

يطلع اهحال صاؤو نم آلا Syslog ءاطخا فاشكتسا Nexus يساسا آلا مازنلا

تايوت حمللا

[عمدقمللا](#)

[قيساسا آلا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[ططخمللا](#)

[قيساسا تامولعم](#)

[يديلقنلا Syslog](#)

[نم آلا Syslog](#)

[تاداهشلا قلسلس](#)

[تاداهش رفوت مزلي اذامل](#)

[قنم آلا Syslog TLS ءحفاصم](#)

[قلسلا يذنيوكتلا](#)

[Cisco Nexus نيوكت](#)

[Ubuntu Syslog مداخ نيوكت](#)

[اهحال صاؤو ءاطخا آلا فاشكتسا](#)

[فدوللا](#)

[ططخمللا حرش](#)

[نم آلا syslog نيوكت نم ققحتلا 1. ءوطخللا](#)

[TrustPoint نيوكت نم ققحتلا 2. ءوطخللا](#)

[IP لاصتا نم ققحتلا 3. ءوطخللا](#)

[TLS لاصتا نم ققحتلا 4. ءوطخللا](#)

[رم آلا اذه ققحتي اذام](#)

[عقوتمللا ججانلا جتانلا](#)

[عمزحلا طاقتلا طابترا](#)

[نم آلا syslog لئاسر لقن نم ققحتلا](#)

[syslog رابتخلا قلسر عاشتا](#)

[قرفشملا TLS قيبطت تانايب نم ققحتلا](#)

[syslog مداخ يطلع لئاسر رلا لابلقتسا نم ققحتلا](#)

[بارقللا](#)

عمدقمللا

لقنلا ءقبط ناما ربع نم آلا Syslog لوكونورب ءاطخا فاشكتسا ءيفيك دنتسملا اذه فصلي
ثلاثلا فرطلا مداوخو Cisco Nexus تالوحم نيب اهحال صاؤو (TLS)

ةيساسأل تاب ل ط ت م ل ا

تاب ل ط ت م ل ا

ةيلالال عيضاوملاب ةفرعم لكي دل نوكت نأب Cisco ي صوت

NX-OS تاصنم

Syslog نمأل

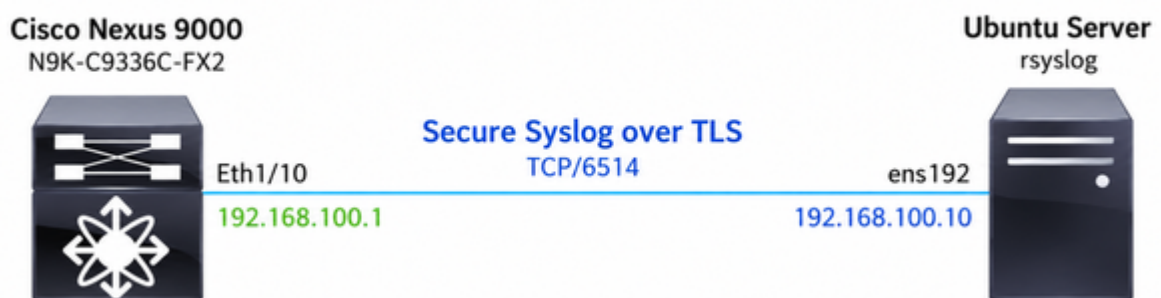
(PKI) ماعلال حاتفم لل ةيساسأل ةينب ل اب ةيساسأل ةفرعم

ةمدختسم ل تانوكم ل ا

10.4(7)	N9K-C9336C-FX2	N9K1
rsyslog 8.2112 OpenSSL 3.x	مداخ Ubuntu	مداخ Syslog

ةصاخ ةيلمعم ةئي ب ي ف ةدوجوم ل ةزهأل نم دن تسم ل ا اذ ي ف ةدراول تامولعمل اءاشنإ م ت
تناك اذإ. (يضا رتفا) حوسمم نيوكتب دن تسم ل ا اذ ي ف ةمدختسم ل ا ةزهأل ا عي م ج ت ادب
رمأ يأل لم تحتحم ل ا ري ثأ تلل كم هف نم دكأت ف، لي غشت ل ا دي ق ك تكبش

ط ط خ م ل ا



ةيساسأل تامولعم

ي دي ل ل ق ت ل ا Syslog

نودب TCP وأ (514 يضا رتفا ل ا ذفنم ل ا) UDP ربع ل ج س ل ل لئاسر ي دي ل ل ق ت ل ا syslog ل سري

لجسلا لئاسر ضارتعا لم تحملا نمف ،حضاو صنب لاصتالا لاسرا متي هنأل ارظنو .ري فشت
مداخلا ةقداصم اضيأ ةيديلقلا Syslog رفوت ال .لقنلا ءانثأ اهليدعت وأ

نمآل Syslog

ري فوتل (6514 ي ضارتفالال ذفنملا) TLS عم TCP لوكوتورب نمآل Syslog لوكوتورب مدختسي
ءاشنإب مداخلاو ليمعلا موقى ،لجسلا لاسر يأ لاسرا لبق .syslog لئاسرل رفشملا لاسرالا
تاداهشلا ةلسلس ةحص نم ققحتلاب ليمعلا موقى و هتداهش مداخلا اهلالخ مدقي TLS ةسلج
لئاسر لاسرا متي ،حاجنب TLS ةحفاصم لامتكأ درجمب .(CA) هب قوثوم قدصم عجرم لباقم
ةرفشملا ءانقلا لالخ نم syslog

ىلع اضيأ نكلو طقف IP لاصتال ىلع نمآل Syslog دمتعي ال ،يديلقلا syslog فالخب
يأ لدابت لبق ريفشتلا تاضوافمو ،ةداهشلا ةحص نم ققحتلا ،ةحجانلا TLS ةحفاصم
syslog ةلاسرا

تاداهشلا ةلسلس

مداخلا ةداهش نيب ةقثلا سيسيأتل ةمدختسملا تاداهشلا ةلسلس يه تاداهشلا ةلسلس
syslog مداخ مدقي ،TLS ةحفاصم ءانثأ .(رذجال قدصملا عجرملا) هب قوثوملا يرذجال عجرملاو
لوحمد مدختسي .ةبولطم ةطيسولا CA تاداهش يأ ىلإ ةفاضلاب هب ةصاخلا مداخلا ةداهش
تاداهشلا ةلسلس ةحص نم ققحتلل هب قوثوملا سيسيأتل قدصملا عجرملا Cisco Nexus
لمالكلا

امئاد ةبولطم تاداهشلا ةلسلس نوكت ال
لئبس ىلع .هب صاخلا PKI ذيفنت ةيفيك ىلع syslog مداخ نم ةمدقملا تاداهشلا دمتعت
لاثلما

لوحمد قثي نأ بجي ،ةلاحلا هذه يف .طقف صاخلا هصيخرت مداخلا مدقي :ايتاذ ةعقوم ةداهش
ةرشابم ايتاذ ةعقوملا ةداهشلا كلت يف Cisco Nexus
اهعيقوت مت هنأل طقف مداخلا ةداهش مداخلا مدقي :ةطيسو CAs نودب CA نم ةعقوم ةداهش
هب قوثوم يزكرم قدصم عجرم نم ةرشابم
CA ةداهش عم هب ةصاخلا مداخلا ةداهش مداخلا مدقي :ةطيسولا CAs عم CA نم ةعقوم ةداهش
عجرملا ىتح ةلماك ةقث ةلسلس ءاشنإب Cisco Nexus لوحمل حمسي امم ،رثكأ وأ ةدحاو ةطيسو
هب قوثوملا يرذجال (CA) قدصملا

ةداهشلا نم ققحتلا ىلع ارداق Cisco Nexus لوحمد نوكتي نأ بجي ،PKI ميمصت نع رظنلا ضغب
TLS ةسلج ءاشنإ لبق مداخلا نم ةمدقملا

ءاهتنا وأ اهتيجالاص مدع وأ نامضلا ةلسلس يف ةبولطم ةداهش يأ نادقف ةلاح يف
ءاشنإ نكمي الو TLS ديكأت لشفي ،هب قوثوم ريغ قدصم عجرم نم اهرادصا وأ اهتيجالاص

نم آل syslog لاصتا

تاداهش رفوت مزلي اذامل

ةلاسري لاسر لبق .مداخل ةقداصم وري فشتال ريفوتل TLS ىلع نم آل Syslog دمتعي زاهج سيلو دوصقم ال syslog مداخل لصتي هأ نم Cisco Nexus لوحم ققحتي نأ بجي ، syslog ، هب حرصم ريغ

لبق syslog مداخل ةيوه ةقداصم ب Nexus لوحمل حامسلا قيرط نع ةقثلا هذه تاداهشال رفوت عاشنإ متي ، حاجنب تاداهشال ةلسلس ةحص نم ققحتال درجم . ةرفشمال ةسلجل عاشنإ . ةرفشمال لاصتال لالخ نم ةيلاتال syslog لئاسر عيجم لاسر متي و نم آ TLS ةانق

، TLS ةسلج عاشنإ نم آل Syslog ل نكمي ال ، اهب قوثوم تاداهش ةلسلسو ةحلص ةداهش نودب . نم آ لكشب لجسل لئاسر لدابت عنمي امم

نم آل Syslog TLS ةحفاصم

TLS ةسلج عاشنإ syslog مداخلو Cisco Nexus لوحم ىلع بجي ، syslog ةلاسري لاسر لبق ريفشت حاتفم ئشنوي ، TLS تاملعم ني زاهجال لك ضوافي ، TLS ةحفاصم ءانثأ . حاجنب ةداهشال ةحص نم ققحتال لالخ نم syslog مداخل ةيوه ىلع قداصمو ، كرتشم

حاجنب TLS ةحفاصم لامتكأ دعب ال رفشمال لاصتال ربع syslog لئاسر لاسر متي ال

ةيلاتال لحارم ال نم TLS ةحفاصم نوكتت

ةوطخ	فصولا
1. TCP لاصتا	نم آل syslog مداخل TCP لاصتا عاشنإ Cisco Nexus switch لوحمل موقي (6514 يضا رتفال ذفنم ال)
2. Client Hello	ةم و ع دم ال TLS تارادصل لاسر قيرط نع TLS ةحفاصم ةئيهت ب Nexus موقي . ةيئوشع ال ميقل او ريفشتال تاعومجم و
3. Server Hello	ةسلجل ةمدختسم ال ريفشتال ةعومجم و TLS رادصل syslog مداخل ددحي
4. لدابت تاداهشال	CA تاداهش ي ، رمأل بلطت اذاو ، هب ةصاخال مداخل ةداهش syslog مداخل مدقي . ةطيسو

فصولا	ةوطخ
م ت ي ذل هب قووثومال قدصملا عجرملا لباقم مداخلا ةداهش نم Nexus ققحتي تاداهشلا ةلسلس نم ققحتلا ققحتلا ققحتلا ةيلمع نمضتت .هنيوكت عئاشلا مسالا لال خ نم مداخلا ةيوهو ردصملاو ةيحالصلا ءاهتنا خيراوتو (SAN) ليدبلا عوضوملا مساو (CN).	نم ققحتلا 5. ةداهشلا ةحص
ةسلجلا حيتافم قاقتشا لجأ نم ريفشتلا تامولعم نيرظنلا لك لدابت ي ريفشتلا ةمدختسملا ةكرتشملا	لدابت - 6 حيتافملا
نيناچلا لك قاقتشا نمو حانچب ةحفاصملا مامتإ نم ريظن لك ققحتي ريفشتلا حيتافم سفن	لئاسرلا 7. ةيهتنملا
تانايب تالچسك syslog لئاسر لاسرا متي ، TLS ةسلج ءاشنا درجمب ةرفشملا TLS قيبطت	نمآلا لاسرالا 8. Syslog ل

ةلصللا يذنيوكتلا

Cisco Nexus نيوكت

يلع يوتحت يثلا ةقثلا ةطقنو ،ةنمآلا syslog ةهجو مادختساب Cisco Nexus لوحم نيوكت بچي ةبسانملا ردصملا ةهجاوو ،هب قووثوملا CA

```
switch(config)# crypto ca trustpoint SYSLOG-TLS-LAB-CA
switch(config-trustpoint)# crypto ca authenticate SYSLOG-TLS-LAB-CA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
<paste>
-----END CERTIFICATE-----

END OF INPUT

Do you accept this certificate? [yes/no]:y
logging server syslog.lab.local 6 secure port 6514 use-vrf default
logging source-interface Eth1/10
```

Ubuntu Syslog مداخ نيوكت

TLS. معد نيكمت عم rsyslog لغشي Ubuntu مداخ وه دنتسملا اذه ي ف مدختسملا syslog مداخ

فئاطول هذه مداخل نيوكت نمضتي

TCP 6514 ذفنم ىلع ةنمآل Syslog تالاصتإ ىلإ عمستا
TLS ءحفاصم ءانثأ TLS مءاخ ءءاهش ميءقت
مءاخ ءءاهش ب طبترم صاخ ءاتفم مءختسأ
ءحفاصم ءانثأ Cisco Nexus ىلإ (ءهقبطت ءنع) ءبولطم ءاءاهش ءلسلس ريءوتب مق
TLS.
ىلحم لءس فلم يف ةنمآل Syslog لئاسر ننءم ىقلت

ءءرم ءا > طيسول ءا > مءاخ ءءاهش : نم ءنءسم ءه يف مءختسم ءا PKI قىبطت نوكتي
رءءال قءصم ءا

ءيئي امم ، TrustPoint ءالء نم ءب قوئول او رءءال ءا ءءاهش ءاريءساب Cisco Nexus لءوم موقى
syslog مءاخ نم ءمءقم ءاءاهش ءلسلس نم ققءءال ءل



نإف ، PKI ءيفنء بسء . رشن ءيلىم ءل ءل ءيمازل ءسئل ءاءاهش ءلسلس : ءءال م
نم ءرءابم ءعقوم مءاخ ءءاهش ، اءاء ءعقوم ءءاهش ميءقت طقف عىطءسي syslog مءاخ
رءءأ وأ ءطيسو ءا ءءاهش ب ءبءصم مءاخ ءءاهش وأ ، رءءال ءا

ءءال صا ءاطءال ءاشءءسا

فءءال

ءالءوم ءنءم ءيئال ءشءال ءالء لزع وه ءه ءءال صا ءاطءال ءاشءءسا ءارء نم فءءال
syslog مءاخ عم ءا ءب نمآل Syslog TLS ءاصءا ءاشن نم Cisco Nexus NX-OS

ربع مءقءال او IP ءاصءا نم ءءب ، ءاصءال ءيلىم نم ءلءرم لك ءءص نم لمءال ريس ققءءي
syslog لئاسر لئاسر نمآل اريءأ ، ءءاهش ءءص نم ققءءال او ، TLS ءاضواءم و ، TCP ءاصءا
ءاصءال ءشء ناءم ءيءء نءمم نم ، لءءسم لكشب ءقبط لك نم ققءءال ءالء نم
ءعرسب

طءءم ءرء

لىمءك هنيوكء مء Cisco Nexus switch لءوم نم ءنءسم ءه يف مءختسم طءءم نوكتي
نمآل Syslog مءاك هنيوكء مء ءل rsyslog لءشي ءل Ubuntu مءاخ نمآل Syslog

لاصتا عاشنإ دع ب 6514 ذفنملا ىلع Syslog مداخل TCP لاصتا ادبب Cisco Nexus لوحم موقى
ةداهش syslog مداخل مدق، ةي لمعلا هذه اناثأ. TLS ةحفاصم عارجاب نيزاهجلا لك موقى، TCP
ةلسلس ةحص نم Nexus لوحم ققحتي. ةبولطم ةطيسو CA تاداهش يأو هب ةصاخلا مداخل
صاخلا TrustPoint ي هنيوكت مت يذلا هب قووثوملا رذجلا قدصملا عجرملا لباقم تاداهشلا
هب.

في Nexus لوحم ادبي و ةرفشملا ةسلجلا عاشنإ متي، حاجنب TLS لاصتا ديكأت لامتكأ درجمب
syslog مداخل ىلإ ةنملا syslog لئاسر لاسرا

لسلست سفن دننسملا اذه في ةمدقملا احوال صا و عا طخال فاشكتسا ةيجهنم مدختست
لكشب ةي لمعلا نم ةلحرم لك نم ققحتلا حيتي امم، لاصتالا ةسسؤمب صاخلا لاصتالا
لقتسم

نملا syslog نيوكت نم ققحتلا 1. ةوطخلا

ىلع فرعتي لوحملا نأو Cisco Nexus لوحم ىلع حيحص لكشب نملا Syslog نيوكت نم ققحت
هنيوكت مت يذلا Syslog مداخل

```
switch# show logging server
Logging server: enabled.          >>>>>>> Secure Syslog is enabled.
{syslog.lab.local}              >>>>>>> The correct destination (IP address or Fully Qualified Domain
server status: No errors found   >>>>>>> No configuration errors are reported.
server severity: notifications
server facility: local7
server VRF: default
server port: 6514                >>>>>>> The destination port is 6514.
server transport: secure         >>>>>>> The transport is secure.
switch#
```

TrustPoint نيوكت نم ققحتلا 2. ةوطخلا

syslog مداخل ةداهش عي قوتل مدختسملا CA في قثي Cisco Nexus لوحم نأ نم ققحت

ةحصلا نم ققحتلا

ةدوجوم ةعقوتملا ةقثلا ةطقن
رذجلا قدصملا عجرملا ةداهش تيبت مت
ةبولطم ةطيسو CA تاداهش يأ دجوت
تاداهشلا ةيحوال ص هتنت مل

ةقوت مالم قلال اءاءهشلا اام صب قباطا

```
switch# show crypto ca certificates
Trustpoint: SYSLOG-TLS-LAB-CA
CA certificate 0:
subject=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root
issuer=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root
serial=4959A9F5A8D174553E0FB4FA01A21DDC2C085F12
notBefore=Jun 30 20:47:09 2026 GMT
notAfter=Jun 29 20:47:09 2031 GMT
SHA1 Fingerprint=24:8A:3A:C0:7C:61:53:3B:BE:A7:BB:51:12:FD:7E:B3:D7:AB:44:4C
purposes: sslserver sslclient
```

```
CA certificate 1:
subject=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root
issuer=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root
serial=3BC9CD3374C4A29A6794AAAEBA270E3116C3D55
notBefore=Jun 30 20:43:04 2026 GMT
notAfter=Jun 27 20:43:04 2036 GMT
SHA1 Fingerprint=C8:AC:81:89:AA:A5:89:13:CA:01:5C:A9:90:15:3E:78:22:DD:34:A5
purposes: sslserver sslclient
```

switch#

ةحص نم ققحتلا لشفي ،ةحلاص ريغ وأ ةدوقم ةبسانملا قءصملا ةءاهش تناك اذا
ةحفاصم ءانثأ ةءاهشلا

IP لاصتا نم ققحتلا 3. ةوطخلا

نم آل syslog مءاخو Cisco Nexus لوم ني ب 3 ةقبطلا لاصتا نم ققحت

ةحصولا نم ققحتلا

- ءاانب (ICMP) تنرتنإلا في مكحتلا لئاسر لوكوتورب إلا لوصولا ةيناكما
- (DNS) لءملا مسا ماظن لئلحت ءيحصت
- ءيوتلا في لكاشم ءوتلا
- مزلل ءق ءويلا

```
switch# ping syslog.lab.local
PING syslog.lab.local (192.168.100.10): 56 data bytes
64 bytes from 192.168.100.10: icmp_seq=0 ttl=63 time=0.672 ms
64 bytes from 192.168.100.10: icmp_seq=1 ttl=63 time=0.331 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=63 time=0.295 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=63 time=0.286 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=63 time=0.285 ms
```

```
--- syslog.lab.local ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.285/0.373/0.672 ms
switch#
```

TCP الاتصال عاشن انكمي الف ، IP الاتصال لش ف اذا

TLS الاتصال نم ققحت ال 4. ةوطخ ال

نم آل syslog م داخو Cisco Nexus لوح نمي لم اش ال TLS الاتصال نم ققحت

كل ذي ف ام ب ، نم آل syslog الاتصال ةددعت الم لحارم ال ةحص نم ققحت ال اب ةوطخ ال هذه موقت

- TCP الاتصال
- TLS ضوافت
- م داخ ال ةداهش ل يم يدقت ال ضرع ال
- تاداهش ال ةلس لس
- ةداهش ال ةحص نم ققحت ال
- ريفش ال ةعوم جم ضوافت

دخاو رم ا م ادخت ساب اه عي مج نم ققحت ال انكمي ، TLS ةحفاصم نم عزجك ثدحت تاي لم عل هذه نأل

```
switch# run bash sudo ip netns exec default openssl s_client -connect 192.168.100.10:6514 -CAfile /boot
```

رمأل اذه ققحتي اذام

فصولا	نم ققحت ال ةحصل
syslog. م داخ ب TCP الاتصال Nexus عاشن انكمي نم ققحت لل	TCP الاتصال
TLS. ةسلج يل ع حاجن ب ناضوافت ي نارقأل الك نأ دكؤي	TLS ةحفاصم
syslog. م داخ لبق نم ةمدقم الم ةداهش ال ضرعي	م داخ ال ةداهش
م داخ ال ةطس اوب ةلس رم ةطي سو CA تاداهش ي ضرعي	ةلس لس تاداهش ال

فصولا	نم ققحتلا ةحصللا
هيلع ضوافتلا مت يذلا TLS رادصا راهظا	TLS رادصا
اهيلع ضوافتلا مت يذلا ريفشتلا ةيمزراوخ ضرعي	ةرفش
CA لباقم تاداهشلا ةلسلس نم ققحتي ،CAfile- راڤخ مادختسا دنع هب قووثوملا ددحملا	ةحص نم ققحتلا ةداهشلا

عقوتملا حجانلا جتانلا

```
switch# run bash sudo ip netns exec default openssl s_client -connect 192.168.100.10:6514 -CAfile /boot
CONNECTED(00000003) >>>>> this confirms that the TCP connection has been established.
Can't use SSL_get_servername
depth=2 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root CA, email=cisco@cs.cisco.com
verify return:1
depth=1 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA, email=cisco@cs.cisco.com
verify return:1
depth=0 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = syslog.lab.local, email=cisco@cs.cisco.com
verify return:1
---
Certificate chain >>>>>>>>>
0 s:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = syslog.lab.local, email=cisco@cs.cisco.com
i:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA, email=cisco@cs.cisco.com
1 s:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA, email=cisco@cs.cisco.com
i:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root CA, email=cisco@cs.cisco.com
---
Server certificate
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
subject=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = syslog.lab.local, email=cisco@cs.cisco.com
issuer=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA, email=cisco@cs.cisco.com
---
Acceptable client certificate CA names
C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root CA, email=cisco@cs.cisco.com
Client Certificate Types: RSA sign, ECDSA sign
Requested Signature Algorithms: RSA+SHA256:RSA-PSS+SHA256:RSA-PSS+SHA256:ECDSA+SHA256:Ed25519:RSA+SHA384:ECDSA+SHA384:Ed25519
Shared Requested Signature Algorithms: RSA+SHA256:RSA-PSS+SHA256:RSA-PSS+SHA256:ECDSA+SHA256:Ed25519:RSA+SHA384:ECDSA+SHA384:Ed25519
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 4177 bytes and written 392 bytes
Verification: OK >>>>>>>>
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 4096 bit
Secure Renegotiation IS supported
```



```

<----- (Intermediate CA)
<----- Server Key Exchange
<----- Server Hello Done
Client Key Exchange ----->
Change Cipher Spec ----->
Finished ----->
<----- Change Cipher Spec
<----- Finished
==== Secure TLS Session Established ====
Encrypted Syslog Messages ----->

```

نلف، لاصتال ديكتات لشف اذا syslog. ةلسرر ي لدابت لبق حاجن TLS ةحفاصم لامكإ بجي ادبأ ةنمآل syslog رورم ةكرح عاشنإ متي

أدبأ، لولوال ةسلجل ي Cisco Nexus لوحمل ىلإ CLI يتسلج حتفا، ققحتل اذه عارجل
رمأل اذه TLS لاصتا

```
switch# run bash sudo ip netns exec default openssl s_client -connect 192.168.100.10:6514 -CAfile /boot
```

TLS ل تبقرار in order to طاقتل رزيلاناث تادب، ةسلج CLI ي ناثل ي ف، تقولا سفن ي ف
لدابت:

```

switch# ethanalyzer local interface inband display-filter "tcp.port==6514" limit-captured-frames 0
Capturing on 'ps-inb'
3 2026-07-01 00:55:00.194836329 192.168.100.1 → 192.168.100.10 TCP 74 18553 → 6514 [SYN] Seq=0 Win=42340 Len=
4 2026-07-01 00:55:00.195053907 192.168.100.10 → 192.168.100.1 TCP 74 6514 → 18553 [SYN, ACK] Seq=0 Ack=1 Win=
2103467794 WS=128
5 2026-07-01 00:55:00.195110969 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=1 Ack=1 Win=4300
6 2026-07-01 00:55:00.195361105 192.168.100.1 → 192.168.100.10 TLSv1 353 Client Hello
7 2026-07-01 00:55:00.195478134 192.168.100.10 → 192.168.100.1 TCP 66 6514 → 18553 [ACK] Seq=1 Ack=288 Win=64
8 2026-07-01 00:55:00.204176209 192.168.100.10 → 192.168.100.1 TLSv1.2 1514 Server Hello
9 2026-07-01 00:55:00.204200237 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=288 Ack=1449 Win=
10 2026-07-01 00:55:00.204207757 192.168.100.10 → 192.168.100.1 TCP 1514 6514 → 18553 [ACK] Seq=1449 Ack=288
P segment of a reassembled PDU]
11 2026-07-01 00:55:00.204219906 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=288 Ack=2897 Win=
12 2026-07-01 00:55:00.204225215 192.168.100.10 → 192.168.100.1 TLSv1.2 1296 Certificate, Server Key Exchange
13 2026-07-01 00:55:00.204234417 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=288 Ack=4127 Win=
14 2026-07-01 00:55:00.206544194 192.168.100.1 → 192.168.100.10 TLSv1.2 171 Certificate, Client Key Exchange,
15 2026-07-01 00:55:00.206818190 192.168.100.10 → 192.168.100.1 TLSv1.2 117 Change Cipher Spec, Encrypted Har
14 16 2026-07-01 00:55:00.249090950 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=393 Ack=417
17 60 2026-07-01 00:56:10.555097655 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=394 Ack=417
61 2026-07-01 00:56:10.887874467 192.168.100.1 → 192.168.100.10 TLSv1.2 226 Application Data
19 62 2026-07-01 00:56:10.888066832 192.168.100.10 → 192.168.100.1 TCP 66 6514 → 60177 [ACK] Seq=1 Ack=161 W
19 65 2026-07-01 00:56:13.891148284 192.168.100.1 → 192.168.100.10 TLSv1.2 189 Application Data
21 66 2026-07-01 00:56:13.891341818 192.168.100.10 → 192.168.100.1 TCP 66 6514 → 60177 [ACK] Seq=1 Ack=284 W

```

TCP ةحفاصم كلذ ي ف امب، لمكلا TLS ةحفاصم لسلسلست ةمزحل طاقتل ضرعي نأ بجي

لئاسرل او، Key Exchange، Certificate، و Server Hello، و Client Hello، و، هاجت إلهة ثالث لمحت ية لة ةرفشم ال TLS قيب طت تانايب تال جس، حاجنب ةحفاصم ال مت اذ، و، ةيئاهن ال ةنم آل syslog لئاسر

نم آل syslog لئاسر لقن نم ققحت ال

دعب syslog م داخ إله Cisco Nexus switch لوحم ال نم حاجنب ةنم آل syslog لئاسر لقن نم ققحت TLS ةسلج عاشن إ

عاشن نم مضى ال هن إف، كلذ عمو؛ ةرفشم ال ةانقل عاشن إ مت هنأ ةحجان ال TLS ةحفاصم دكؤت اهم لست و syslog لئاسر

ديكأت و رابتخ إ ةل اسر عاشن إ قيرط نع لم اك ال نم آل syslog لمع ريس نم ةوطخل هذه ققحت اهال بقت ساو اهال اسرا

syslog رابتخ إ ةل اسر عاشن إ

```
switch# logit test1-FromN9K
2026 Jul 1 01:04:04 switch %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: systest from 0: test1-FromN9K - vsh.bin[15]

switch# logit test2-FromN9K
2026 Jul 1 01:12:44 switch %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: systest from 0: test2-FromN9K - vsh.bin[15]
```

مت يذل نم آل syslog م داخ إله اهال اسرا بجي ةي لحم syslog ةل اسر عاشن إ رمأل اذه موقى ةدووم ال TLS لمع ةسلج ربع هنيوكت

ةرفشم ال TLS قيب طت تانايب نم ققحت ال

، (قباسل مسقل ي ف حضوم وه امك) لعفلاب ليغشت ال دي ق Ethanalyzer طاقن ال كانه ناك اذ، رابتخ ال ةل اسر عاشن إ دعب ةدي دجل ال TLS قيب طت تانايب مزح لاسرا نم ققحت ف

```
switch# ethanalyzer local interface inband display-filter "tcp.port==6514" limit-captured-frames 0
25 483 2026-07-01 01:05:33.547471509 192.168.100.1 → 192.168.100.10 TLSv1.2 199 Application Data
27 484 2026-07-01 01:05:33.547728284 192.168.100.10 → 192.168.100.1 TCP 66 6514 → 60177 [ACK] Seq=1 Ack=707
27 489 2026-07-01 01:05:40.582487840 192.168.100.1 → 192.168.100.10 TLSv1.2 198 Application Data
29 490 2026-07-01 01:05:40.582705431 192.168.100.10 → 192.168.100.1 TCP 66 6514 → 60177 [ACK] Seq=1 Ack=839
```

TLS ةسلج لالځ نم اهلاسرا م تي syslog لئاسر نأ ىلإ TLS قيبطت تانايب دوجو ري شي
syslog ةلاسرا تايوتحم زيمرت ك ف Ethalyzer ل نكمي ال ، ةلومحل ريفشتل ارظن . ةرفشم ال



ي syslog لئاسر عي مج ني مضت م تي ، حاجنپ TLS لاصتا ديكتا لامتكا دعب : ةظحالم
طاقتل مزح ي ف ةيئرم ريغ اهتايوتحم . ةرفشم ال TLS قيبطت تانايب تالجم

syslog م داخ ىل ع لئاسرل لابقتسا نم ققحتل

. ةهولالجم فلم ىل اهتباتك و حاجنپ ةلاسرل يقلت نم ققحت ، syslog م داخ ىل ع

```
calo@calo-ubuntu22 ~ % sudo tail -20 /var/log/remote.log 8:03:45
Jun 30 20:04:36 192.168.100.1 : 2026 Jul 1 01:05:40 UTC: %LOCAL0-2-SYSTEM_MSG: systest from 0: test1-Fr
Jun 30 20:11:41 192.168.100.1 : 2026 Jul 1 01:12:45 UTC: %LOCAL0-2-SYSTEM_MSG: systest from 0: test2-Fr
```

:ي لي ام اهواشن م تي تال رابتخالا ةلاسر دوجو دكوي

حاجنپ syslog ةلاسر عاشناب Cisco Nexus لوحم ماق
ةرفشم ال TLS لمع ةسلج رب ع ةلاسرل لاسرا م
حاجنپ اهتجالعمو ةلاسرل ريفشت ك فب Syslog م داخ ماق
ةياهن ىل اهواشن نم حيحص لكشب نم آل syslog نيوكت لمعي

رورم ةكرح طشن لكشب لمحت TLS ةسلج نأ Ethalyzer ي ف TLS قيبطت تانايب روهظ دكوي
وه حيحص لكشب لمعي نم آل Syslog نأ ىل ع طاقلا ليلدل ناف ، كلذعمو . ةرفشم قيبطت
syslog م داخ ىل ع اهواشن م تي تال syslog ةلاسرل حجانل لابقتسالا

رارقالا

TLS، ضوافت ، حجانل TCP و IP لاصتا ىل ع Cisco Nexus تالوحم ىل ع نم آل Syslog دمتعي
ةقبط لك نم ققحتل دعاسي . ةرفشم ال لئاسرل ميلستو ، ةداهشال ءحص نم ققحتل او
لاسرا لكاشمو ، صيخرتل ، TLS ، لاصتالا زيمي و لشفال ةطقن لز ع ىل ع لقتسم لكشب
دكوي امنيب ، ةرفشم ال ةسلجل عاشن م هنأ حجانل TLS ءحفاصم دكوت . لئاسرل
ىل اهواشن نم نم آل syslog ةي لمع syslog م داخ ىل ع اهواشن م تي رابتخا ةلاسرل لابقتسا
ةياهن .

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 ج 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج 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 ج 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 ج 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 ج 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