تكوين SDWAN Cisco IOS XE TLS Syslog على خادم syslog-ng

المحتويات

المقدمة

يصف هذا المستند دليل شامل لتكوين خادم TLS syslog على أجهزة SD-WAN Cisco IOS® XE.

المتطلبات الأساسية

قبل متابعة تكوين خادم TLS syslog على أجهزة SD-WAN Cisco IOS XE، تأكد من استيفاء المتطلبات:

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدات التحكم في شبكة WAN-SD - تأكد من أن شبكتك تحتوي على وحدات تحكم SD-

WAN تم تكوينها بشكل صحيح.

- موجه Cisco IOS XE SD-WAN - موجه متوافق يشغل صورة Cisco IOS XE SD-WAN.
- Syslog Server - خادم syslog مستند إلى Ubuntu، مثل syslog-ng، لجمع بيانات السجل وإدارتها.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- vManage: الإصدار 20.9.4
- IOS XE SD-WAN من Cisco: الإصدار 17.9.4
- أوبونتو: الإصدار 22.04
- syslog-ng: الإصدار 3.27

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

1. تثبيت syslog-ng على جهاز Ubuntu

من أجل إعداد syslog-ng على خادم Ubuntu، اتبع هذه الخطوات لضمان التثبيت والتكوين المالئمين.

الخطوة 1. تكوين إعدادات الشبكة

بعد تثبيت خادم Ubuntu، قم بتكوين عنوان IP ثابت وخادم DNS لضمان إمكانية وصول الجهاز إلى الإنترنت. يعد ذلك أمرا حيويا لتنزيل الحزم والتحديثات.

الخطوة 2. قم بتثبيت syslog-ng

فتح وحدة طرفية على جهاز Ubuntu وتشغيلها:

```
sudo apt-get install syslog-ng sudo apt-get install syslog-ng openssl
```

2. تثبيت المرجع المصدق الجذر على Syslog Server لمصادقة الخادم

إنشاء أدلة وإنشاء مفاتيح

```
cd /etc/syslog-ng mkdir cert.d key.d ca.d cd cert.d openssl genrsa -out ca.key 2048 openssl req -new -x
```

حساب بصمة الإصبع

قم بتشغيل الأمر وانسخ المخرجات:

openssl x509 -in proxy-signature-ca.ca -finger -noout | awk -f "=" '{print$2}' | سعيد 's/://g' | بصمة الإصبع.txt
ماثل الإخراج: 54F371C8EE2BFB06E2C2D0944245C288FBB07163

3. تكوين ملف تكوين خادم syslog-ng

حرر الـ syslog-ng تشكيل مبرد:

```
sudo nano /etc/syslog-ng/syslog-ng.conf
```

إضافة التكوين:

```
source s_src { network( ip(0.0.0.0) port(6514) transport("tls") tls( key-file("/etc/syslog-ng/key.d/ca.
```

4. تثبيت مرجع الشهادة الجذر على جهاز Cisco IOS XE SD-WAN لمصادقة الخادم

التكوين من CLI

1. ادخل إلى وضع التكوين:

```
config-t
```

2. تكوين TrustPoint:

<#root>

```
crypto pki trustpoint PROXY-SIGNING-CA enrollment url bootflash: revocation-check none rsakeypair PROXY
```

>> The fingerprint configured was obtained from the fingerprint.txt file above

```
 commit
```

3. انسخ توقيع الوكيل-CA.CA ملف من خادم syslog إلى ذاكرة التمهيد للموجه باستخدام نفس الاسم.

4. مصادقة نقطة الثقة:

<#root>

```
crypto pki authenticate PROXY-SIGNING-CA
```

example:

```
Router#crypto pki authenticate PROXY-SIGNING-CA


Reading file from bootflash:PROXY-SIGNING-CA.ca
Certificate has the attributes:
Fingerprint MD5: 7A97B30B 2AE458FF D9E7D91F 66488DCF
Fingerprint SHA1: 21E0F09B B67B2E9D 706DBE69 856E5AA3 D39A268A
Trustpoint Fingerprint: 21E0F09B B67B2E9D 706DBE69 856E5AA3 D39A268A
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
```

5. تسجيل نقطة الثقة:

<#root>

```
crypto pki enroll PROXY-SIGNING-CA
```

example:

```
vm32#crypto pki enroll PROXY-SIGNING-CA


Start certificate enrollment ..
The subject name in the certificate will include: cn=proxy-signing-cert
The fully-qualified domain name will not be included in the certificate
Certificate request sent to file system
The 'show crypto pki certificate verbose PROXY-SIGNING-CA' commandwill show the fingerprint.
```

6. انسخ توقيع الوكيل-CA.req ملف من الموجه إلى خادم syslog.

توقيع الشهادة على Syslog Server

```
openssl x509 -in PROXY-SIGNING-CA.req -req -CA PROXY-SIGNING-CA.ca -CAkey ca.key -out PROXY-SIGNING-CA.
```

7. نسخ الملف الذي تم إنشاؤه (توقيع الوكيل-CA.CRT) إلى ذاكرة التمهيد للموجه. نسخ SCP: ذاكرة التمهيد المؤقتة (bootflash):

8. إستيراد الشهادة:

<#root>

```
crypto pki import PROXY-SIGNING-CA certificate
example:
```

Router# crypto pki import PROXY-SIGNING-CA certificate

```
% The fully-qualified domain name will not be included in the certificate
% Request to retrieve Certificate queued
```

التحقق من صحة التكوين

<#root>

```
show crypto pki trustpoint PROXY-SIGNING-CA status

example:
```

Router#show crypto pki trustpoint PROXY-SIGNING-CA status

```
Trustpoint PROXY-SIGNING-CA:
Issuing CA certificate configured:
Subject Name:
o=Internet Widgits Pty Ltd,st=Some-State,c=AU
Fingerprint MD5: 7A97B30B 2AE458FF D9E7D91F 66488DCF
Fingerprint SHA1: 21E0F09B B67B2E9D 706DBE69 856E5AA3 D39A268A
Router General Purpose certificate configured:
Subject Name:
cn=proxy-signing-cert
Fingerprint MD5: 140A1EAB FE945D56 D1A53855 FF361F3F
Fingerprint SHA1: ECA67413 9C102869 69F582A4 73E2B98C 80EFD6D5
Last enrollment status: Granted
State:
Keys generated ..... Yes (General Purpose, non-exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

5. قم بتكوين خادم TLS syslog على موجه Cisco IOS XE SD-WAN

شكلت ال syslog ادل يستعمل ألامر:

```
logging trap syslog-format rfc5424 logging source-interface GigabitEthernet0/0/0 logging tls-profile tl
```

6 - عمليات التحقق

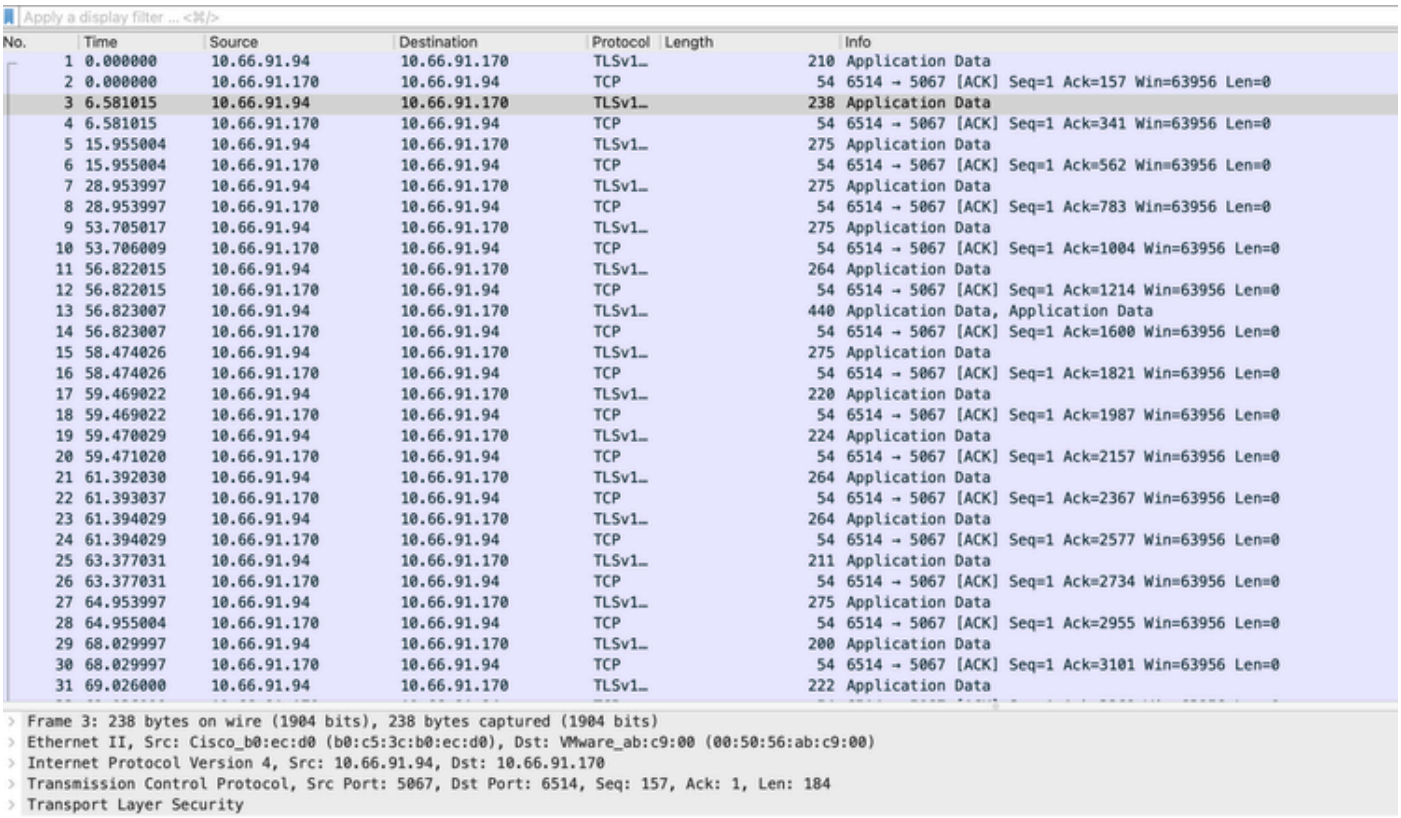
التحقق من السجلات على الموجه

```
show logging

Showing last 10 lines
Log Buffer (512000 bytes):
Apr 9 05:59:48.025: %DMI-5-CONFIG_I: R0/0: dmiauthd: Configured from NETCONF/RESTCONF by admin, transac
Apr 9 05:59:48.709: %DMI-5-AUTH_PASSED: R0/0: dmiauthd: User 'vmanage-admin' authenticated successfully
Apr 9 05:59:50.015: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to administratively
Apr 9 05:59:51.016: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state
Apr 9 05:59:52.242: %SYS-5-CONFIG_P: Configured programmatically by process iosp_dmiauthd_conn_100001_v
```

التحقق من السجلات على خادم syslog

```
tail -f /var/log/syslog

root@server1:/etc/syslog-ng# tail -f /var/log/syslog
Apr 9 15:51:14 10.66.91.94 188 <189>1 2024-04-09T05:51:51.037Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: dm
Apr 9 15:59:10 10.66.91.94 177 <189>1 2024-04-09T05:59:47.463Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:10 10.66.91.94 177 <189>1 2024-04-09T05:59:47.463Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:10 10.66.91.94 143 <189>1 2024-04-09T05:59:47.463Z - - - - - BOM%DMI-5-CONFIG_I: R0/0: dmia
Apr 9 15:59:11 10.66.91.94 188 <189>1 2024-04-09T05:59:48.711Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: dm
Apr 9 15:59:13 10.66.91.94 133 <189>1 2024-04-09T05:59:50.016Z - - - - - BOM%LINK-5-CHANGED: Interface
Apr 9 15:59:13 10.66.91.94 137 <189>1 2024-04-09T05:59:50.016Z - - - - - BOM%LINEPROTO-5-UPDOWN: Line p
Apr 9 15:59:15 10.66.91.94 177 <189>1 2024-04-09T05:59:52.242Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:15 10.66.91.94 177 <189>1 2024-04-09T05:59:52.242Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:18 10.66.91.94 188 <189>1 2024-04-09T05:59:55.286Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: dm
Apr 9 15:59:21 10.66.91.94 113 <187>1 2024-04-09T05:59:58.882Z - - - - - BOM%LINK-3-UPDOWN: Interface G
Apr 9 15:59:21 10.66.91.94 135 <189>1 2024-04-09T05:59:59.882Z - - - - - BOM%LINEPROTO-5-UPDOWN: Line p
Apr 9 15:59:28 10.66.91.94 177 <189>1 2024-04-09T06:00:05.536Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:43 10.66.91.94 188 <189>1 2024-04-09T06:00:20.537Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: dm
```

لقطة شاشة لالتقاط الحزمة ويمكنك مشاهدة الاتصالات المشفرة تحدث:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.66.91.94	10.66.91.170	TLSv1…	210	Application Data
2	0.000000	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=157 Win=63956 Len=0
3	6.581015	10.66.91.94	10.66.91.170	TLSv1…	238	Application Data
4	6.581015	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=341 Win=63956 Len=0
5	15.955004	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
6	15.955004	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=562 Win=63956 Len=0
7	28.953997	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
8	28.953997	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=783 Win=63956 Len=0
9	53.705017	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
10	53.706009	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1004 Win=63956 Len=0
11	56.822015	10.66.91.94	10.66.91.170	TLSv1…	264	Application Data
12	56.822015	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1214 Win=63956 Len=0
13	56.823007	10.66.91.94	10.66.91.170	TLSv1…	440	Application Data, Application Data
14	56.823007	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1600 Win=63956 Len=0
15	58.474026	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
16	58.474026	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1821 Win=63956 Len=0
17	59.469022	10.66.91.94	10.66.91.170	TLSv1…	220	Application Data
18	59.469022	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1987 Win=63956 Len=0
19	59.470029	10.66.91.94	10.66.91.170	TLSv1…	224	Application Data
20	59.471020	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2157 Win=63956 Len=0
21	61.392030	10.66.91.94	10.66.91.170	TLSv1…	264	Application Data
22	61.393037	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2367 Win=63956 Len=0
23	61.394029	10.66.91.94	10.66.91.170	TLSv1…	264	Application Data
24	61.394029	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2577 Win=63956 Len=0
25	63.377031	10.66.91.94	10.66.91.170	TLSv1…	211	Application Data
26	63.377031	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2734 Win=63956 Len=0
27	64.953997	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
28	64.955004	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2955 Win=63956 Len=0
29	68.029997	10.66.91.94	10.66.91.170	TLSv1…	200	Application Data
30	68.029997	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=3101 Win=63956 Len=0
31	69.026000	10.66.91.94	10.66.91.170	TLSv1…	222	Application Data

```
> Frame 3: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)
> Ethernet II, Src: Cisco_b0:ec:d0 (b0:c5:3c:b0:ec:d0), Dst: VMware_ab:c9:00 (00:50:56:ab:c9:00)
> Internet Protocol Version 4, Src: 10.66.91.94, Dst: 10.66.91.170
> Transmission Control Protocol, Src Port: 5067, Dst Port: 6514, Seq: 157, Ack: 1, Len: 184
> Transport Layer Security
```

التسجيل ISR4331-Branch-new_Branch#show

```
Trap logging: level informational, 6284 message lines logged
    Logging to 10.66.91.170  (tls port 6514, audit disabled,
          link up),
          131 message lines logged,
          0 message lines rate-limited,
          0 message lines dropped-by-MD,
          xml disabled, sequence number disabled
          filtering disabled
          tls-profile: tls-proile
    Logging Source-Interface:       VRF Name:
    GigabitEthernet0/0/0
TLS Profiles:
    Profile Name: tls-proile
          Ciphersuites: Default
          Trustpoint: Default
          TLS version: TLSv1.2
```

التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).