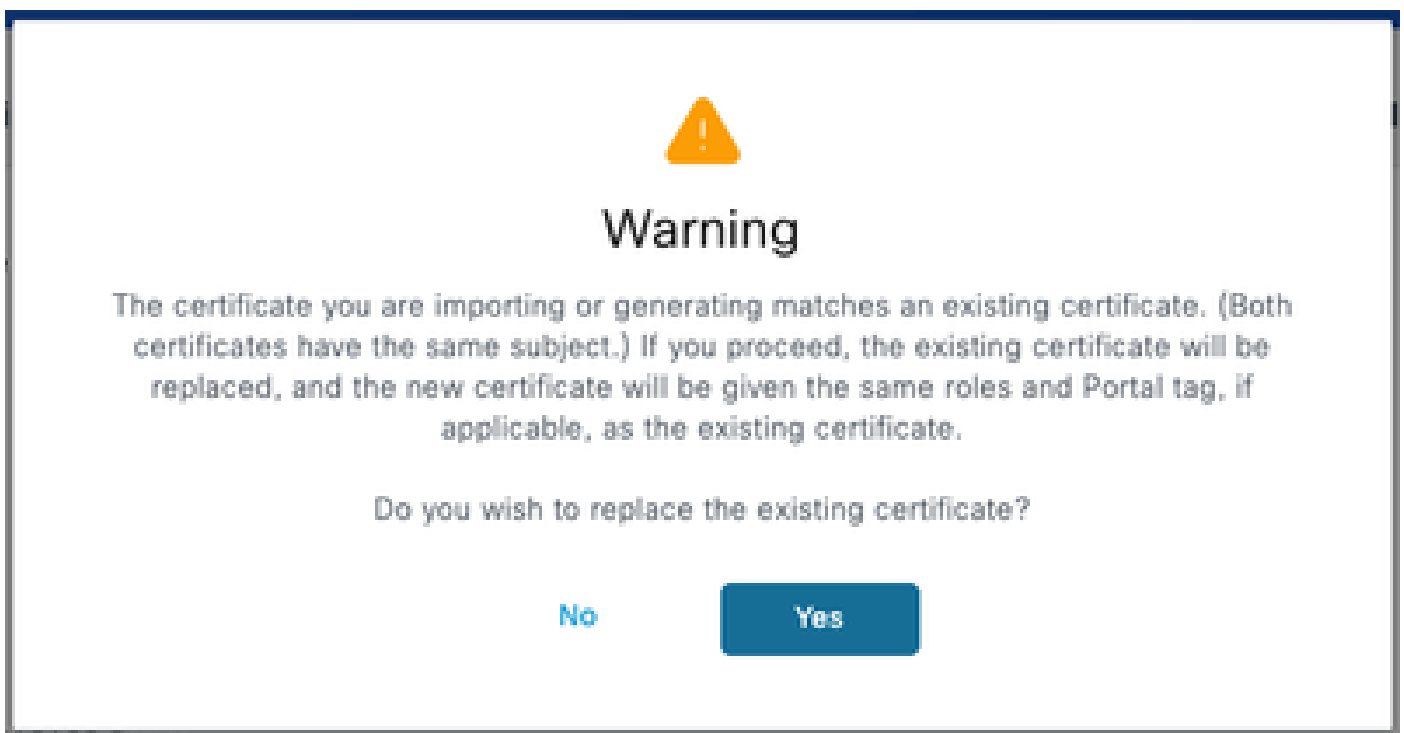
View Export Delete Bind Certificate

☐	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
--------------------------	---------------	---------------------	------------	---------------	-----------	------

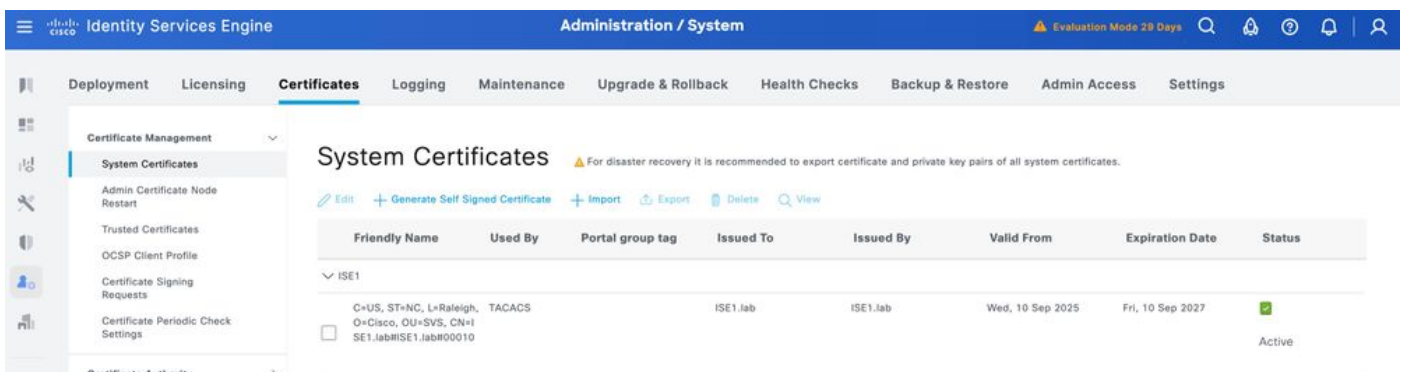
مادختسالا تحت ةدوجومل TACACS رايتخالال ةناخ نأ نم دكأتو ةعقوقم ةداهشل دح . 2 ةوطخل ةددم لازت ال



معن قوف رقنا ،ةدوجومال ةداهشلا لادبتسا لوح اريذحت تيقلت اذا .لاسرا قوف رقنا .3 ةوطخلل ةعباتملل



م.اظنل تاداهش نمض كلذ نم ققحتلا كنكمي .حيحص لكشب نآلا ةداهشلا تيبت بجي



TLS 1.3 نيكم

ايودي اهنى كم ت ب جي ISE 3.4.x ي ف يضارت فا لك ش ب TLS 1.3 نى كم ت م تى ال

ت اداع ال > م اظن ال > ة راد ال ال ل ق ت نا 1. ة و ط خ ال

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Deployment

Licensing

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings

رادصا تادادعإ نمض TLS1.3 ل ةرواجملا رايثخالا ةناخ ددحو، نامألا تادادعإ قوف رقنا 2. ةوطخل
ظفح قوف رقنا مث، TLS.

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture

Profiling

Protocols

Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

☐ TLS 1.0

☐ TLS 1.1

☒ TLS 1.2

☒ TLS 1.3

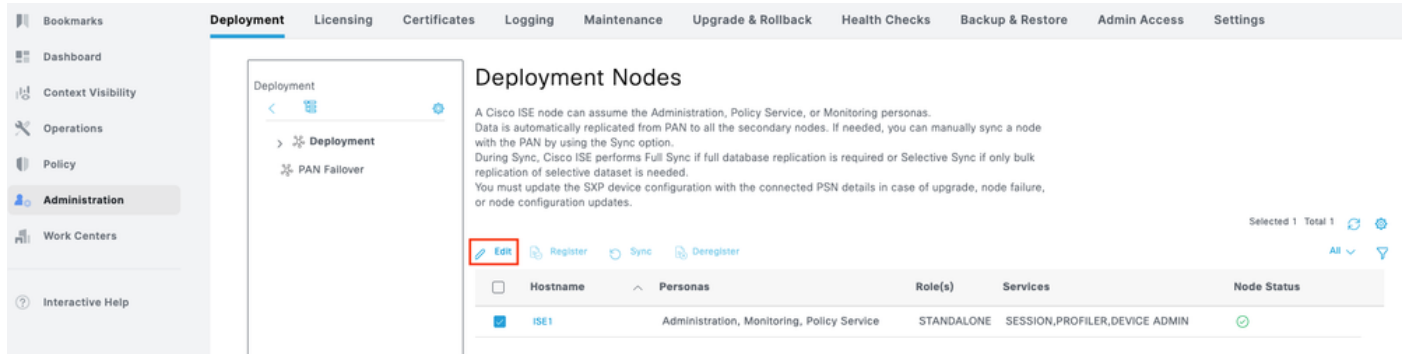


عيمج ىلع Cisco ISE قيبطت مداخل ليغشت ةداعإ متت، TLS رادصا رييغت دنع: ريذخت
Cisco ISE رشنللا ةزهجأ.

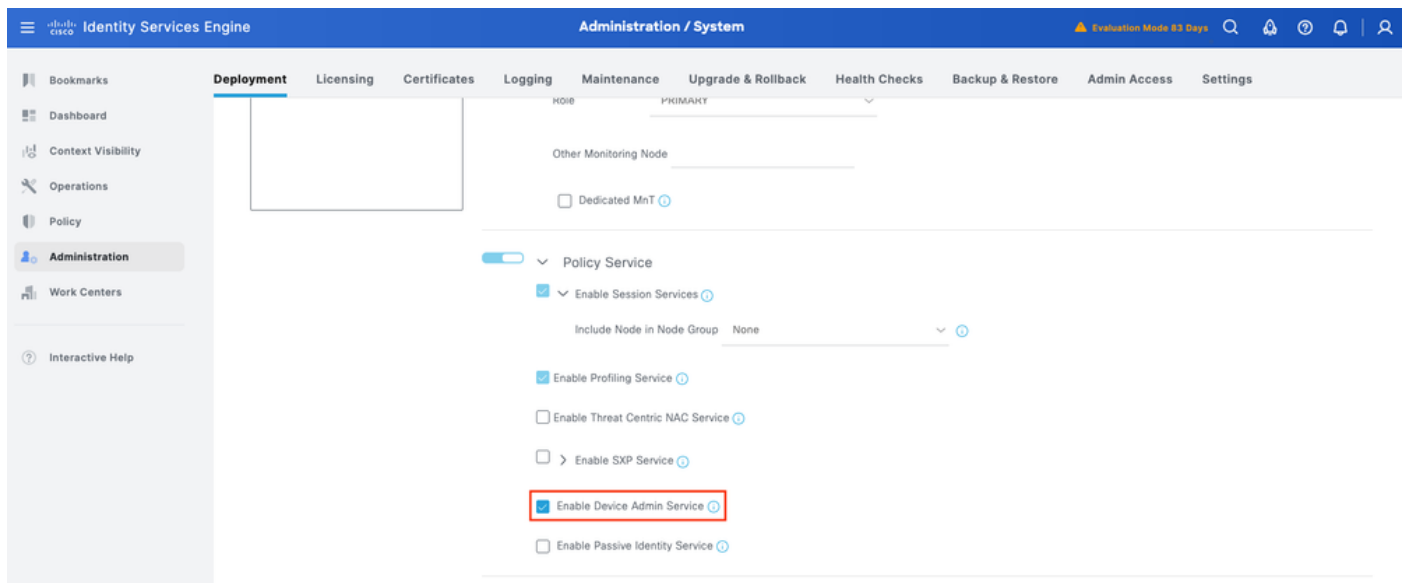
ISE ىل عزهجالا ةرادا نيكمت

نيكمت ب مق ISE ةدق ىل ع يضارتفا لكشب (TACACS+) عزهجالا ةرادا ةمدخ نيكمت م تي ال PSN ةدق ىل ع TACACS+.

رقناو ISE ةدق ل ةرواجم ال راي تخالال ةناخ دح .رشننل > ماظنل > ةرادال ىل ل لقتنا 1. ةوطخل ريرحت قوف.



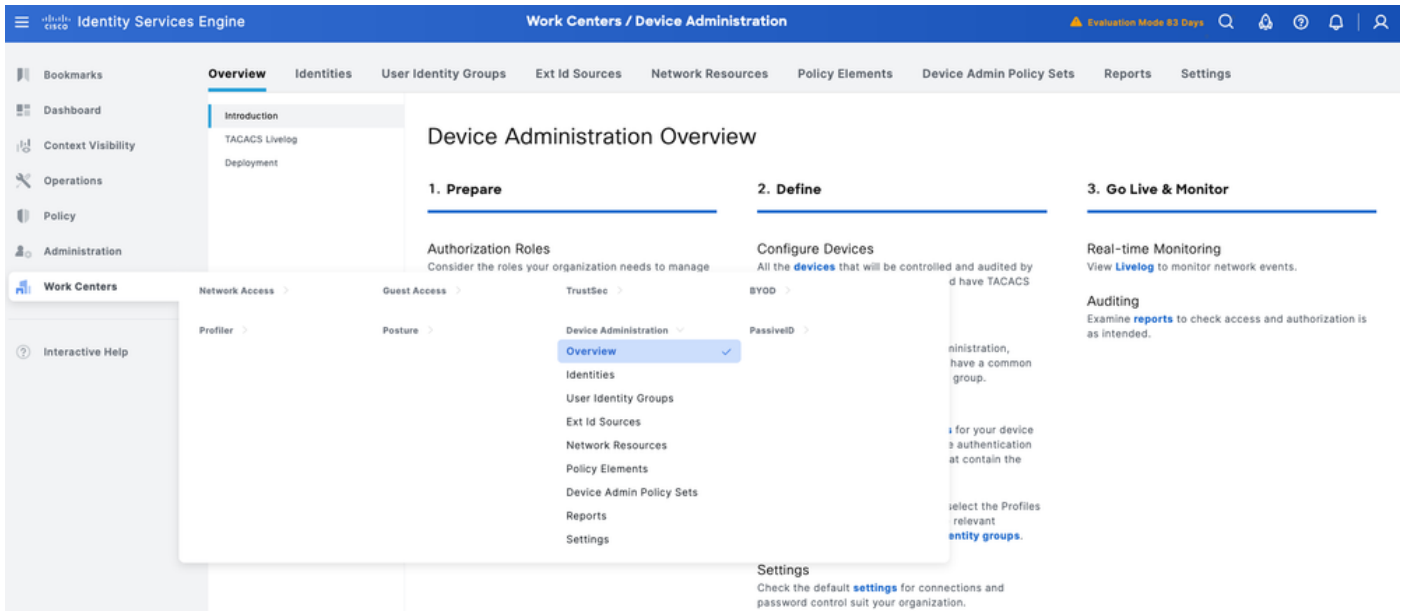
نيكمت ل ةرواجم ال راي تخالال ةناخ دحو لفسا ىل ل ريرمتلاب مق ، ةماع ال تادادع ال تحت 2. ةوطخل ةزهجالا ةرادا ةمدخ.



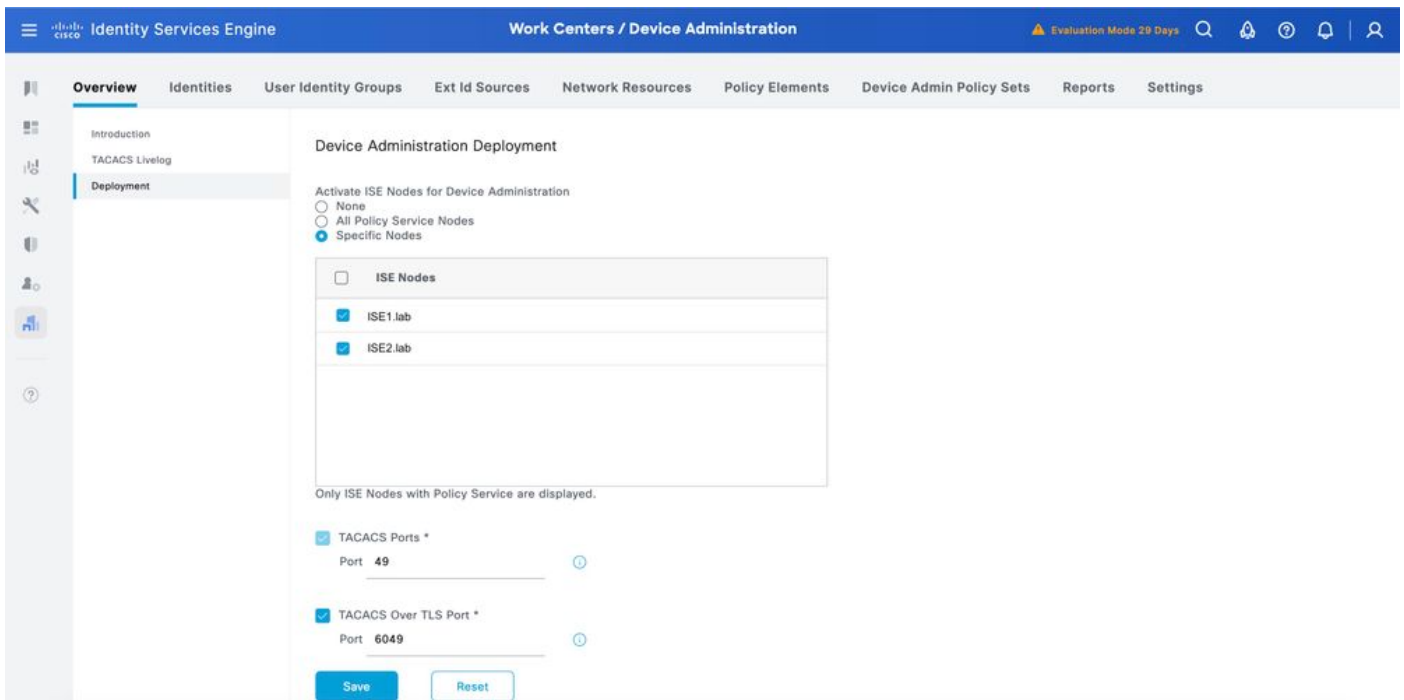
ISE ىل نال "زاهجالا لوؤسم ةمدخ" نيكمت م .نيوكتل ظفح 3. ةوطخل

TLS ربع TACACS نيكمت

ةماع ةرطن > عزهجالا ةرادا > لمع ال زكارم ىل ل لقتنا 1. ةوطخل



2. عوطخل TLS ربع TACACS ني كم ت ديرت شيح PSN دقع دح .رشنللا قوف رقنا 2. عوطخل



م ث ، TLS ربع TACACS ل فلتخم TCP ذفنم دح وأ 6049 يضارثفالا ذفنملا طفا 3. عوطخللا طفا قوف رقنا

ةكبشلا ةزهجأ تاعومجمو ةكبشلا ةزهجأ

لك لثمي .ةزهجالا تاعومجمل ةددعتم ةيمره تالسلستب ةزهجالا ايوق اعيمجت ISE رفوي .ةكبشلا ةزهجالا القتسم وازيتمتم افينصت يللكيه لسلست

ةزهجأ تاعومجم قوف رقنا .ةكبشلا دروم > ةزهجالا ةرادإ > لمعالا زكارم ىلإ لقتنا 1. عوطخللا ةكبشلا

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 72 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

All Groups

Choose group

Add

Duplicate

Edit

Trash

Show group members

Import

Export

Flat Table

Expand All

Collapse All

☐	Name	Description	No. of Network Devices
☐	> All Device Types	All Device Types	--
☐	> All Locations	All Locations	--
☐	Atlanta		0
☐	Los Angeles		0
☐	New York		0
☐	> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

External MDM

More

Network Devices

Default Device

Device Security Settings

☐ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☒ TACACS over TLS Authentication Settings

This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.

Subject Alternative Name (SAN) *

Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

☐ IP Address

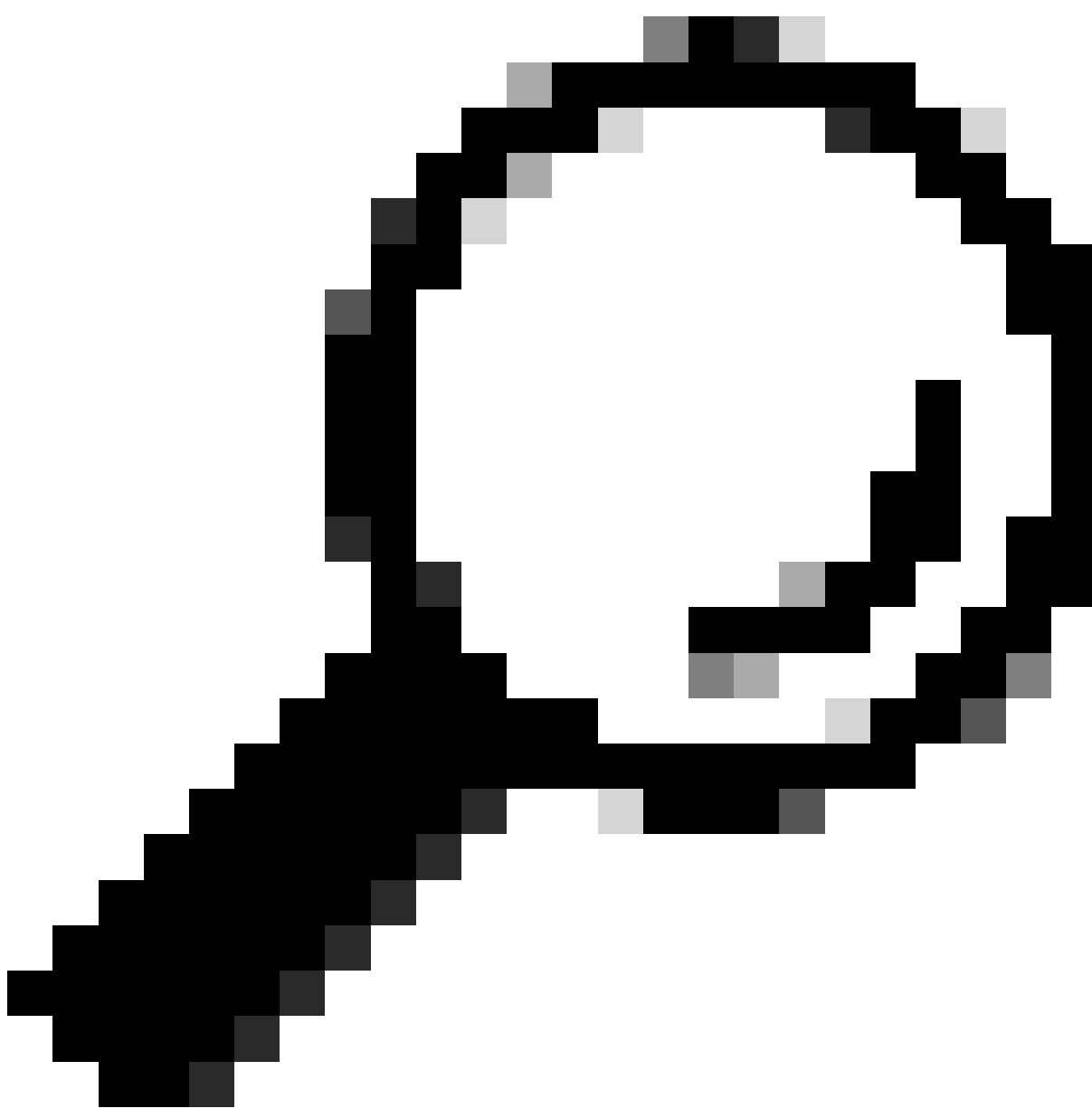
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

Additional SAN Attributes

☒ Enable Single Connect Mode

Allow a network device to use one TCP connection for all TACACS+ requests, reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

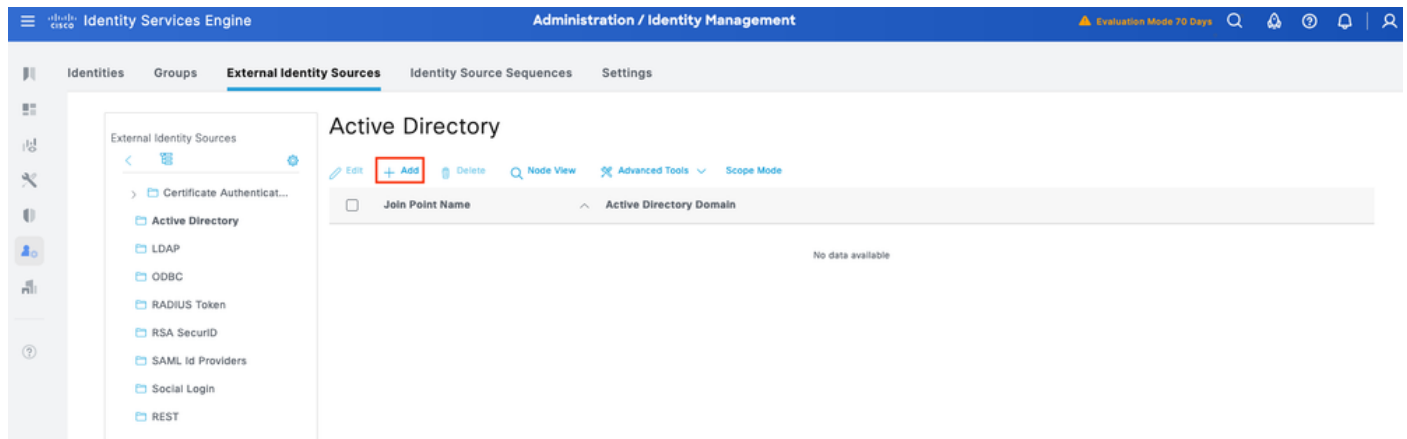


لمع ةسلج ليغشت ةداع| بنحتل درفملا لاصتالا عضو نيكمتب ىصوي :خيملت زاهجلا ىلا اهي رما لاسرا متي ةرم لك في TCP.

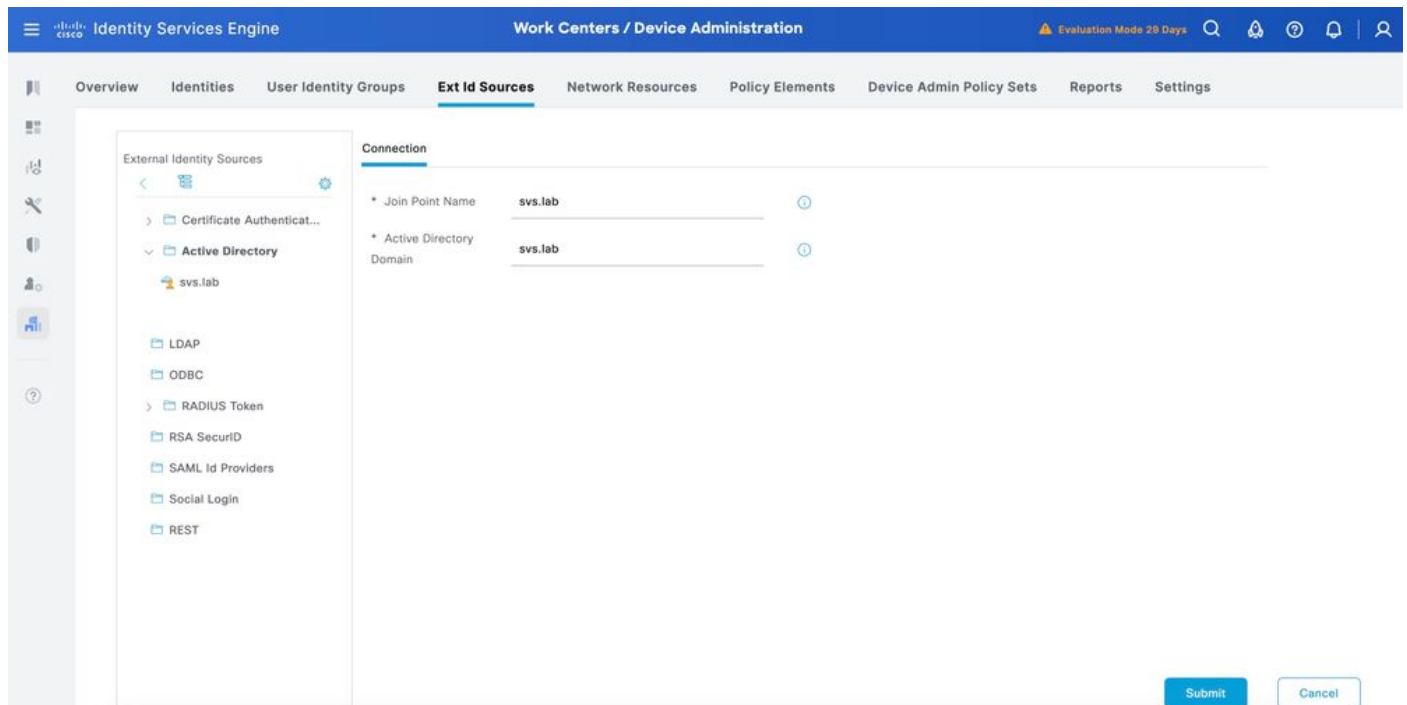
ةيوهلا نزاخم نيوكت

نييلخادلا ISE يمدختسم نوكي نأ نكمي يذلاو، ةزهجالا يلوؤسم ةيوه نزاخم مسقلا اذه ددحي جيراخ ةيوه ردصم ،(Active Directory) ممدختسي انه . ةمومدم ةيجراخ ةيوه رداصم يأو

رقنا . Active Directory > ةيجراخلا ةيوهلا نزاخم > ةيوهلا ةرادا > ةرادالا ىلا لقتنا . 1. ةوطخلا ةديج ةكرتشم AD ةطقن ديدحتل ةفاضلا



لاسرا رقناو AD لاجم مساو طبرلا ةطقن مسا ددح . 2. ةوطخلا



Active Directory لاجم ىلا ISE دقع عيمج مض ي ف بغرت له " كتبلاطم دنع معن قوف رقنا . 3. ةوطخلا اذه ؟ "



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

الرجاء الانتباه إلى أن عملية AD Join تتطلب اسم المستخدم وكلمة المرور الخاصة بـ Administrator. إذا كنت لا ترغب في إجراء العملية، فقم بالضغط على No. إذا كنت ترغب في إجراء العملية، فقم بالضغط على Yes.



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name  administrator

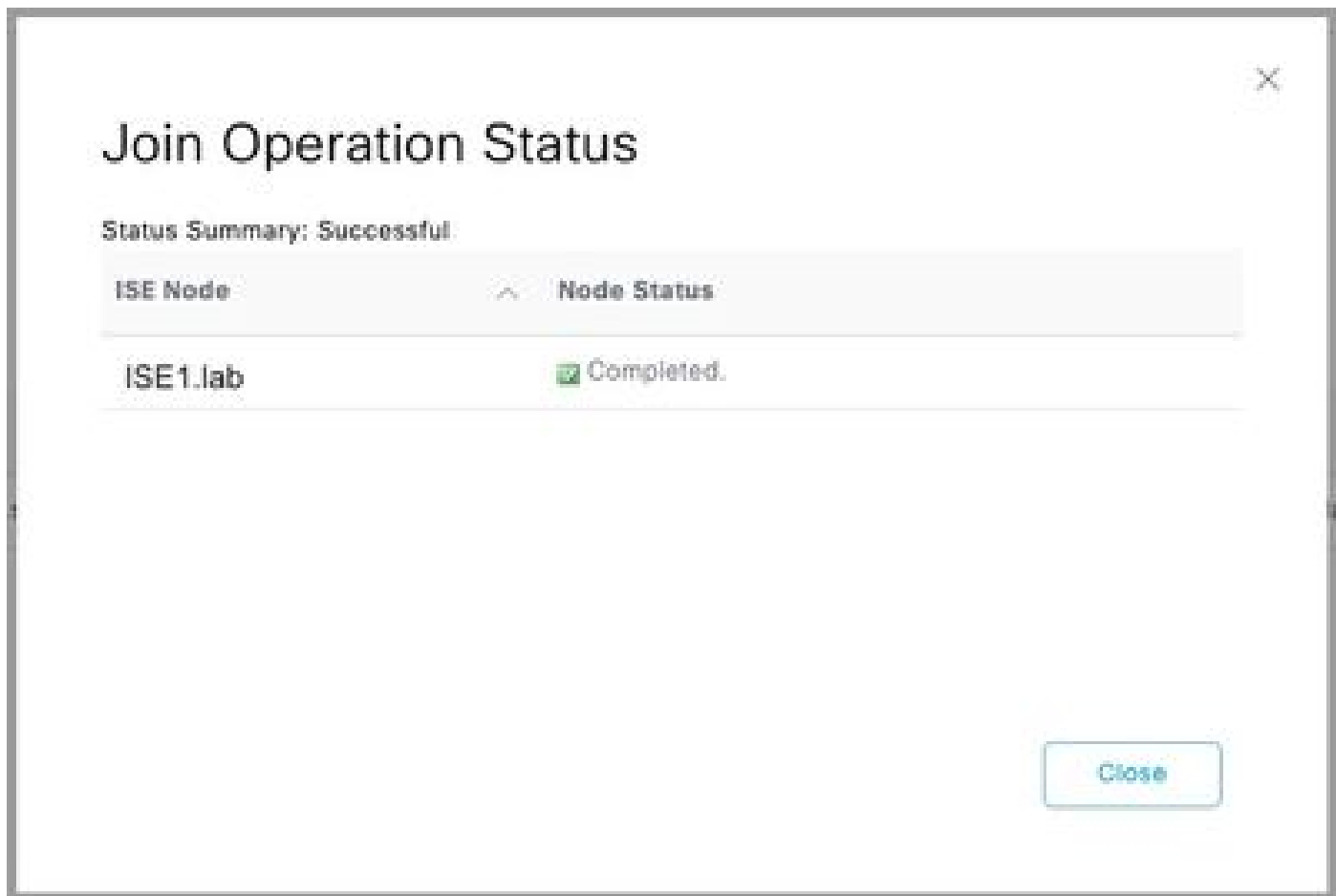
* Password

☐ Specify Organizational Unit 

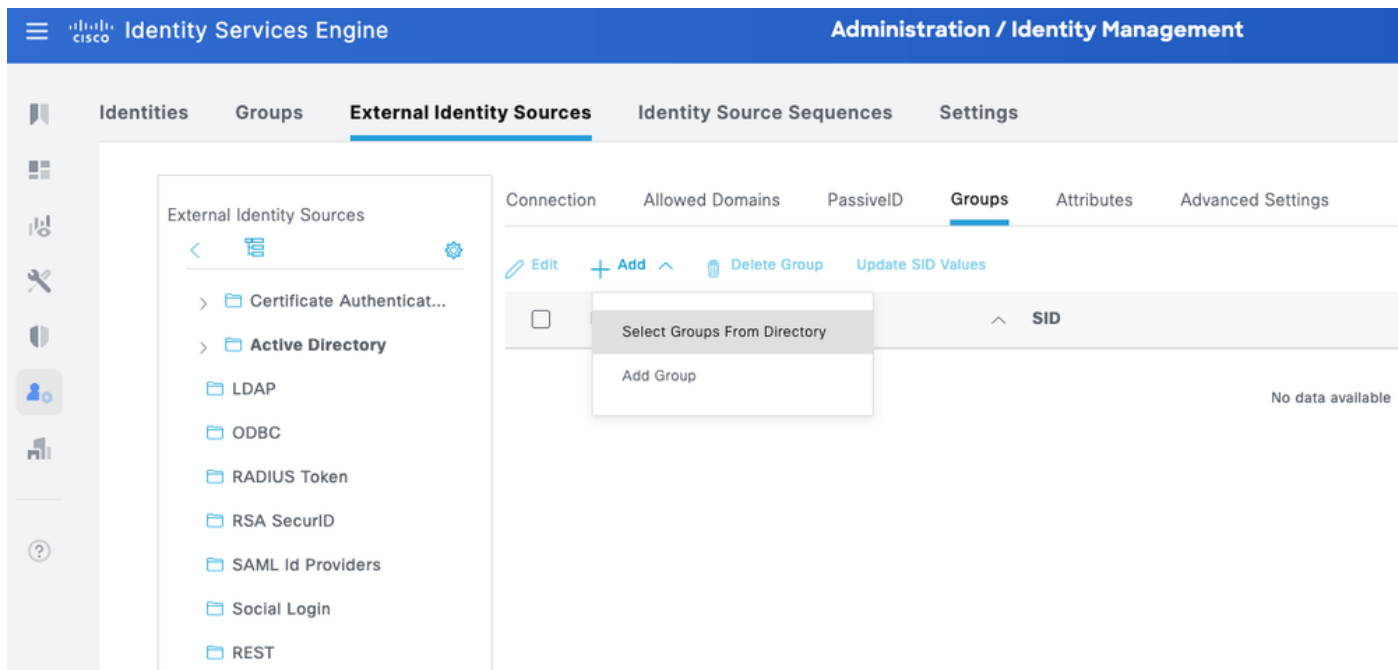
☒ Store Credentials 

Cancel

OK



عيج ىل لوصحلل ةفاضل قوف رقناو ،تاعومجم بيوبتل ةمالع ىل لقتنا 5. ةوطخل لبق نم اهلى لوصولاب نيمدختسملل حومسمل تاعومجملا ساسأ ىل عبولطملا تاعومجملا لىلدل اذه فى لىوختل جهن فى ةمدختسمل تاعومجملا لثمل اذه حضوى .زاهجل



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

svs.lab

Name

Device *

SID *

Type

Filter

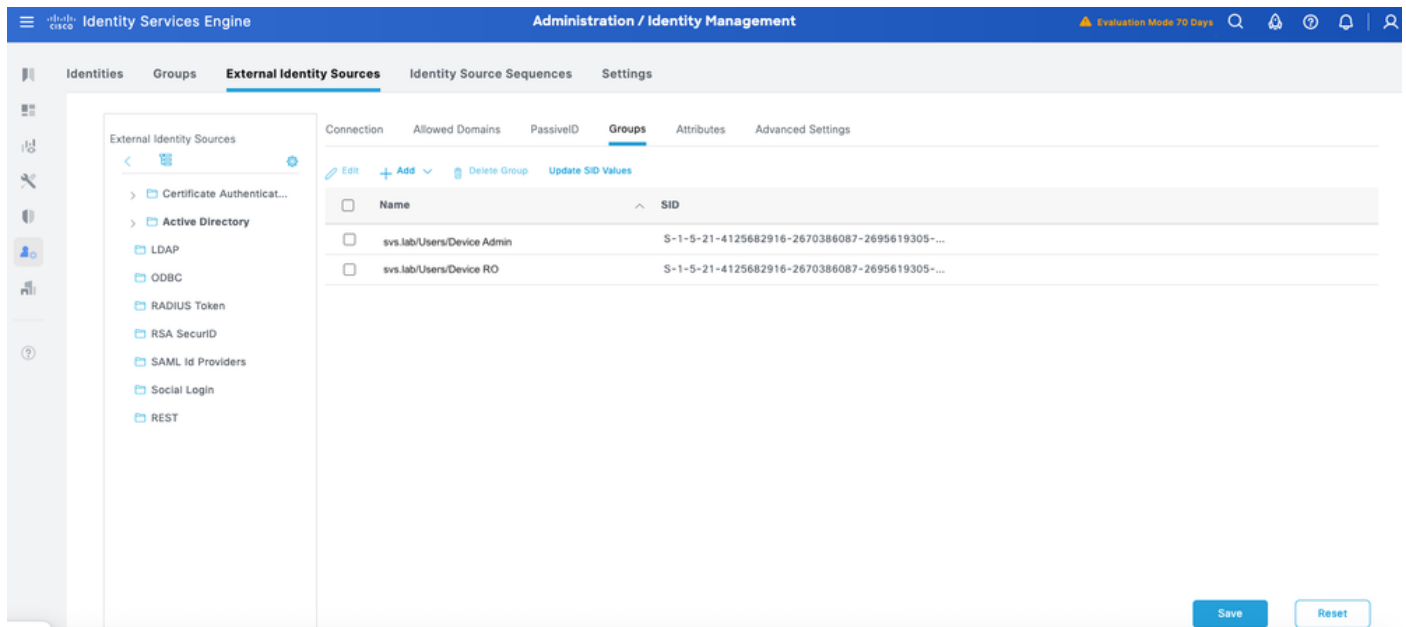
Filter

ALL

Retrieve Groups...

2 Groups Retrieved.

☐	Name	Group SID	Group Type
☐	svs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
☐	svs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



TACACS+ Shell في رعت تافل م نيوكت

Cisco عزة ءأ موقت ،ضيوف لل تازاي تمالا تايوتسم مدختست ي تال، Cisco IOS عزة ءأ فالخ ب نيي عت كنكم ي ISE، ي ف (RBAC) رودلأ ل دن تسم ل لوصول ي ف مكحتل ذي فنن ب NX-OS مامم ل مادختساب Cisco NX-OS عزة ءأ ل ع ني مدختسم ل راودأ TACACS+ تافي صوت Nexus. عون نم ءكرتشم ل

نم نانثا. ڀي ساس ال NX-OS ڀمظنا ڀي NX-OS ڀڙهجا ڀل ع اقب سم ڀدڊم ال راوڊال فلخت
:امه ڀڙاش ال اڀاش ال

- **network-admin** - رودة يوتحي - ددحملا ءكبشلا لوؤسم رود يوتحي - **network-admin** يضا رتفالا يرهاظلا زاهجلا قايس يف رفوتم ؛لوحملال يلع رماوألل عيملل ءباتكلال او نم ديدعلال يلع يوتحت (Nexus 7000، لاثملال ليلبس يلع) ءزهجال تناك اذا طقف (VDC) يلع عالطالل **admin**-ءكبشلا راودأ ءانب NX-OS CLI show cli رمال مدختسا. VDC ذفانم

رودلا اذهل ةرفوتملا ةلماكلا رماوأل ةمئاق

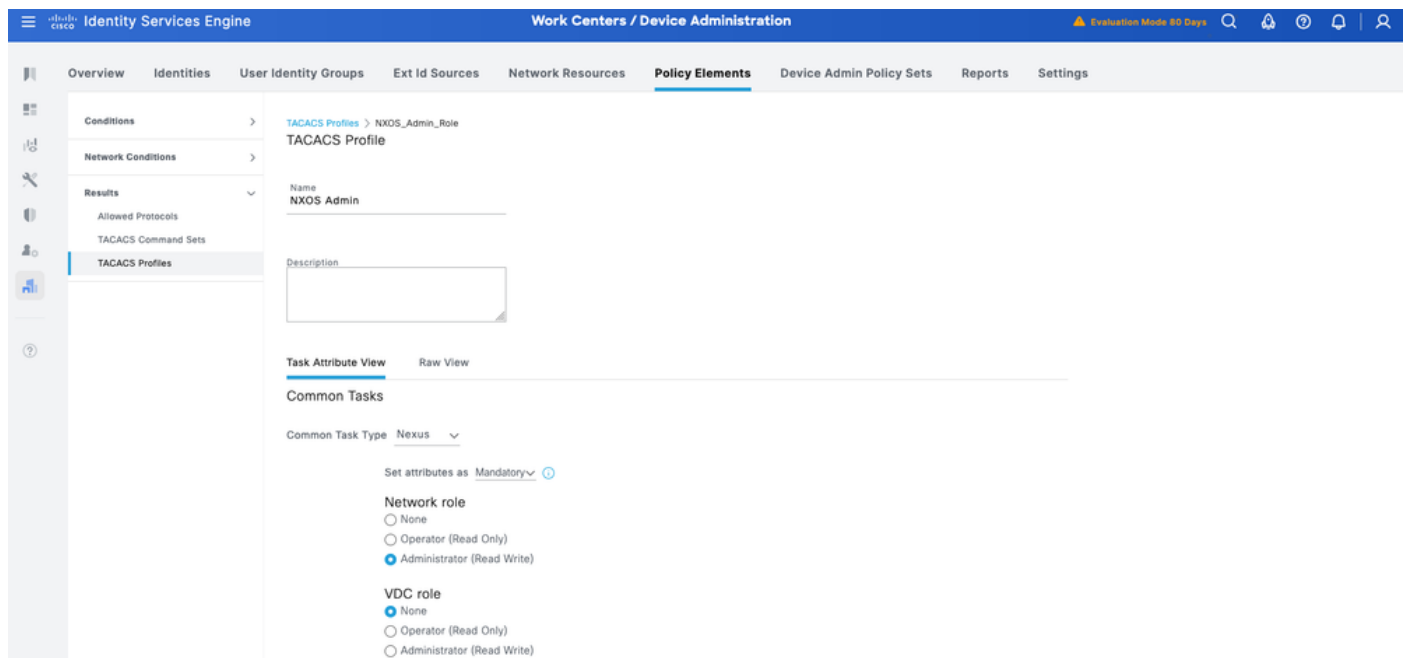
- network-operator لماكل لوصول قحب اقبس م دحمل ةكبشلا لوؤسم رود عتم تي - network-operator دعب نع لوصول يف مكحتلا ةدحو يف رفوتم ؛لوحمل ىلع رماوأل عيمج ىلى ةءارقلل ىلع يوتحت (Nexus 7000 ؛لاثلما لىبس ىلع) ةزهجال تناك اذا طقف ةيضارتفالا (VDC) NX-OS CLI show cli syntax roles رمالا مدختسا . (VDC) دعب نع لوصول طاقن نم ديدعل رودلا اذهل ةرفوتملا ةلماكلا رماوأل ةمئاق ضرعل network-operator

NXOS ةدعاسملا بكتكم و NXOS لوؤسم - TACACS فيرعت فلم ديدحت متي ،كلذ دعبو

NX-OS ةرادإ

NX-OS ةرادإ همساو رخآ فيرعت فلم فضا 1. ةوطخل

ةكبشلا رود راڤخ نم لوؤسم دح .ةلدسنم ةمئاقك تامسلا نييعت نم يمازل دح 2. ةوطخل ةكرتشملا ماهملا نمض



فيرعتلا فلم ظفحل لاسرا ىلع رقنا 3. ةوطخل

NX-OS ةدعاسم بكتكم

> ةسايسلا رصانع > ةزهجال ةرادإ > لمعلال زكارم ىلى لقتنا ،ISE مدختسم ةهجاو نم 1. ةوطخل هتيمست و ديدج TACACS فيرعت فلم ةفاضاب مق .TACACS فيرعت تافل م > جئاتنلا Nexus رتخاو "ةكرتشملا ةمهمل عون" ةلدسنملا ةمئاقلا ىلى لقتنا .NXOS HelpDesk

تاراڤخلا هذه ديدحت كنكمي .مدختسملا رودب ةصاخلا بلالقا تاريغيغت ةيؤر كنكمي .هنوكت ديرت يذلا مدختسملا رود عم ةقفاوتملا

رود راڤخ نم ليغشتلا لماع دح .ةلدسنم ةمئاقك تامسلا نييعت نم يمازل دح 2. ةوطخل ةكرتشملا ماهملا نمض ةكبشلا

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar contains navigation links: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The main content area is titled 'TACACS Profile' and includes a breadcrumb 'TACACS Profiles > NXOS HelpDesk'. The 'Name' field is set to 'NXOS HelpDesk'. Below it is a 'Description' text area. There are tabs for 'Task Attribute View' and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'Nexus'. Below this, there are two sections: 'Set attributes as' (set to 'Optional') and 'Network role' (with options: None, Operator (Read Only) - selected, Administrator (Read Write)). The 'VDC role' section has options: None - selected, Operator (Read Only), and Administrator (Read Write).

صيصختال فلم ظفحل ظفح ىلع رقنا 3. ةوطخل

زاهجال لوؤسم جهن تاعومجم نيوكت

تاعومجم مسقت نأ نكمي .ةزهجال ةرادإل يضارتفا لكشب جهنل تاعومجم نيكمت متي ىلع TACACS فيرعت تافلم قيبطت ليهستل ةزهجال عاونأ ىلإ ادا نسا تاسايسلا امنيب رماوال تاعومجم وأ/و تازايتمال تاويوتسم Cisco IOS ةزهجال مدختست ،لا ثمل ليبس ةصصخم تامس Cisco نم NX-OS ةزهجال مدختست .

ةزهجال ةفاضل .ةزهجال ةرادإ تاسايس تاعومجم > ةزهجال ةرادإ > لمعل زكارم ىلإ لقتنا 1. ةوطخل عاونأ عيمج يواسي DEVICE:Device Type دح ،طرش تحت .ةديج جهن ةعومجل NX-OS يضا رتفال زاهجال لوؤسم دح ،اهب حومسمل تالوكوتوربل تحت .NXOS#ةزهجال

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar is the same as the previous screenshot. The main content area is titled 'Policy Sets' and includes buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save'. Below these is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. There is a search bar above the table. The table contains one entry: 'NX-OS Devices' with a status of 'ON' and a condition of 'DEVICE Device Type EQUALS All Device Types#NXOS'. At the bottom right, there is a 'Default Device Admin' label and a '+ -' button.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
ON	NX-OS Devices		DEVICE Device Type EQUALS All Device Types#NXOS				

هذه جهنل ةعومجم نيوكتل نميال مهسلال قوف رقناو ظفح قوف رقنا 2. ةوطخل

تارايلال كرتأ .فرعم نزخم ك AD مدختست ،ةقداصلل .ةقداصلال ةسايس عاشنإ 3. ةوطخل تلشف اذوا مدختسملال ىلع روثعلال متي مل اذإ ،ةقداصلال تلشف اذإ تحت يضا رتفال ةيلعمل .

Identity Services Engine Work Centers / Device Administration Evaluation Mode 29 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
+	Search				
	+				
●	Default		svs.lab		
			Options		
			If Auth fail		
			REJECT		
			If User not found		
			REJECT		
			If Process fail		
			DROP		

ضيفوالت ةسايس ديحت 4. ةوطخل

Active Directory (AD) في نيمدختسمل اتاعومجم إلى ادانتسا ليوختال جهن عاشناب مق

الاثمل ليلبس إلى

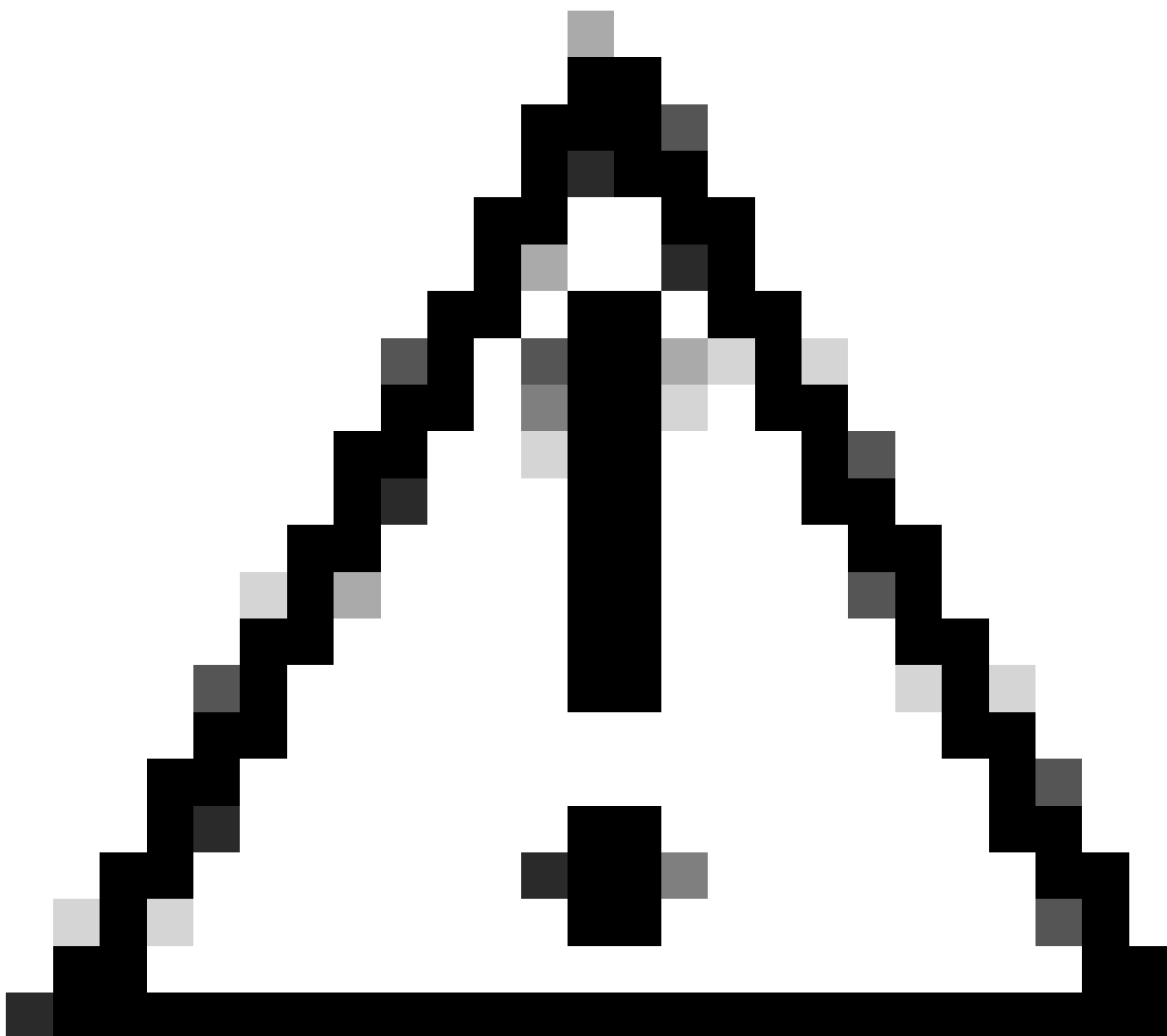
ةعومجم لوؤسم في نيمدختسمل NXOS ةراداب صاخل TACACS فيرت فلم نييغت متي . AD.

ةعومجم زاهج في نيمدختسمل NXOS تاميملت بتكمل TACACS فيرت فلم نييغت متي . AD أو.

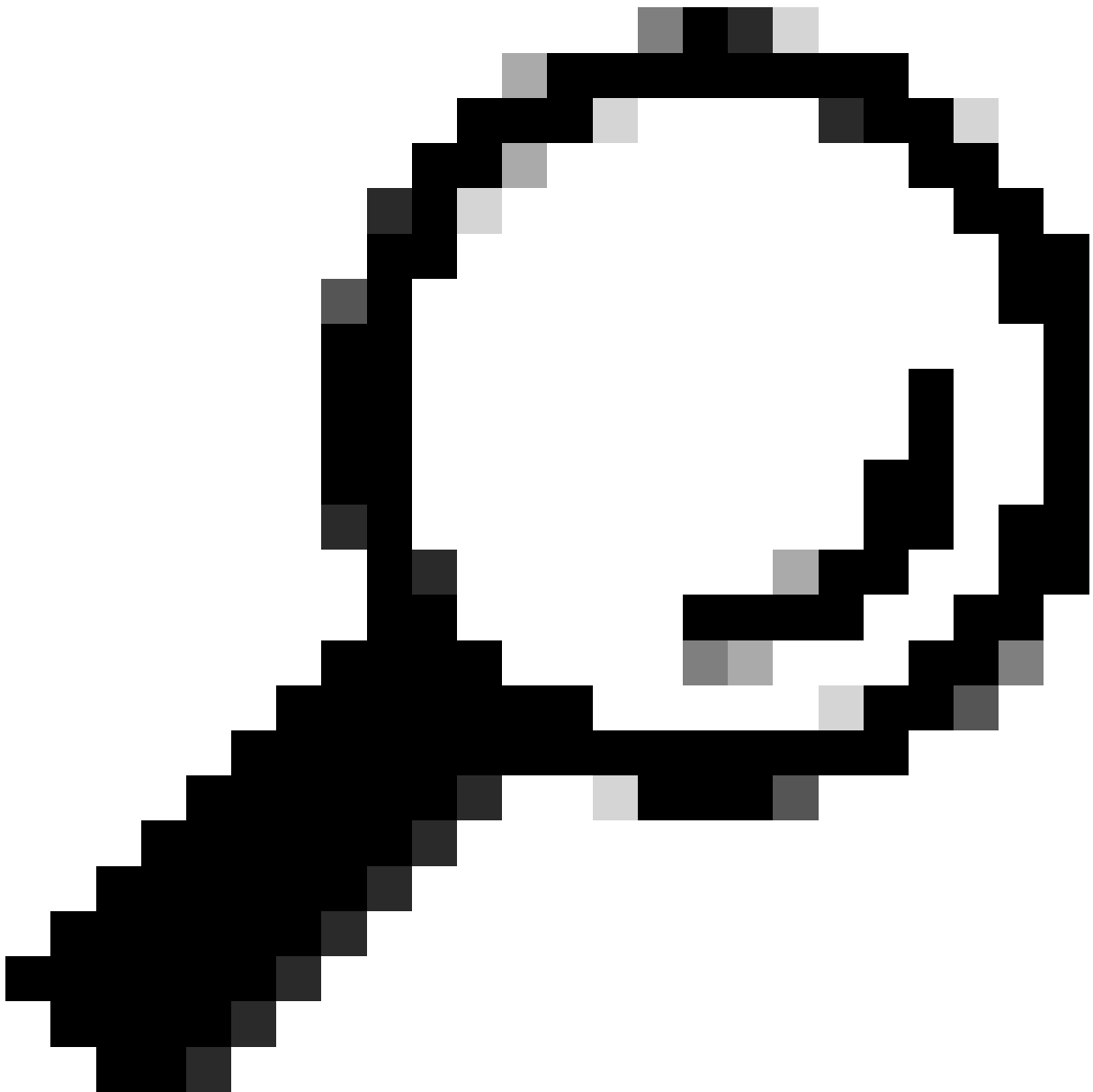
Authorization Policy(3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
+	Search						
●	Authorization Rule RO	svs.lab-ExternalGroups EQUALS	svs.lab/Users/Device RO	Select from list	NXOS HelpDe	0	
●	Authorization Rule RW	svs.lab-ExternalGroups EQUALS Admin	svs.lab/Users/Device	Select from list	NXOS Admin	2	
●	Default		DenyAllCommands	Deny All Shell Profile		0	

TLS ربع Cisco NX-OS ل TACACS+ نيوكت



حيحص لكش ب هلمعو مكحتلا ةدحو لاصتا ىلإ لوصولا ةيناكمإ نم دكأت :ريذحت



ضيوفتالو AAA ةقداصم قرط ريغيغتو تقؤم مدختسم نيوكتب ىصوي :خيملت
،نيوكتلتا ريغيغت ارجا ءانثا TACACS نم ال دب ةيلحملا دامتعالا تانايب مادختسال
زاهجل جراخ هباسح لفق بئجتل

TACACS+ مداخ نيوكت

يلوالا نيوكتلا 1. ةوطخلا

```
POD2IPN2# sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server host 10.225.253.209 key 7 "F1whg.123"  
aaa group server tacacs+ tacacs2
```

```
server 10.225.253.209
use-vrf management
```

TrustPoint نيوكت

ECC. حيتافم جوز مدختسأ، كتلاح يف، حاتفم ةيمست عاشنإب مق 1. ةوطخل

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto key generate ecc label ec521-label exportable modulus 521
```

ةقث ةطقنب اذه طبرأ 2. ةوطخل

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca trustpoint ec521-tp
```

```
POD2IPN2(config-trustpoint)#
```

```
ecckeypair ec521-label
```

CA. ماعل حاتفم لاتيبتت مق 3. ةوطخل

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca authenticate ec521-tp
```

```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwaJELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMjUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUUA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJT+y+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBCnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAAQDAgAHMBkGCWCGSAGG+EIBDQQMFGpTV1MgTGF1IENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj061qJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8tFITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

Fingerprint(s): SHA1

Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

Do you accept this certificate? [yes/no]:yes

POD2IPN2(config)#

POD2IPN2(config)#

show crypto ca certificates ec521-tp

Trustpoint: ec521-tp

CA certificate 0:

subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

serial=20CD7402C4DA37F5

notBefore=Apr 28 17:05:00 2025 GMT

notAfter=Apr 28 17:05:00 2035 GMT

SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

purposes: sslserver sslclient

POD2IPN2(config)#

لوحمل اةيوه ةداهش بلط عاشنإ. 4. ةوطخل

<#root>

POD2IPN2(config)#

crypto ca enroll ec521-tp

Create the certificate request ..

Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.

For security reasons your password will not be saved in the configuration.

Please make a note of it.

Password:C1sco.123

The subject name in the certificate will be the name of the switch.

Include the switch serial number in the subject name? [yes/no]:

yes

The serial number in the certificate will be: FD026490P4T
Include an IP address in the subject name [yes/no]:

yes

```
ip address:10.225.253.177
Include the Alternate Subject Name ? [yes/no]:
```

no

```
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwIUE9EMk1QTjIxFDASBgNVBAU0COZETzI2
NDkwUDRUMIGBMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw70vqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfNwVj7xTBWjDNX
/iyBm6E7Hd7q420Mc8Mef+bqJBdJ9wzpyEjhI2lIIOxT4814nBx0bkIWwYR5cZN
iIXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MCOGCSqGSIB3DQEJJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMk1QTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCvOHAuq1v2cr0n3NenS/441u1
+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt30hpaDD0TWzzvZY7qFf1C015p6pvUpHigqoZNg5
9xhNdM1CQSyk0g==
-----END CERTIFICATE REQUEST-----
```

CA. لبق نم ةعقوم ل ل و ح م ل ا ة ي و ه ة د ا ه ش د ا ر ي ت س ا 5. ة و ط خ ل ا

<#root>

POD2IPN2(config)#

```
crypto ca import ec521-tp certificate
```

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMU1ZTMRIwEAYDVQQDEw1TV1MgTGF1
Q0EwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
T0QySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwZSwEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMfAMM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3D0n
ISOEjaUgihe3jzXiche5UqhZbJH1xk0iJdMuTw/ggxm8+ryNGCqTfH3xEaNAMd4w
HgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAzBgNVHREBAf8EEjaQgggQ
T0QySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msod0QK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZ01PUXNTyZidXpGd/yTrdQA15Jzpw4pEudrbCJMZEYy tqoP
wD+40E8vkoYEGyWlDrpRZ0ZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rou++ISACpH/PJ61Ln1VxhXombiS6
INoa0GvQONr1+1FT8ADIdZ/Ukd5Ubhc9bh/sYzf4MwtKk1wV016Hv7vGpSMYonD6
a271im+tJPyKneezQ60yKz1GqsL/Ta6J0dip/fEYp8UmRq9InDh23gDjgrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTiDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sg006Y6wIXyTP0UB3FwhD+GxtTkmEce
ZnA0bqxpxrqg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXE0wtIe8CwFjSnch
```

```
1fKuuebdZkbwz72r70yyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

ل. ورحملا ةي وه ةداهش لي ج ست نم ق قحت

<#root>

POD2IPN2(config)#

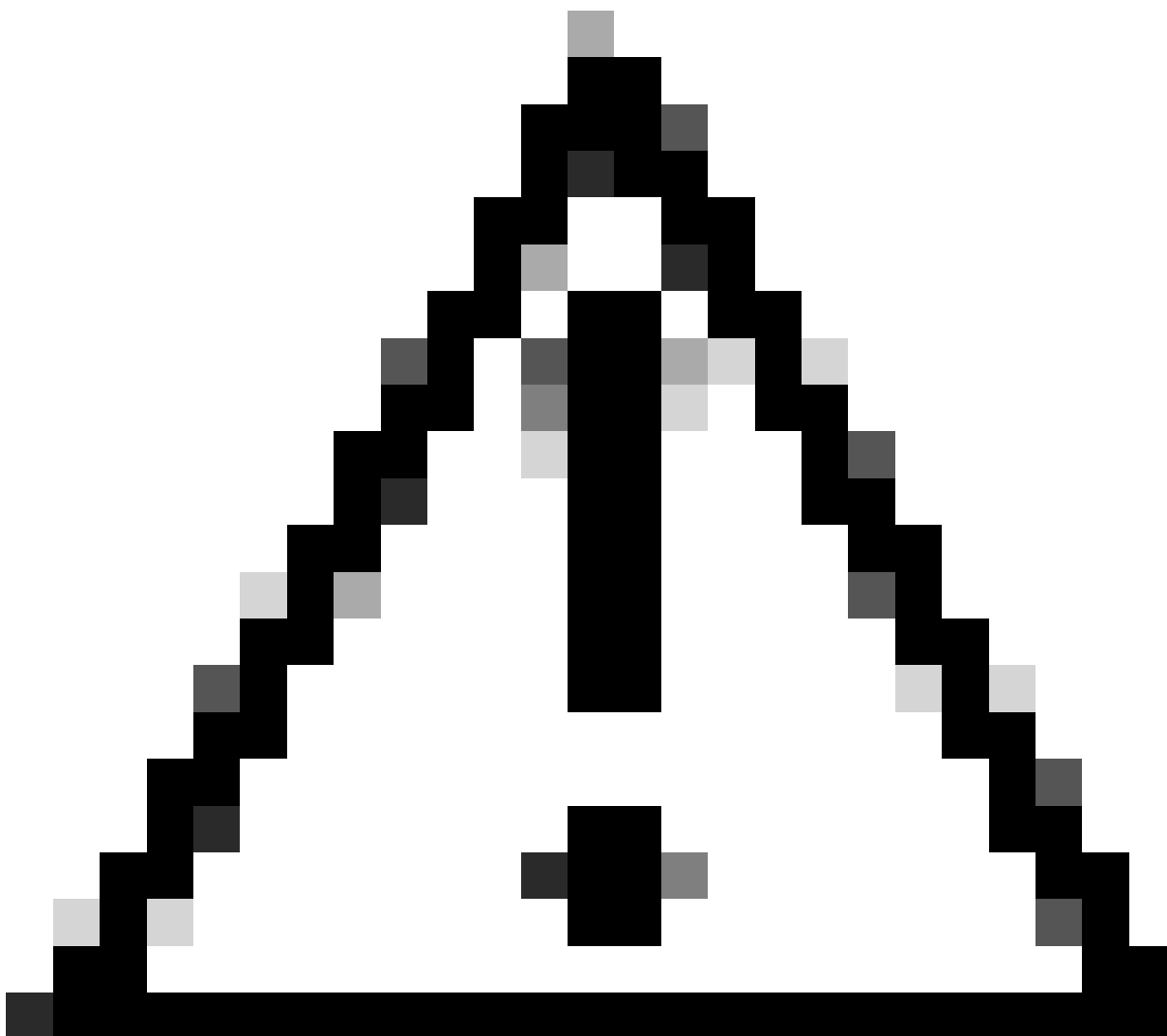
show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FD026490P4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D80E6F
notBefore=May 7 19:10:00 2025 GMT
notAfter=May 7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient
```

```
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
```

POD2IPN2(config)#

TACACS+ TLS ني وكت



تانايب مادختساب مكحتال ةدحو لال خ نم هذه نيوكتالت تاريغيغت ءارجاب مق :ريذحت
ةلحمل دامتعالا

ةماعال (TACACS) لوصولا في مكحتال مئاوق نيوكتب مق 1. ةوطخال

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server secure tls
```

هـب ISE مداخ نيوكت مت يذال TLS ذفنم الى ISE ذفنم ريغيغت مق 2. ةوطخال

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

TLS. لاصتال ةقثال ةطقنب لوحملا لىل ع ISE مداخ نيوكت طبرأ 3. ةوطخل

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

TACACS. مداو ةومجم ءاشنإ 4. ةوطخل

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa group server tacacs+ tacacs2
```

```
POD2IPN2(config-tacacs+)#
```

```
server 10.225.253.209
```

```
POD2IPN2(config-tacacs+)#
```

```
use-vrf management
```

نيوكتل نم ققحت 5. ةوطخل

```
<#root>
```

```
POD2IPN2#
```

```
sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server secure tls
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

```
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

```
aaa group server tacacs+ tacacs2
```

```
server 10.225.253.209
```

```
use-vrf management
```

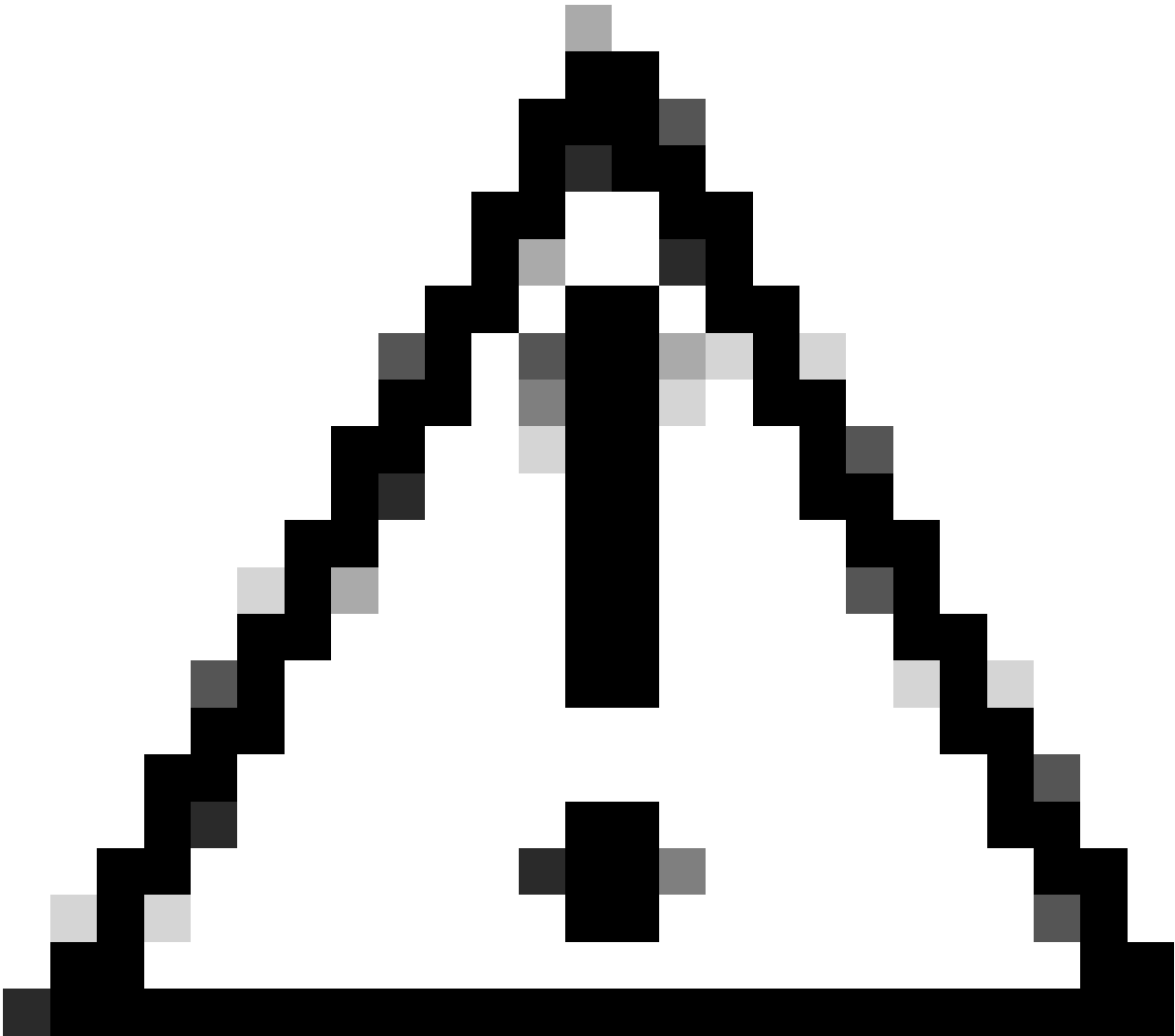
AAA. ةقداصم نيوكتل لبق ديعبل مداختسملا ربتخا 6. ةوطخل

```
<#root>
```

```
POD2IPN2#  
test aaa group tacacs2
```

```
user has been authenticated  
POD2IPN2#
```

AAA نڧوكت



AAA تانڧوكت ةعباتم لبق دعب نع مدختسم لا ةقداصم حاجن نم دكأت :ريذحت

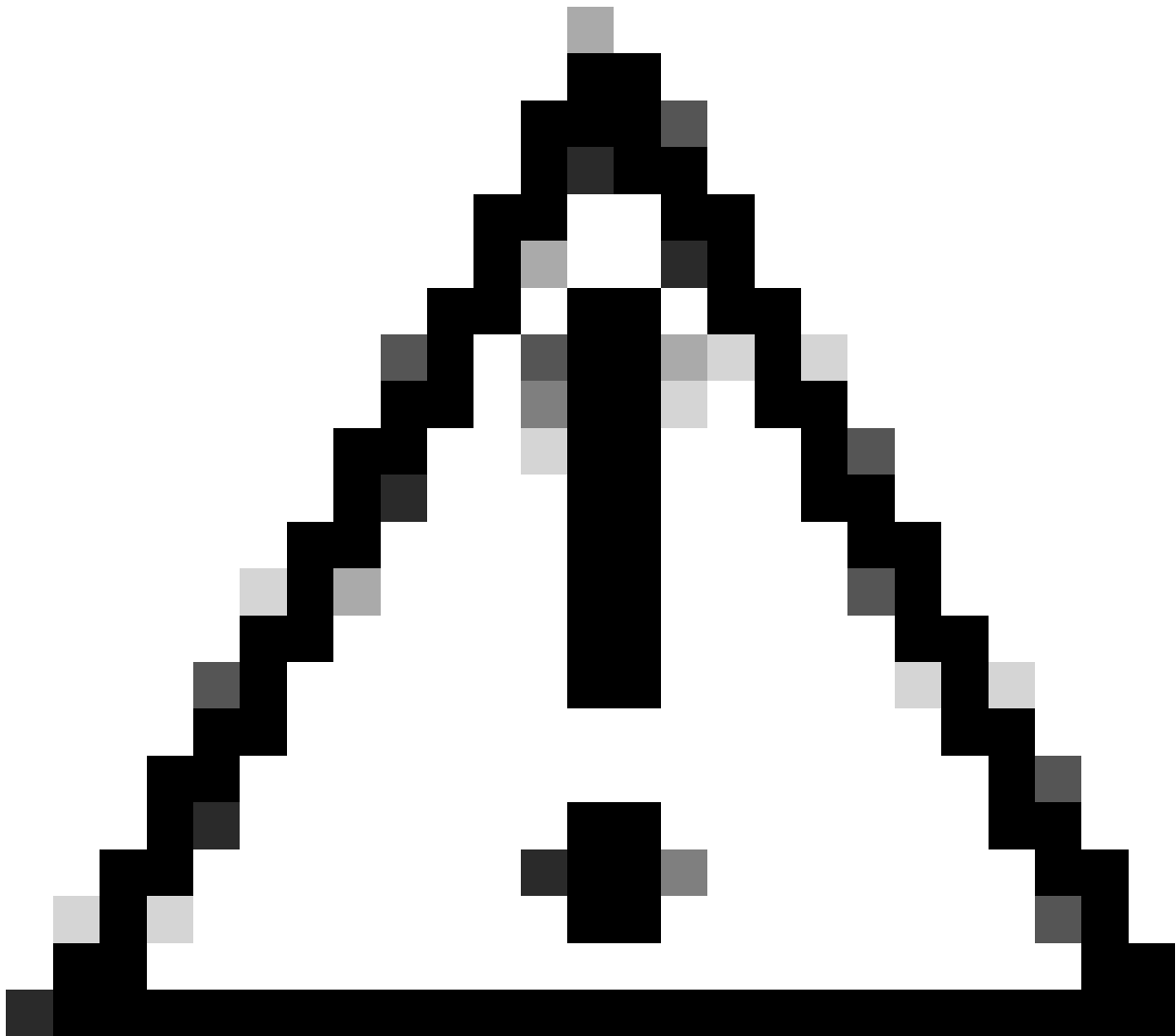
دع ب ن ع AAA ة ق د اص م ني و ك ت 1. ة و ط خ ل ا

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa authentication login default group tacacs2
```

ر م أ ل ا ر ا ب ت خ ا د ع ب AAA ل د ع ب ن ع ض ي و ف ت ل ا ن ي و ك ت ب م ق 2. ة و ط خ ل ا



aaa_author_status_pass_add. ي ه ل ي و خ ت ل ا ة ل ا ح ن ا ن م د ك ا ت : ر ي ذ ح ت

```
<#root>
```

```
POD2IPN2#
```

```
test aaa authorization command-type config-commands default user
```

```
command "feature bgp"
```

```
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"  
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)
```

config-command. ضيفت و AAA رمأ نيوكت 3. ةوطخلإ

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa authorization config-commands default group tacacs2 local
```

```
POD2IPN2(config)#
```

```
aaa authorization commands default group tacacs2 local
```

NX-OS إلى مدخستسمال لوصو ءاطخأ فاشكستساو رابتخإ اهالصلإو

ققحتلإ

نيوكتلإ ءحص نم ققحتلإ إلى جاتحت Cisco NX-OS. ل زاهجلإ ءرادإ نيوكت لمكتلإ

ةفلتخم راودأك NX-OS ءزهجأ إلى لوخدلإ ليجستو SSH لوكوتورب 1. ةوطخلإ

نېمي رمألا إلى ذفنم ىقلتي لمعتسمال نأ تققد (CLI) نراق طخةادألا ىلع نإ ام 2. ةوطخ
لاصلتا رابتخإ ىلع ارداق ءدعاسمال بتكم يمدختسم دحأ نوكتي نأ بجي، لاثلما لىبس ىلع
يراجلل نيوكتلإ راهظال هضفرمت نكلو (10.225.253.129، لاثلما لىبس ىلع) يداع IP ناونع
هليغشت.

```
POD2IPN1# ping 10.225.253.129 vrf management  
PING 10.225.253.129 (10.225.253.129): 56 data bytes  
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms  
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms  
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms  
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms  
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms
```

```
--- 10.225.253.129 ping statistics ---  
5 packets transmitted, 5 packets received, 0.00% packet loss
```

```
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

اهحال صإو ءاطخألا فاشكتسا

NX-OS. نيوكت ةحص نم ققحتلا

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

رمأوالا هذه مدختسأ، (راودألا) رودلاو مدختسملا تالاصتإ راهظإل

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

اهحال صإو TACACS+ ءاطخأ فاشكتسأ يف ةديفم ءاطخأ يه هذه

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]: process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]: process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]: process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]: process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]: state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]: is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]: is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]: debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]: 35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]: 36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]: 36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]: debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]: tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]: num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]: non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]: non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]: non_blocking_connect(388): setsockopt success error:22
```

```
2016 Jan 11 03:03:08.656694 TACACS[6288]: non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]: tplus_decode_authen_response: copying hostname into context
```

SSL. ءاطخأ حيحصت نيكم تب مق

```
touch '/bootflash/.enable_ssl_debugs'
```

ءاطخأل حيحصت فلم تايوتحم راهظا.

```
cat /tmp/ssl_wrapper.log.*
```

TACACS > تاي لمعل الى ل لقتنا ، ISE لي غشتالماظنل (GUI) ةيموسرلما دختسمل ا هجاو نم لي صافاتال رز رفويو ،انه ضيوفتالو TACACS ةقداصم تابلط عي مج طاقاتال متي . Livelog . ةنعم ةلماعم لشف/ري رمت ببس لوح ةيلي صفت تامولعم

زهجأل ا قراا > ريراقتال > زهجال ا قراا > لمعلال زكارم الى ل لقتنا :ةيخي راتال ريراقتال ي ف ةبسا حمل او ضيوفتالو ةقداصم ل ريراقت الى ل لوصحلل

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Export Summary

My Reports

Reports

Device Administration Reports

Authentication Summary

TACACS Accounting

TACACS Authentication

TACACS Authorization

TACACS Command Accounting

Top N Authentication by Failure Reason

Top N Authentication by Network Device

Top N Authentication by User

Scheduled Reports

TACACS Authentication

From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0

Reports exported in last 7 days 0

Add to My Reports

Export To

Schedule

Filter

Refresh

Logged Time	Status	Details	Identity	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure
Today			Identity	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure
2025-05-15 19:39:57.061			Admin-ro	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:39:54.443			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:39:43.001			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:35:39.809			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 18:49:11.209			pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 18:49:10.303			Admin-ro	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	

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