快速入门指南 — 针对各种SD-WAN问题的数据收集

目录

简介

本文档介绍在打开TAC案例之前必须先收集的相关数据中的几个SD-WAN问题，以提高故障排除和/或问题解决速度。本文档分为两个主要技术部分：vManage和Edge路由器。根据相关设备提供相关输出和命令语法。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科的SDWAN架构
- 对解决方案的一般了解，包括vManage控制器以及cEdge（IOS-XE SD-WAN路由器）和vEdge设备（ViptelaOS路由器）

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

请求的基本信息

- 描述问题及其对网络和用户的影响： 描述预期行为。详细描述观察到的行为。尽可能准备带编址的拓扑图，即使是手动绘制。
- 问题是何时开始的？ 注意第一次观察/注意到问题的日期和时间。
- 此问题的潜在触发因素可能是什么？ 记录问题开始之前所做的任何最近更改。请注意发生的任何可能触发问题启动的特定操作或事件。此问题是否与任何其他网络事件或操作相对应？
- 问题的频率是多少？ 这是一次吗？如果不是，问题多久发生一次？
- 提供有关相关设备的信息： 如果特定设备受到影响（非随机），它们有什么共同点？每台设备的系统IP和站点ID。如果问题出在vManage群集上，请提供节点详细信息（如果不是在群集中所有节点上相同）。对于vManage GUI中的一般问题，请将所有屏幕截图捕获到显示错误消息或其他需要调查的异常/异常的文件。
- 提供有关TAC预期结果和您的优先级的信息： 是否要尽快从故障中恢复或找出故障的根本原因？

vManage

此处的问题是报告给vManage的常见问题情况，以及除admin-tech文件外必须收集的每**个问题**的有用输出。 对于云托管控制器，如果您明确同意，技术支持中心(TAC)工程师可以根据“基本信息请求”部分中的反馈收集设备所需的**admin-tech**输出。但是，如果此处描述的**步骤确保其中包含的**数据与问题发生时间相关，我们建议捕获admin-tech输出。如果问题不是持续的，即问题在TAC参与时可能消失。对于内部控制器**,admin-tech** 也必须包含在每组数据中**。**对于vManage群集，请确保为群集中的**每个节**点或仅为受影响的节点捕获管理技术。

慢/懒

问题报告：访问vManage GUI的速度慢、在GUI内执行操作时的延迟、在vManage内普遍的速度慢或速度慢

步骤1.捕获2-3个线程打印实例，在每个线程打印文件后**用数字**名称重命名每个线程打印文件（注意在文件路径中使用您登录vManage时使用的用户名），例如：

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

步骤2.登录vshell并**按**如下方**式运**行vmstat:

```
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:~$
```

步骤3.从vshell收集其他详细**信息**:

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

步骤4.捕获所有NMS服务诊断：

```
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故障/问题

问题报告：API调用无法返回任何数据或正确的数据，执行查询时出现一般问题

步骤1.检查可用内存：

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

步骤2.捕获2-3个线程打印实例，其间有5秒的间隙，在每次运行命令后，使用数字名称重命名每个**线程打印**文件（注意在文件路径中使用您登录到vManage的用户名）：

```
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
```

步骤3.收集所有活动HTTP会话的详细信息：

```
vManage# request nms application-server jcmd gc-class-histo | i
io.undertow.server.protocol.http.HttpServerConnection
```

步骤4.提供以下详细信息：

1.执行的API调用

2.调用频率

3.登录方法（即使用单个令牌执行后续API调用或使用基本身份验证执行调用然后注销）

4. JSESSIONID是否正在重新使用？

> **注**意从19.2 vManage软件开始，API调用仅支持基于令牌的身份验证。有关令牌生成、超时和过期的详细信息，请参阅此链接。

深度数据包检测(DPI)统计信息/慢度

问题报告：启用DPI后，统计处理速度可能会变慢，或在vManage GUI内引入速度变慢。

步骤1.导航至Administration > Settings > Statistics Database > Configuration，检查为vManage内部的DPI分**配的磁盘大小**。

步骤2.从vManage运行以下CLI命令，检查索引运行状况：

```
vManage# request nms statistics-db diagnostics
```

步骤3.确认是否在外部执行与DPI统计信息相关的任何API调用。

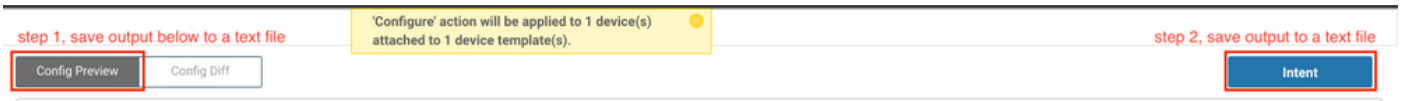
步骤4.在vManage中使用此CLI命令帮助检查磁盘I/O统计信息：

```
vManage# request nms application-server diagnostics
```

模板推送失败

问题报告：模板推送或设备模板更新失败或超时。

步骤1.在单击"配置设**备"按**钮之前，**从vManage捕获"配置预**览"和**意图"**配置（此处提供的导航示例）：



步骤2.从**logsettings页面启**用**viptela.enable.rest.log**（捕获所需信息后必须禁用此功能）：

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

步骤3.如果模板推送失败涉及NETCONF问题或错误，请在步骤1中除REST日志外启用**viptela.enable.device.netconf.log**。请注意，在捕获步骤3和步骤4的输出后，还必须禁用此日志。

步骤4.尝试再次从vManage附加失败模板，并使用此CLI**捕获管理**技术（为群集的每个节点捕获此）：

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

步骤5.提供vManage和配置差异中任务的屏幕截图，以确认故障详细信息以及用于模板的任何CSV文件。

步骤6.包括有关故障和任务的详细信息，包括推送失败的时间、发生故障的设备的**system-ip**和您在vManage GUI中看到的错误消息。

步骤7.如果模板推送失败，且设备自身报告了配置的错误消息，请从设**备收集**管理技术。

群集相关问题

问题报告：群集不稳定导致GUI超时、延迟或其他异常。

步骤1.从集群中的每个vManage节点捕获server_configs.json的输出。例如：

```
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"
}
```


步骤2.捕获每个节点启用或禁用服务的详细信息。为此，请导航至**vManage GUI中的Administration** > Cluster Management。

步骤3.确认集群接口上的底层可达性。为此，从VPN 0中**的每个vManage节点**对其他节点的集群接口IP运行ping <ip-address>。

步骤4.从集群中每个vManage节点的所有NMS服务收集诊断信息：

```
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
```

边缘(vEdge/cEdge)

此处的问题是为边缘设备报告的常见问题情况，以及必须收集的每个设备的有用输出。确保针对每个问题收集**所有必**要且相关的边缘设备的管理技术。对于云托管控制器，TAC可以根据“基本信息请求”部分中的反馈收集设备所需的管理技**术输出**信息。但是，与vManage一样，在您提交TAC案例前，可能需要捕获这些数据，以确保其中包含的数据与问题发生时间相关。如果问题不是持续的，则具体如此，这意味着在TAC参与时，问题可能消失。

设备和控制器之间未形成控制连接

问题报告：控制连接不从vEdge/cEdge到一个或多个控制器

步骤1.确定控制连接失败的本地/远程错误：

- 对于vEdge:show control connections-**history命令的输**出。
- 对于cEdge:show sdwan control connection-history**命令的输**出。

步骤2.确认TLOC的状态，并确认any和all显示为“up”：

- 对于vEdge:show control local-**properties命令的输**出。
- 对于cEdge:show sdwan control local-**properties命令的输**出。

步骤3.对于超时或连接故障（如DCONFAIL或VM_TMO）的错误，请在边缘设备和相关控制器上执行控制平面捕获：

- 对于控制器：

```
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
```

- 对于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
```

- 对于cEdge(以下捕获假设设备已移至CLI模式，并且已创建名为**CTRL-CAP**的访问控制列表(ACL)进行过滤 — 请参阅应用/网络性能场景中EPC捕获示例中的更**多详细**信息):

```
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
```

步骤4.有关控制连接历史记录输出中观察到的其他错误以及所描述问题的更多详细信息，请参阅以下指南。

控制边缘设备和控制器之间的连接抖动

问题报告：vEdge/cEdge和一个或多个控制器之间的一个或多个控制连接摆动。这在本质上可以是频繁、间歇或随机的。

- 控制连接摆动通常是设备与控制器之间丢包或转发问题的结果。通常，这会与TMO错**误相**关，具体取决于故障的方向性。要进一步检查，请首先验证抖动的原因： 对于vEdge/控制器：show control connections**-history命令的输**出。对于cEdge:show sdwan control connection-history**命令的输**出。
- 确认TLOC的状态，并确认发生抖动时any和all显示为“up”： 对于vEdge:show control local**-properties命令的**输出。对于cEdge:show sdwan control local**-properties命令的**输出。
- 收集控制器和边缘设备上的数据包捕获。有关各端捕获参**数的详细信息，请参**阅设备和控制器之间未形成控制连接部分。

边缘设备之间未形成或抖动的双向转发检测(BFD)会话

问题报告：BFD会话关闭或在两个边缘设备之间摆动。

步骤1.收集每台设备上BFD会话的状态：

- 对于vEdge:show bfd sessions**命令的输**出。
- 对于cEdge:show sdwan bfd sessions**命令的输**出。

步骤2.收集每个边缘路由器上的Rx和Tx数据包计数：

- 对于vEdge:show tunnel statistics bfd**命令的输**出。
- 对于cEdge:show platform hardware qfp active feature bfd datapath sdwan summary命**令的输**

出。
步骤3.如果上述输出中隧道一端的BFD会话计数不增加，则可以使用ACL捕获数据，以确认是否在本地接收数据包。有关此操作的更多详细信息以及可执行的其他验证，请点击。

设备崩溃

问题报告：设备意外重新加载，排除电源问题。来自设备的指示表明它可能崩溃。

步骤1.检查设备以确认是否观察到崩溃或意外重新加载：

- 对于vEdge:show reboot history**命令的输**出。
- 对于cEdge:show sdwan reboot history**命令的输**出。
- 或者，导航至**Monitor > Network**，选择设备，然后导航至**System Status > Reboot，以确**认是否发现任何意外重新加载。

步骤2.如果确认，请导航至Tools > Operational Commands，通过vManage从设备捕获管理技术。在该位置后，选择设**备的**“选项”按钮并选择“**管理技术**”。确保选中所有复选框，其中将包括设备上的所有日志和核心文件。

站点间应用/网络性能降低或失败

问题报告：应用不工作/HTTP页面未加载、性能缓慢/延迟、策略或配置更改后出现故障

步骤1.确定出现问题的应用或流的源/目的IP对。

步骤2.确定路径中的所有边缘设备，并通过vManage从**每个设备**收集管理技术。

步骤3.发现问题时，在每个站点的边缘设备上捕获此流的数据包：

- 对于vEdge: 在“管理”**>“主机名**设置”**字段**下，输入vManage的系统IP。对于**VPN**，输入**0**确保在vManage VPN 0接口**的允许服**务配置下启用HTTPS。按照此处的步骤捕获服务端VPN接口上的流量。
- 对于cEdge: 通过Configuration > Devices > Change Mode > CLI模式将cEdge移**动到CLI模式**在cEdge上，配置扩展ACL以双向匹配流量。请尽可能具体地包括协议和端口，以限制捕获中的大小和数据。
- 使用(b)中创建的ACL过滤流量，为服务端接口在两个方向上配置嵌入式数据包捕获(EPC)。捕获可导出为PCAP格式并从框中复制。此处提供了使用名为BROKEN-FLOW的ACL的路由器上GigabitEthernet0/0/0的**配置示例**:

```
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
```

- 使用(b)中创建的ACL为两个方向的流量配置数据包跟踪。下面提供了配置示例：

```
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
```

步骤4.如果可能，在工作场景中重复步骤3进行比较。

提示：如果没有其他方法可以直接将相应文件从cEdge中复制出来，则可以首先使用此处所述的方法将文件复制到vManage。在vManage上运行命令：**request execute scp -P 830 <username>@<cEdge system-IP>:/bootflash/<filename> 。**然后，此文件将存储在**/home/<username>/**目录中，用于登录vManage的用户名。从中，您可以使用安全文件传输协议(SFTP)的安全复制协议(SCP)，使用第三方SCP/SFTP客户端或带有OpenSSH实用程序的Linux/Unix计算机CLI将文件从vManage中复制。