

Dépannage de Secure Syslog sur la plate-forme Nexus

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Topologie](#)

[Informations générales](#)

[Syslog traditionnel](#)

[Syslog sécurisé](#)

[Chaîne De Certificats](#)

[Pourquoi les certificats sont-ils requis ?](#)

[Connexion TLS Syslog sécurisée](#)

[Configuration appropriée](#)

[Configuration de Cisco Nexus](#)

[Configuration du serveur Syslog Ubuntu](#)

[Dépannage](#)

[Objectif](#)

[Explication de topologie](#)

[Étape 1 : vérification de la configuration Syslog sécurisée](#)

[Étape 2 : vérification de la configuration Trustpoint](#)

[Étape 3 : vérification de la connectivité IP](#)

[Étape 4. Vérification de la connectivité TLS](#)

[Que vérifie cette commande ?](#)

[Sortie réussie attendue](#)

[Corrélation de capture de paquets](#)

[Vérification de la transmission sécurisée des messages Syslog](#)

[Générer un message Syslog de test](#)

[Vérification des données d'application TLS chiffrées](#)

[Vérification de la réception des messages sur le serveur Syslog](#)

[Conclusion](#)

Introduction

Ce document décrit comment dépanner Secure Syslog sur Transport Layer Security (TLS) entre les commutateurs Cisco Nexus et les serveurs tiers.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Plates-formes NX-OS
- Syslog sécurisé
- Connaissances de base sur l'infrastructure à clé publique (PKI)

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie



Informations générales

Syslog traditionnel

Le Syslog traditionnel transmet les messages de journal via UDP (port par défaut 514) ou TCP sans cryptage. Puisque la communication est envoyée en texte clair, les messages de journal peuvent potentiellement être interceptés ou modifiés pendant le transit. Le Syslog traditionnel ne fournit pas non plus d'authentification serveur.

Syslog sécurisé

Secure Syslog utilise TCP avec TLS (port par défaut 6514) afin de fournir une transmission chiffrée des messages Syslog. Avant l'envoi d'un message de journal, le client et le serveur établissent une session TLS, au cours de laquelle le serveur présente son certificat et le client valide la chaîne de certificats par rapport à une autorité de certification (CA) approuvée. Une fois la connexion TLS terminée, les messages syslog sont transmis via le canal chiffré.

Contrairement au Syslog traditionnel, le Syslog sécurisé dépend non seulement de la connectivité IP, mais aussi d'une connexion TLS réussie, de la validation du certificat et de la négociation du chiffrement avant qu'un message Syslog puisse être échangé.

Chaîne De Certificats

Une chaîne de certificats est la séquence de certificats utilisée afin d'établir la confiance entre le certificat du serveur et une autorité de certification racine (CA racine) de confiance. Au cours de la connexion TLS, le serveur Syslog présente son certificat de serveur ainsi que tous les certificats d'autorité de certification intermédiaires requis. Le commutateur Cisco Nexus utilise son autorité de certification racine de confiance pour valider l'ensemble de la chaîne de certificats.

Une chaîne de certificats n'est pas toujours requise.

Les certificats présentés par le serveur Syslog dépendent de la façon dont son PKI a été implémenté. Exemple :

Certificat auto-signé : Le serveur présente uniquement son propre certificat. Dans ce cas, le commutateur Cisco Nexus doit approuver directement ce certificat auto-signé.

Certificat signé par une autorité de certification sans AC intermédiaire : Le serveur présente uniquement son certificat de serveur, car il a été signé directement par une autorité de certification racine approuvée.

Certificat signé par une autorité de certification avec des autorités de certification intermédiaires : Le serveur présente son certificat de serveur avec un ou plusieurs certificats d'autorité de certification intermédiaires, ce qui permet au commutateur Cisco Nexus d'établir une chaîne complète de confiance jusqu'à l'autorité de certification racine de confiance.

Quelle que soit la conception PKI, le commutateur Cisco Nexus doit être en mesure de valider le

certificat présenté par le serveur avant que la session TLS puisse être établie.

Si un certificat requis dans la chaîne d'approbation est manquant, non valide, expiré ou émis par une autorité de certification non approuvée, la connexion TLS échoue et la connexion Syslog sécurisée ne peut pas être établie.

Pourquoi les certificats sont-ils requis ?

Secure Syslog s'appuie sur TLS pour fournir le chiffrement et l'authentification du serveur. Avant de transmettre un message Syslog, le commutateur Cisco Nexus doit vérifier qu'il communique avec le serveur Syslog prévu et non avec un périphérique non autorisé.

Les certificats fournissent cette confiance en permettant au commutateur Nexus d'authentifier l'identité du serveur Syslog avant d'établir la session chiffrée. Une fois la chaîne de certificats validée, un canal TLS sécurisé est créé et tous les messages syslog suivants sont transmis via la connexion chiffrée.

Sans certificat valide et sans chaîne de certificats approuvée, Secure Syslog ne peut pas établir la session TLS, ce qui empêche l'échange sécurisé des messages de journal.

Connexion TLS Syslog sécurisée

Avant de transmettre un message Syslog, le commutateur Cisco Nexus et le serveur Syslog doivent établir une session TLS. Au cours de la connexion TLS, les deux périphériques négocient les paramètres TLS, établissent une clé de cryptage partagée et authentifient l'identité du serveur Syslog via la validation du certificat.

Les messages syslog transmis via la connexion chiffrée ne sont transmis qu'une fois la connexion TLS établie.

La connexion TLS se compose des phases suivantes :

Étape	Description
1. Connexion TCP	Le commutateur Cisco Nexus établit une connexion TCP au serveur Secure Syslog (port par défaut 6514).
2. Client Hello	Le Nexus initie la connexion TLS en envoyant les versions TLS prises en charge, les suites de chiffrement et les valeurs aléatoires.

Étape	Description
3. Hello du serveur	Le serveur Syslog sélectionne la version TLS et la suite de chiffrement utilisées pour la session.
4. Échange de certificats	Le serveur Syslog présente son certificat de serveur et, si nécessaire, les certificats d'autorité de certification intermédiaires.
5. Validation du certificat	Le Nexus valide le certificat du serveur par rapport à l'autorité de certification approuvée configurée. La validation inclut la vérification de la chaîne de certificats, des dates d'expiration, de l'émetteur et de l'identité du serveur via le nom commun (CN) et le nom alternatif du sujet (SAN).
6. Échange de clés	Les deux homologues échangent des informations de chiffrement afin de dériver les clés de session partagées utilisées pour le chiffrement.
7. Messages terminés	Chaque homologue vérifie que la connexion s'est terminée correctement et que les deux côtés ont dérivé les mêmes clés cryptographiques.
8. Transmission Syslog sécurisée	Une fois la session TLS établie, les messages syslog sont transmis sous forme d'enregistrements chiffrés de données d'application TLS.

Configuration appropriée

Configuration de Cisco Nexus

Le commutateur Cisco Nexus doit être configuré avec la destination Syslog sécurisée, un point de confiance contenant l'autorité de certification approuvée et l'interface source appropriée.

```
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
```

Configuration du serveur Syslog Ubuntu

Le serveur Syslog utilisé dans ce document est un serveur Ubuntu exécutant rsyslog avec la prise en charge TLS activée.

La configuration du serveur inclut les fonctions suivantes :

Écoutez les connexions Syslog sécurisées sur le port TCP 6514.

Présenter un certificat de serveur TLS lors de la connexion TLS.

Utilisez une clé privée associée au certificat du serveur.

Fournir la chaîne de certificats requise (le cas échéant) à Cisco Nexus lors de la connexion TLS.

Stocker les messages Syslog sécurisés reçus dans un fichier journal local.

L'implémentation PKI utilisée dans ce document se compose de : Server Certificate > Intermediate CA > Root CA

Le commutateur Cisco Nexus importe et approuve le certificat CA racine via un point de confiance, ce qui lui permet de valider la chaîne de certificats présentée par le serveur Syslog.



Remarque : Une chaîne de certificats n'est pas obligatoire pour chaque déploiement. Selon l'implémentation de l'ICP, le serveur Syslog peut présenter uniquement un certificat auto-signé, un certificat de serveur signé directement par une autorité de certification racine ou un certificat de serveur accompagné d'un ou plusieurs certificats d'autorité de certification intermédiaires.

Dépannage

Objectif

L'objectif de cette procédure de dépannage est d'isoler et d'identifier les pannes qui empêchent les commutateurs Cisco Nexus NX-OS d'établir avec succès une connexion TLS Syslog sécurisée avec un serveur Syslog.

Le workflow valide chaque étape du processus de communication, en commençant par la

connectivité IP et en progressant par la connectivité TCP, la négociation TLS, la validation de certificat et enfin la transmission sécurisée des messages Syslog. En vérifiant chaque couche indépendamment, il est possible de déterminer rapidement où la communication échoue.

Explication de topologie

La topologie utilisée dans ce document se compose d'un commutateur Cisco Nexus configuré en tant que client Syslog sécurisé et d'un serveur Ubuntu exécutant rsyslog configuré en tant que serveur Syslog sécurisé.

Le commutateur Cisco Nexus initie une connexion TCP au serveur Syslog sur le port 6514. Une fois la connexion TCP établie, les deux périphériques effectuent la connexion TLS. Au cours de ce processus, le serveur Syslog présente son certificat de serveur et tous les certificats d'autorité de certification intermédiaires requis. Le commutateur Nexus valide la chaîne de certificats par rapport à l'autorité de certification racine de confiance configurée dans son point de confiance.

Une fois la connexion TLS terminée, la session chiffrée est établie et le commutateur Nexus commence à transmettre des messages Syslog sécurisés au serveur Syslog.

La méthodologie de dépannage présentée dans ce document utilise la même séquence de communication que l'établissement de la connexion, ce qui permet à chaque phase du processus d'être validée indépendamment.

Étape 1 : vérification de la configuration Syslog sécurisée

Vérifiez que Secure Syslog est correctement configuré sur le commutateur Cisco Nexus et que le commutateur reconnaît le serveur Syslog configuré.

```
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#
```

Étape 2 : vérification de la configuration Trustpoint

Vérifiez que le commutateur Cisco Nexus approuve l'autorité de certification utilisée pour signer le certificat du serveur Syslog.

Vérifier :

Le point de confiance attendu existe.

Le certificat d'autorité de certification racine est installé.

Tous les certificats CA intermédiaires requis sont présents.

Les certificats n'ont pas expiré.

Les empreintes de certificat correspondent aux valeurs attendues.

```
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 le certificat d'autorité de certification approprié est manquant ou non valide, la validation du certificat échoue lors de la connexion TLS.

Étape 3 : vérification de la connectivité IP

Vérifiez la connectivité de couche 3 entre le commutateur Cisco Nexus et le serveur Secure Syslog.

Vérifier :

- Accessibilité ICMP (Internet Control Message Protocol) réussie.
- Résolution DNS (Domain Name System) correcte.
- Aucun problème de routage.
- Aucune perte de paquets.

```
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 la connectivité IP échoue, aucune connexion TCP ne peut être établie.

Étape 4. Vérification de la connectivité TLS

Vérifiez la connectivité TLS de bout en bout entre le commutateur Cisco Nexus et le serveur Secure Syslog.

Cette étape valide plusieurs étapes de la connexion Syslog sécurisée, notamment :

- connectivité TCP
- négociation TLS
- Présentation du certificat du serveur
- Chaîne de certificats
- Validation du certificat
- Négociation de la suite de chiffrements

Ces opérations étant effectuées dans le cadre de la connexion TLS, elles peuvent toutes être vérifiées à l'aide d'une seule commande.

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

Que vérifie cette commande ?

Validation	Description
Connectivité TCP	Vérifie que le Nexus peut établir une connexion TCP au serveur Syslog.
Connexion TLS	Confirme que les deux homologues ont réussi à négocier une session TLS.
certificat du serveur	Affiche le certificat présenté par le serveur Syslog.
Chaîne De Certificats	Affiche tous les certificats CA intermédiaires envoyés par le serveur.
Version TLS	Affiche la version TLS négociée.
Suite de chiffrement	Affiche l'algorithme de chiffrement négocié.
Validation de certificat	Lorsque l'option -CAfile est utilisée, vérifie la chaîne de certificats par rapport à l'autorité de certification approuvée spécifiée.

Sortie réussie attendue

```
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, C
verify return:1
depth=1 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = DCRS, CN = Cisco Lab Intermedi
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, C
---
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 Inter
---
Acceptable client certificate CA names
```

Capture de connexion TLS Syslog sécurisée

Flux de connexion 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 ----->
```

La connexion TLS doit s'effectuer correctement avant qu'un message Syslog puisse être échangé. Si la connexion échoue, le trafic Syslog sécurisé n'est jamais généré.

Pour effectuer cette vérification, ouvrez deux sessions CLI sur le commutateur Cisco Nexus. Dans la première session, lancez la connexion TLS avec cette commande :

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

Dans le même temps, dans la deuxième session CLI, démarrez une capture Ethalyzer afin de surveiller l'échange 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

```

La capture de paquets doit afficher la séquence d'échange TLS complète, y compris l'échange en trois étapes TCP, Client Hello, Server Hello, Certificate, Key Exchange, Finished messages et, si l'échange réussit, les enregistrements de données d'application TLS chiffrés portant les messages Syslog sécurisés.

Vérification de la transmission sécurisée des messages Syslog

Vérifiez que les messages Syslog sécurisés sont correctement transmis du commutateur Cisco Nexus au serveur Syslog une fois la session TLS établie.

Une connexion TLS réussie confirme que le canal chiffré a été créé ; cependant, elle ne garantit pas que les messages syslog sont générés ou remis.

Cette étape valide l'ensemble du workflow Syslog sécurisé en générant un message de test et en confirmant sa transmission et sa réception.

Générer un message Syslog de test

```

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]

```

Cette commande génère un message syslog local qui doit être transmis au serveur Syslog sécurisé configuré sur la session TLS existante.

Vérification des données d'application TLS chiffrées

Si une capture Ethanalyzer est déjà en cours d'exécution (comme décrit dans la section précédente), vérifiez que les nouveaux paquets de données d'application TLS sont transmis après la génération du message de test.

```
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
```

La présence de données d'application TLS indique que les messages Syslog sont transmis via la session TLS chiffrée. Comme la charge utile est chiffrée, Ethanalyzer ne peut pas décoder le contenu du message Syslog.



Remarque : Une fois la connexion TLS terminée, tous les messages Syslog sont encapsulés dans des enregistrements chiffrés de données d'application TLS. Leur contenu n'est pas visible dans les captures de paquets.

Vérification de la réception des messages sur le serveur Syslog

Sur le serveur Syslog, vérifiez que le message a bien été reçu et écrit dans le fichier journal de destination.

```
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 présence du message de test généré confirme que :

Le commutateur Cisco Nexus a correctement généré le message syslog.

Le message a été transmis via la session TLS chiffrée.

Le serveur Syslog a correctement déchiffré et traité le message.

La configuration Syslog sécurisée fonctionne correctement de bout en bout.

L'affichage des données d'application TLS dans Ethanalyzer confirme que la session TLS achemine activement le trafic d'application chiffré. Cependant, la preuve définitive que Secure Syslog fonctionne correctement est la réception réussie du message syslog généré sur le serveur

Syslog.

Conclusion

La sécurité de Syslog sur les commutateurs Cisco Nexus dépend de la réussite de la connectivité IP et TCP, de la négociation TLS, de la validation des certificats et de la remise des messages chiffrés. La vérification indépendante de chaque couche permet d'isoler le point de défaillance et de distinguer les problèmes de connectivité, de TLS, de certificat et de transmission de messages. Une connexion TLS réussie confirme que la session chiffrée est établie, tandis que la réception d'un message de test généré sur le serveur Syslog confirme le fonctionnement de bout en bout de Secure Syslog.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.