排除SD-WAN控制连接故障

目录

简介

背景信息

问题场景

- DTLS连接故障(DCONFAIL)
- TLOC禁用(DISTLOC)
- Board-ID not Initialized(BIDNTPR)
- BDSGVERFL — 主板ID签名失败
- 停滞在连接中：路由问题
- 套接字错误(LISFD)
- 对等体超时问题(VM_TMO)
- 序列号不存在(CRTREJSER、BIDNTVRFD)
- 组织不匹配(CTORGNMIS)
- vEdge/vSmart证书已撤销/无效(VSCRTREV/CRTVERFL)
- vManage中未附加vEdge模板
- 瞬态条件(DISCVBD、SYSIPCHNG)
- DNS故障

相关信息

简介

本文档介绍导致控制连接出现问题的某些可能原因，以及如何排除这些原因的故障。

背景信息

> 注意：本文档中介绍的大多数命令输出来自vEdge路由器。但是，运行Cisco IOS® XE SD-WAN软件的路由器采用相同的方法。输入关键字 **sdwan**，以便在Cisco IOS XE SD-WAN软件上获得相同的输出。例如 **show sdwan control connections**，不用 **show control connections**.

在进行故障排除之前，请确保有问题的WAN Edge已正确配置。

此命令包括：

- 已安装的有效证书。

- 这些配置已放置在块下system方：
  - 系统IP
  - 站点ID
  - 组织名称
  - vBond address
- 使用Tunnel选项和IP地址配置的VPN 0传输接口。
- 在vEdge上正确配置的系统时钟以及与其他设备/控制器匹配的系统时钟：

该命**show clock**令确认当前设置的时间。

输入命**clock set**令以在设备上设置正确的时间。

对于前面提到的所有情况，请确保传输定位器(TLOC)已启用。使用命令检查此**show control local-properties**项。

有效输出的示例如下所示：

<#root>

```
branch-vE1#

show control local-properties

personality                    vedge
organization-name              vIPtela Inc Regression
certificate-status             Installed
root-ca-chain-status           Installed

certificate-validity           Valid
certificate-not-valid-before Sep 06 22:39:01 2018 GMT
certificate-not-valid-after  Sep 06 22:39:01 2019 GMT

dns-name                       vbond-dns-name.cisco.com
site-id                        10
domain-id                      1
protocol                       dtls
tls-port                       0
system-ip                      10.1.10.1
chassis-num/unique-id          66cb2a8b-2eeb-479b-83d0-0682b64d8190
serial-num                     12345718
vsmart-list-version            0
keygen-interval                1:00:00:00
retry-interval                 0:00:00:17
no-activity-exp-interval       0:00:00:12
dns-cache-ttl                  0:00:02:00
port-hopped                    TRUE
time-since-last-port-hop       20:16:24:43
number-vbond-peers             2

INDEX   IP                  PORT
------------------------------
```

```
0       10.3.25.25          12346
1       10.4.30.30          12346

number-active-wan-interfaces 2

 PUBLIC      PUBLIC  PRIVATE     PRIVATE                                    RESTRICT/   LAST         MAX
INTERFACE  IPv4        PORT    IPv4        PORT     VS/VM COLOR       CARRIER  STATE CONTROL     CONNEC
-------------------------------------------------------------------------------------------------------
ge0/1      10.1.7.11    12346   10.1.7.11    12346     2/1  gold        default  up      no/yes    0:00
ge0/2      10.2.9.11    12366   10.2.9.11    12366     2/0  silver      default  up      no/yes    0:00
```

在vEdge软件版本16.3及更高版本中，输出还有几个附加字段：

```
number-vbond-peers           1
number-active-wan-interfaces 1


NAT TYPE: E -- indicates End-point independent mapping
          A -- indicates Address-port dependent mapping
          N -- indicates Not learned
          Note: Requires minimum two vbonds to learn the NAT type

          PUBLIC        PUBLIC PRIVATE      PRIVATE                PRIVATE                          MAX
INTERFACE  IPv4          PORT   IPv4         IPv6                    PORT   VS/VM COLOR         STATE CN
                                                                                                STUN
-------------------------------------------------------------------------------------------------------
ge0/4  172.16.0.20   12386  192.168.0.20  2601:647:4380:ca75::c2  12386  2/1  public-internet  up   2
```

问题场景

DTLS连接故障(DCONFAIL)

这是控制连接的常见问题之一，但无法实现。可能的原因包括防火墙或某些其他连接问题。

有可能是某些或所有数据包在某个位置被丢弃/过滤。文中给出了较大值情况下的算例**tcpdump** 。

- 下一跳(NH)路由器无法到达。
- 路由信息库(RIB)中未安装默认网关。
- 控制器中的数据报传输层安全(DTLS)端口未打开。

可以使用以下show命令：

<#root>

```
#Check that Next hop

show ip route vpn 0


#Check ARP table for Default GW

show arp


#Ping default GW
ping <...>
#Ping Google DNS
ping 8.8.8.8
#Ping vBond if ICMP is allowed on vBond
ping <vBond IP>
#Traceroute to vBond DNS
traceroute <...>
```

当发生DTLS连接故障时，您可以在命令输出中看**show control connections-history**到它。

```
                                                                                    PEER
          PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------------
0         vsmart   tls      10.0.1.5          160000000   1      10.0.2.73        23456    10.0.2.73
```

当您在SD-WAN(vSmart)端使用大数据包无法到达vEdge**tcpdump**,时，会出现这种情况：

```
tcpdump vpn 0 interface eth1 options "host 198.51.100.162 -n"

13:51:35.312109 IP 198.51.100.162.9536 > 172.18.10.130.12546: UDP, length 140 <<<< 1 (packet number)
13:51:35.312382 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 <<< not reached vEdege
13:51:35.318654 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 <<< not reached vEdege
13:51:35.318726 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 853 <<< not reached vEdege
13:51:36.318087 IP 198.51.100.162.9536 > 172.18.10.130.12546: UDP, length 140 <<<< 5
13:51:36.318185 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 79 <<<< 6
13:51:36.318233 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 << not reached vEdege
13:51:36.318241 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 879 << not reached vEdege
13:51:36.318257 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 804 << not reached vEdege
13:51:36.318266 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 65 <<<< 10
13:51:36.318279 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 25 <<<< 11
```

vEdge端的示例如下所示：

```
tcpdump vpn 0 interface ge0/1 options "host 203.0.113.147 -n"
```

```
13:51:35.250077 IP 198.51.100.162.12426 > 203.0.113.147.12746: UDP, length 140 <<<< 1
13:51:36.257490 IP 198.51.100.162.12426 > 203.0.113.147.12746: UDP, length 140 <<<< 5
13:51:36.325456 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 79 <<<< 6
13:51:36.325483 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 65 <<<< 10
13:51:36.325538 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 25 <<<< 11
```

注意：在Cisco IOS XE SD-WAN软件上，您可以使用嵌入式数据包捕获(EPC)而不是 **tcpdump**.

您也可以使用或实用程序来生成具有不同数据包大小和差分服务代码点(DSCP)标记的流**nping**，以检查连接，因为您的服务提供商可能会在传送较大的UDP数据包、分段的UDP数据包（尤其是UDP小分段）或DSCP标记的数据包时遇到问题。以下是连接成功**nping**时的示例。

从vSmart:

<#root>

```
vSmart#
```

tools nping vpn 0 198.51.100.162 options "--udp -p 12406 -g 12846 --source-ip 172.18.10.130 --df --data-

```
Nping in VPN 0
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2019-05-17 23:28 UTC
SENT (0.0220s) UDP 172.18.10.130:12846 > 198.51.100.162:12406 ttl=64 id=16578 iplen=583
SENT (1.0240s) UDP 172.18.10.130:12846 > 198.51.100.162:12406 ttl=64 id=16578 iplen=583
```

vEdge的示例如下所示：

<#root>

```
vEdge#
```

tcpdump vpn 0 interface ge0/1 options "-n host 203.0.113.147 and udp"

```
tcpdump -i ge0_1 -s 128 -n host 203.0.113.147 and udp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 128 bytes
18:29:43.492632 IP 203.0.113.147.12846 > 198.51.100.162.12406: UDP, length 555
18:29:44.494591 IP 203.0.113.147.12846 > 198.51.100.162.12406: UDP, length 555
```

下面是一个在vSmart上使用命令（从**traceroute**vShell运行）连接不成功的示例：

<#root>

```
vSmart$
```

traceroute 198.51.100.162 1400 -F -p 12406 -U -t 192 -n -m 20

```
traceroute to 198.51.100.162.162 (198.51.100.162.162), 20 hops max, 1400 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  10.65.14.177  0.435 ms 10.65.13.225  0.657 ms  0.302 ms
 7  10.10.28.115  0.322 ms 10.93.28.127  0.349 ms 10.93.28.109  1.218 ms
 8  * * *
 9  * * *
10  * 10.10.114.192  4.619 ms *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  10.68.72.61  2.162 ms * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

vEdge不接收从vSmart发送的数据包（仅接收某些其他流量或分段）：

<#root>

```
vEdge#
```

tcpdump vpn 0 interface ge0/1 options "-n host 203.0.113.147 and udp"

```
tcpdump -i ge0_1 -s 128 -n host 203.0.113.147 and udp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 128 bytes
18:16:30.232959 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 65
18:16:30.232969 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 25
18:16:33.399412 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
18:16:34.225796 IP 198.51.100.162.12386 > 203.0.113.147.12846: UDP, length 140
18:16:38.406256 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
18:16:43.413314 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
```

TLOC禁用(DISTLOC)

对TLOC Disabled消息的触发器可能由以下原因引起：

- 清除控制连接
- 更改TLOC的颜色
- 系统IP的变化

更改在系统块或命令输出中的隧道属性中提及的**show control connections-history**任何配置。

```
                                                                    PEER                        PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vmanage  dtls     192.168.30.101   1           0      192.168.20.101   12346    192.168.20.101   12346
vsmart   dtls     192.168.30.103   1           1      192.168.20.103   12346    192.168.20.103   12346
vbond    dtls     0.0.0.0          0           0      192.168.20.102   12346    192.168.20.102   12346
```

Board-ID not Initialized(BIDNTPR)

在网络连接不断摆动的高度不稳定的网络中，您可以看到"TXCHTOBD - failed to send a challenge to Board ID failed"和/或“RDSIGFBD — 从板ID读取签名失败”。 此外，有时由于锁定问题，发送到主板ID的质询失败，当发生这种情况时，请重置主板ID并重试。这种情况不经常发生，而且会延迟控制连接的形式。这在后续版本中是固定的。

```
                                                                    PEER                        P
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER             P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP        P
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.109    12346    203.0.113.109    1
vbond    dtls     -                0           0           203.0.113.56     12346    203.0.113.56     1
```

BDSGVERFL — 主板ID签名失败

这表示vEdge拒绝了vBond的机箱编号/唯一id/序列号。发生这种情况时，请确认命令输出中显示**show control local-properties**的vEdge信息，并将该输出与vBond**show orchestrator valid-vedges**上的相比较。

如果vEdge的条目不存在，请确保您具有：

- 已将vEdge添加到智能帐户。
- 已将该文件正确上传到vManage。

点击下**Send to Controllers** 方 **Configuration** > **Certificates**.

如果存在，请检查valid-vEdge表中的重复条目，并与Cisco技术支持中心(TAC)联系，进一步排除此故障

停滞在连接中：路由问题

如果网络中存在路由问题，则不会出现控制连接。 确保RIB中具有正确的NH/TLOC的有效路由。

示例包括：

- 在RIB中指向vBond的更具体的路由指向不用于建立控制连接的NH/TLOC。
- TLOC IP在上游服务提供商之间泄漏，从而导致路由不正确。

输入以下命令进行验证：

```
show ip route
show ip routes vpn 0 <prefix/mask>
ping <vBond IP>
```

查找IP前缀的距离值和协议。

vEdge尝试建立控制连接失败，或者与控制器的连接不断抖动。

使用和/**show control connections**或命令进行验**show sdwan control connections-history** 证。

<#root>

```
vedge1#

show control connections


                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      192.168.20.102                       12346 192.168.20
```

套接字错误(LISFD)

如果网络中存在重复的IP，则控制连接不会出现。您会看到消"LISFD - Listener Socket FD Error"息。这也可能出于其他原因，例如数据包损坏、RESET、vEdge与TLS和DTLS端口上的控制器之间的不匹配（如果FW端口未打开）等等。

最常见的原因是传输IP重复。检查连通性并确保地址唯一。

```
                                                                                PEER                    P
PEER     PEER     PEER             SITE        DOMAIN      PEER               PRIVATE  PEER           P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP         PORT     PUBLIC IP      P
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.21       12346    203.0.113.21   1
```

对等体超时问题(VM_TMO)

当vEdge无法与有问题的控制器连接时，会触发对等超时条件。

在本例中，它捕获了包括对等体vBondvManage Timeout msg (peer VM_TMO).、vSmart和/或vEdge超时(vEdge timeouts)在内的其他VB_TMO, VP_TMO, VS_TMO事件。

作为故障排除的一部分，请确保您已连接到控制器。使用Internet控制消息协议(ICMP)和/或**traceroute**到所讨论的IP地址。存在大量流量丢弃的情况（丢失率较高）。 快速**ping**并确保它是良好的。

```
                                                                                PEER                    P
PEER     PEER     PEER             SITE        DOMAIN      PEER               PRIVATE  PEER           P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP         PORT     PUBLIC IP      P
-------------------------------------------------------------------------------------------------------
vmanage  tls      10.0.1.3          3           0           10.0.2.42          23456    203.0.113.124  2
```

此外，请检查命**show control connections-history detail**令输出以查看TX/RX控制统计信息，查看计数器中是否存在任何重大差异。注意输出中RX和TX hello数据包编号之间的差异。

```
-----------------------------------------------------------------------------
 LOCAL-COLOR- biz-internet SYSTEM-IP- 192.168.30.103   PEER-PERSONALITY- vsmart
-----------------------------------------------------------------------------
site-id             1
domain-id           1
protocol            dtls
private-ip          192.168.20.103
```

```
private-port        12346
public-ip           192.168.20.103
public-port         12346
UUID/chassis-number 4fc4bf2c-f170-46ac-b217-16fb150fef1d
state               tear_down [Local Err: ERR_DISABLE_TLOC] [Remote Err: NO_ERROR]
downtime            2019-06-01T14:52:49+0200
repeat count        5
previous downtime   2019-06-01T14:43:11+0200

  Tx Statistics-
  --------------
    hello                   597
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                1
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0
  Rx Statistics-
  --------------
    hello                   553
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     0
```

序列号不存在(CRTREJSER、BIDNTVRFD)

如果给定设备的控制器上不存在序列号，则控制连接失败。

它可以通过输出验**show controllers [valid-vsmarts | valid-vedges]**证，并且大部分时间是固定的。从vManage**Configuration > Certificates > Send to Controllers or Send to vBond**选项卡导航至按钮。在vBond上，**show orchestrator valid-vedges/ show orchestrator valid-vsmarts**。

在vBond的日志中，您观察这些消息是有原因的 ERR_BID_NOT_VERIFIED:

```
messages:local7 info: Dec 21 01:13:31 vBond-1 VBOND[1677]: %Viptela-vBond-1-vbond_0-6-INFO-1400002: Not
y-level:major host-name:"vBond-1" system-ip:10.0.1.11 uuid:"11OG301234567" organization-name:"Example_O
```

解决此类问题时，请确保在PnP门户(software.cisco.com)和vManage上配置和调配了正确的序列号

和设备型号。

为了检查机箱编号和证书序列号，可以在vEdge路由器上使用此命令：

```
<#root>

vEdge1#

show control local-properties | include  "chassis-num|serial-num"

chassis-num/unique-id        11OG528180107
serial-num                   1001247E
```

在运行Cisco IOS XE SD-WAN软件的路由器上，输入以下命令：

```
<#root>

cEdge1#

show sdwan control local-properties | include chassis-num|serial-num

chassis-num/unique-id            C1111-4PLTEEA-FGL223911LK
serial-num                       016E9999
```

或此命令：

```
<#root>

Router#

show crypto pki certificates CISCO_IDEVID_SUDI | s ^Certificate

Certificate
  Status: Available
  Certificate Serial Number (hex): 016E9999
  Certificate Usage: General Purpose
  Issuer:
    o=Cisco
    cn=High Assurance SUDI CA
  Subject:
    Name: C1111-4PLTEEA
    Serial Number: PID:C1111-4PLTEEA SN:FGL223911LK
    cn=C1111-4PLTEEA
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:C1111-4PLTEEA SN:FGL223911LK
  Validity Date:
    start date: 15:33:46 UTC Sep 27 2018
```

```
    end   date: 20:58:26 UTC Aug 9 2099
  Associated Trustpoints: CISCO_IDEVID_SUDI
```

有关vEdge/vSmart的问题

以下是在命令输出中错误在vEdge/vSmart上**show control connections-history**的表现：

```
                                                                    PEER                      PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231    12346
```

在vBond的命令**show orchestrator connections-history**输出中：

```
                                                                                  PEER     PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0        192.168.1
```

此外，vBond上的设备序列号不在有效的vEdge列表中：

<#root>

vbond1#

show orchestrator valid-vedges | i 11OG528180107

有关控制器的问题

如果控制器之间的串行文件本身不匹配，vBond上的本地错误是不存在与vSmarts/vManage的证书已撤销的序列号。

在vBond上：

```
                                                                                  PEER     PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
```

```
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        unknown  dtls     -               0           0           ::               0        192.168.0
```

<#root>

```
vbond1#
```

show orchestrator valid-vsmarts

```
SERIAL
NUMBER  ORG
-----------------------
0A      SAMPLE - ORGNAME
0B      SAMPLE - ORGNAME
0C      SAMPLE - ORGNAME
0D      SAMPLE - ORGNAME
```

在受影响的vSmart/vManage上：

```
                                                                                PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER            PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP      PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        vbond    dtls     0.0.0.0          0           0      192.168.0.231   12346    192.168.0.231
```

<#root>

```
vsmart#
```

show control local-properties| i serial-num

```
serial-num                      0F
```

此外，您会在受影响的vSmart上看到有关vEdge的ORPTMO消息：

```
                                                                                PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER            PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP      PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        unknown  tls      -               0           0      ::              0        192.168.10.238
0        unknown  tls      -               0           0      ::              0        192.168.10.238
0        unknown  tls      -               0           0      ::              0        198.51.100.100
0        unknown  tls      -               0           0      ::              0        198.51.100.100
0        unknown  tls      -               0           0      ::              0        192.168.10.240
```

在受vEdge影响的vSmart上，**show control connections-history**输出中显示SERNTPRES错误：

```
                                                                    PEER                        PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229    23456
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229    23456
```

错误的Chassis-Num/Unique-Id

如果在PnP门户上使用错误的产品ID（型号），则也可以看到同一个错误CRTREJSER/NOERR的另一个示例。例如：

```
<#root>
vbond#
show orchestrator valid-vedges | include ASR1002
ASR1002-HX-DNA-JAE21050110            014EE30A                          valid     Cisco SVC N1
```

但是，实际设备型号不同（注意DNA后缀不在名称中）：

```
<#root>
ASR1k#
show sdwan control local-properties | include chassis-num
chassis-num/unique-id        ASR1002-HX-JAE21050110
```

组织不匹配(CTORGNMIS)

组织名称是启用控制连接的重要组件。对于给定的重叠，组织名称必须在所有控制器和vEdge之间匹配，以便控制连接可以启动。

如果没有，则存在“证书组织”。名称不匹配”错误，如下所示：

```
                                                                    PEER                    PEER
PEER     PEER     PEER             SITE        DOMAIN PEER         PRIVATE  PEER           PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP   PORT     PUBLIC IP      PORT
-------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0      203.0.113.197    12346    203.0.113.197    12346
vbond    dtls     -                0           0      198.51.100.137   12346    198.51.100.137   12346
```

vEdge/vSmart证书已撤销/无效(VSCRTREV/CRTVERFL)

如果证书在控制器上被撤销，或vEdge序列号被无效，则会分别显示vSmart或vEdge认证撤销消息。

以下是vSmart证书撤销消息的示例输出。这是在vSmart上撤销的证书：

```
                                                                PEER                    PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER         PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP   PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------
0        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
1        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
```

同样，在同一重叠中的另一个vSmart上，这是它查看证书被撤销的vSmart的方式：

```
                                                            PEER                    PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER         PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP   PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------
0        vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229
```

下面是vBond如何看待这一点：

```
                                                                    PEER     PEER
         PEER     PEER     PEER             SITE        DOMAIN     PEER         PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID         PRIVATE IP   PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------
0        vsmart   dtls     10.10.10.229     1           1          192.168.0.229    12346    192.168.0
```

证书验证失败是指无法通过安装根证书来验证证书：

1.使用命令检查时**show clock**间。它必须至少在vBond证书有效范围内（使用命令**show orchestrator local-properties**检查）。

2.这可能是由于vEdge上的根证书损坏导致的。

然后**show control connections-history**vEdge路由器上的命令会显示类似的输出：

```
                                                                                PEER                    P
PEER     PEER     PEER             SITE        DOMAIN      PEER               PRIVATE  PEER            P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP         PORT     PUBLIC IP       P
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.82       12346    203.0.113.82    1
vbond    dtls     -                0           0           203.0.113.81       12346    203.0.113.81    1
```

在这种情况下，vEdge无法同时验证控制器证书。要解决此问题，您可以重新安装根证书链。如果使用Symantec Certificate Authority，您可以从只读文件系统复制根证书链：

```
<#root>
vEdge1#

vshell

vEdge1:~$

cp /rootfs.ro/usr/share/viptela/root-ca-sha1-sha2.crt /home/admin/

vEdge1:~$

exit

exit
vEdge1#

request root-cert-chain install /home/admin/root-ca-sha1-sha2.crt

Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/root-ca-sha1-sha2.crt via VPN 0
Installing the new root certificate chain
Successfully installed the root certificate chain
```

vManage中未附加vEdge模板

当启动设备时，如果设备未在vManage上附加模板，则会显"NOVMCFG - No Config in vManage for device"示错误消息。

```
                                                                    PEER                    PEER
PEER     PEER     PEER             SITE        DOMAIN PEER         PRIVATE  PEER           PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP   PORT     PUBLIC IP      PORT
-------------------------------------------------------------------------------------------------
vmanage  dtls     10.0.1.1          1           0      10.0.2.80     12546    203.0.113.128    12546
```

瞬态条件(DISCVBD、SYSIPCHNG)

以下是一些瞬变情况，其中控制连接摆动。此类设备包括：

- vEdge上的系统IP已更改。
- 到vBond的拆解消息（到vBond的控制连接是临时的）。

```
                                                                    PEER                    PEER
PEER     PEER     PEER             SITE        DOMAIN PEER         PRIVATE  PEER           PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP   PORT     PUBLIC IP      PORT
-------------------------------------------------------------------------------------------------
vmanage  dtls     10.0.0.1          1           0      198.51.100.92   12646     198.51.100.92    12646
```

DNS故障

当命令中看不到任何连接尝试**show control connection-history**时，您可以按照以下步骤检查针对vBond的DNS解析故障：

- 对vBond的DNS地址执行ping操作。

```
ping vbond-dns-name.cisco.com
ping vbond-dns-name.cisco.com: Temporary failure in name resolution
```

- 从源接口Ping Google DNS(8.8.8.8)，以验证Internet可达性。

```
ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
```

- 端口53上的DNS流量的嵌入式数据包捕获，用于检查已发送和已接收的DNS流量。

```
monitor capture mycap interface <interface that forms control>
monitor capture mycap match ipv4 <source IP> <vBond IP>
```

参考文档：嵌入式数据包捕获。

启动监控器捕获，让它运行几分钟，然后停止捕获。继续检查数据包捕获，查看是否发送和接收DNS查询。

相关信息

- 配置基本参数以在Cisco Edge路由器上形成控制连接
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。