

Risoluzione dei problemi relativi a Secure Syslog sulla piattaforma Nexus

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia](#)

[Premesse](#)

[Syslog tradizionale](#)

[Syslog protetto](#)

[Catena di certificati](#)

[Perché sono necessari i certificati](#)

[Handshake TLS syslog protetto](#)

[Configurazione rilevante](#)

[Cisco Nexus Configuration](#)

[Configurazione Ubuntu Syslog Server](#)

[Risoluzione dei problemi](#)

[Obiettivo](#)

[Spiegazione topologia](#)

[Passaggio 1. Verificare la configurazione sicura del syslog](#)

[Passaggio 2. Verificare la configurazione del punto di trust](#)

[Passaggio 3. Verifica della connettività IP](#)

[Passaggio 4. Verifica della connettività TLS](#)

[Verifica di questo comando](#)

[Output previsto riuscito](#)

[Correlazione acquisizione pacchetti](#)

[Verifica della trasmissione sicura dei messaggi di syslog](#)

[Genera un messaggio di syslog di prova](#)

[Verifica dati applicazione TLS crittografati](#)

[Verifica della ricezione dei messaggi sul server Syslog](#)

[Conclusioni](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a Secure Syslog over Transport Layer Security (TLS) tra gli switch Cisco Nexus e i server di terze parti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Piattaforme NX-OS
- Syslog protetto
- Conoscenze di base dell'infrastruttura a chiave pubblica (PKI)

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia



Premesse

Syslog tradizionale

Il syslog tradizionale trasmette i messaggi di log su UDP (porta predefinita 514) o TCP senza crittografia. Poiché la comunicazione viene inviata come testo non crittografato, i messaggi di registro possono essere intercettati o modificati durante la trasmissione. Anche il Syslog tradizionale non fornisce l'autenticazione del server.

Syslog protetto

Secure Syslog utilizza TCP con TLS (porta predefinita 6514) per fornire la trasmissione crittografata dei messaggi syslog. Prima dell'invio di qualsiasi messaggio di registro, il client e il server stabiliscono una sessione TLS, durante la quale il server presenta il proprio certificato e il client convalida la catena di certificati rispetto a un'Autorità di certificazione (CA) attendibile. Una volta completato l'handshake TLS, i messaggi syslog vengono trasmessi tramite il canale crittografato.

A differenza del syslog tradizionale, la protezione del syslog dipende non solo dalla connettività IP, ma anche da un handshake TLS, dalla convalida del certificato e dalla negoziazione della cifratura riusciti prima che qualsiasi messaggio syslog possa essere scambiato.

Catena di certificati

Una catena di certificati è la sequenza di certificati utilizzata per stabilire un trust tra il certificato del server e un'Autorità di certificazione (CA radice) attendibile. Durante l'handshake TLS, il server Syslog presenta il proprio certificato server insieme a tutti i certificati CA intermedi richiesti. Lo switch Cisco Nexus utilizza la propria CA radice attendibile per convalidare l'intera catena di certificati.

Non è sempre necessaria una catena di certificati.

I certificati presentati dal server Syslog dipendono da come è stata implementata la relativa PKI. Ad esempio:

Certificato autofirmato: Il server presenta solo il proprio certificato. In questo caso, lo switch Cisco Nexus deve considerare attendibile direttamente il certificato autofirmato.

Certificato firmato dalla CA senza CA intermedie: Il server presenta solo il proprio certificato server perché è stato firmato direttamente da una CA radice attendibile.

Certificato firmato dalla CA con CA intermedie: Il server presenta il proprio certificato server insieme a uno o più certificati CA intermedi, consentendo allo switch Cisco Nexus di creare una catena di trust completa fino alla CA radice disponibile nell'elenco locale.

Indipendentemente dalla struttura della PKI, lo switch Cisco Nexus deve essere in grado di convalidare il certificato presentato dal server prima che sia possibile stabilire la sessione TLS.

Se un certificato richiesto nella catena di attendibilità è mancante, non valido, scaduto o rilasciato da una CA non attendibile, l'handshake TLS ha esito negativo e non è possibile stabilire la connessione Syslog sicura.

Perché sono necessari i certificati

Secure Syslog si basa su TLS per fornire la crittografia e l'autenticazione del server. Prima di trasmettere un messaggio syslog, lo switch Cisco Nexus deve verificare che stia comunicando con il server Syslog desiderato e non con un dispositivo non autorizzato.

I certificati forniscono questa attendibilità consentendo allo switch Nexus di autenticare l'identità del server Syslog prima di stabilire la sessione crittografata. Una volta convalidata la catena di certificati, viene creato un canale TLS sicuro e tutti i successivi messaggi syslog vengono trasmessi attraverso la connessione crittografata.

Senza un certificato valido e una catena di certificati attendibili, Secure Syslog non è in grado di stabilire la sessione TLS, impedendo lo scambio protetto dei messaggi di registro.

Handshake TLS syslog protetto

Prima di trasmettere un messaggio syslog, lo switch Cisco Nexus e il server Syslog devono stabilire correttamente una sessione TLS. Durante l'handshake TLS, entrambi i dispositivi negoziano i parametri TLS, stabiliscono una chiave di crittografia condivisa e autenticano l'identità del server Syslog tramite la convalida del certificato.

I messaggi syslog vengono trasmessi tramite la connessione crittografata solo dopo il completamento dell'handshake TLS.

L'handshake TLS è costituito dalle fasi seguenti:

Passaggio	Descrizione
1. Connessione TCP	Lo switch Cisco Nexus stabilisce una connessione TCP al server Syslog sicuro (porta predefinita 6514).
2. Salve al cliente	Il Nexus avvia l'handshake TLS inviando le versioni TLS, le suite di cifratura e i valori casuali supportati.
3. Server Hello	Il server Syslog seleziona la versione TLS e la suite di cifratura utilizzata per la

Passaggio	Descrizione
	sessione.
4. Scambio di certificati	Il server Syslog presenta il proprio certificato server e, se necessario, qualsiasi certificato CA intermedio.
5. Convalida dei certificati	Il Nexus convalida il certificato del server a fronte della CA attendibile configurata. La convalida include il controllo della catena di certificati, delle date di scadenza, dell'emittente e dell'identità del server tramite il nome comune (CN) e il nome alternativo del soggetto (SAN).
6. Scambio di chiavi	Entrambi i peer si scambiano informazioni di crittografia per derivare le chiavi di sessione condivise utilizzate per la crittografia.
7. Messaggi completati	Ogni peer verifica che l'handshake sia stato completato correttamente e che entrambi i lati derivino le stesse chiavi di crittografia.
8. Trasmissione sicura del syslog	Una volta stabilita la sessione TLS, i messaggi syslog vengono trasmessi come record crittografati dei dati dell'applicazione TLS.

Configurazione rilevante

Cisco Nexus Configuration

Lo switch Cisco Nexus deve essere configurato con la destinazione Secure Syslog, un trust point contenente l'autorità di certificazione attendibile e l'interfaccia di origine appropriata.

```

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

```

Configurazione Ubuntu Syslog Server

Il server Syslog utilizzato in questo documento è un server Ubuntu che esegue rsyslog con il supporto TLS abilitato.

La configurazione del server include le seguenti funzioni:

Attendere le connessioni Syslog protette sulla porta TCP 6514.

Presenta un certificato server TLS durante l'handshake TLS.

Utilizzare una chiave privata associata al certificato del server.

Fornire la catena di certificati richiesta (se applicabile) a Cisco Nexus durante l'handshake TLS.

Messaggi Syslog protetti ricevuti dall'archivio in un file di log locale.

L'implementazione PKI utilizzata in questo documento è costituita da: Certificato server > CA intermedia > CA radice

Lo switch Cisco Nexus importa e considera attendibile il certificato della CA radice tramite un trust point, consentendogli di convalidare la catena di certificati presentata dal server Syslog.



Nota: Una catena di certificati non è obbligatoria per ogni distribuzione. A seconda dell'implementazione PKI, il server Syslog può presentare solo un certificato autofirmato, un certificato server firmato direttamente da una CA radice o un certificato server accompagnato da uno o più certificati CA intermedi.

Risoluzione dei problemi

Obiettivo

L'obiettivo di questa procedura di risoluzione dei problemi è isolare e identificare i guasti che impediscono agli switch Cisco Nexus NX-OS di stabilire una connessione TLS Syslog sicura con un server Syslog.

Il flusso di lavoro convalida ogni fase del processo di comunicazione, iniziando dalla connettività IP e passando attraverso la connettività TCP, la negoziazione TLS, la convalida dei certificati e infine la trasmissione sicura dei messaggi Syslog. Verificando ogni livello in modo indipendente, è possibile determinare rapidamente dove la comunicazione non riesce.

Spiegazione topologia

La topologia utilizzata in questo documento è costituita da uno switch Cisco Nexus configurato come client Secure Syslog e da un server Ubuntu che esegue rsyslog configurato come server Secure Syslog.

Lo switch Cisco Nexus avvia una connessione TCP al server Syslog sulla porta 6514. Dopo aver stabilito la connessione TCP, entrambi i dispositivi eseguono l'handshake TLS. Durante questo processo, il server Syslog presenta il proprio certificato server e tutti i certificati CA intermedi richiesti. Lo switch Nexus convalida la catena di certificati rispetto alla CA radice attendibile configurata nel relativo trust point.

Una volta completato l'handshake TLS, la sessione crittografata viene stabilita e lo switch Nexus inizia a trasmettere i messaggi Secure Syslog al server Syslog.

La metodologia di risoluzione dei problemi illustrata in questo documento utilizza la stessa sequenza di comunicazione utilizzata per stabilire la connessione, consentendo di convalidare in modo indipendente ogni fase del processo.

Passaggio 1. Verificare la configurazione sicura del syslog

Verificare che Secure Syslog sia configurato correttamente sullo switch Cisco Nexus e che lo switch riconosca il server Syslog configurato.

```
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#
```

Passaggio 2. Verificare la configurazione del punto di trust

Verificare che lo switch Cisco Nexus consideri attendibile la CA utilizzata per firmare il certificato del server Syslog.

Verifica:

Il punto di fiducia previsto esiste.

Il certificato CA radice è installato.

Sono presenti tutti i certificati CA intermedi richiesti.

I certificati non sono scaduti.

Le impronte digitali del certificato corrispondono ai valori previsti.

```
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#
```

Se il certificato CA appropriato è mancante o non valido, la convalida del certificato non riesce durante l'handshake TLS.

Passaggio 3. Verifica della connettività IP

Verificare la connettività di layer 3 tra lo switch Cisco Nexus e il server Secure Syslog.

Verifica:

- Raggiungibilità del protocollo ICMP (Internet Control Message Protocol) riuscita.
- Risoluzione DNS (Domain Name System) corretta.
- Nessun problema di routing.
- Nessuna perdita di pacchetti.

```
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#
```

Se la connettività IP non riesce, non è possibile stabilire alcuna connessione TCP.

Passaggio 4. Verifica della connettività TLS

Verificare la connettività TLS end-to-end tra lo switch Cisco Nexus e il server Secure Syslog.

Questo passaggio consente di convalidare più fasi della connessione Syslog sicura, tra cui:

- connettività TCP
- Negoziazione TLS
- Presentazione certificato server
- Catena di certificati
- Convalida certificato
- Negoziazione suite di cifratura

Poiché queste operazioni fanno parte dell'handshake TLS, possono essere verificate tutte con un unico comando.

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

Verifica di questo comando

Convalida	Descrizione
Connettività TCP	Verifica che Nexus possa stabilire una connessione TCP al server Syslog.
Handshake TLS	Conferma che entrambi i peer hanno completato la negoziazione di una

Convalida	Descrizione
	sessione TLS.
Certificato server	Visualizza il certificato presentato dal server Syslog.
Catena di certificati	Visualizza tutti i certificati CA intermedi inviati dal server.
Versione TLS	Mostra la versione TLS negoziata.
Cipher Suite	Visualizza l'algoritmo di crittografia negoziato.
Convalida certificato	Quando si utilizza l'opzione -CAfile, verifica la catena di certificati rispetto alla CA attendibile specificata.

Output previsto riuscito

```
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, email=
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:RSA+SHA384
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 successful
Extended master secret: yes

switch#

Correlazione acquisizione pacchetti

L'output s_client openssl può essere correlato con le acquisizioni dei pacchetti ottenute utilizzando Ethanalzyer per verificare ogni fase dell'handshake TLS.

tcp.stream eq 1									
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=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		

Secure Syslog TLS Handshake Capture

Flusso handshake TLS

```

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 ----->

```

L'handshake TLS deve essere completato correttamente prima che sia possibile scambiare qualsiasi messaggio syslog. Se l'handshake ha esito negativo, il traffico Syslog protetto non viene mai generato.

Per eseguire questa verifica, aprire due sessioni CLI sullo switch Cisco Nexus. Nella prima sessione, avviare la connessione TLS con questo comando:

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

Allo stesso tempo, nella seconda sessione CLI, avviare un'acquisizione di Ethalyzer per monitorare lo scambio TLS:

```

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=4234
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=
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
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 W
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=14
10 2026-07-01 00:55:00.204207757 192.168.100.10 → 192.168.100.1 TCP 1514 6514 → 18553 [ACK] Seq=1449 Ack
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=2
12 2026-07-01 00:55:00.204225215 192.168.100.10 → 192.168.100.1 TLSv1.2 1296 Certificate, Server Key Ex
13 2026-07-01 00:55:00.204234417 192.168.100.1 → 192.168.100.10 TCP 66 18553 → 6514 [ACK] Seq=288 Ack=4
14 2026-07-01 00:55:00.206544194 192.168.100.1 → 192.168.100.10 TLSv1.2 171 Certificate, Client Key Exch
15 2026-07-01 00:55:00.206818190 192.168.100.10 → 192.168.100.1 TLSv1.2 117 Change Cipher Spec, Encrypt
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

```

```
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=61
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=19
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=21
```

L'acquisizione del pacchetto deve visualizzare la sequenza completa dell'handshake TLS, inclusi l'handshake a tre vie TCP, Client Hello, Server Hello, Certificate, Key Exchange, Finished messages e, se l'handshake viene completato correttamente, i record crittografati TLS Application Data che contengono i messaggi Secure Syslog.

Verifica della trasmissione sicura dei messaggi di syslog

Verificare che i messaggi Secure Syslog vengano trasmessi correttamente dallo switch Cisco Nexus al server Syslog dopo aver stabilito la sessione TLS.

Un handshake TLS riuscito conferma che il canale crittografato è stato creato; tuttavia, non garantisce che i messaggi syslog vengano generati o recapitati.

Questo passaggio consente di convalidare l'intero flusso di lavoro Secure Syslog generando un messaggio di prova e confermando la trasmissione e la ricezione del messaggio.

Genera un messaggio di syslog di prova

```
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]
```

Questo comando genera un messaggio syslog locale che deve essere trasmesso al server Secure Syslog configurato tramite la sessione TLS esistente.

Verifica dati applicazione TLS crittografati

Se è già in esecuzione un'acquisizione di Ethernetalyzer (come descritto nella sezione precedente), verificare che i nuovi pacchetti di dati dell'applicazione TLS vengano trasmessi dopo la generazione del messaggio di prova.

```
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=
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=
```

La presenza di dati dell'applicazione TLS indica che i messaggi syslog vengono trasmessi tramite la sessione TLS crittografata. Poiché il payload è crittografato, Ethanalyzer non può decodificare il contenuto del messaggio syslog.



Nota: Al termine dell'handshake TLS, tutti i messaggi syslog vengono incapsulati nei record TLS Application Data crittografati. Il loro contenuto non è visibile nelle acquisizioni dei pacchetti.

Verifica della ricezione dei messaggi sul server Syslog

Sul server Syslog, verificare che il messaggio sia stato ricevuto e scritto correttamente nel file di log di destinazione.

```
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
```

La presenza del messaggio di prova generato conferma che:

- Messaggio syslog generato correttamente dallo switch Cisco Nexus.
- Il messaggio è stato trasmesso tramite la sessione TLS crittografata.
- Il server Syslog ha decrittografato ed elaborato correttamente il messaggio.
- La configurazione Secure Syslog funziona correttamente in modo completo.

La comparsa dei dati dell'applicazione TLS in Ethanalyzer conferma che la sessione TLS sta trasportando attivamente il traffico dell'applicazione crittografato. Tuttavia, la prova definitiva del corretto funzionamento di Secure Syslog è la ricezione del messaggio syslog generato sul server Syslog.

Conclusioni

La protezione del syslog sugli switch Cisco Nexus dipende dalla riuscita della connettività IP e TCP, della negoziazione TLS, della convalida dei certificati e del recapito dei messaggi crittografati. La verifica indipendente di ciascun livello consente di isolare il punto di errore e di distinguere i problemi di connettività, TLS, certificato e trasmissione dei messaggi. Un handshake TLS riuscito conferma che la sessione crittografata è stabilita, mentre la ricezione di un messaggio di prova generato sul server Syslog conferma l'operazione end-to-end Secure Syslog.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).