syslog-ngサーバ上のSDWAN Cisco IOS XE TLS syslog設定

内容

はじめに
前提条件
- 要件
- 使用するコンポーネント

コンフィギュレーション
- 1. UbuntuマシンへのSyslog-ngのインストール
  - ステップ 1：ネットワーク設定の構成
  - ステップ 2：syslog-ngのインストール
- 2. サーバ認証用のルート認証局をsyslogサーバにインストールする
  - ディレクトリの作成とキーの生成
  - 指紋の計算
- 3. syslog-ngサーバ設定ファイルの設定
- 4. Cisco IOS XE SD-WANデバイスでのサーバ認証用ルート認証局のインストール
  - CLIからの設定
  - Syslogサーバでの証明書の署名
  - 構成の検証
- 5. Cisco IOS XE SD-WANルータでのTLS syslogサーバの設定
- 6. 検証
  - ルータのログを確認する
  - Syslogサーバのログを確認する

確認
トラブルシュート

はじめに

このドキュメントでは、SD-WAN Cisco IOS® XEデバイスでTLS Syslogサーバを設定するための包括的なガイドについて説明します。

前提条件

SD-WAN Cisco IOS XEデバイスでTLS Syslogサーバの設定を進める前に、次の要件を満たしていることを確認してください。

要件

次の項目に関する知識があることが推奨されます。

- SD-WANコントローラ：ネットワークに適切に設定されたSD-WANコントローラが含まれ

ていることを確認します。

- Cisco IOS XE SD-WANルータ：Cisco IOS XE SD-WANイメージを実行する互換性のあるルータ。
- Syslogサーバ：ログデータを収集して管理するための、syslog-ngなどのUbuntuベースのSyslogサーバ。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- vManage:バージョン20.9.4
- Cisco IOS XE SD-WAN:バージョン17.9.4
- Ubuntu:バージョン22.04
- syslog-ng:バージョン3.27

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンフィギュレーション

1. UbuntuマシンへのSyslog-ngのインストール

Ubuntuサーバにsyslog-ngを設定するには、次の手順を実行して適切なインストールと設定を行います。

ステップ 1：ネットワーク設定の構成

Ubuntu Serverをインストールした後、マシンがインターネットにアクセスできるように、固定IPアドレスとDNSサーバを設定します。これは、パッケージと更新プログラムをダウンロードする際に重要です。

ステップ 2：syslog-ngのインストール

Ubuntuマシンで端末を開き、次のコマンドを実行します。

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

2. サーバ認証用のルート認証局をsyslogサーバにインストールする

ディレクトリの作成とキーの生成

```
cd /etc/syslog-ng
mkdir cert.d key.d ca.d
cd cert.d
openssl genrsa -out ca.key 2048
openssl req -new -x509 -key ca.key -out PROXY-SIGNING-CA.ca -days 730

# Copy key to the key.d folder
cp ca.key ../key.d
```

指紋の計算

次のコマンドを実行し、出力をコピーします。

openssl x509 -in PROXY-SIGNING-CA.ca -fingerprint -noout | awk -F "=" '{print $2}' | sed 's/://g' | tee fingerprint.txt
#出力例： 54F371C8EE2BFB06E2C2D0944245C288FBB07163

3. syslog-ngサーバ設定ファイルの設定

syslog-ngコンフィギュレーションファイルを編集します。

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

設定を追加します。

```
source s_src {
    network(
        ip(0.0.0.0) port(6514)
        transport("tls")
        tls(
            key-file("/etc/syslog-ng/key.d/ca.key")
            cert-file("/etc/syslog-ng/cert.d/PROXY-SIGNING-CA.ca")
            peer-verify(optional-untrusted)
        )
    );
};

destination remote {
    file("/var/log/syslog");
};

log { source(s_src); destination(remote); };
```

4. Cisco IOS XE SD-WANデバイスでのサーバ認証用ルート認証局のインストール

CLIからの設定

1. 次の設定モードを入力します。

```
config-t
```

2. トラストポイントを設定します。

<#root>

```
crypto pki trustpoint PROXY-SIGNING-CA
  enrollment url bootflash:
  revocation-check none
  rsakeypair PROXY-SIGNING-CA 2048
  subject-name cn=proxy-signing-cert
  fqdn none
  fingerprint 54F371C8EE2BFB06E2C2D0944245C288FBB07163
```

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

```
commit
```

3. syslogサーバからルータのブートフラッシュに同じ名前でPROXY-SIGNING-CA.caファイルをコピーします。

4. トラスト ポイントを認証します。

<#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. トラストポイントを登録します。

<#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. ルータからsyslogサーバにPROXY-SIGNING-CA.req ファイルをコピーします。

Syslogサーバでの証明書の署名

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

7. 生成されたファイル(PROXY-SIGNING-CA.crt)をルータのブートフラッシュにコピーします。copy scp: bootflash:
8. 証明書をインポートします。

<#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
```

構成の検証

<#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. Cisco IOS XE SD-WANルータでのTLS syslogサーバの設定

次のコマンドを使用して、syslogサーバを設定します。

```
logging trap syslog-format rfc5424
logging source-interface GigabitEthernet0/0/0
logging tls-profile tls-profile
logging host X.X.X.X transport tls profile tls-profile
tls-version TLSv1.2
```

6. 検証

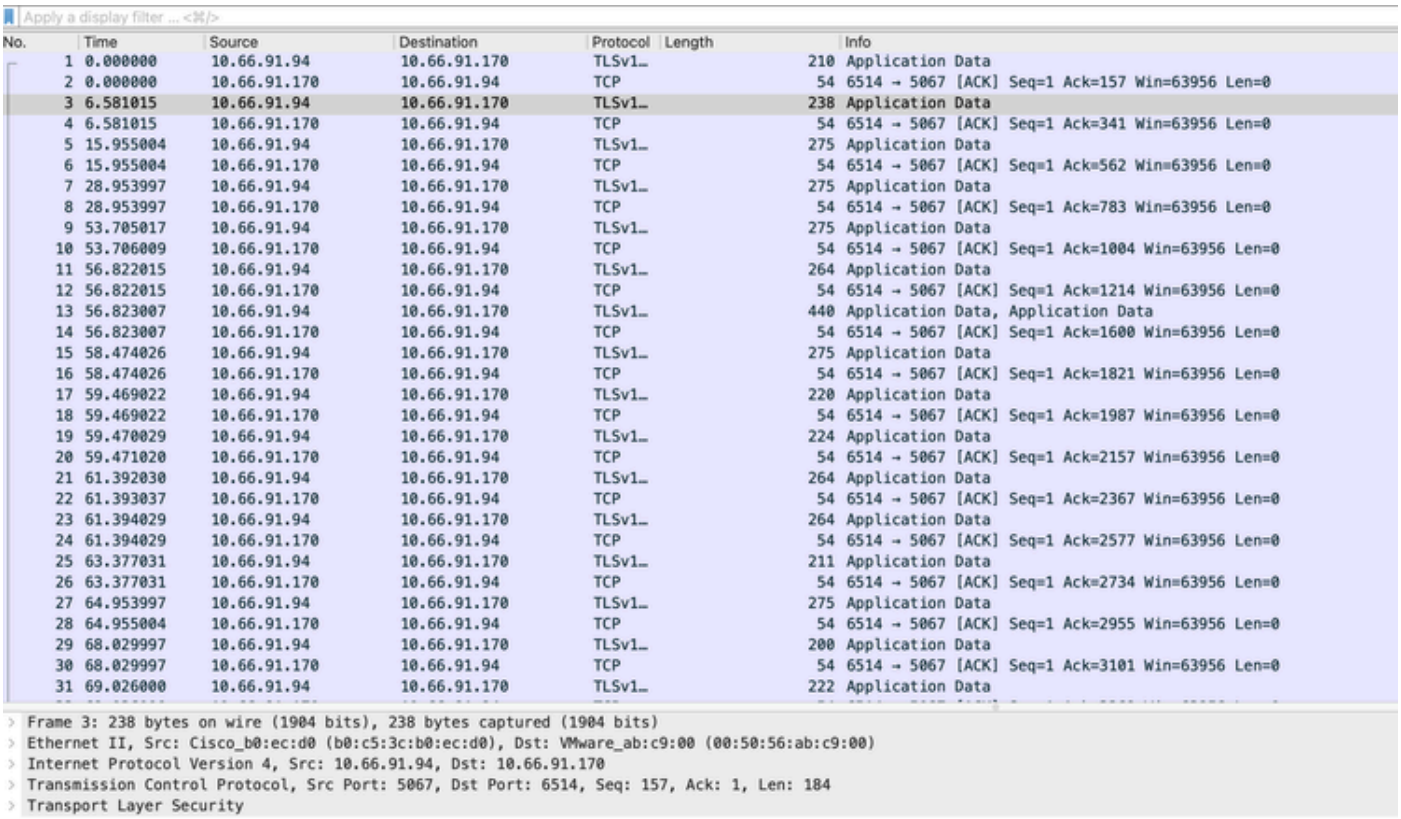
ルータのログを確認する

```
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
```

Syslogサーバのログを確認する

```
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: d
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: d
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: d
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: d
```

パケットキャプチャのスクリーンショットを見ると、暗号化された通信が行われていることがわかります。



Apply a display filter ... <⌘/>

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

ISR4331-branch-NEW_Branch#show logging

```
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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。