

Solucionar problemas do Syslog seguro na plataforma Nexus

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia](#)

[Informações de Apoio](#)

[Syslog tradicional](#)

[Syslog seguro](#)

[Cadeia de Certificados](#)

[Por que os certificados são necessários?](#)

[Handshake TLS de Syslog seguro](#)

[Configuração relevante](#)

[Configuração do Cisco Nexus](#)

[Configuração do servidor Ubuntu Syslog](#)

[Troubleshooting](#)

[Objetivo](#)

[Explicação de Topologia](#)

[Etapa 1. Verificar a configuração segura do Syslog](#)

[Etapa 2. Verificar a Configuração do Ponto de Confiança](#)

[Etapa 3. Verificar a Conectividade IP](#)

[Etapa 4. Verificar a conectividade TLS](#)

[O que este comando verifica](#)

[Saída Bem-sucedida Esperada](#)

[Correlação de captura de pacote](#)

[Verificar a transmissão segura de mensagens do Syslog](#)

[Gerar uma mensagem de Syslog de teste](#)

[Verificar dados criptografados do aplicativo TLS](#)

[Verifique a recepção de mensagens no Servidor Syslog](#)

[Conclusão](#)

Introdução

Este documento descreve como solucionar problemas do Secure Syslog over Transport Layer Security (TLS) entre switches Cisco Nexus e servidores de terceiros.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Plataformas NX-OS
- Syslog seguro
- Conhecimento básico de infraestrutura de chave pública (PKI)

Componentes Utilizados

N9K1	N9K-C933C-FX2	10.4(7)
Servidor Syslog	Servidor Ubuntu	rsyslog 8.2112 OpenSSL 3.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia



Informações de Apoio

Syslog tradicional

O Syslog tradicional transmite mensagens de log por UDP (porta padrão 514) ou TCP sem criptografia. Como a comunicação é enviada em texto não criptografado, as mensagens de log podem ser potencialmente interceptadas ou modificadas enquanto estão em trânsito. O Syslog tradicional também não fornece autenticação de servidor.

Syslog seguro

O Secure Syslog usa TCP com TLS (porta padrão 6514) para fornecer transmissão criptografada de mensagens de syslog. Antes que qualquer mensagem de log seja enviada, o cliente e o servidor estabelecem uma sessão TLS, durante a qual o servidor apresenta seu certificado e o cliente valida a cadeia de certificados em relação a uma CA (Autoridade de Certificação) confiável. Quando o handshake TLS é concluído com êxito, as mensagens de syslog são transmitidas pelo canal criptografado.

Diferentemente do Syslog tradicional, o Syslog seguro depende não apenas da conectividade IP, mas também de um handshake TLS bem-sucedido, da validação de certificados e da negociação de cifras antes que qualquer mensagem de syslog possa ser trocada.

Cadeia de Certificados

Uma cadeia de certificados é a sequência de certificados usada para estabelecer confiança entre o certificado do servidor e uma Autoridade de Certificação Raiz (CA Raiz) confiável. Durante o handshake TLS, o servidor Syslog apresenta seu certificado de servidor junto com todos os certificados de CA intermediários necessários. O switch Cisco Nexus usa sua CA raiz confiável para validar toda a cadeia de certificados.

Nem sempre é necessária uma cadeia de certificados.

Os certificados apresentados pelo servidor Syslog dependem de como sua PKI foi implementada. Por exemplo:

Certificado autoassinado: O servidor apresenta apenas seu próprio certificado. Nesse caso, o switch Cisco Nexus deve confiar diretamente nesse certificado autoassinado.

Certificado assinado pela autoridade de certificação sem autoridades de certificação intermediárias: O servidor apresenta apenas seu certificado de servidor porque foi assinado diretamente por uma CA raiz confiável.

Certificado assinado pela autoridade de certificação com autoridades de certificação intermediárias: O servidor apresenta seu certificado de servidor junto com um ou mais certificados CA intermediários, permitindo que o switch Cisco Nexus crie uma cadeia completa de confiança até a CA raiz confiável.

Independentemente do projeto de PKI, o switch Cisco Nexus deve ser capaz de validar o certificado apresentado pelo servidor antes que a sessão TLS possa ser estabelecida.

Se algum certificado necessário na cadeia de confiança estiver ausente, for inválido, tiver expirado ou tiver sido emitido por uma CA não confiável, o handshake TLS falhará e a conexão Syslog Segura não poderá ser estabelecida.

Por que os certificados são necessários?

O Secure Syslog depende do TLS para fornecer criptografia e autenticação de servidor. Antes que qualquer mensagem de syslog seja transmitida, o switch Cisco Nexus deve verificar se está se comunicando com o servidor Syslog desejado e não com um dispositivo não autorizado.

Os certificados fornecem essa confiança permitindo que o switch Nexus autentique a identidade do servidor Syslog antes de estabelecer a sessão criptografada. Depois que a cadeia de certificados tiver sido validada com êxito, um canal TLS seguro será criado e todas as mensagens de syslog subsequentes serão transmitidas por meio da conexão criptografada.

Sem um certificado válido e uma cadeia de certificados confiáveis, o Secure Syslog não pode estabelecer a sessão TLS, evitando que as mensagens de log sejam trocadas com segurança.

Handshake TLS de Syslog seguro

Antes que qualquer mensagem de syslog seja transmitida, o switch Cisco Nexus e o servidor Syslog devem estabelecer com êxito uma sessão TLS. Durante o handshake TLS, ambos os dispositivos negociam os parâmetros TLS, estabelecem uma chave de criptografia compartilhada e autenticam a identidade do servidor Syslog através da validação do certificado.

Somente depois que o handshake TLS é concluído com êxito é que as mensagens de syslog são transmitidas por meio da conexão criptografada.

O handshake TLS consiste nestas fases:

Etapa	Descrição
1. Conexão TCP	O switch Cisco Nexus estabelece uma conexão TCP com o servidor Secure Syslog (porta padrão 6514).
2. Hello do cliente	O Nexus inicia o handshake TLS enviando as versões TLS, conjuntos de cifras

Etapa	Descrição
	e valores aleatórios suportados.
3. Saudação do servidor	O servidor Syslog seleciona a versão TLS e o conjunto de cifras usados para a sessão.
4. Intercâmbio de certificados	O Servidor Syslog apresenta seu certificado de servidor e, se necessário, quaisquer certificados CA intermediários.
5. Validação do certificado	O Nexus valida o certificado do servidor em relação à CA confiável configurada. A validação inclui a verificação da cadeia de certificados, datas de expiração, emissor e identidade do servidor por meio de Nome comum (CN) e Nome alternativo do assunto (SAN).
6. Intercâmbio de chaves	Ambos os peers trocam informações criptográficas para derivar as chaves de sessão compartilhadas usadas para criptografia.
7. Mensagens concluídas	Cada peer verifica se o handshake foi concluído com êxito e se ambos os lados derivaram as mesmas chaves criptográficas.
8. Transmissão Segura de Syslog	Quando a sessão TLS é estabelecida, as mensagens do syslog são transmitidas como registros criptografados de dados de aplicativos TLS.

Configuração relevante

Configuração do Cisco Nexus

O switch Cisco Nexus deve ser configurado com o destino Secure Syslog, um ponto confiável que contenha a CA confiável e a interface de origem apropriada.

```
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
```

Configuração do servidor Ubuntu Syslog

O servidor Syslog usado neste documento é um servidor Ubuntu executando rsyslog com suporte TLS habilitado.

A configuração do servidor inclui estas funções:

Escute as conexões Syslog seguras na porta TCP 6514.

Apresente um certificado de servidor TLS durante o handshake TLS.

Use uma chave privada associada ao certificado do servidor.

Fornecer a cadeia de certificados necessária (quando aplicável) ao Cisco Nexus durante o handshake TLS.

O armazenamento recebeu mensagens de Syslog Seguro em um arquivo de log local.

A implementação da PKI usada neste documento consiste em: Certificado do servidor > CA intermediária > CA raiz

O switch Cisco Nexus importa e confia no certificado de CA raiz por meio de um ponto de confiança, permitindo que ele valide a cadeia de certificados apresentada pelo servidor Syslog.



Note: Uma cadeia de certificados não é obrigatória para cada implantação. Dependendo da implementação de PKI, o servidor Syslog pode apresentar apenas um certificado autoassinado, um certificado de servidor assinado diretamente por uma CA raiz ou um certificado de servidor acompanhado por um ou mais certificados de CA intermediários.

Troubleshooting

Objetivo

O objetivo deste procedimento de solução de problemas é isolar e identificar falhas que impedem que os switches Cisco Nexus NX-OS estabeleçam com êxito uma conexão TLS de Syslog Seguro com um servidor Syslog.

O fluxo de trabalho valida cada estágio do processo de comunicação, começando com a conectividade IP e progredindo através da conectividade TCP, negociação TLS, validação de certificado e, finalmente, transmissão segura de mensagens Syslog. Verificando cada camada de forma independente, é possível determinar rapidamente onde a comunicação falha.

Explicação de Topologia

A topologia usada neste documento consiste em um switch Cisco Nexus configurado como o cliente Secure Syslog e um servidor Ubuntu executando o rsyslog configurado como o servidor Secure Syslog.

O switch Cisco Nexus inicia uma conexão TCP com o servidor Syslog na porta 6514. Depois que a conexão TCP é estabelecida, ambos os dispositivos executam o handshake TLS. Durante esse processo, o servidor Syslog apresenta seu certificado de servidor e todos os certificados de CA intermediários necessários. O switch Nexus valida a cadeia de certificados em relação à CA raiz confiável configurada em seu ponto de confiança.

Quando o handshake TLS for concluído com êxito, a sessão criptografada será estabelecida e o switch Nexus começará a transmitir mensagens de Syslog seguras ao servidor Syslog.

A metodologia de identificação e solução de problemas apresentada neste documento usa a mesma sequência de comunicação que o estabelecimento da conexão, permitindo que cada fase do processo seja validada independentemente.

Etapa 1. Verificar a configuração segura do Syslog

Verifique se o Secure Syslog está configurado corretamente no switch Cisco Nexus e se o switch reconhece o 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#
```

Etapa 2. Verificar a Configuração do Ponto de Confiança

Verifique se o switch Cisco Nexus confia na CA usada para assinar o certificado do servidor Syslog.

Verifique:

O ponto de confiança esperado existe.

O certificado CA raiz está instalado.

Todos os certificados de Autoridade de Certificação Intermediária necessários estão presentes.

Os certificados não expiraram.

As impressões digitais do certificado correspondem aos 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#
```

Se o certificado CA apropriado estiver faltando ou for inválido, a validação do certificado falhará durante o handshake TLS.

Etapa 3. Verificar a Conectividade IP

Verifique a conectividade da camada 3 entre o switch Cisco Nexus e o servidor Secure Syslog.

Verifique:

- Êxito na acessibilidade do Internet Control Message Protocol (ICMP).
- Corrija a resolução do Sistema de Nomes de Domínio (DNS).
- Sem problemas de roteamento.
- Sem perda de pacotes.

```
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 a conectividade IP falhar, nenhuma conexão TCP pode ser estabelecida.

Etapa 4. Verificar a conectividade TLS

Verifique a conectividade TLS de ponta a ponta entre o switch Cisco Nexus e o servidor Secure Syslog.

Esta etapa valida várias etapas da conexão Syslog Segura, incluindo:

- conectividade TCP
- negociação TLS
- Apresentação do certificado do servidor
- Cadeia de certificados
- Validação de certificado
- Negociação do conjunto de cifras

Como essas operações ocorrem como parte do handshake TLS, todas elas podem ser verificadas com um único comando.

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

O que este comando verifica

Validação	Descrição
Conectividade TCP	Verifica se o Nexus pode estabelecer uma conexão TCP com o servidor Syslog.
Handshake TLS	Confirma que os dois pares negociam com êxito uma sessão TLS.
Server Certificate	Exibe o certificado apresentado pelo servidor Syslog.
Cadeia de Certificados	Exibe todos os certificados CA intermediários enviados pelo servidor.
Versão TLS	Mostra a versão TLS negociada.
Conjunto de Cifras	Exibe o algoritmo de criptografia negociado.
Validação de certificado	Quando a opção <code>-CAfile</code> é usada, verifica a cadeia de certificados em relação à CA confiável especificada.

Saída Bem-sucedida Esperada

```
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
---
```

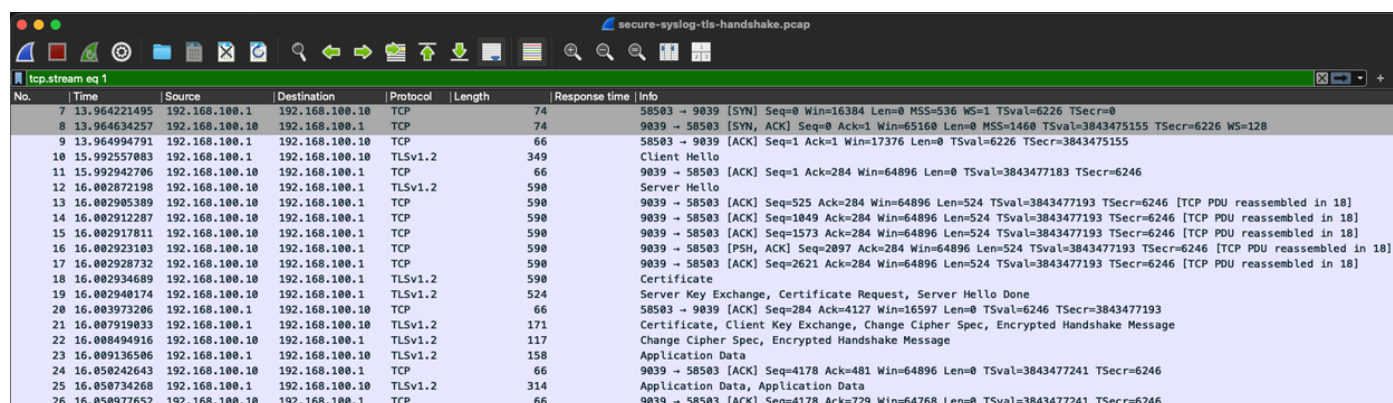
```

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#

```

Correlação de captura de pacote

A saída de openssl s_client pode ser correlacionada com capturas de pacotes obtidas usando o Ethalyzer para verificar cada fase do handshake 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=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, 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 handshake TLS de syslog seguro

Fluxo de 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 ----->
```

O handshake TLS deve ser concluído com êxito antes que qualquer mensagem de syslog possa ser trocada. Se o handshake falhar, o tráfego Syslog seguro nunca é gerado.

Para realizar essa verificação, abra duas sessões CLI no switch Cisco Nexus. Na primeira sessão, inicie a conexão TLS com este comando:

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

Ao mesmo tempo, na segunda sessão da CLI, inicie uma captura do Ethalyzer para monitorar a troca de 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=
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

```

A captura de pacotes deve exibir a sequência completa de handshake TLS, incluindo o handshake triplo do TCP, o Hello do cliente, o Hello do servidor, o certificado, a troca de chaves, as mensagens concluídas e, se o handshake for concluído com êxito, os registros criptografados dos dados do aplicativo TLS que transportam as mensagens Syslog seguras.

Verificar a transmissão segura de mensagens do Syslog

Verifique se as mensagens de Syslog seguras são transmitidas com êxito do switch Cisco Nexus para o servidor Syslog após o estabelecimento da sessão TLS.

Um handshake TLS bem-sucedido confirma que o canal criptografado foi criado; no entanto, ele não garante que as mensagens de syslog estejam sendo geradas ou entregues.

Esta etapa valida o fluxo de trabalho completo do Secure Syslog gerando uma mensagem de teste e confirmando sua transmissão e recepção.

Gerar uma mensagem de Syslog de teste

```

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]

```

Esse comando gera uma mensagem de syslog local que deve ser transmitida ao servidor Syslog seguro configurado pela sessão TLS existente.

Verificar dados criptografados do aplicativo TLS

Se uma captura do Ethalyzer já estiver em execução (conforme descrito na seção anterior), verifique se os novos pacotes de dados do aplicativo TLS são transmitidos após a geração da mensagem de teste.

```
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
```

A presença de dados de aplicativos TLS indica que as mensagens de syslog estão sendo transmitidas por meio da sessão TLS criptografada. Como o payload é criptografado, o Ethalyzer não pode decodificar o conteúdo da mensagem de syslog.



Note: Após a conclusão bem-sucedida do handshake TLS, todas as mensagens de syslog são encapsuladas em registros criptografados de dados de aplicativos TLS. Seu conteúdo não é visível em capturas de pacotes.

Verifique a recepção de mensagens no Servidor Syslog

No servidor Syslog, verifique se a mensagem foi recebida com êxito e gravada no arquivo de log 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
```

A presença da mensagem de teste gerada confirma que:

O switch Cisco Nexus gerou com êxito a mensagem do syslog.

A mensagem foi transmitida pela sessão TLS criptografada.

O servidor Syslog descriptografou e processou a mensagem com êxito.

A configuração do Syslog Seguro está operando corretamente de ponta a ponta.

A aparência dos Dados de aplicativos TLS no Ethalyzer confirma que a sessão TLS está transportando ativamente o tráfego de aplicativos criptografados. No entanto, a prova definitiva de que o Syslog seguro está funcionando corretamente é a recepção bem-sucedida da mensagem

de syslog gerada no servidor Syslog.

Conclusão

O Syslog seguro em switches Cisco Nexus depende da conectividade IP e TCP bem-sucedida, da negociação TLS, da validação de certificados e da entrega de mensagens criptografadas. A verificação de cada camada de forma independente ajuda a isolar o ponto de falha e a distinguir problemas de conectividade, TLS, certificado e transmissão de mensagens. Um handshake TLS bem-sucedido confirma que a sessão criptografada está estabelecida, enquanto a recepção de uma mensagem de teste gerada no servidor Syslog confirma a operação Secure Syslog de ponta a ponta.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.