SD-WAN展開でのNTP同期のベストプラクティスの設定

内容

はじめに

このドキュメントでは、SD-WANファブリック内のデバイス間で正確な時刻の同期を維持するためにNTPがいかに重要であるかについて説明します。

背景

適切な時刻同期を行わないと、セキュアな通信、証明書の検証、ロギングなどの重要な操作が失敗する可能性があります。SD-WANは、証明書ベースのセキュアなポリシー駆動型ネットワークソリューションです。SD-WANファブリックの整合性、セキュリティ、および機能を維持するための基盤は、NTPを使用した時刻同期です。

前提条件

要件

Cisco Software Defined Wide Area Network(SDWAN)ソリューションに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- C8000Vバージョン17.15.03a
- vManageバージョン20.15.03.1

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。

主な理由

- SD-WANでは、デバイス認証にデジタル証明書が使用されます。これらの証明書には、有効開始日と有効期限があります。デバイスクロックが正確でない場合は、証明書が期限切れか、まだ有効ではないと判断される可能性があります。

```
vbond-west# show orchestrator connections-history
          PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
INSTANCE  TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBL
-------------------------------------------------------------------------------------------------
0         vmanage  dtls     10.1.1.7          101019      0           10.1.2.190       12646    192
```

CRTVERFL：ピア証明書の検証に失敗する

この場合、時刻は証明書の有効期限外であるため、「Fail to Verify Peer Certificate」エラーが発生します。

- エッジルータとコントローラ間のDTLS/TLSトンネルは、証明書ベースの認証に依存します。時刻の不一致により、ハンドシェイクが失敗し、コントロール接続が切断される可能性があります。
- エッジデバイスとコントローラのログにはタイムスタンプが付いています。時刻が同期されていない場合、異なるデバイスからのログが正しく調整されないため、イベントの関連付けとトラブルシューティングが困難になります。
- vAnalyticsや外部モニタリングシステムなどのツールは、SLAモニタリング、パフォーマンスレポート、およびイベント相関の正確なタイムスタンプに依存しています。

設定

このドキュメントでは、機能テンプレート、設定グループ、およびCLIを使用してNTPを設定する方法について説明します。

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/systems-interfaces.html#c-NTP-12298
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-02system-and-interfaces.html#ntp-server-cg

リファレンス構成

コントローラ

```
system
 ntp
  keys
   authentication 1001 md5 $4$KXLzYT9k6M8zj4BgLEFXKw==
   authentication 1002 md5 $4$KXLzYTxk6M8zj4BgLEFXKw==
```

```
   authentication 1003 md5 $4$KXLzYT1k6M8zj4BgLEFXKw==
   trusted 1001 1002
  !
  server 192.168.15.243
   key     1001
   vpn     512
   version 4
  exit
  server 192.168.15.242
   key     1002
   vpn     512
   version 4
  exit
  server us.pool.ntp.org
   vpn     512
   version 4
  exit
 !
!
```

Ciscoエッジルータ

```
cEdge_DC1_West_R01#show running-config | sec ntp
ntp server time.google.com prefer
ntp server pool.ntp.org

cEdge_DC1_West_R01#show sdwan running-config ntp
ntp server pool.ntp.org version 4
ntp server time.google.com prefer version 4

If Mgmt VRF is used:
ntp server vrf Mgmt-intf pool.ntp.org version 4
```

注:NTP設定にVPN 0を使用する場合、NTPサービスはトンネルインターフェイスで許可されている必要があります。FQDNホストがNTPサーバに使用される場合、デバイスはFQDNをIPアドレスに解決できるようにDNSが設定されている必要があります。

トラブルシュート

このドキュメントは、NTPを検証し、NTP同期のさまざまな段階を理解して、コントローラおよびエッジデバイスの問題をトラブルシューティングするために使用できます。

アクセス ポイント グループ:
https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/221015-understand-ntp-association-

codes-in-sd-w.html

vEdge:

https://www.cisco.com/c/en/us/support/docs/routers/vedge-router/220330-troubleshoot-network-time-protocol-ntp.html

cEdge:
https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html

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。