クイックスタートガイド – さまざまなSD-WAN問題のデータ収集

内容

概要

このドキュメントでは、TACケースをオープンする前に事前に収集する必要がある関連データに沿って、SD-WANに関するいくつかの問題について説明します。この問題を解決すると、トラブルシューティングの速度が向上します。このドキュメントは、次の2つの主要なテクニカルセクションに分かれています。vManageおよびEdgeルータ。関連する出力とコマンド構文は、対象のデバイスに応じて提供されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコのSDWANアーキテクチャ
- vManageコントローラ、cEdge（IOS-XE SD-WANルータ）およびvEdgeデバイス（ViptelaOSルータ）を含むソリューションに関する一般的な知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョン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、初期（デフォルト）設定の状態から起動しています。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。

基本情報の要求

- ネットワークおよびユーザに対する問題とその影響について説明する。 予想される動作を説明する。観察された動作を詳細に説明します。可能な場合は、手動で作成しても、アドレッシングを使用してトポロジ図を作成します。
- 問題はいつ始まったのですか。 問題が最初に発生した日時、または最初に発生した時刻を記録します。
- この問題の潜在的な引き金はどれか？ 問題が発生する前に行った最近の変更を文書化します。問題の発生を引き起こした特定のアクションまたはイベントに注意してください。この問題は、他のネットワークイベントやアクションに対応していますか。
- 問題はどの程度の頻度で発生するか これは1回限りの出来事でしたか？そうでない場合、問題はどの程度の頻度で発生しますか。
- 対象のデバイスに関する情報を提供します。 ランダムなデバイスではなく、特定のデバイスが影響を受ける場合、影響を受けるデバイスの共通点は何か各デバイスのシステムIPおよびサイトID。vManageクラスタに問題がある場合は、ノードの詳細を指定します（クラスタ内のすべてのノードで同じでない場合）。vManage GUI内の一般的な問題については、すべてのスクリーンショットをファイルにキャプチャして、エラーメッセージやその他の異常/不具合点を示し、調査する必要があります。
- TACの希望する結果と優先事項に関する情報を提供します。 できるだけ早く障害から回復するか、障害の根本原因を特定しますか？

vManage

ここでの問題は、vManageに関して報告される一般的な問題の状態と、admin-techファイルに加えて収集する必要がある問題ごとの有用な出力です。 クラウドホスト型コントローラの場合は、Technical Assistance Center(TAC)エンジニアは、明示的な同意を得たら、「Base Information Requested」セクションのフィードバックに基づいて、デバイスに必要な**admin-tech出力を収集できます**。ただし、に含まれるデータが問題の発生時刻に関連していることを確認するために、ここで説明する手順が必要な場合は、admin-techの出力をキャプチャすることをお勧めします。これは、問題が永続的でない場合に特に当てはまります。つまり、TACが取り組む間に問題が消える可能性があります。オンプレミスのコントローラの場合は、**admin-techを各データセットに含める必要があります。**vManageクラスタの場合は、クラスタ内の各ノー**ドまたは影響を受ける**ノードのadmin-techをキャプチャしてください。

遅さ/緩慢

問題レポート：vManage GUIへのアクセスの遅さ、GUI内で操作を実行するときの遅延、vManage内での一般的な速度低下または速度低下

ステップ1：スレッド印刷の2 ~ 3インスタンスをキャプチャし、各スレッド印刷ファイルの名前

を数字で指定した名前に変更します（ファイルパスでvManageにログインするユーザ名を使用することに注意してください）。

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.1
```

ステップ2:vshellにログインし、次のようにvmstatを実行します。

```
vManage# vshell
vManage:~$ vmstat 1 10
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
1 0 0 316172 1242608 5867144 0 0 1 22 3 5 6 1 93 0 0
0 0 0 316692 1242608 5867336 0 0 0 8 2365 4136 6 1 93 0 0
0 0 0 316204 1242608 5867344 0 0 0 396 2273 4009 6 1 93 0 0
0 0 0 316780 1242608 5867344 0 0 0 0 2322 4108 5 2 93 0 0
0 0 0 318136 1242608 5867344 0 0 0 0 2209 3957 9 1 90 0 0
0 0 0 318300 1242608 5867344 0 0 0 0 2523 4649 5 1 94 0 0
1 0 0 318632 1242608 5867344 0 0 0 44 2174 3983 5 2 93 0 0
0 0 0 318144 1242608 5867344 0 0 0 64 2182 3951 5 2 94 0 0
0 0 0 317812 1242608 5867344 0 0 0 0 2516 4289 6 1 93 0 0
0 0 0 318036 1242608 5867344 0 0 0 0 2600 4421 8 1 91 0 0
vManage:~$
```

ステップ3:vshellから詳細を収集します。

```
vManage:~$ top (press '1' to get CPU counts)
vManage:~$ free -h
vManage:~$ df -kh
```

ステップ4：すべてのNMSサービス診断をキャプチャします。

```
vManage# request nms application-server diagnostics
vManage# request nms configuration-db diagnostics
vManage# request nms messaging-server diagnostics
vManage# request nms coordination-server diagnostics
vManage# request nms statistics-db diagnostics
```

APIの障害/問題

問題レポート：API呼び出しは、データまたは正しいデータを返すことができず、クエリを実行する一般的な問題です

ステップ1：使用可能なメモリを確認します。

```
vManage:~$ free -h
total used free shared buff/cache available
Mem: 31Gi 24Gi 280Mi 60Mi 6.8Gi 6.9Gi
Swap: 0B 0B 0B
vManage:~$
```

ステップ2:5秒のギャップを持つスレッド印刷の2-3インスタンスをキャプチャし、コマンドの実行のたびにに、各スレッド印刷ファイルの名前を数字で変更します（ファイルパスでvManageにログインするユーザ名を使用します）。

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.1
<WAIT 5 SECONDS>
```

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.2
```
ステップ3：アクティブなHTTPセッションの詳細を収集します。

```
vManage# request nms application-server jcmd gc-class-histo | i
io.undertow.server.protocol.http.HttpServerConnection
```
ステップ4：次の詳細を入力します。

1.実行されたAPIコール

（二）呼び出し回数

3.ログイン方式（1つのトークンを使用して後続のAPI呼び出しを実行する方法、または基本認証を使用して呼び出しを実行してからログアウトする方法）

4. JSESSIONIDは再利用されていますか？

> **注**19.2 vManageソフトウェア以降、API呼び出しではトークンベース認証だけがサポートされています。トークンの生成、タイムアウト、有効期限の詳細については、このリンクを参照し[てください](#)。

ディープパケットインスペクション(DPI)統計情報/速度低下

問題レポート：DPIを有効にすると、vManage GUI内で統計処理が遅くなったり、速度低下が発生したりする可能性があります。

ステップ1:vManage内部のDPIに割り当てられたディスクサイズを確認するには、**[Administration] > [Settings] > [Statistics Database] > [Configuration]に移動します。**

ステップ2:vManageから次のCLIコマンドを実行して、インデックスの健全性を確認します。

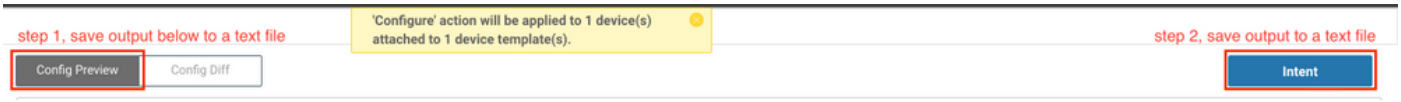
```
vManage# request nms statistics-db diagnostics
```
ステップ3:DPI統計に関連するAPIコールが外部で実行されているかどうかを確認します。

ステップ4:vManageから次のCLIコマンドを使用して、ディスクI/O統計情報を確認します。

```
vManage# request nms application-server diagnostics
```
テンプレートプッシュの失敗

問題レポート：テンプレートプッシュまたはデバイステンプレートの更新が失敗するか、タイムアウトします。

ステップ1:[Configure Devices]ボタンをクリックする前に、vManageから**Config Preview**と**Intent** configをキャプチャします(**次のナビゲーションの例を参照)。**



ステップ2:**logsettings**ページから**viptela.enable.rest.logを有効にします**（必要な情報をキャプチャ

した後は、無効にする必要があります）。

```
https://<vManage IP>:8443/logsettings.html
```

ステップ3：テンプレートプッシュの失敗にNETCONFの問題またはエラーが含まれる場合は、ステップ1のREST口グに加えて**viptela.enable.device.netconf.logを有効にします。ステップ3とステップ4の出力がキャプチャされた後も、この口グを無効にします。**

ステップ4：次のCLIを使用して、vManageから失敗したテンプレートを再び添付し、**admin-techをキャプチャします**（クラスタの各ノードに対してキャプチャします）。

```
vManage# request admin-tech
```

ステップ5:vManageおよびConfig Diffのタスクのスクリーンショットを提供して、テンプレートに使用するCSVファイルとともに障害の詳細を確認します。

ステップ6：障害が発生したプッシュの時間、障害が発生したデバイスの**system-ip**、vManage GUIに表示されるエラーメッセージなど、障害とタスクの詳細を含めます。

ステップ7：デバイス自体によって設定に関して報告されたエラーメッセージでテンプレートプッシュの失敗が発生した場合は、デバイスからも**admin-techを収集**してください。

クラスタ関連の問題

問題レポート：クラスタの不安定性が原因で、GUIのタイムアウトや不調、その他の異常が発生する。

ステップ1：クラスタ内の各vManageノードから**server_configs.json**の出力をキャプチャします。以下に、いくつかの例を示します。

```
vmanage# vshell
vmanage:~$ cd /opt/web-app/etc/
vmanage:/opt/web-app/etc$ more server_configs.json | python -m json.tool
{
"clusterid": "",
"domain": "",
"hostsEntryVersion": 12,
"mode": "SingleTenant",
"services": {
"cloudAgent": {
"clients": {
"0": "localhost:8553"
},
"deviceIP": "localhost:8553",
"hosts": {
"0": "localhost:8553"
},
"server": true,
"standalone": false
},
"container-manager": {
"clients": {
"0": "169.254.100.227:10502"
},
"deviceIP": "169.254.100.227:10502",
"hosts": {
```

```
"0": "169.254.100.227:10502"
},
"server": true,
"standalone": false
},
"elasticsearch": {
"clients": {
"0": "169.254.100.227:9300",
"1": "169.254.100.254:9300",
"2": "169.254.100.253:9300"
},
"deviceIP": "169.254.100.227:9300",
"hosts": {
"0": "169.254.100.227:9300",
"1": "169.254.100.254:9300",
"2": "169.254.100.253:9300"
},
"server": true,
"standalone": false
},
"kafka": {
"clients": {
"0": "169.254.100.227:9092",
"1": "169.254.100.254:9092",
"2": "169.254.100.253:9092"
},
"deviceIP": "169.254.100.227:9092",
"hosts": {
"0": "169.254.100.227:9092",
"1": "169.254.100.254:9092",
"2": "169.254.100.253:9092"
},
"server": true,
"standalone": false
},
"neo4j": {
"clients": {
"0": "169.254.100.227:7687",
"1": "169.254.100.254:7687",
"2": "169.254.100.253:7687"
},
"deviceIP": "169.254.100.227:7687",
"hosts": {
"0": "169.254.100.227:5000",
"1": "169.254.100.254:5000",
"2": "169.254.100.253:5000"
},
"server": true,
"standalone": false
},
"orientdb": {
"clients": {},
"deviceIP": "localhost:2424",
"hosts": {},
"server": false,
"standalone": false
},
"wildfly": {
"clients": {
"0": "169.254.100.227:8443",
"1": "169.254.100.254:8443",
"2": "169.254.100.253:8443"
},
"deviceIP": "169.254.100.227:8443",
```

```
"hosts": {
"0": "169.254.100.227:7600",
"1": "169.254.100.254:7600",
"2": "169.254.100.253:7600"
},
"server": true,
"standalone": false
},
"zookeeper": {
"clients": {
"0": "169.254.100.227:2181",
"1": "169.254.100.254:2181",
"2": "169.254.100.253:2181"
},
"deviceIP": "169.254.100.227:2181",
"hosts": {
"0": "169.254.100.227:2888:3888",
"1": "169.254.100.254:2888:3888",
"2": "169.254.100.253:2888:3888"
},
"server": true,
"standalone": false
}
},
"vmanageID": "0"
}
```


ステップ2：各ノードで有効または無効になっているサービスの詳細をキャプチャします。これを行うには、vManage GUIで**[Administration] > [Cluster Management]**に移動します。

ステップ3：クラスタインターフェイスでアンダーレイの到達可能性を確認します。このため、**VPN 0の各vManageノードから他のノードのクラスタインターフェイスIPにping <ip-address>**を実行します。

ステップ4：クラスタ内の各vManageノードのすべてのNMSサービスから診断を収集します。

```
vManage# request nms application-server diagnostics
vManage# request nms configuration-db diagnostics
vManage# request nms messaging-server diagnostics
vManage# request nms coordination-server diagnostics
vManage# request nms statistics-db diagnostics
```

エッジ(vEdge/cEdge)

ここで問題となるのは、エッジデバイスに関して報告される一般的な問題の状態と、収集する必要があるそれぞれの有用な出力です。各問題について、必要な関連するエッジデバイス**すべてに対して**admin-techが収集されていることを確認します。クラウドホスト型コントローラの場合、TACは、「**Base Information Requested**」セクションのフィードバックに基づいて、デバイスに必要な管理者テクノロジー出力を収集するアクセス権を持つことができます。ただし、vManageの場合と同様に、TACケースをオープンする前に、これらの情報をキャプチャする必要があり、に含まれるデータが問題の発生時刻に関連していることを確認できます。これは、問題が永続的でない場合に特に当てはまります。つまり、TACが取り組む時点で問題が消失する可能性があります。

デバイスとコントローラの間に形成されない制御接続

問題レポート：vEdge/cEdgeから1つ以上のコントローラへの制御接続が形成されない

ステップ1：制御接続の失敗のローカル/リモートエラーを特定します。

- vEdge:**show control connections**-history**コマンドの出**力。
- cEdge:**show sdwan control connection**-history**コマンドの出**力。

ステップ2:TLOCの状態を確認し、anyとすべての表示が「up」であることを確認します。

- vEdge:**show control local-properties**コマンドの出力。
- cEdge:**show sdwan control local-properties**コマンドの出力。

ステップ3：タイムアウトまたは接続障害（DCONFAILまたはVM_TMOなど）に関するエラーの場合は、エッジデバイスと問題のコントローラの両方でコントロールプレーンキャプチャを取得します。

- コントローラの場合：

```
vManage# tcpdump vpn 0 interface eth1 options "-vvvvvv host 192.168.44.6"
tcpdump -p -i eth1 -s 128 -vvvvvv host 192.168.44.6 in VPN 0
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 128 bytes
20:02:07.427064 IP (tos 0xc0, ttl 61, id 50139, offset 0, flags [DF], proto UDP (17), length
168)
192.168.44.6.12346 > 192.168.40.1.12346: UDP, length 140
20:02:07.427401 IP (tos 0xc0, ttl 64, id 37220, offset 0, flags [DF], proto UDP (17), length
210)
192.168.40.1.12346 > 192.168.44.6.12346: UDP, length 182
```

- vEdge:

```
vEdge-INET-Branch2# tcpdump vpn 0 interface ge0/2 options "-vvvvvv host 192.168.40.1"
tcpdump -p -i ge0_2 -vvvvvv host 192.168.40.1 in VPN 0
tcpdump: listening on ge0_2, link-type EN10MB (Ethernet), capture size 262144 bytes
20:14:16.136276 IP (tos 0xc0, ttl 64, id 55858, offset 0, flags [DF], proto UDP (17), length
277)
10.10.10.1 > 192.168.40.1.12446: [udp sum ok] UDP, length 249
20:14:16.136735 IP (tos 0xc0, ttl 63, id 2907, offset 0, flags [DF], proto UDP (17), length 129)
192.168.40.1.12446 > 10.10.10.1.12346: [udp sum ok] UDP, length 101
```

- cEdge(以下のキャプチャは、デバイスがCLIモードに移行し、フィルタ用に**CTRL-CAPと呼ばれるアクセスコントロールリスト(ACL)が作成されたことを前提としています。**アプリケーション/ネットワークパフォーマンスのシナリオのEPCキャプチャの例を参照):

```
cEdge-Branch1#config-transaction
cEdge-Branch1(config)# ip access-list extended CTRL-CAP
cEdge-Branch1(config-ext-nacl)# 10 permit ip host 10.10.10.1 host 192.168.40.1
cEdge-Branch1(config-ext-nacl)# 20 permit ip host 192.168.40.1 host 10.10.10.1
cEdge-Branch1(config-ext-nacl)# commit
cEdge-Branch1(config-ext-nacl)# end

cEdge-Branch1#monitor capture CAP control-plane both access-list CTRL-CAP buffer size 10
cEdge-Branch1#monitor capture CAP start

cEdge-Branch1#show monitor capture CAP buffer brief
------------------------------------------------------------------------
# size timestamp source destination dscp protocol
------------------------------------------------------------------------
0 202 0.000000 192.168.20.1 -> 50.50.50.3 48 CS6 UDP
1 202 0.000000 192.168.20.1 -> 50.50.50.4 48 CS6 UDP
2 220 0.000000 50.50.50.3 -> 192.168.20.1 48 CS6 UDP
3 66 0.000992 192.168.20.1 -> 50.50.50.3 48 CS6 UDP
```

```
4 220 0.000992 50.50.50.4 -> 192.168.20.1 48 CS6 UDP
5 66 0.000992 192.168.20.1 -> 50.50.50.4 48 CS6 UDP
6 207 0.015991 50.50.50.1 -> 12.12.12.1 48 CS6 UDP
```

ステップ4：制御接続履歴の出力で確認されたその他のエラーや、説明されている問題の詳細については、次のガイドを参照してください。

エッジデバイスとコントローラ間のコントロール接続のフラッピング

問題レポート：vEdge/cEdgeと1つ以上のコントローラの間で1つ以上の制御接続がフラップします。これは、本質的に頻繁に発生する、断続的な、またはランダムな場合があります。

- 制御の接続フラップは、通常、デバイスとコントローラ間のパケット損失または転送の問題の結果です。障害の方向性に応じて、TMOエラーに結び付けられることが多いです。これを確認するには、最初にフラップの理由を確認します。 vEdge/コントローラの場合：**show control connections**-history**コマンドの出**力。cEdge:**show sdwan control connection**-history**コマンドの出**力。
- TLOCの状態を確認し、フラッピングが発生したときにanyとすべてのデバイスが「up」であることを確認します。 vEdge:**show control local-properties**コマンドの出力を確認します。cEdge:**show sdwan control local-properties**コマンドの出力
- コントローラとエッジデバイスの両方でパケットキャプチャを収集します。各サイドのキャプチャ**パラメータの詳細は、「デバイスとコントローラ間の制御接**続が形成されない」セクションを参照してください。

エッジデバイス間で形成またはフラッピングを行わない双方向フォワーディング検出(BFD)セッション

問題レポート：BFDセッションがダウンしているか、2つのエッジデバイス間でフラッピングが発生しています。

ステップ1：各デバイスのBFDセッションの状態を収集します。

- vEdge:**show bfd sessionsコマンドの**出力。
- cEdge:**show sdwan bfd sessionsコマンドの**出力。

ステップ2：各エッジルータでRxおよびTxパケットカウントを収集します。

- vEdge:**show tunnel statistics bfdコマンドの**出力。
- cEdge:**show platform hardware qfp active feature bfd datapath sdwan summaryコマンドの出力**です。

ステップ3：上記の出力のトンネルの一方の端でBFDセッションのカウンタが増加しない場合は、ACLを使用してキャプチャを行い、パケットがローカルで受信されているかどうかを確認できます。他の検証と同様に、この検証に関する詳細については、こちらをご覧ください。

デバイスのクラッシュ

問題レポート：デバイスが予期せずリロードされ、電源に関する問題は除外されます。デバイスから、クラッシュが発生した可能性があることが示されています。

ステップ1：デバイスを確認して、クラッシュまたは予期しないリロードが発生したかどうかを確認します。

- vEdge:show reboot historyコマンドの出力。
- cEdge:show sdwan reboot historyコマンドの出力を確認します。
- または、[Monitor] > [Network]に移動し、デバイスを選択し、[System Status] > [Reboot]に移動して、予期しないリロードが発生したかどうかを確認します。

ステップ2：確認したら、[Tools] > [Operational Commands]の順に移動して、vManageを使用してデバイスからadmin-techをキャプチャします。その後、デバイスの[Options]ボタンを選択し、[Admin Tech]を選択します。すべてのチェックボックスがオンになっていることを確認します。デバイス上のすべてのログとコアファイルが含まれます。

サイト間のアプリケーション/ネットワークパフォーマンスの低下または障害

問題レポート：アプリケーションが動作しない、またはHTTPページがロードされない、パフォーマンスの遅れ/遅延、ポリシーまたは設定変更の後の障害

ステップ1：問題が発生しているアプリケーションまたはフローの送信元/宛先IPペアを特定します。

ステップ2：パス内のすべてのエッジデバイスを特定し、vManageを介して各デバイスからadmin-techを収集します。

ステップ3：問題が発生したときに、このフローの各サイトのエッジデバイスでパケットキャプチャを実行します。

- vEdge: [管理(Administration)] > [ホスト名の設定(Settings)]フィールドで[Data Stream]を有効にし、vManageのシステムIPを入力します。VPN 0には、0と入力しますvManage VPN 0インターフェイスのallow-service設定でHTTPSが有効になっていることを確認します。次の手順に従って、サービス側のVPNインターフェイスのトラフィックをキャプチャします。
- cEdge: [Configuration] > [Devices] > [Change Mode] > [CLI mode]を使用して、cEdgeをCLIモードに移動しますcEdgeで、トラフィックを双方向に照合するように拡張ACLを設定します。キャプチャのサイズとデータを制限するために、プロトコルとポートを含めるようにできるだけ具体的にします。
- (b)で作成したACLを使用してトラフィックをフィルタし、サービス側インターフェイスにEmbedded Packet Capture(EPC)を両方向で設定します。キャプチャはPCAP形式にエクスポートし、ボックスからコピーできます。BROKEN-FLOWという名前のACLを使用したルータ上のGigabitEthernet0/0/0の設定例を次に示します。

```
monitor capture CAP interface GigabitEthernet0/0/0 both access-list BROKEN-FLOW buffer size 10
monitor capture CAP start

show monitor capture CAP parameter
show monitor capture CAP buffer [brief]

monitor capture CAP export bootflash:cEdge1-Broken-Flow.pcap
```

- (b)で作成したACLを使用して、両方向のトラフィックのパケットトレースを設定します。設定例を次に示します。

```
debug platform packet-trace packet 2048 fia-trace
debug platform packet-trace copy packet input l3 size 2048
debug platform condition ipv4 access-list BROKEN-FLOW both
debug platform condition start
```

```
show platform packet-trace summary
show platform packet-trace packet all | redirect bootflash:cEdge1-PT-OUTPUT.txt
```

ステップ4：可能であれば、作業シナリオでステップ3を繰り返して比較します。

ヒント: cEdgeから対応するファイルを直接コピーする方法が他にない場合は、ここで説明する方法を使用して、最初にファイルをvManageにコピーできます。vManageでコマンドを実行します。
scp -P 830 <username>@<cEdge system-IP>:/bootflash/<filename>を実行します。
このファイルは、vManageへのログインに使用したユーザ名の**ディレクトリ /home/<username>/**に保存されます。そこから、Secure Copy Protocol(SCP)のSFTP(Secure File Transfer Protocol)を使用して、サードパーティのSCP/SFTPクライアントまたはOpenSSHユーティリティを使用したLinux/UNIXマシンCLIを使用してvManageからファイルをコピーできます。