

Problemen oplossen met Secure Syslog op Nexus Platform

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie](#)

[Achtergrondinformatie](#)

[Traditionele syslogan](#)

[Secure Syslog](#)

[certificaatketen](#)

[Waarom zijn certificaten nodig?](#)

[Secure Syslog TLS Handshake](#)

[Relevante configuratie](#)

[Cisco Nexus-configuratie](#)

[Ubuntu Syslog Server-configuratie](#)

[Probleemoplossing](#)

[Doel](#)

[uitleg over de topologie](#)

[Stap 1. Configuratie van beveiligd syslog verifiëren](#)

[Stap 2. Configuratie van TrustPoint verifiëren](#)

[Stap 3. Verifieer de IP-connectiviteit](#)

[Stap 4. TLS-connectiviteit verifiëren](#)

[Wat verifieert dit commando?](#)

[Verwachte geslaagde output](#)

[pakketopnamecorrelatie](#)

[Verifieer de veilige verzending van SYSLOG-berichten](#)

[Een testsyslog-bericht genereren](#)

[Versleutelde TLS-toepassingsgegevens verifiëren](#)

[Berichtenontvangst op de Syslog-server verifiëren](#)

[Conclusie](#)

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met Secure Syslog over Transport Layer Security (TLS) tussen Cisco Nexus-switches en servers van derden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- NX-OS-platforms
- Secure Syslog
- Kennis van Public Key Infrastructure (PKI)

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



Achtergrondinformatie

Traditionele syslogan

Traditionele Syslog verzendt logberichten via UDP (standaardpoort 514) of TCP zonder codering. Aangezien de communicatie in duidelijke tekst wordt verzonden, kunnen logberichten tijdens het transport mogelijk worden onderschept of gewijzigd. Traditioneel Syslog biedt ook geen serververificatie.

Secure Syslog

Secure Syslog gebruikt TCP met TLS (standaardpoort 6514) om versleutelde overdracht van syslog-berichten te bieden. Voordat een logbericht wordt verzonden, stellen de client en de server een TLS-sessie op, waarbij de server zijn certificaat presenteert en de client de certificaatketen valideert aan de hand van een vertrouwde certificeringsinstantie (CA). Zodra de TLS-handshake met succes is voltooid, worden syslog-berichten verzonden via het gecodeerde kanaal.

In tegenstelling tot Traditional Syslog is Secure Syslog niet alleen afhankelijk van IP-connectiviteit, maar ook van een succesvolle TLS-handshake, certificaatvalidatie en coderingsonderhandeling voordat een syslog-bericht kan worden uitgewisseld.

certificaatketen

Een certificaatketen is de reeks certificaten die wordt gebruikt om vertrouwen te creëren tussen het servercertificaat en een vertrouwde basiscertificeringsinstantie (Root CA). Tijdens de TLS-handshake presenteert de Syslog-server zijn servercertificaat samen met eventuele vereiste tussentijdse CA-certificaten. De Cisco Nexus switch gebruikt zijn vertrouwde Root CA om de gehele certificaatketen te valideren.

Een certificaatketen is niet altijd nodig.

De certificaten die door de Syslog-server worden aangeboden, zijn afhankelijk van de manier waarop de PKI is geïmplementeerd. Voorbeeld:

Zelfondertekend certificaat: de server presenteert alleen zijn eigen certificaat. In dit geval moet de Cisco Nexus-switch dat zelfondertekende certificaat rechtstreeks vertrouwen.

CA-ondertekend certificaat zonder tussenliggende CA's: de server presenteert alleen zijn servercertificaat omdat het rechtstreeks is ondertekend door een vertrouwde Root CA.

CA-signed certificate met intermediate CA's: de server presenteert zijn servercertificaat samen met een of meer intermediate CA-certificaten, waardoor de Cisco Nexus-switch een volledige vertrouwensketen kan opbouwen tot aan de vertrouwde Root CA.

Ongeacht het PKI-ontwerp moet de Cisco Nexus-switch het door de server gepresenteerde certificaat kunnen valideren voordat de TLS-sessie kan worden ingesteld.

Als een vereist certificaat in de vertrouwensketen ontbreekt, ongeldig is, is verlopen of is uitgegeven door een niet-vertrouwde certificeringsinstantie, mislukt de TLS-handshake en kan de Secure Syslog-verbinding niet worden gemaakt.

Waarom zijn certificaten nodig?

Secure Syslog vertrouwt op TLS om codering en serververificatie te bieden. Voordat een syslog-bericht wordt verzonden, moet de Cisco Nexus-switch controleren of deze communiceert met de beoogde Syslog-server en niet met een niet-geautoriseerd apparaat.

Certificaten bieden dit vertrouwen door de Nexus-switch toe te staan de identiteit van de Syslog-server te verifiëren voordat de gecodeerde sessie wordt ingesteld. Zodra de certificaatketen met succes is gevalideerd, wordt een beveiligd TLS-kanaal gemaakt en worden alle daaropvolgende syslog-berichten verzonden via de gecodeerde verbinding.

Zonder een geldig certificaat en een vertrouwde certificaatketen kan Secure Syslog de TLS-sessie niet instellen, waardoor logberichten niet veilig kunnen worden uitgewisseld.

Secure Syslog TLS Handshake

Voordat een syslog-bericht wordt verzonden, moeten de Cisco Nexus-switch en de Syslog-server met succes een TLS-sessie instellen. Tijdens de TLS-handshake onderhandelen beide apparaten over de TLS-parameters, stellen ze een gedeelde coderingssleutel vast en verifiëren ze de identiteit van de Syslog-server door middel van certificaatvalidatie.

Pas nadat de TLS-handshake succesvol is voltooid, worden syslog-berichten verzonden via de gecodeerde verbinding.

De TLS handshake bestaat uit de volgende fases:

trede	Beschrijving
1. TCP-verbinding	De Cisco Nexus-switch maakt een TCP-verbinding met de Secure Syslog-server (standaardpoort 6514).
2. Hallo client	De Nexus initieert de TLS-handdruk door de ondersteunde TLS-versies, coderingssuites en willekeurige waarden te verzenden.
3. Hallo server	De Syslog-server selecteert de TLS-versie en de coderingssuite die voor

trede	Beschrijving
	de sessie worden gebruikt.
4. Certificaatuitwisseling	De Syslog-server presenteert zijn servercertificaat en, indien vereist, eventuele tussentijdse CA-certificaten.
5. Certificaatvalidatie	De Nexus valideert het servercertificaat aan de hand van de geconfigureerde vertrouwde CA. Validatie omvat het controleren van de certificaatketen, vervaldata, uitgever en serveridentiteit via de Common Name (CN) en Subject Alternative Name (SAN).
6. Sleuteluitwisseling	Beide peers wisselen cryptografische informatie uit om de gedeelde sessiesleutels af te leiden die worden gebruikt voor codering.
7. Voltooide berichten	Elke peer verifieert dat de handdruk met succes is voltooid en dat beide zijden dezelfde cryptografische sleutels hebben afgeleid.
8. Beveiligde syslog-transmissie	Zodra de TLS-sessie is ingesteld, worden syslog-berichten verzonden als gecodeerde TLS Application Data-records.

Relevante configuratie

Cisco Nexus-configuratie

De Cisco Nexus-switch moet worden geconfigureerd met de bestemming Secure Syslog, een vertrouwenspunt met de vertrouwde CA en de juiste broninterface.

```
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 Server-configuratie

De Syslog-server die in dit document wordt gebruikt, is een Ubuntu-server waarop rsyslog wordt uitgevoerd met TLS-ondersteuning ingeschakeld.

De serverconfiguratie omvat de volgende functies:

Luister naar Secure Syslog verbindingen op TCP poort 6514.

Een TLS-servercertificaat presenteren tijdens de TLS-handdruk.

Gebruik een privésleutel die is gekoppeld aan het servercertificaat.

Verstrek de vereiste certificaatketen (indien van toepassing) aan Cisco Nexus tijdens de TLS-handdruk.

De ontvangen Secure Syslog-berichten opslaan in een lokaal logbestand.

De PKI-implementatie die in dit document wordt gebruikt, bestaat uit: Servercertificaat > Intermediate CA > Root CA

De Cisco Nexus-switch importeert en vertrouwt het Root CA-certificaat via een vertrouwenspunt, waardoor het de certificaatketen kan valideren die door de Syslog-server wordt gepresenteerd.



Opmerking: een certificaatketen is niet verplicht voor elke implementatie. Afhankelijk van de PKI-implementatie kan de Syslog-server alleen een zelfondertekend certificaat presenteren, een servercertificaat dat rechtstreeks door een root-CA is ondertekend of een servercertificaat dat vergezeld gaat van een of meer intermediaire CA-certificaten.

Probleemoplossing

Doel

Het doel van deze probleemoplossingsprocedure is het isoleren en identificeren van storingen die voorkomen dat Cisco Nexus NX-OS-switches met succes een Secure Syslog TLS-verbinding met een Syslog-server tot stand kunnen brengen.

De workflow valideert elke fase van het communicatieproces, te beginnen met IP-connectiviteit en vordert via TCP-connectiviteit, TLS-onderhandelingen, certificaatvalidatie en ten slotte Secure Syslog-berichtverzending. Door elke laag onafhankelijk te verifiëren, is het mogelijk om snel te

bepalen waar de communicatie faalt.

uitleg over de topologie

De in dit document gebruikte topologie bestaat uit een Cisco Nexus-switch die is geconfigureerd als de Secure Syslog-client en een Ubuntu-server waarop rsyslog wordt uitgevoerd die is geconfigureerd als de Secure Syslog-server.

De Cisco Nexus-switch initieert een TCP-verbinding met de Syslog-server op poort 6514. Nadat de TCP-verbinding tot stand is gebracht, voeren beide apparaten de TLS-handdruk uit. Tijdens dit proces presenteert de Syslog-server zijn servercertificaat en alle vereiste tussentijdse CA-certificaten. De Nexus-switch valideert de certificaatketen aan de hand van de vertrouwde Root CA die is geconfigureerd in het vertrouwenspunt.

Zodra de TLS-handshake met succes is voltooid, wordt de gecodeerde sessie tot stand gebracht en begint de Nexus-switch met het verzenden van Secure Syslog-berichten naar de Syslog-server.

De methodologie voor probleemoplossing die in dit document wordt gepresenteerd, maakt gebruik van dezelfde communicatiesequentie als de verbindinginstelling, waardoor elke fase van het proces onafhankelijk kan worden gevalideerd.

Stap 1. Configuratie van beveiligd syslog verifiëren

Controleer of Secure Syslog correct is geconfigureerd op de Cisco Nexus-switch en of de switch de geconfigureerde Syslog-server herkent.

```
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#
```

Stap 2. Configuratie van TrustPoint verifiëren

Controleer of de Cisco Nexus-switch de CA vertrouwt die is gebruikt om het Syslog-servercertificaat te ondertekenen.

Verifiëren:

Het verwachte Trustpoint bestaat.

Het Root CA-certificaat is geïnstalleerd.

Eventuele vereiste tussentijdse CA-certificaten zijn aanwezig.

Certificaten zijn niet verlopen.

Certificaatvingerafdrukken komen overeen met de verwachte waarden.

```
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 Int  
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 Roo  
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#
```

Als het juiste CA-certificaat ontbreekt of ongeldig is, mislukt de certificaatvalidatie tijdens de TLS-handdruk.

Stap 3. Verifieer de IP-connectiviteit

Controleer de Layer 3-connectiviteit tussen de Cisco Nexus switch en de Secure Syslog-server.

Verifiëren:

- Succesvolle Internet Control Message Protocol (ICMP) bereikbaarheid.
- Correcte DNS-resolutie (Domain Name System).

- Geen routeringsproblemen.
- Geen pakketverlies.

```
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#
```

Als de IP-verbinding uitvalt, kan er geen TCP-verbinding tot stand worden gebracht.

Stap 4. TLS-connectiviteit verifiëren

Controleer de end-to-end TLS-connectiviteit tussen de Cisco Nexus switch en de Secure Syslog-server.

Deze stap valideert meerdere fasen van de Secure Syslog-verbinding, waaronder:

- TCP-connectiviteit
- TLS-onderhandeling
- Presentatie servercertificaat
- Certificaatketen
- Certificaatvalidatie
- Onderhandelingen over coderingssuite

Omdat deze bewerkingen plaatsvinden als onderdeel van de TLS-handdruk, kunnen ze allemaal worden geverifieerd met een enkele opdracht.

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

Wat verifieert dit commando?

validering	Beschrijving
TCP-connectiviteit	Controleert of de Nexus een TCP-verbinding met de Syslog-server tot stand kan brengen.
TLS Handshake	Bevestigt dat beide peers succesvol onderhandelen over een TLS-sessie.
servercertificaat	Geeft het certificaat weer dat wordt aangeboden door de Syslog-server.
certificaatketen	Geeft alle tussenliggende CA-certificaten weer die door de server zijn verzonden.
TLS-versie	Geeft de onderhandelde TLS-versie weer.
Cipher Suite	Geeft het onderhandelde coderingsalgoritme weer.
certificaatvalidatie	Wanneer de optie <code>-CAfile</code> wordt gebruikt, wordt de certificaatketen geverifieerd aan de hand van de opgegeven vertrouwde CA.

Verwachte geslaagde output

```
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
verify return:1
depth=1 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA
verify return:1
depth=0 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = syslog.lab.local
verify return:1
---
Certificate chain >>>>>>>>>
0 s:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = syslog.lab.local,
i:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA
1 s:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA
i:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root CA,
---
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
issuer=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermediate CA
---
```

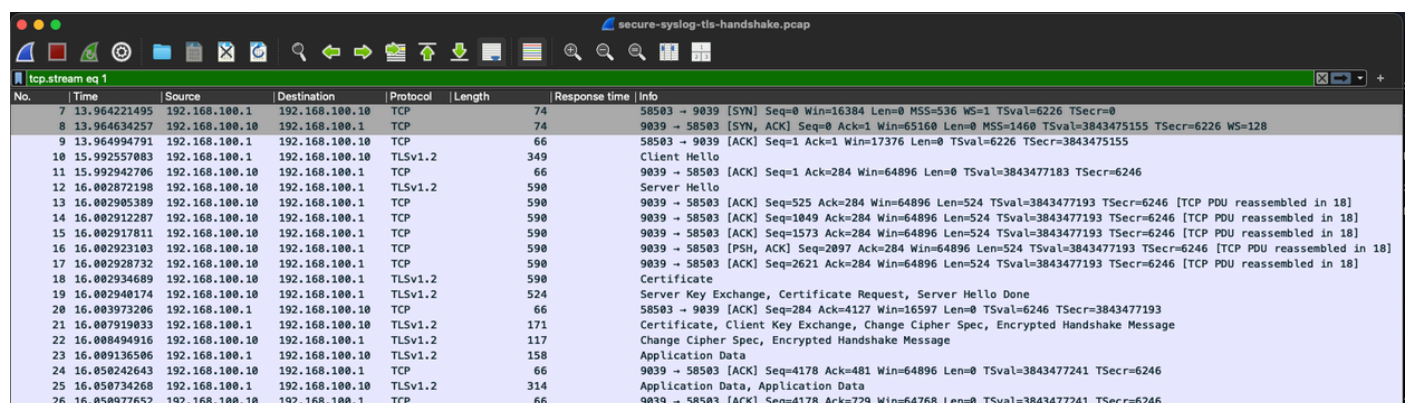
```

Acceptable client certificate CA names
C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Root CA, em
Client Certificate Types: RSA sign, ECDSA sign
Requested Signature Algorithms: RSA+SHA256:RSA-PSS+SHA256:RSA-PSS+SHA256:ECDSA+SHA256:Ed25519:RSA+SHA384
Shared Requested Signature Algorithms: RSA+SHA256:RSA-PSS+SHA256:RSA-PSS+SHA256:ECDSA+SHA256:Ed25519:RS
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
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
Protocol : TLSv1.2.                >>>>>>>>>> The negotiated protocol
Cipher : ECDHE-RSA-AES256-GCM-SHA384  >>>>>>>>>> The negotiated cipher
Session-ID: E67D3C91AB57212C16C2A240668CBC5BA1720BC5DA6AD69C69B209C90E828483
Session-ID-ctx:
Master-Key: 5C45FC4ACE18657DBCDC0946A68A9BE480ECB0CF24313C56C3067EA9D23D68EB5090A4DFE36D4E4CB72BA282D0A
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1782867300
Timeout : 7200 (sec)
Verify return code: 0 (ok).        >>>>>>>>>> indicates that the certificate chain was success
Extended master secret: yes
---
switch#

```

pakketopnamecorrelatie

De output van openssl_s kan worden gecorreleerd met pakketopnames die zijn verkregen met behulp van Ethalyzer om elke fase van de TLS-handdruk te verifiëren.



No.	Time	Source	Destination	Protocol	Length	Response time	Info
7	13.964221495	192.168.100.1	192.168.100.10	TCP	74		58503 → 9039 [SYN] Seq=0 Win=16384 Len=0 MSS=536 WS=1 TSval=6226 TSecr=0
8	13.964634257	192.168.100.10	192.168.100.1	TCP	74		9039 → 58503 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 TSval=3843475155 TSecr=6226 WS=128
9	13.964994791	192.168.100.1	192.168.100.10	TCP	66		58503 → 9039 [ACK] Seq=1 Ack=1 Win=17376 Len=0 TSval=6226 TSecr=3843475155
10	15.992557083	192.168.100.1	192.168.100.10	TLSv1.2	349		Client Hello
11	15.992942706	192.168.100.10	192.168.100.1	TCP	66		9039 → 58503 [ACK] Seq=1 Ack=284 Win=64896 Len=0 TSval=3843477193 TSecr=6246
12	16.002872198	192.168.100.10	192.168.100.1	TLSv1.2	590		Server Hello
13	16.002905389	192.168.100.10	192.168.100.1	TCP	590		9039 → 58503 [ACK] Seq=525 Ack=284 Win=64896 Len=524 TSval=3843477193 TSecr=6246 [TCP PDU reassembled in 18]
14	16.002912287	192.168.100.10	192.168.100.1	TCP	590		9039 → 58503 [ACK] Seq=1049 Ack=284 Win=64896 Len=524 TSval=3843477193 TSecr=6246 [TCP PDU reassembled in 18]
15	16.002917811	192.168.100.10	192.168.100.1	TCP	590		9039 → 58503 [ACK] Seq=1573 Ack=284 Win=64896 Len=524 TSval=3843477193 TSecr=6246 [TCP PDU reassembled in 18]
16	16.002923103	192.168.100.10	192.168.100.1	TCP	590		9039 → 58503 [PSH, ACK] Seq=2097 Ack=284 Win=64896 Len=524 TSval=3843477193 TSecr=6246 [TCP PDU reassembled in 18]
17	16.002928732	192.168.100.10	192.168.100.1	TCP	590		9039 → 58503 [ACK] Seq=2621 Ack=284 Win=64896 Len=524 TSval=3843477193 TSecr=6246 [TCP PDU reassembled in 18]
18	16.002934689	192.168.100.10	192.168.100.1	TLSv1.2	590		Certificate
19	16.002940174	192.168.100.10	192.168.100.1	TLSv1.2	524		Server Key Exchange, Certificate Request, Server Hello Done
20	16.003973206	192.168.100.1	192.168.100.10	TCP	66		58503 → 9039 [ACK] Seq=284 Ack=4127 Win=16597 Len=0 TSval=6246 TSecr=3843477193
21	16.007919033	192.168.100.1	192.168.100.10	TLSv1.2	171		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
22	16.008494916	192.168.100.10	192.168.100.1	TLSv1.2	117		Change Cipher Spec, Encrypted Handshake Message
23	16.009136506	192.168.100.1	192.168.100.10	TLSv1.2	158		Application Data
24	16.050242643	192.168.100.10	192.168.100.1	TCP	66		9039 → 58503 [ACK] Seq=4178 Ack=481 Win=64896 Len=0 TSval=3843477241 TSecr=6246
25	16.050734268	192.168.100.1	192.168.100.10	TLSv1.2	314		Application Data
26	16.050977652	192.168.100.10	192.168.100.1	TCP	66		9039 → 58503 [ACK] Seq=4178 Ack=729 Win=64768 Len=0 TSval=3843477241 TSecr=6246

Secure Syslog TLS Handshake Capture

TLS Handshake Flow

```
Cisco Nexus                Syslog Server
-----
TCP SYN ----->
<----- TCP SYN/ACK
TCP ACK ----->
Client Hello ----->
<----- Server Hello
<----- Certificate
<----- (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 ----->
```

De TLS-handshake moet met succes worden voltooid voordat een syslog-bericht kan worden uitgewisseld. Als de handdruk mislukt, wordt er nooit Secure Syslog-verkeer gegenereerd.

Om deze verificatie uit te voeren, opent u twee CLI-sessies naar de Cisco Nexus-switch. Start in de eerste sessie de TLS-verbinding met deze opdracht:

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

Start tegelijkertijd in de tweede CLI-sessie een Ethalyzer-opname om de TLS-uitwisseling te bewaken:

```
switch# ethalyzer 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 Wi
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=65536 Len=0
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 Handshake
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=4177 Win=65536 Len=0
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=4177 Win=65536 Len=0
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 Win=65536 Len=0
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 Win=65536 Len=0

```

De pakketopname moet de volledige TLS-handshake-reeks weergeven, inclusief de TCP-drieweghandshake, Client Hello, Server Hello, Certificate, Key Exchange, Voltooide berichten en, als de handshake met succes is voltooid, versleutelde TLS Application Data-records met de Secure Syslog-berichten.

Verifieer de veilige verzending van SYSLOG-berichten

Controleer of Secure Syslog-berichten succesvol worden verzonden van de Cisco Nexus-switch naar de Syslog-server nadat de TLS-sessie is ingesteld.

Een succesvolle TLS-handdruk bevestigt dat het gecodeerde kanaal is gemaakt; het garandeert echter niet dat syslog-berichten worden gegenereerd of afgeleverd.

Deze stap valideert de volledige Secure Syslog-workflow door een testbericht te genereren en de verzending en ontvangst ervan te bevestigen.

Een testsyslog-bericht genereren

```

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

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

```

Met deze opdracht wordt een lokaal syslog-bericht gegenereerd dat via de bestaande TLS-sessie naar de geconfigureerde Secure Syslog-server moet worden verzonden.

Versleutelde TLS-toepassingsgegevens verifiëren

Als er al een Ethanalyzer-opname wordt uitgevoerd (zoals beschreven in de vorige sectie), controleert u of er nieuwe TLS Application Data-pakketten worden verzonden nadat het testbericht is gegenereerd.

```
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
```

De aanwezigheid van TLS Application Data geeft aan dat de syslog-berichten worden verzonden via de gecodeerde TLS-sessie. Omdat de payload versleuteld is, kan Ethanalyzer de inhoud van het syslog-bericht niet decoderen.



Opmerking: Nadat de TLS-handshake met succes is voltooid, worden alle syslog-berichten ingekapseld in gecodeerde TLS Application Data-records. De inhoud ervan is niet zichtbaar in pakketopnames.

Berichtenontvangst op de Syslog-server verifiëren

Controleer op de Syslog-server of het bericht is ontvangen en naar het bestemmingslogbestand is geschreven.

```
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
```

De aanwezigheid van het gegenereerde testbericht bevestigt dat:

- De Cisco Nexus-switch heeft het syslog-bericht met succes gegenereerd.
- Het bericht is verzonden via de gecodeerde TLS-sessie.
- De Syslog-server heeft het bericht ontsleuteld en verwerkt.
- De Secure Syslog-configuratie werkt van begin tot eind correct.

Het verschijnen van TLS Application Data in Ethanalyzer bevestigt dat de TLS-sessie actief gecodeerd applicatieverkeer vervoert. Het definitieve bewijs dat Secure Syslog correct werkt, is echter de succesvolle ontvangst van het gegenereerde syslog-bericht op de Syslog-server.

Conclusie

Secure Syslog op Cisco Nexus-switches is afhankelijk van een geslaagde IP- en TCP-connectiviteit, TLS-onderhandeling, certificaatvalidatie en versleutelde berichtlevering. Het onafhankelijk verifiëren van elke laag helpt het storingspunt te isoleren en onderscheid te maken tussen problemen met connectiviteit, TLS, certificaat en berichtverzending. Een succesvolle TLS-handshake bevestigt dat de gecodeerde sessie is ingesteld, terwijl de ontvangst van een gegenereerd testbericht op de Syslog-server end-to-end Secure Syslog-bewerking bevestigt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.