Troubleshoot SD-WAN Control Connections

Contents

Introduction

Background Information

Problem Scenarios

- DTLS Connection Failure (DCONFAIL)
- TLOC Disabled (DISTLOC)
- Board-ID not Initialized (BIDNTPR)
- BDSGVERFL - Board ID Signature Failure
- Stuck in Connect: Routing Issues
- Socket Errors (LISFD)
- Peer Timeout Issue (VM_TMO)
- Serial Number(s) not Present (CRTREJSER, BIDNTVRFD)
- Organization Mismatch (CTORGNMMIS)
- vEdge/vSmart Certificate Revoked/Invalidated (VSCRTREV/CRTVERFL)
- vEdge Template not Attached in vManage
- Transient Conditions (DISCVBD, SYSIPCHNG)
- DNS Failure

Related Information

Introduction

This document describes some of the probable causes that lead to a problem with Control Connections and how to troubleshoot them.

Background Information

Note: Most of the command outputs presented in this document are from vEdge routers. However, the approach is the same for routers that run Cisco IOS® XE SD-WAN software. Enter the **sdwan** keyword in order to get the same outputs on Cisco IOS XE SD-WAN software. For example, **show sdwan control connections** instead of **show control connections**.

Before you troubleshoot, ensure that the WAN Edge that is in question has been configured properly.

It includes:

- A valid certificate that is installed.

- These configurations are put in place under the system block:
  - System-IP
  - Site-ID
  - Organization-Name
  - vBond address
- VPN 0 Transport interface that is configured with the Tunnel option and IP address.
- System Clock that is configured correctly on the vEdge and those that match with other devices/controllers:

The **show clock** command confirms the current time set.

Enter the **clock set** command in order to set the correct time on the device.

For all the cases mentioned earlier, ensure that Transport Locator (TLOC) is up. Check this with the **show control local-properties** command.

An example of a valid output is shown here:

<#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
```

In vEdge software Version 16.3 and later, the output has a few additional fields:

```
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
```

Problem Scenarios

DTLS Connection Failure (DCONFAIL)

This is one of the common issues of control connectivity that does not come up. Probable causes include a firewall or some other connectivity issues.

It could be that some or all packets are dropped/filtered somewhere. The example with larger ones is given in**tcpdump** results here.

- The next hop (NH) router is not reachable.
- The default gateway is not installed in the Routing Information Base (RIB).
- The Datagram Transport Layer Security (DTLS) port is not open in the controllers.

These show commands can be used:

<#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 <...>

When you have a DTLS connection failure, you can see it in the **show control connections-history** command output.

```
                                                                                    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
```

This is what happens when large packets do not reach vEdge when you use **tcpdump**,for example, on the SD-WAN (vSmart) side:

```
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
```

An example of the vEdge side is shown here:

```
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
```

Note: On Cisco IOS XE SD-WAN software, you can use Embedded Packet Capture (EPC) instead of **tcpdump**.

You can use **traceroute** or **nping** utilities as well in order to generate traffic with different packet sizes and Differentiated Services Code Point (DSCP) marks in order to check connectivity because your service provider can have problems with the delivery of larger UDP packets, fragmented UDP packets (especially UDP small fragments) or DSCP marked packet. Here is an example with **nping** when connectivity is successful.

From 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
```

An example from vEdge is shown here:

<#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
```

And here is an example of unsuccessful connectivity with the **traceroute** command (that runs from vShell) on vSmart:

<#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 does not receive packets sent from vSmart (only some other traffic or fragments):

<#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 Disabled (DISTLOC)

Triggers to TLOC Disabled messages can be due to these probable causes:

- Clear Control Connections
- Change the color on TLOC
- Change in the System IP

Change in any of the configurations mentioned in the system block or in the tunnel properties in the **show control connections-history** command output.

```
                                                                    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)

In a highly unstable network, where network connections flap continuously, you can see "TXCHTOBD - failed to send a challenge to Board ID failed" and/or "RDSIGFBD -Read Signature from Board ID failed". Also, sometimes due to lock issues, a challenge sent to board-ID fails and when that happens, reset the board-ID and try again. It does not happen often, and it delays the form of control connections. This is fixed in later versions.

```
                                                                    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 - Board ID Signature Failure

This indicates that the vEdge chassis-num/unique-id/serial number is rejected by the vBond. When this occurs, confirm the vEdge information shown in the **show control local-properties** command output and compare that output to **show orchestrator valid-vedges** on the vBond.

If an entry does not exist for the vEdge, ensure that you have:

- Added the vEdge to the smart account.
- Uploaded that file correctly to vManage.

Click **Send to Controllers** under **Configuration** > **Certificates**.

If it does exist, check for duplicate entries in the valid-vEdge table and engage the Cisco Technical Assistance Center (TAC) to troubleshoot this further

Stuck in Connect: Routing Issues

Control connections do not come up if there are routing issues in the network. Ensure that there is a valid route in the RIB with the correct NH/TLOC.

Examples include:

- A more specific route to vBond in the RIB points to an NH/TLOC which is not used to establish control connections.
- TLOC IP is leaked between the upstream service provider which causes incorrect routing.

Enter these commands for verification:

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

Look for the distance value and the protocol for the IP-Prefix.

vEdge tries to establish a control connection with no success or connections to controllers keep flapping.

Verify with the **show control connections** and/or the **show sdwan control connections-history** commands.

<#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
```

Socket Errors (LISFD)

If there is a duplicate IP in the network, control connections do not come up. You see the "LISFD - Listener Socket FD Error" message. This can happen for other reasons as well, such as packet corruption, a RESET, a mismatch between vEdge and controllers on TLS versus DTLS ports, if the FW ports are not open, and so on.

The most common cause is a duplicate transport IP. Check connectivity and ensure that the addresses are unique.

```
                                                                                  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
```

Peer Timeout Issue (VM_TMO)

A peer timeout condition is triggered when a vEdge loses reachability to the controller in question.

In this example, it captures a**v**Manage Timeout msg (peer VM_TMO). Others include peer vBond, vSmart and/or vEdge timeouts (VB_TMO, VP_TMO, VS_TMO).

As part of troubleshooting, ensure that you have connectivity to the controller. Use Internet Control Message Protocol (ICMP) and/or **traceroute** to the IP address in question. Cases where there are lots of traffic drops (loss is high). Rapid **ping** and ensure that it is good.

```
                                                                                  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
```

In addition, check the **show control connections-history detail** command output in order to look at the TX/RX control statistics to see if there is any significant discrepancy in the counters. Notice in the output the difference between RX and TX hello packet numbers.

```
-----------------------------------------------------------------------------------
 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
```

Serial Number(s) not Present (CRTREJSER, BIDNTVRFD)

If the serial number is not present on the controllers for a given device, the control connections fail.

It can be verified with **show controllers [valid-vsmarts | valid-vedges]** outputs and fixed most of the time. Navigate to **Configuration > Certificates > Send to Controllers or Send to vBond** buttons from the vManage tabs. On vBond, check **show orchestrator valid-vedges / show orchestrator valid-vsmarts.**

In the logs on vBond, you observe these messages with reason 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
```

When you troubleshoot such a problem, ensure that the correct serial number and device model was configured and provisioned on the PnP portal (software.cisco.com) and vManage.

In order to check the chassis number and the certificate serial number, this command can be used on vEdge routers:

<#root>

vEdge1#

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

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

On a router that runs Cisco IOS XE SD-WAN software, enter this command:

<#root>

cEdge1#

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

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

Or this command:

<#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
```

For Issues with vEdge/vSmart

Here is how the error looks on vEdge/vSmart in the **show control connections-history** command output:

```
                                                                    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
```

On vBond in the **show orchestrator connections-history** command output:

```
                                                                                  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
```

Also, the device serial number on vBond is not in the list of valid vEdges:

<#root>

vbond1#

show orchestrator valid-vedges | i 11OG528180107

For Issues with Controllers

If the serial file between the controllers itself does not match, the local error on vBond is the serial number that is not present versus the certificate revoked for vSmarts/vManage.

On vBond:

```
                                                                                  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
```

On affected vSmart/vManage:

```
                                                                                    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
```

Also, you see ORPTMO messages on the affected vSmart with regards to vEdge:

```
                                                                                    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
```

On vEdge affected vSmart, in the **show control connections-history** output the SERNTPRES error is seen:

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

Wrong Chassis-Num/Unique-Id

Another example of the same error CRTREJSER/NOERR can be seen if the wrong Product ID (model) is used on the PnP portal. For example:

```
<#root>

vbond#

show orchestrator valid-vedges | include ASR1002

ASR1002-HX-DNA-JAE21050110            014EE30A                            valid     Cisco SVC N1
```

However, the real device model is different (note that DNA postfix is not in the name):

```
<#root>

ASR1k#

show sdwan control local-properties | include chassis-num

chassis-num/unique-id        ASR1002-HX-JAE21050110
```

Organization Mismatch (CTORGNMMIS)

Organization Name is a critical component for bring up of the control connection. For a given overlay, the Organization name has to match across all the controllers and vEdges so that control connections can come up.

If not, there is a "Certificate Org. name mismatch" error as shown here:

```
                                                                                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 Certificate Revoked/Invalidated (VSCRTREV/CRTVERFL)

In cases when the certificate is revoked on controllers or vEdge serial number is invalidated, a vSmart or vEdge Certification revoked message, respectively, is displayed.

Here are example outputs of vSmart Certificate revoke messages. This is the certificate that is revoked on vSmart:

```
                                                                                    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
```

Likewise, on another vSmart in the same overlay, this is how it sees the vSmart whose certificate is revoked:

```
                                                                                  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
```

And here is how vBond sees this:

```
                                                                                                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
```

Certification verification failure is when the certificate cannot be verified with the root certificate installed:

1. Check the time with the **show clock** command. It must be at least within vBond certificate validity range (check with the **show orchestrator local-properties** command).

2. This can be caused by root certificate corruption on vEdge.

Then **show control connections-history** command on the vEdge router shows a similar output:

```
                                                                    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
```

In this case, vEdge cannot validate the controller certificate as well. In order to fix this issue, you can reinstall the root certificate chain. In case the Symantec Certificate Authority is used, you can copy the Root certificate chain from the read-only filesystem:

```
<#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
```

vEdge Template not Attached in vManage

At the time the device is brought up if the device is not attached with a template on vManage, the "NOVMCFG - No Config in vManage for device" error message is displayed.

```
                                                                    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
```

Transient Conditions (DISCVBD, SYSIPCHNG)

Here are some transient conditions where the control connections flap. They include:

- System-IP changed on the vEdge.
- Tear-down message to vBond (control connection to vBond is transient).

```
                                                                    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 Failure

When no connection attempts are seen in the **show control connection-history** command, you can check for DNS resolution failure towards the vBond with these steps:

- Ping towards the DNS address of the vBond.

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

- Ping google DNS (8.8.8.8) from the source interface to verify internet reachability.

```
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:
```

- Embedded Packet Capture for DNS traffic on port 53 to check for sent and received DNS traffic.

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

Reference Document: Embedded Packet Capture.

Start the monitor capture and let it run for a couple of minutes and then stop the capture. Proceed to examine the packet capture to see if DNS queries are sent and received.

Related Information

- Configure Basic Parameters to Form Control Connections on Cisco Edge Router
- Technical Support & Documentation - Cisco Systems