vEdgeでのネットワークタイムプロトコル(NTP)の問題のトラブルシューティング

内容

概要

このドキュメントでは、vEdgeプラットフォームのshow ntpコマンドとパケットキャプチャツールを使用して、ネットワークタイムプロトコル(NTP)の問題をトラブルシューティングする方法について説明しますを参照。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアバージョンやvEdgeモデルに限定されるものではありません。

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。

NTP問題の症例例

vEdgeに対するNTP同期の喪失は、次のようないくつかの異なる方法で現れる可能性があります。

- デバイスのshow clock出力に不正確な時刻が示される。
- 有効範囲外の不正確な時間が原因で、証明書が無効と見なされます。
- ログのタイムスタンプが正しくない。

NTP show コマンド

NTPの問題の切り分けを開始するには、次の2つの主要なコマンドの使用方法と出力について理解する必要があります。

- NTPアソシエーションの表示
- show ntp peer

特定のコマンドの詳細については、「SD-WANコマンドリファレンス」を参照してください。

NTPアソシエーションの表示

```
vedge1# show ntp associations

                                                                    LAST
IDX  ASSOCID  STATUS  CONF  REACHABILITY  AUTH  CONDITION  EVENT      COUNT
-------------------------------------------------------------------------------
1    56368    8011    yes   no            none  reject     mobilize   1
2    56369    911a    yes   yes           none  falsetick  sys_peer   1
3    56370    9124    yes   yes           none  falsetick  reachable  2
```

IDX	ローカルインデックス番号
関連付け	Association Id
状態	ピアステータスワード（16進数）
会議	設定（持続性または一時的）
到達可能性	到達可能性（yesまたはno）
AUTH	認証（ok、yes、bad、またはnone）
条件	選択ステータス
[Event]	このピアの最後のイベント
COUNT	イベントカウント

NTPピアの表示

```
vedge1# show ntp peer | tab

INDEX  REMOTE          REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
-------------------------------------------------------------------------------------
1      192.168.18.201  .STEP.    16  u     37    1024  0      0.000    0.000    0.000
2      x10.88.244.1    LOCAL(1)  2   u     7     64    377    108.481  140.642  20.278
3      x172.18.108.15  .GPS.     1   u     66    64    377    130.407  -24883.  55.334
```

インデックス	ローカルインデックス番号
REMOTE	NTPサーバアドレス
REFID	ピアからの現在の同期ソース
ST	ストラタム NTP では、ストラタムという概念を使用して、信頼できる時間ソースからマシンがどれだけ離れているかを NTP ホップ数で示します。たとえば、ストラタム 1 のタイム サーバに電波時計または原子時計が直接接続されているとします。このタイム サーバからストラタム 2 のタイム サーバに NTP によって時刻が送信され、同様にストラタム 16 まで順番に時刻が送信されます。NTPを実行するマシンは、通信可能なストラタム番号が最も低いマシンを自動的に選択し、NTPを時刻源として使用します。
タイプ	種類
時期	ピアから最後の NTP パケットを受信してから経過した時間を秒単位で報告します。この値はポーリング間隔より小さくする必要があります。
POLL	ポーリング間隔（秒）
REACH	到達（直近の8接続に基づく8進数値で指定） 377 (1 1 1 1 1 1 1) – 最後の8個はすべて正常でした 376 (1 1 1 1 1 1 0) – 最後の接続が不正です .... 177 (0 1 1 1 1 1 1) – 最も古い接続は不良で、すべて良好でした

	以上です。
遅延	ピアへのラウンド トリップ遅延がミリ秒単位で報告されます。クロックをより正確に設定するには、クロック時間を設定するときにこの遅延を考慮に入れます。
OFFSET	オフセット（ミリ秒） Offsetは、ピア間、またはプライマリとクライアント間のクロック時間差です。この値は、クライアント クロックを同期するために適用される補正値です。正の値はサーバ クロックのほうが高いことを示しています。負の値はクライアント クロックのほうが高いことを示しています。
ジッター	ジッター（ミリ秒）

vManageおよびパケットキャプチャツールを使用したNTPのトラブルシューティング

vManageでのフローのシミュレートによる出力の確認

1. Monitor > Networkの順に選択して、Network Deviceダッシュボードを選択します。
2. 適切なvEdgeを選択します。
3. Troubleshootingオプションをクリックしてから、Simulate Flowsをクリックします。
4. ドロップダウンから送信元VPNとインターフェイスを指定し、宛先IPを設定し、アプリケーションをntpとして設定します。
5. Simulateをクリックします。

これにより、vEdgeからのNTPトラフィックに対して想定される転送動作が得られます。

vEdgeからのTCPDumpの収集

NTPトラフィックがvEdgeのコントロールプレーンを通過するときには、TCPdumpを使用してキャプチャできます。 一致条件では、標準UDPポート123を使用してNTPトラフィックをフィルタリングする必要があります。

tcpdump vpn 0オプション「dst port 123」

```
vedge1# tcpdump interface ge0/0 options "dst port 123"
tcpdump -p -i ge0_0 -s 128 dst port 123 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:05:44.364567 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:05:44.454385 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:05:45.364579 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:05:45.373547 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:52.364470 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:06:52.549536 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:54.364486 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:06:54.375065 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
```

verboseフラグ-vを追加して、NTPパケット内からタイムスタンプをデコードします。

tcpdump vpn 0オプション「dst port 123 -v」

```
vedge1# tcpdump interface ge0/0 options "dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:10:13.364515 IP (tos 0xb8, ttl 64, id 62640, offset 0, flags [DF], proto UDP (17), length 76)
    192.168.19.55.123 > 192.168.18.201.123: NTPv4, length 48
        Client, Leap indicator: clock unsynchronized (192), Stratum 3 (secondary reference), poll 6 (64
        Root Delay: 0.103881, Root dispersion: 1.073425, Reference-ID: 10.88.244.1
          Reference Timestamp:  3889015198.468340729 (2023/03/28 17:59:58)
          Originator Timestamp: 3889019320.559000091 (2023/03/28 19:08:40)
          Receive Timestamp:    3889019348.377538353 (2023/03/28 19:09:08)
          Transmit Timestamp:   3889019413.364485614 (2023/03/28 19:10:13)
            Originator - Receive Timestamp:  +27.818538262
            Originator - Transmit Timestamp: +92.805485523
19:10:13.365092 IP (tos 0xc0, ttl 255, id 7977, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002166, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889019384.881000144 (2023/03/28 19:09:44)
          Originator Timestamp: 3889019413.364485614 (2023/03/28 19:10:13)
          Receive Timestamp:    3889019385.557000091 (2023/03/28 19:09:45)
          Transmit Timestamp:   3889019385.557000091 (2023/03/28 19:09:45)
            Originator - Receive Timestamp:  -27.807485523
            Originator - Transmit Timestamp: -27.807485523
```

vManageからのWiresharkキャプチャの実行

vManageからパケットキャプチャが有効になっている場合は、Wiresharkで読み取り可能なファイルに直接NTPトラフィックをキャプチャすることもできます。

1. Monitor > Networkの順に選択して、Network Deviceダッシュボードを選択します。
2. 適切なvEdgeを選択します。
3. Troubleshootingオプションをクリックし、続いてPacket Captureをクリックします。
4. ドロップダウンメニューからVPN 0と外部インターフェイスを選択します。
5. Traffic Filterをクリックします。ここでは、宛先ポート123と、必要に応じて特定の宛先サーバを指定できます。

> 注:IPアドレスによるフィルタリングは、送信元または宛先によるIPフィルタであるため、一方向のパケットのみをキャプチャします。 宛先のレイヤ4ポートは両方向とも123であるため、ポートでフィルタリングして双方向トラフィックをキャプチャします。

6. [Start (スタート)] をクリックします。

vManageはvEdgeと通信して、5分間、または5 MBのバッファがいっぱいになるまでのいずれか早い方の時間のパケットキャプチャを収集します。完了したら、キャプチャをダウンロードして確認できます。

一般的なNTPの問題

NTP パケットが受信されない

パケットキャプチャは、設定されたサーバに送信された発信パケットを示しますが、応答は受信されていません。

```
vedge1# tcpdump interface ge0/0 options "dst 192.168.18.201 && dst port 123 -n"
tcpdump -p -i ge0_0 -s 128 dst 192.168.18.201 && dst port 123 -n in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
14:24:49.364507 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:25:55.364534 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:27:00.364521 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

NTPパケットが受信されていないことを確認したら、次の操作を実行できます。

- NTP が正しく設定されているかを確認します。
- トラフィックがVPN 0のトンネルを通過する場合、トンネルインターフェイスでallow-service ntpまたはallow-service allが有効になっていることを確認します。
- NTPがアクセスリストまたは中継装置によってブロックされているかどうかを確認します。
- NTPの送信元と宛先の間のルーティングの問題を確認します。

同期の喪失

サーバの分散値や遅延値が非常に高くなると、同期が失われる可能性があります。 高い値は、クロックのルートを基準として、サーバ/ピアからクライアントにパケットが到達するまでに時間がかかりすぎることを示します。 そのため、ローカルマシンは、パケットが到着するまでにかかった時間がわからないため、パケット内に存在する時間の精度を信頼できません。

パス内に輻輳したリンクがあり、それが原因でバッファリングが行われる場合、パケットは

NTPクライアントに到達すると遅延されます。

同期が失われる場合は、次のリンクを確認する必要があります。

- パスに輻輳またはオーバーサブスクリプションがあるか。
- ドロップされたパケットは確認されましたか。
- 暗号化は含まれていますか。

show ntp peerのreach値は、NTPトラフィックの損失を示している可能性があります。 この値が377未満の場合、パケットが断続的に受信され、クライアントの同期が失われます。

デバイスのクロックが手動で設定されている

NTPから学習したクロック値は、clock setコマンドで上書きできます。 この場合、すべてのピアのオフセット値が大幅に増加します。

```
vedge1# show ntp peer | tab

INDEX  REMOTE           REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
-------------------------------------------------------------------------------------
1      x10.88.244.1     LOCAL(1)  2   u     40    64    1      293.339  -539686  88.035
2      x172.18.108.15   .GPS.     1   u     39    64    1      30.408   -539686  8.768
3      x192.168.18.201  LOCAL(1)  8   u     38    64    1      5.743    -539686  2.435
```

詳細キャプチャでは、参照タイムスタンプと発信元タイムスタンプが一致していないことも示されます。

```
vedge1# tcpdump interface ge0/0 options "src 192.168.18.201 && dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 src 192.168.18.201 && dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
00:01:28.156796 IP (tos 0xc0, ttl 255, id 8542, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002365, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889091263.881000144 (2023/03/29 15:07:43)
          Originator Timestamp: 133810392.155976055 (2040/05/05 00:01:28)
          Receive Timestamp:    3889091277.586000096 (2023/03/29 15:07:57)
          Transmit Timestamp:   3889091277.586000096 (2023/03/29 15:07:57)
            Originator - Receive Timestamp:  -539686410.569975959
            Originator - Transmit Timestamp: -539686410.569975959
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
```

vEdgeに時刻源としてのNTPの設定を再開させるには、system ntpで設定を削除、コミット、再追加、および再コミットします。

参考資料および関連情報

- NTPの問題のトラブルシューティングとデバッグ（Cisco IOSデバイス）
- Cisco SD-WANコマンドリファレンス
- show ntp associations コマンドによる NTP ステータスの確認

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。