SDWAN Cisco IOS XE TLS系統日誌伺服器配置

目錄

簡介

本文檔介紹在SD-WAN Cisco IOS® XE裝置上配置TLS系統日誌伺服器的全面指南。

必要條件

在SD-WAN Cisco IOS XE裝置上繼續配置TLS系統日誌伺服器之前，請確保滿足以下要求：

需求

思科建議您瞭解以下主題：

- SD-WAN控制器 — 確保您的網路包括正確配置的SD-WAN控制器。
- Cisco IOS XE SD-WAN路由器 — 運行Cisco IOS XE SD-WAN映像的相容路由器。
- 系統日誌服務器 — 基於Ubuntu的系統日誌伺服器，例如syslog-ng，用於收集和管理日誌資料。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- vManage:版本20.9.4
- Cisco IOS XE SD-WAN:版本17.9.4
- Ubuntu:版本22.04
- syslog-ng:版本3.27

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

1.在Ubuntu電腦上安裝系統日誌

要在Ubuntu伺服器上設定syslog-ng，請執行以下步驟以確保正確安裝和配置。

步驟1.配置網路設定

安裝Ubuntu伺服器後，請配置靜態IP地址和DNS伺服器，以確保電腦可以訪問Internet。這對於下載軟體包和更新至關重要。

步驟2.安裝系統日誌 — ng

在Ubuntu電腦上開啟終端並運行：

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

2.在Syslog伺服器上安裝用於伺服器身份驗證的根證書頒發機構

建立目錄並生成金鑰

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

計算指紋

執行命令並複製輸出：

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

3.配置syslog-ng伺服器配置檔案

編輯syslog-ng配置檔案：

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

新增配置：

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

4.在Cisco IOS XE SD-WAN裝置上安裝根證書頒發機構以進行伺服器身份驗證

從CLI配置

1. 進入組態設定模式：

```
config-t
```

2. 配置信任點：

```
<#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. 複製 PROXY-SIGNING-CA.ca 使用相同的名稱將檔案從系統日誌伺服器傳送到路由器 bootflash。
4. 驗證信任點：

```
<#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. 註冊信任點：

<#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. 複製 PROXY-SIGNING-CA.req 將檔案從路由器傳送到syslog伺服器。

在Syslog伺服器上簽署證書

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

7. 複製生成的檔案(PROXY-SIGNING-CA.crt)，到路由器bootflash。複製scp:bootflash:

8. 匯入證書：

<#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
```

驗證設定

<#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.在Cisco IOS XE SD-WAN路由器上配置TLS系統日誌伺服器

使用以下命令配置syslog伺服器：

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

6.核查

檢查路由器上的日誌

```
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
```

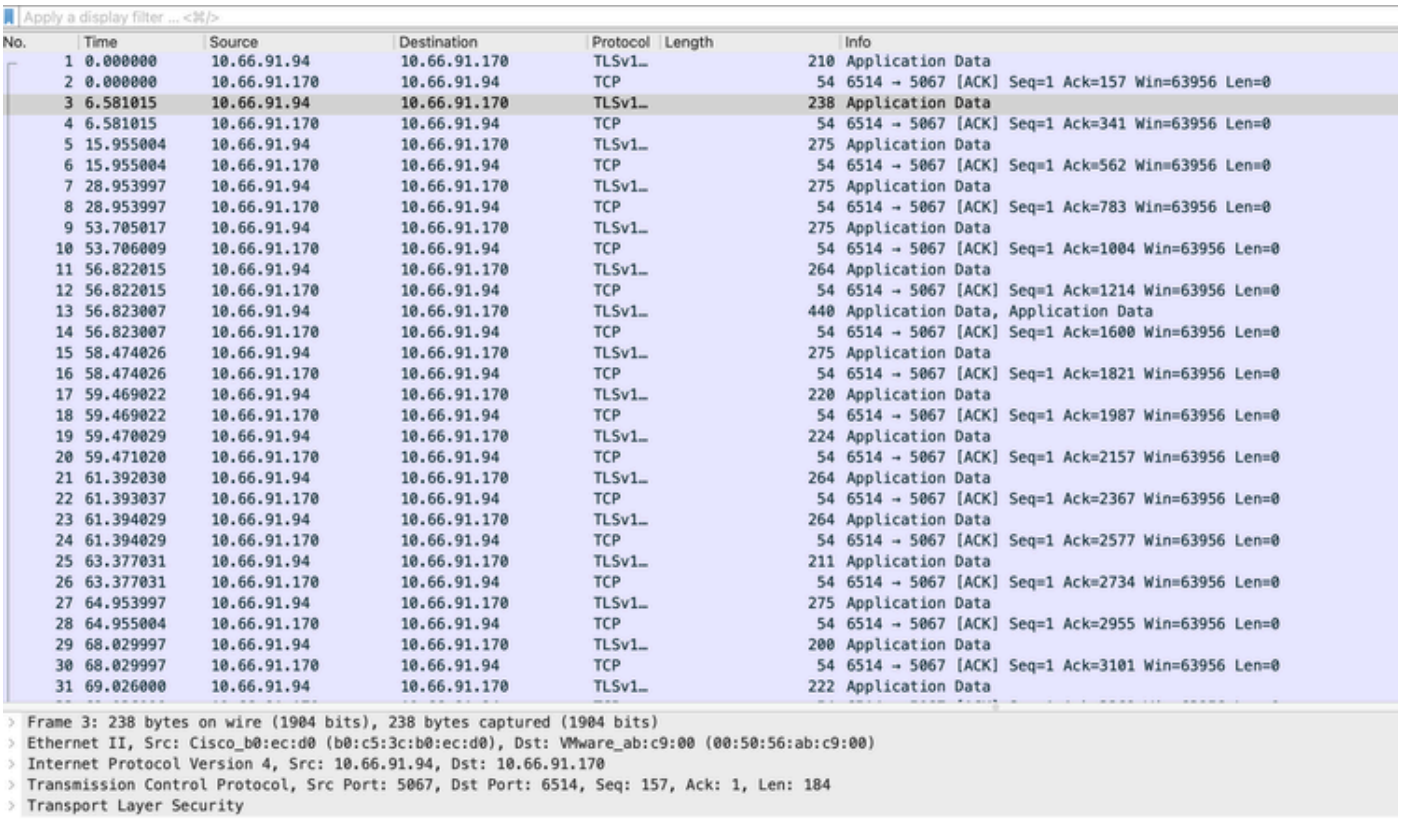
```
Apr 9 05:59:50.015: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to administratively
Apr 9 05:59:51.016: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state
Apr 9 05:59:52.242: %SYS-5-CONFIG_P: Configured programmatically by process iosp_dmiauthd_conn_100001_v
```

檢查系統日誌伺服器上的日誌

```
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
```

資料包捕獲螢幕截圖，您可以看到正在發生的加密通訊：



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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。