

Fehlerbehebung für Secure Syslog auf der Nexus-Plattform

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Topologie](#)

[Hintergrundinformationen](#)

[Traditionelles Syslog](#)

[Sicheres Syslog](#)

[Zertifikatkette](#)

[Warum sind Zertifikate erforderlich?](#)

[Sicherer Syslog-TLS-Handshake](#)

[Relevante Konfiguration](#)

[Cisco Nexus-Konfiguration](#)

[Ubuntu Syslog-Serverkonfiguration](#)

[Fehlerbehebung](#)

[Ziel](#)

[Topologie-Erläuterung](#)

[Schritt 1: Überprüfen der sicheren Syslog-Konfiguration](#)

[Schritt 2: Überprüfen der Vertrauenspunktconfiguration](#)

[Schritt 3: Überprüfen der IP-Verbindung](#)

[Schritt 4: Überprüfen der TLS-Verbindung](#)

[Was überprüft dieser Befehl?](#)

[Erwartete erfolgreiche Ausgabe](#)

[Korrelation der Paketerfassung](#)

[Sichere Syslog-Nachrichtenübertragung überprüfen](#)

[Erstellen einer Test-Syslog-Meldung](#)

[Überprüfung verschlüsselter TLS-Anwendungsdaten](#)

[Überprüfung des Nachrichtenempfangs auf dem Syslog-Server](#)

[Schlussfolgerung](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung für Secure Syslog über Transport Layer Security (TLS) zwischen Cisco Nexus-Switches und Servern von Drittanbietern beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- NX-OS-Plattformen
- Sicheres Syslog
- Grundlegendes PKI-Wissen (Public Key Infrastructure)

Verwendete Komponenten

N9K1	N9K-C9336C-FX2	10.4(7)
Syslog-Server	Ubuntu-Server	rsyslog 8,2112 OpenSSL 3.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Hintergrundinformationen

Traditionelles Syslog

Herkömmliche Syslog-Protokolle werden unverschlüsselt über UDP (Standard-Port 514) oder TCP übertragen. Da die Kommunikation als Klartext gesendet wird, können Protokollnachrichten während der Übertragung möglicherweise abgefangen oder geändert werden. Herkömmliches Syslog bietet auch keine Serverauthentifizierung.

Sicheres Syslog

Secure Syslog verwendet TCP mit TLS (Standard-Port 6514), um eine verschlüsselte Übertragung von Syslog-Meldungen bereitzustellen. Bevor eine Protokollmeldung gesendet wird, richten der Client und der Server eine TLS-Sitzung ein, in der der Server sein Zertifikat präsentiert und der Client die Zertifikatskette mit einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) vergleicht. Nach erfolgreichem TLS-Handshake werden Syslog-Meldungen über den verschlüsselten Kanal übertragen.

Im Gegensatz zu herkömmlichem Syslog ist sicheres Syslog nicht nur von der IP-Konnektivität abhängig, sondern auch von einem erfolgreichen TLS-Handshake, der Zertifikatsvalidierung und der Verschlüsselungsverhandlung, bevor Syslog-Meldungen ausgetauscht werden können.

Zertifikatskette

Eine Zertifikatskette ist die Sequenz von Zertifikaten, die verwendet wird, um eine Vertrauensstellung zwischen dem Serverzertifikat und einer vertrauenswürdigen Stammzertifizierungsstelle (Stammzertifizierungsstelle) herzustellen. Während des TLS-Handshakes stellt der Syslog-Server sein Serverzertifikat zusammen mit allen erforderlichen zwischengeschalteten Zertifizierungsstellenzertifikaten bereit. Der Cisco Nexus-Switch verwendet seine vertrauenswürdige Stammzertifizierungsstelle zur Validierung der gesamten Zertifikatskette.

Eine Zertifikatskette ist nicht immer erforderlich.

Die vom Syslog-Server vorgelegten Zertifikate hängen davon ab, wie die PKI implementiert wurde. Beispiele:

Selbstsigniertes Zertifikat: Der Server präsentiert nur sein eigenes Zertifikat. In diesem Fall muss der Cisco Nexus-Switch diesem selbstsignierten Zertifikat direkt vertrauen.

CA-signiertes Zertifikat ohne zwischengeschaltete CAs: Der Server stellt nur sein Serverzertifikat dar, da es direkt von einer vertrauenswürdigen Stammzertifizierungsstelle signiert wurde.

CA-signiertes Zertifikat mit zwischengeschalteten CAs: Der Server stellt sein Serverzertifikat zusammen mit einem oder mehreren Zwischenzertifikaten der Zertifizierungsstelle dar, sodass der Cisco Nexus-Switch eine vollständige Vertrauenskette bis zur vertrauenswürdigen Stammzertifizierungsstelle aufbauen kann.

Unabhängig vom PKI-Design muss der Cisco Nexus-Switch in der Lage sein, das vom Server vorgelegte Zertifikat zu validieren, bevor die TLS-Sitzung hergestellt werden kann.

Wenn ein erforderliches Zertifikat in der Vertrauenskette fehlt, ungültig oder abgelaufen ist oder von einer nicht vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde, schlägt der TLS-Handshake fehl, und die sichere Syslog-Verbindung kann nicht hergestellt werden.

Warum sind Zertifikate erforderlich?

Secure Syslog verwendet TLS, um Verschlüsselung und Serverauthentifizierung bereitzustellen. Bevor eine Syslog-Meldung übertragen wird, muss der Cisco Nexus-Switch überprüfen, ob er mit dem beabsichtigten Syslog-Server und nicht mit einem nicht autorisierten Gerät kommuniziert.

Zertifikate stellen diese Vertrauensstellung bereit, indem sie es dem Nexus-Switch ermöglichen, die Identität des Syslog-Servers zu authentifizieren, bevor die verschlüsselte Sitzung eingerichtet wird. Nach der erfolgreichen Validierung der Zertifikatskette wird ein sicherer TLS-Kanal erstellt, und alle nachfolgenden Syslog-Meldungen werden über die verschlüsselte Verbindung übertragen.

Ohne ein gültiges Zertifikat und eine vertrauenswürdige Zertifikatskette kann Secure Syslog die TLS-Sitzung nicht herstellen und verhindert so den sicheren Austausch von Protokollnachrichten.

Sicherer Syslog-TLS-Handshake

Bevor eine Syslog-Meldung übertragen wird, müssen der Cisco Nexus-Switch und der Syslog-Server erfolgreich eine TLS-Sitzung herstellen. Während des TLS-Handshakes handeln beide Geräte die TLS-Parameter aus, legen einen gemeinsamen Verschlüsselungsschlüssel fest und authentifizieren die Identität des Syslog-Servers durch Zertifikatsvalidierung.

Erst wenn der TLS-Handshake erfolgreich abgeschlossen wurde, werden Syslog-Meldungen über die verschlüsselte Verbindung übertragen.

Der TLS-Handshake besteht aus den folgenden Phasen:

Schritt	Beschreibung
1. TCP-Verbindung	Der Cisco Nexus-Switch stellt eine TCP-Verbindung zum sicheren Syslog-Server her (Standardport 6514).

Schritt	Beschreibung
2. Client-Begrüßung	Der Nexus initiiert den TLS-Handshake, indem er die unterstützten TLS-Versionen, Verschlüsselungssuiten und Zufallswerte sendet.
3. Server-Hello	Der Syslog-Server wählt die TLS-Version und die für die Sitzung verwendete Verschlüsselungs-Suite aus.
4. Zertifikataustausch	Der Syslog-Server stellt sein Serverzertifikat und ggf. alle dazwischen liegenden Zertifizierungsstellenzertifikate dar.
5. Validierung von Zertifikaten	Der Nexus validiert das Serverzertifikat anhand der konfigurierten vertrauenswürdigen Zertifizierungsstelle. Die Validierung umfasst die Überprüfung der Zertifikatskette, der Ablaufdaten, des Ausstellers und der Serveridentität mithilfe des Common Name (CN) und des Subject Alternative Name (SAN).
6. Schlüsselaustausch	Beide Peers tauschen kryptografische Informationen aus, um die zur Verschlüsselung verwendeten freigegebenen Sitzungsschlüssel abzuleiten.
7. Abgeschlossene Nachrichten	Jeder Peer überprüft, ob der Handshake erfolgreich abgeschlossen wurde und beide Seiten dieselben kryptografischen Schlüssel abgeleitet haben.
8. Sichere Syslog-Übertragung	Nach Einrichtung der TLS-Sitzung werden Syslog-Meldungen als verschlüsselte TLS-Anwendungsdatensätze übertragen.

Relevante Konfiguration

Cisco Nexus-Konfiguration

Der Cisco Nexus-Switch muss mit dem sicheren Syslog-Ziel, einem Vertrauenspunkt, der die vertrauenswürdige Zertifizierungsstelle enthält, und der entsprechenden Quellschnittstelle konfiguriert werden.

```
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-Serverkonfiguration

Der in diesem Dokument verwendete Syslog-Server ist ein Ubuntu-Server, auf dem rsyslog mit aktivierter TLS-Unterstützung ausgeführt wird.

Die Serverkonfiguration umfasst folgende Funktionen:

Achten Sie auf sichere Syslog-Verbindungen am TCP-Port 6514.
Stellen Sie während des TLS-Handshakes ein TLS-Serverzertifikat bereit.
Verwenden Sie einen privaten Schlüssel, der mit dem Serverzertifikat verknüpft ist.
Stellen Sie die erforderliche Zertifikatskette (falls zutreffend) für Cisco Nexus während des TLS-Handshakes bereit.
Empfangene sichere Syslog-Meldungen in einer lokalen Protokolldatei speichern.

Die in diesem Dokument verwendete PKI-Implementierung besteht aus: Serverzertifikat >
Erweiterte Zertifizierungsstelle > Stammzertifizierungsstelle

Der Cisco Nexus-Switch importiert das Zertifikat der Root-Zertifizierungsstelle und vertraut ihm über einen Vertrauenspunkt, sodass er die Zertifikatskette validieren kann, die vom Syslog-Server dargestellt wird.



Anmerkung: Eine Zertifikatskette ist nicht für jede Bereitstellung erforderlich. Je nach PKI-Implementierung kann der Syslog-Server nur ein selbstsigniertes Zertifikat, ein direkt von einer Stammzertifizierungsstelle signiertes Serverzertifikat oder ein Serverzertifikat mit einem oder mehreren Zwischenzertifikaten der Zertifizierungsstelle präsentieren.

Fehlerbehebung

Ziel

Ziel dieser Fehlerbehebung ist es, Fehler zu isolieren und zu identifizieren, die verhindern, dass Cisco Nexus NX-OS-Switches erfolgreich eine sichere Syslog TLS-Verbindung mit einem Syslog-Server herstellen.

Der Workflow validiert alle Phasen des Kommunikationsprozesses, angefangen bei der IP-Verbindung über die TCP-Verbindung, die TLS-Aushandlung, die Zertifikatsvalidierung und schließlich die sichere Syslog-Nachrichtenübertragung. Durch die unabhängige Überprüfung jeder Schicht kann schnell festgestellt werden, wo die Kommunikation fehlschlägt.

Topologie-Erläuterung

Die in diesem Dokument verwendete Topologie besteht aus einem Cisco Nexus-Switch, der als sicherer Syslog-Client konfiguriert ist, und einem Ubuntu-Server, auf dem rsyslog ausgeführt wird, der als sicherer Syslog-Server konfiguriert ist.

Der Cisco Nexus-Switch initiiert eine TCP-Verbindung zum Syslog-Server an Port 6514. Nachdem die TCP-Verbindung hergestellt wurde, führen beide Geräte den TLS-Handshake aus. Während dieses Vorgangs stellt der Syslog-Server sein Serverzertifikat und alle erforderlichen zwischengeschalteten Zertifizierungsstellenzertifikate dar. Der Nexus-Switch validiert die Zertifikatkette anhand der vertrauenswürdigen Root-CA, die in ihrem Vertrauenspunkt konfiguriert wurde.

Sobald der TLS-Handshake erfolgreich abgeschlossen wurde, wird die verschlüsselte Sitzung hergestellt, und der Nexus-Switch beginnt mit der Übertragung sicherer Syslog-Meldungen an den Syslog-Server.

Die in diesem Dokument vorgestellte Methode zur Fehlerbehebung nutzt dieselbe Kommunikationssequenz wie der Verbindungsaufbau, sodass jede Phase des Prozesses unabhängig validiert werden kann.

Schritt 1: Überprüfen der sicheren Syslog-Konfiguration

Überprüfen Sie, ob Secure Syslog auf dem Cisco Nexus-Switch ordnungsgemäß konfiguriert ist und ob der Switch den konfigurierten Syslog-Server erkennt.

```
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#
```

Schritt 2: Überprüfen der Vertrauenspunktconfiguration

Vergewissern Sie sich, dass der Cisco Nexus-Switch der CA vertraut, die zum Signieren des Syslog-Serverzertifikats verwendet wird.

Überprüfung:

Der erwartete Vertrauenspunkt ist vorhanden.

Das Zertifikat der Stammzertifizierungsstelle ist installiert.

Alle erforderlichen Zwischenzertifikate sind vorhanden.

Zertifikate sind nicht abgelaufen.

Die Zertifikatfingerabdrücke stimmen mit den erwarteten Werten überein.

```
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 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#
```

Wenn das entsprechende Zertifizierungsstellenzertifikat fehlt oder ungültig ist, schlägt die Zertifikatsvalidierung während des TLS-Handshakes fehl.

Schritt 3: Überprüfen der IP-Verbindung

Überprüfen der Layer-3-Verbindung zwischen dem Cisco Nexus-Switch und dem sicheren Syslog-Server

Überprüfung:

- Erfolgreiche Erreichbarkeit des Internet Control Message Protocol (ICMP)
- Korrekte DNS-Auflösung (Domain Name System)
- Keine Routing-Probleme.
- Kein Paketverlust.

```
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#
```

Wenn die IP-Verbindung ausfällt, kann keine TCP-Verbindung hergestellt werden.

Schritt 4: Überprüfen der TLS-Verbindung

Überprüfen der End-to-End-TLS-Verbindung zwischen dem Cisco Nexus-Switch und dem sicheren Syslog-Server

In diesem Schritt werden mehrere Phasen der sicheren Syslog-Verbindung validiert, darunter:

TCP-Verbindung
TLS-Verhandlung
Serverzertifikatpräsentation
Zertifikatskette
Zertifikatsüberprüfung
Verhandlung über die Verschlüsselungssuite

Da diese Vorgänge als Teil des TLS-Handshakes ausgeführt werden, können sie mit einem

einzigsten Befehl überprüft werden.

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

Was überprüft dieser Befehl?

Validierung	Beschreibung
TCP-Verbindung	Überprüft, ob der Nexus eine TCP-Verbindung zum Syslog-Server herstellen kann.
TLS-Handshake	Bestätigt, dass beide Peers eine TLS-Sitzung erfolgreich aushandeln.
Serverzertifikat	Zeigt das vom Syslog-Server vorgelegte Zertifikat an.
Zertifikatkette	Zeigt alle zwischengeschalteten Zertifizierungsstellenzertifikate an, die vom Server gesendet wurden.
TLS-Version	Zeigt die ausgehandelte TLS-Version an.
Cipher-Suite	Zeigt den ausgehandelten Verschlüsselungsalgorithmus an.
Zertifikatsvalidierung	Wenn die Option -CAfile verwendet wird, wird die Zertifikatkette anhand der angegebenen vertrauenswürdigen Zertifizierungsstelle überprüft.

Erwartete erfolgreiche Ausgabe

```
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
verify return:1
depth=1 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Int
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 Intermedi
1 s:C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Interme
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.1o

issuer=C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Inte

---
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+SHA38
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#

```

Korrelation der Paketerfassung

Die Ausgabe von openssl s_client kann mit Paketerfassungen korreliert werden, die mit Ethalyzer ermittelt wurden, um jede Phase des TLS-Handshakes zu überprüfen.

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	15.992557883	192.168.100.1	192.168.100.10	TLSv1.2	349		Client Hello
11	15.992942786	192.168.100.10	192.168.100.1	TCP	66	9039 → 58503	[ACK] Seq=1 Ack=284 Win=64896 Len=0 TSval=3843477183 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, 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

Sichere Syslog TLS-Handshake-Erfassung

TLS-Handshake-Fluss

```

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 ----->

```

Der TLS-Handshake muss erfolgreich abgeschlossen werden, bevor Syslog-Meldungen ausgetauscht werden können. Wenn der Handshake fehlschlägt, wird niemals sicherer Syslog-Datenverkehr generiert.

Öffnen Sie zur Durchführung dieser Überprüfung zwei CLI-Sitzungen mit dem Cisco Nexus-Switch. Initiieren Sie in der ersten Sitzung die TLS-Verbindung mit folgendem Befehl:

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

Beginnen Sie gleichzeitig in der zweiten CLI-Sitzung eine Erfassung durch Ethalyzer, um den TLS-Austausch zu überwachen:

```
switch# ethalyzer local interface inbound 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
```

Bei der Paketerfassung muss die vollständige TLS-Handshake-Sequenz angezeigt werden, einschließlich des TCP-Drei-Wege-Handshakes, Client Hello, Server Hello, Certificate, Key Exchange, Finished Messages, und bei erfolgreichem Abschluss des Handshakes der verschlüsselte TLS-Anwendungsdatensatz, der die Secure Syslog-Meldungen enthält.

Sichere Syslog-Nachrichtenübertragung überprüfen

Überprüfen Sie, ob sichere Syslog-Meldungen erfolgreich vom Cisco Nexus-Switch zum Syslog-Server übertragen werden, nachdem die TLS-Sitzung hergestellt wurde.

Ein erfolgreicher TLS-Handshake bestätigt, dass der verschlüsselte Kanal erstellt wurde. Es ist jedoch keine Garantie dafür, dass Syslog-Meldungen generiert oder übermittelt werden.

In diesem Schritt wird der vollständige sichere Syslog-Workflow validiert, indem eine Testnachricht generiert und Übertragung und Empfang bestätigt werden.

Erstellen einer Test-Syslog-Meldung

```
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
```

Dieser Befehl generiert eine lokale Syslog-Meldung, die über die vorhandene TLS-Sitzung an den konfigurierten sicheren Syslog-Server übertragen werden muss.

Überprüfung verschlüsselter TLS-Anwendungsdaten

Wenn bereits eine Erfassung durch Ethanalyzer ausgeführt wird (wie im vorherigen Abschnitt beschrieben), stellen Sie sicher, dass neue TLS-Anwendungsdatenpakete übertragen werden, nachdem die Testnachricht generiert wurde.

```
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
```

Wenn TLS-Anwendungsdaten vorhanden sind, werden die Syslog-Meldungen über die verschlüsselte TLS-Sitzung übertragen. Da die Nutzlast verschlüsselt ist, kann Ethanalyzer den Inhalt der Syslog-Nachricht nicht decodieren.



Anmerkung: Nachdem der TLS-Handshake erfolgreich abgeschlossen wurde, werden alle Syslog-Meldungen in verschlüsselte TLS-Anwendungsdatensätze gekapselt. Ihr Inhalt ist bei der Paketerfassung nicht sichtbar.

Überprüfung des Nachrichtenempfangs auf dem Syslog-Server

Überprüfen Sie auf dem Syslog-Server, ob die Nachricht erfolgreich empfangen und in die Zielprotokolldatei geschrieben wurde.

```
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
```

Das Vorhandensein der generierten Testnachricht bestätigt Folgendes:

Der Cisco Nexus-Switch hat die Syslog-Meldung erfolgreich generiert.
Die Nachricht wurde über die verschlüsselte TLS-Sitzung übertragen.
Der Syslog-Server hat die Nachricht erfolgreich entschlüsselt und verarbeitet.
Die Konfiguration für das sichere Syslog funktioniert durchgängig korrekt.

Das Auftreten von TLS-Anwendungsdaten in Ethalyzer bestätigt, dass die TLS-Sitzung aktiv verschlüsselten Anwendungsdatenverkehr überträgt. Der definitive Beweis dafür, dass Secure Syslog korrekt funktioniert, ist jedoch der erfolgreiche Empfang der generierten Syslog-Meldung auf dem Syslog-Server.

Schlussfolgerung

Sicheres Syslog auf Cisco Nexus-Switches hängt von einer erfolgreichen IP- und TCP-Verbindung, TLS-Aushandlung, Zertifikatvalidierung und verschlüsselter Nachrichtenübermittlung ab. Durch die unabhängige Überprüfung der einzelnen Layer können der Fehlerpunkt isoliert und Verbindungs-, TLS-, Zertifikat- und Nachrichtenübertragungsprobleme unterschieden werden. Ein erfolgreicher TLS-Handshake bestätigt, dass die verschlüsselte Sitzung hergestellt wurde, während der Empfang einer generierten Testnachricht auf dem Syslog-Server den sicheren End-to-End-Syslog-Vorgang bestätigt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.