

Solución de problemas de Secure Syslog en la plataforma Nexus

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Topología](#)

[Antecedentes](#)

[Syslog tradicional](#)

[Syslog seguro](#)

[Cadena de certificados](#)

[¿Por qué se requieren certificados?](#)

[Protocolo de enlace TLS de Syslog seguro](#)

[Configuración relevante](#)

[Configuración de Cisco Nexus](#)

[Configuración del servidor Ubuntu Syslog](#)

[Resolución de problemas](#)

[Objetivo](#)

[Explicación de topología](#)

[Paso 1. Verificar la configuración de Syslog seguro](#)

[Paso 2. Verificar la configuración de Trustpoint](#)

[Paso 3. Verificar la conectividad IP](#)

[Paso 4. Verificar la conectividad TLS](#)

[¿Qué Verifica Este Comando?](#)

[Resultado correcto esperado](#)

[Correlación de captura de paquetes](#)

[Verificar la transmisión segura de mensajes Syslog](#)

[Generar un mensaje de Syslog de prueba](#)

[Verificar datos de la aplicación TLS cifrada](#)

[Verifique la recepción de mensajes en el servidor Syslog](#)

[Conclusión](#)

Introducción

Este documento describe cómo resolver problemas de Secure Syslog sobre Seguridad de la Capa de Transporte (TLS) entre los switches Cisco Nexus y los servidores de terceros.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Plataformas NX-OS
- Syslog seguro
- Conocimiento básico de la infraestructura de clave pública (PKI)

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología



Antecedentes

Syslog tradicional

El Syslog tradicional transmite mensajes de registro a través de UDP (puerto predeterminado 514) o TCP sin cifrado. Dado que la comunicación se envía en texto no cifrado, es posible que los mensajes de registro se intercepten o modifiquen durante el tránsito. El Syslog tradicional tampoco proporciona autenticación de servidor.

Syslog seguro

Secure Syslog utiliza TCP con TLS (puerto predeterminado 6514) para proporcionar transmisión cifrada de mensajes de syslog. Antes de enviar cualquier mensaje de registro, el cliente y el servidor establecen una sesión TLS, durante la cual el servidor presenta su certificado y el cliente valida la cadena de certificados con una autoridad de certificados (CA) de confianza. Una vez que el intercambio de señales TLS se completa con éxito, los mensajes de syslog se transmiten a través del canal cifrado.

A diferencia del Syslog tradicional, Secure Syslog depende no sólo de la conectividad IP, sino también de un intercambio de señales TLS exitoso, validación de certificados y negociación de cifrado antes de que se pueda intercambiar cualquier mensaje de syslog.

Cadena de certificados

Una cadena de certificados es la secuencia de certificados utilizada para establecer la confianza entre el certificado del servidor y una entidad emisora de certificados raíz (CA raíz) de confianza. Durante el intercambio de señales TLS, el servidor Syslog presenta su certificado de servidor junto con cualquier certificado de CA intermedio requerido. El switch Cisco Nexus utiliza su CA raíz de confianza para validar toda la cadena de certificados.

No siempre se requiere una cadena de certificados.

Los certificados presentados por el servidor Syslog dependen de cómo se ha implementado su PKI. Por ejemplo:

Certificado autofirmado: El servidor sólo presenta su propio certificado. En este caso, el switch Cisco Nexus debe confiar directamente en ese certificado autofirmado.

Certificado firmado por CA sin CA intermedias: El servidor presenta sólo su certificado de servidor porque fue firmado directamente por una CA raíz de confianza.

Certificado firmado por CA con CA intermedias: El servidor presenta su certificado de servidor junto con uno o más certificados de CA intermedios, lo que permite al switch Cisco Nexus crear una cadena completa de confianza hasta la CA raíz de confianza.

Independientemente del diseño de PKI, el switch Cisco Nexus debe poder validar el certificado presentado por el servidor antes de poder establecer la sesión TLS.

Si falta algún certificado necesario en la cadena de confianza, éste no es válido, ha caducado o lo ha emitido una CA que no es de confianza, el intercambio de señales TLS falla y no se puede establecer la conexión de Syslog seguro.

¿Por qué se requieren certificados?

Secure Syslog se basa en TLS para proporcionar cifrado y autenticación del servidor. Antes de transmitir cualquier mensaje de syslog, el switch Cisco Nexus debe verificar que se está comunicando con el servidor Syslog deseado y no con un dispositivo no autorizado.

Los certificados proporcionan esta confianza al permitir que el switch Nexus autentique la identidad del servidor Syslog antes de establecer la sesión cifrada. Una vez validada correctamente la cadena de certificados, se crea un canal TLS seguro y todos los mensajes syslog subsiguientes se transmiten a través de la conexión cifrada.

Sin un certificado válido y una cadena de certificados de confianza, Secure Syslog no puede establecer la sesión TLS, lo que impide que los mensajes de registro se intercambien de forma segura.

Protocolo de enlace TLS de Syslog seguro

Antes de transmitir cualquier mensaje de syslog, el switch Cisco Nexus y el servidor Syslog deben establecer correctamente una sesión TLS. Durante el intercambio de señales de TLS, ambos dispositivos negocian los parámetros de TLS, establecen una clave de cifrado compartida y autentican la identidad del servidor Syslog a través de la validación de certificados.

Los mensajes de syslog se transmiten a través de la conexión cifrada sólo después de que el intercambio de señales TLS se haya completado correctamente.

El intercambio de señales TLS consta de estas fases:

Paso	Descripción
1. Conexión TCP	El switch Cisco Nexus establece una conexión TCP con el servidor Secure Syslog (puerto predeterminado 6514).
2. Saludo del cliente	Nexus inicia el intercambio de señales de TLS enviando las versiones de TLS compatibles, conjuntos de cifrado y valores aleatorios.

Paso	Descripción
3. Saludo del servidor	El servidor Syslog selecciona la versión de TLS y el conjunto de cifrado utilizado para la sesión.
4. Intercambio de certificados	El servidor Syslog presenta su certificado de servidor y, si es necesario, cualquier certificado de CA intermedio.
5. Validación de certificados	Nexus valida el certificado de servidor con la CA de confianza configurada. La validación incluye la comprobación de la cadena de certificados, las fechas de caducidad, el emisor y la identidad del servidor mediante el nombre común (CN) y el nombre alternativo del sujeto (SAN).
6. Intercambio de claves	Ambos pares intercambian información criptográfica para derivar las claves de sesión compartidas utilizadas para el cifrado.
7. Mensajes finalizados	Cada par comprueba que el protocolo de enlace se completó correctamente y que ambos extremos derivaron las mismas claves criptográficas.
8. Transmisión segura de Syslog	Una vez establecida la sesión TLS, los mensajes de syslog se transmiten como registros cifrados de datos de la aplicación TLS.

Configuración relevante

Configuración de Cisco Nexus

El switch Cisco Nexus debe configurarse con el destino Secure Syslog, un punto de confianza que contenga la CA de confianza y la interfaz de origen adecuada.

```
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
```

Configuración del servidor Ubuntu Syslog

El servidor Syslog utilizado en este documento es un servidor Ubuntu que ejecuta rsyslog con la compatibilidad con TLS habilitada.

La configuración del servidor incluye estas funciones:

Espere conexiones de Syslog seguras en el puerto TCP 6514.

Presente un certificado de servidor TLS durante el intercambio de señales TLS.

Utilice una clave privada asociada al certificado del servidor.

Proporcione la cadena de certificados necesaria (cuando corresponda) a Cisco Nexus durante el intercambio de señales TLS.

Almacenar los mensajes recibidos de Syslog seguro en un archivo de registro local.

La implementación PKI utilizada en este documento consiste en: Certificado de servidor > CA intermedia > CA raíz

El switch Cisco Nexus importa y confía en el certificado de CA raíz a través de un punto de confianza, lo que le permite validar la cadena de certificados presentada por el servidor Syslog.



Nota: Una cadena de certificados no es obligatoria para cada implementación. Según la implementación de PKI, el servidor Syslog sólo puede presentar un certificado autofirmado, un certificado de servidor firmado directamente por una CA raíz o un certificado de servidor acompañado de uno o más certificados de CA intermedios.

Resolución de problemas

Objetivo

El objetivo de este procedimiento de solución de problemas es aislar e identificar los fallos que impiden que los switches Cisco Nexus NX-OS establezcan correctamente una conexión TLS de Syslog seguro con un servidor Syslog.

El flujo de trabajo valida cada etapa del proceso de comunicación, comenzando con la

conectividad IP y avanzando a través de la conectividad TCP, la negociación TLS, la validación de certificados y, finalmente, la transmisión segura de mensajes de Syslog. Mediante la verificación independiente de cada capa, es posible determinar rápidamente dónde falla la comunicación.

Explicación de topología

La topología utilizada en este documento consiste en un switch Cisco Nexus configurado como el cliente Secure Syslog y un servidor Ubuntu que ejecuta rsyslog configurado como el servidor Secure Syslog.

El switch Cisco Nexus inicia una conexión TCP con el servidor Syslog en el puerto 6514. Una vez establecida la conexión TCP, ambos dispositivos realizan el intercambio de señales TLS. Durante este proceso, el servidor Syslog presenta su certificado de servidor y cualquier certificado de CA intermedio requerido. El switch Nexus valida la cadena de certificados frente a la CA raíz de confianza configurada en su punto de confianza.

Una vez que el intercambio de señales TLS se completa correctamente, se establece la sesión cifrada y el switch Nexus comienza a transmitir mensajes de Syslog seguro al servidor Syslog.

La metodología de solución de problemas presentada en este documento utiliza la misma secuencia de comunicación que el establecimiento de conexión, lo que permite que cada fase del proceso se valide de forma independiente.

Paso 1. Verificar la configuración de Syslog seguro

Verifique que Secure Syslog esté correctamente configurado en el switch Cisco Nexus y que el switch reconozca el servidor Syslog configurado.

```
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#
```

Paso 2. Verificar la configuración de Trustpoint

Verifique que el switch Cisco Nexus confíe en la CA utilizada para firmar el certificado del servidor Syslog.

Controle lo siguiente:

El Trustpoint esperado existe.

El certificado de CA raíz está instalado.

Todos los certificados CA intermedios requeridos están presentes.

Los certificados no han caducado.

Las huellas digitales del certificado coinciden con los valores esperados.

```
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#
```

Si falta el certificado de CA apropiado o éste no es válido, la validación del certificado falla durante el intercambio de señales TLS.

Paso 3. Verificar la conectividad IP

Verifique la conectividad de capa 3 entre el switch Cisco Nexus y el servidor Secure Syslog.

Controle lo siguiente:

- Alcance correcto del protocolo de mensajes de control de Internet (ICMP).
- Resolución correcta del sistema de nombres de dominio (DNS).
- Sin problemas de ruteo.
- Sin pérdida de paquetes.

```
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#
```

Si falla la conectividad IP, no se puede establecer ninguna conexión TCP.

Paso 4. Verificar la conectividad TLS

Verifique la conectividad TLS de extremo a extremo entre el switch Cisco Nexus y el servidor Secure Syslog.

Este paso valida varias etapas de la conexión Syslog segura, incluidas:

- conectividad TCP
- negociación TLS
- Presentación del certificado de servidor
- Cadena de certificados
- Validación del certificado
- Negociación de conjunto de cifrado

Debido a que estas operaciones ocurren como parte del intercambio de señales TLS, todas se pueden verificar con un solo comando.

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

¿Qué Verifica Este Comando?

Validación	Descripción
Conectividad TCP	Comprueba que Nexus puede establecer una conexión TCP con el servidor Syslog.
Protocolo de enlace TLS	Confirma que ambos peers negociaron satisfactoriamente una sesión TLS.
Certificado de servidor	Muestra el certificado presentado por el servidor Syslog.
Cadena de certificados	Muestra los certificados de CA intermedios enviados por el servidor.
Versión de TLS	Muestra la versión de TLS negociada.
Cipher Suite	Muestra el algoritmo de cifrado negociado.
Validación de certificados	Cuando se utiliza la opción <code>-CAfile</code> , verifica la cadena de certificados con respecto a la CA de confianza especificada.

Resultado correcto esperado

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

```

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#

```

Correlación de captura de paquetes

El resultado de openssl s_client se puede correlacionar con las capturas de paquetes obtenidas mediante Ethalyzer para verificar cada fase del intercambio de señales TLS.

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=1 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=1849 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

Captura de intercambio de señales TLS de Syslog seguro

Flujo de intercambio de señales 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 ----->
```

El intercambio de señales TLS debe completarse correctamente antes de que se pueda intercambiar cualquier mensaje de syslog. Si el intercambio de señales falla, el tráfico de Syslog seguro nunca se genera.

Para realizar esta verificación, abra dos sesiones CLI en el switch Cisco Nexus. En la primera sesión, inicie la conexión TLS con este comando:

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

Al mismo tiempo, en la segunda sesión de CLI, inicie una captura de Ethalyzer para monitorear el intercambio TLS:

```
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=64
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=0 Len=0
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 Win=65536 Len=0
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=0 Len=0
12 2026-07-01 00:55:00.204225215 192.168.100.10 → 192.168.100.1 TLSv1.2 1296 Certificate, Server Key Exchange, Server Hello Done
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=0 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, Client Hello Done
15 2026-07-01 00:55:00.206818190 192.168.100.10 → 192.168.100.1 TLSv1.2 117 Change Cipher Spec, Encrypted Handshake Message
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=0 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=0 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=0 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=0 Len=0

```

La captura de paquetes debe mostrar la secuencia de intercambio de señales TLS completa, incluidos el intercambio de señales de tres vías TCP, el saludo del cliente, el saludo del servidor, el certificado, el intercambio de claves, los mensajes finalizados y, si el intercambio de señales se completa correctamente, los registros de datos de la aplicación TLS cifrados que llevan los mensajes de Syslog seguro.

Verificar la transmisión segura de mensajes Syslog

Verifique que los mensajes de Syslog seguro se transmitan correctamente desde el switch Cisco Nexus al servidor Syslog después de que se haya establecido la sesión TLS.

Un intercambio de señales TLS exitoso confirma que se ha creado el canal cifrado; sin embargo, no garantiza que los mensajes syslog se estén generando o entregando.

Este paso valida el flujo de trabajo completo de Secure Syslog mediante la generación de un mensaje de prueba y la confirmación de su transmisión y recepción.

Generar un mensaje de Syslog de prueba

```

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]

```

Este comando genera un mensaje syslog local que debe transmitirse al servidor Syslog seguro configurado a través de la sesión TLS existente.

Verificar datos de la aplicación TLS cifrada

Si ya se está ejecutando una captura de Ethalyzer (como se describe en la sección anterior), verifique que los nuevos paquetes de datos de la aplicación TLS se transmitan después de que se genere el mensaje de prueba.

```
switch# ethalyzer 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
```

La presencia de datos de la aplicación TLS indica que los mensajes de syslog se transmiten a través de la sesión TLS cifrada. Debido a que la carga está cifrada, Ethalyzer no puede decodificar el contenido del mensaje syslog.



Nota: Una vez que el intercambio de señales TLS se completa correctamente, todos los mensajes de syslog se encapsulan dentro de los registros cifrados de datos de la aplicación TLS. Su contenido no es visible en las capturas de paquetes.

Verifique la recepción de mensajes en el servidor Syslog

En el servidor Syslog, compruebe que el mensaje se ha recibido y escrito correctamente en el archivo de registro de destino.

```
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 presencia del mensaje de prueba generado confirma que:

El switch Cisco Nexus generó correctamente el mensaje de syslog.

El mensaje se transmitió a través de la sesión TLS cifrada.

El servidor Syslog descifró y procesó correctamente el mensaje.

La configuración de Secure Syslog funciona correctamente de extremo a extremo.

La aparición de los datos de la aplicación TLS en Ethalyzer confirma que la sesión TLS transporta de forma activa tráfico de aplicaciones cifrado. Sin embargo, la prueba definitiva de que Secure Syslog funciona correctamente es la recepción correcta del mensaje syslog generado en el servidor Syslog.

Conclusión

Secure Syslog en switches Cisco Nexus depende de una conectividad IP y TCP satisfactoria, la negociación TLS, la validación de certificados y la entrega de mensajes cifrados. La verificación independiente de cada capa ayuda a aislar el punto de fallo y a distinguir los problemas de conectividad, TLS, certificados y transmisión de mensajes. Un intercambio de señales TLS exitoso confirma que la sesión cifrada está establecida, mientras que la recepción de un mensaje de prueba generado en el servidor Syslog confirma la operación de registro del sistema seguro de extremo a extremo.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).