SD-WAN制御接続のトラブルシューティング

内容

[概要](#)
[背景説明](#)
[問題のシナリオ](#)
[DTLS接続障害(DCONFAIL)](#)
[TLOC無効(DISTLOC)](#)
[ボードIDが初期化されていません(BIDNTPR)](#)
[BDSGVERFL – ボードIDの署名エラー](#)
[「Connect」でスタック：ルーティングの問題](#)
[ソケットエラー(LISFD)](#)
[ピアタイムアウトの問題(VM_TMO)](#)
[シリアル番号がない(CRTREJSER、BIDNTVRFD)](#)
[組織の不一致(CTORGNMMIS)](#)
[vEdge/vSmart証明書の失効/無効化(VSCRTREV/CRTVERFL)](#)
[vManageにアタッチされていないvEdgeテンプレート](#)
[一時的な状態(DISCVBD、SYSIPCHNG)](#)
[DNS障害](#)
[関連情報](#)

概要

このドキュメントでは、制御接続の問題の原因となる可能性のある原因の一部と、そのトラブルシューティング方法について説明します。

背景説明

> **注**：このドキュメントに記載されているコマンド出力のほとんどは、vEdgeルータのものです。ただし、Cisco IOS® XE SD-WANソフトウェアを実行するルータのアプローチは同じです。次を入力します。 **sdwan** Cisco IOS XE SD-WANソフトウェアで同じ出力を取得するには、次のキーワードを使用します。たとえば、 **show sdwan control connections** 代わりに **show control connections** .

トラブルシューティングを行う前に、問題のWAN工ッジが正しく設定されていることを確認します。

内容は以下を含みます。

- インストールされている有効な証明書。
- これらの設定は、 **system** block:
  - system-ip
  - site-id
  - Organization-Name
  - vBondアドレス

- トンネルオプションとIPアドレスが設定されたVPN 0トランスポートインターフェイス。
- vEdgeで正しく設定されているシステムクロックと、他のデバイス/コントローラと一致するシステムクロック：

「 **show clock** コマンドは、現在の時刻セットを確認します。

次を入力します。 **clock set** コマンドを発行して、デバイスに正しい時刻を設定します。

前述のすべてのケースについて、Transport Locator(TLOC)が起動していることを確認します。これを次のコマンドで確認します。 **show control local-properties** コマンドが表示されない場合もあります。

有効な出力の例を次に示します。

```
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   SPI TIME    LAST-
RESORT   INTERFACE  IPv4         PORT    IPv4         PORT     VS/VM COLOR       CARRIER  STATE
CONTROL     CONNECTION   CNTRL REMAINING   INTERFACE ----------------------------------------
-------------------------------------------------------------------------------------------
-- ge0/1      10.1.7.11    12346   10.1.7.11    12346     2/1  gold        default  up
     no/yes    0:00:00:16   2     0:07:33:55  No ge0/2      10.2.9.11    12366   10.2.9.11
   12366     2/0  silver      default  up      no/yes    0:00:00:12   2     0:07:35:16  No
```

vEdgeソフトウェアバージョン16.3以降では、出力に次の追加フィールドがあります。

```
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   RESTRICT/           LAST         SPI TIME
   NAT  VM INTERFACE  IPv4          PORT   IPv4          IPv6                   PORT   VS/VM
COLOR         STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON
                                                                                          STU
N                                          PRF ----------------------------------------
-------------------------------------------------------------------------------------------
------- ge0/4  172.16.0.20   12386  192.168.0.20  2601:647:4380:ca75::c2  12386  2/1  public-
internet  up   2  no/yes/no   No/Yes 0:10:34:16  0:03:03:26  E    5
```

問題のシナリオ

DTLS接続障害(DCONFAIL)

これは、制御接続が確立されない一般的な問題の1つです。考えられる原因には、ファイアウォールまたはその他の接続の問題があります。

一部またはすべてのパケットが、どこかでドロップまたはフィルタリングされている可能性があります。より大きいサイズの例については、を参照してください。**tcpdump** 結果を示します。

- ネクストホップ(NH)ルータに到達できない。
- デフォルトゲートウェイがRouting Information Base（RIB；ルーティング情報ベース）にインストールされていない。
- Datagram Transport Layer Security(DTLS)ポートがコントローラで開いていません。

次のshowコマンドを使用できます。

```
#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 <...>
```

DTLS接続に失敗した場合は、DTLS接続の失敗を **show control connections-history** コマンド出力.

```
                                                                                                    PEER
PEER
         PEER     PEER     PEER             SITE         DOMAIN PEER             PRIVATE  PEER
PUBLIC                                   LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID           ID     PRIVATE IP       PORT     PUBLIC
IP         PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
---
0        vsmart   tls      10.0.1.5          160000000   1      10.0.2.73        23456
10.0.2.73        23456   default          trying          DCONFAIL   NOERR      10407 2019-04-
07T22:03:45+0000
```

これは、サイズの大きいパケットがvEdgeに到達しない場合に発生する現象です。 **tcpdump** (SD-WAN(vSmart)側など)。

```
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側の例を次に示します。

```
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**:Cisco IOS XE SD-WANソフトウェアでは、Embedded Packet Capture(EPC)の代わりに、 **tcpdump**.

Output Interpreter **traceroute** または **nping** また、サービスプロバイダーが大きなUDPパケット、フラグメント化されたUDPパケット（特にUDPの小さなフラグメント）、またはDSCPでマークされたパケットの配信に関する問題を抱えている可能性があるため、さまざまなパケットサイズとDiffServコードポイント(DSCP)マークを持つトラフィックを生成して接続を確認するユーティリティもあります。次に例を示します **nping** 接続が成功した場合。

vSmartから：

```
vSmart# tools nping vpn 0 198.51.100.162 options "--udp -p 12406 -g 12846 --source-ip
172.18.10.130 --df --data-length 555 --tos 192"
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
```

次にvEdgeの例を示します。

```
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
```

次に示すのは、Cisco IOSソフトウェアが正常に動作していない **traceroute** vSmart上のコマンド（vShellから実行）：

```
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はvSmartから送信されたパケットを受信しません（他の一部のトラフィックまたはフラグメントのみ）。

```
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無効(DISTLOC)

TLOC Disabledメッセージのトリガーは、次の考えられる原因が原因である可能性があります。

- コントロール接続をクリアします。
- TLOCの色を変更します。
- システムIPの変更。

システムブロックまたはトンネルプロパティに記載されている設定を、**show control connections-history**コマンド出力.

```
                                                                                PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
vmanage  dtls     192.168.30.101   1           0      192.168.20.101   12346    192.168.20.101
12346   biz-internet     tear_down       DISTLOC    NOERR      3     2019-06-01T14:43:11+0200
vsmart   dtls     192.168.30.103   1           1      192.168.20.103   12346    192.168.20.103
```

```
12346   biz-internet     tear_down       DISTLOC    NOERR      4     2019-06-01T14:43:11+0200
vbond    dtls     0.0.0.0          0           0      192.168.20.102   12346    192.168.20.102
12346   biz-internet     tear_down       DISTLOC    NOERR      4     2019-06-01T14:43:11+0200
```

ボードIDが初期化されていません(BIDNTPR)

ネットワーク接続が連続的にフラップする、非常に不安定なネットワークでは、次の点が分かります TXCHTOBD - failed to send a challenge to Board ID failed または RDSIGFBD - Read Signature from Board ID failed.また、ロックの問題が原因で、board-idに送信されたチャレンジが失敗する場合があります。その場合は、board-idをリセットして再試行してください。これは頻繁には発生せず、制御接続の形式が遅延します。この問題は、それ以降のバージョンで修正されています。

```
                                                                                    PEER
PEER
PEER      PEER      PEER              SITE         DOMAIN      PEER              PRIVATE  PEER
PUBLIC                                      LOCAL      REMOTE     REPEAT
TYPE      PROTOCOL SYSTEM IP         ID           ID           PRIVATE IP        PORT     PUBLIC IP
PORT     LOCAL COLOR       STATE            ERROR       ERROR       COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
vbond    dtls      -                0           0           203.0.113.109     12346
203.0.113.109     12346   silver           challenge       TXCHTOBD   NOERR      2     2019-05-
22T05:53:47+0000
vbond    dtls      -                0           0           203.0.113.56      12346
203.0.113.56      12346   silver           challenge       TXCHTOBD   NOERR      0     2019-05-
21T09:50:41+0000
```

BDSGVERFL – ボードIDの署名エラー

これは、vEdgeシャーシ番号/一意のID/シリアル番号がvBondによって拒否されたことを示します。これが発生した場合は、に示すvEdge情報を確認します。 **show control local-properties** コマンドの出力を比較し、 **show orchestrator valid-vedges** vBond上で

vEdgeのエントリが存在しない場合は、次のことを確認します。

- スマートアカウントにvEdgeを追加。
- そのファイルをvManageに正しくアップロードしました。

クリック **Send to Controllers** 通常の **Configuration > Certificates**.

存在する場合は、valid-vEdgeテーブルに重複するエントリがないか確認し、Cisco Technical Assistance Center(TAC)に連絡して、この問題のトラブルシューティングを進めてください

「Connect」でスタック：ルーティングの問題

ネットワークにルーティングの問題がある場合、制御接続は確立されません。 正しいNH/TLOCを持つ有効なルートがRIBにあることを確認します。

次に例を示します。

- RIB内のvBondへのより具体的なルートは、制御接続の確立に使用されないNH/TLOCを指しています。
- アップストリームサービスプロバイダー間でTLOC IPがリークされ、誤ったルーティングが

引き起こされる。
確認のために次のコマンドを入力します。

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

IPプレフィクスのディスタンス値とプロトコルを探します。

vEdgeがコントロール接続の確立を試みても成功しないか、コントローラへの接続がフラッピングし続けます。

Cisco IOSソフトウェアリリース12.1以降の **show control connections** または **show sdwan control connections-history** コマンドを発行します。

```
vedge1# show control connections
                                                                                    PEER
PEER                                          CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                  PRIV
PEER                                      PUB                                        GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                            PORT
PUBLIC IP                                 PORT  LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      192.168.20.102                        12346
192.168.20.102                            12346 biz-internet    -     connect           0
```

ソケットエラー(LISFD)

ネットワーク内に重複したIPがある場合、制御接続は確立されません。次のように表示されます。 LISFD - Listener Socket FD Error メッセージに応答します。これは、パケットの破損、RESET、FWポートが開いていない場合のTLSポートとDTLSポートのvEdgeとコントローラの不一致など、他の理由でも発生する可能性があります。

最も一般的な原因は、トランスポートIPの重複です。接続をチェックし、アドレスが一意であることを確認します。

```
                                                                        PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER            PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP      PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.21    12346
203.0.113.21     12346   default          up              LISFD      NOERR      0     2019-04-
30T15:46:25+0000
```

ピアタイムアウトの問題(VM_TMO)

ピアタイムアウト状態は、vEdgeが対象コントローラへの到達可能性を失ったときにトリガーされます。

この例では、**vManage Timeout msg (peer VM_TMO)**. その他には、ピアvBond、vSmartおよび/またはvEdgeタイムアウト(**VB_TMO, VP_TMO, VS_TMO** ）。

トラブルシューティングの一環として、コントローラに接続できることを確認します。インターネット制御メッセージプロトコル(ICMP)を使用する **traceroute** IPアドレスに変換します。トラフィックドロップが多い（損失が大きい）場合。迅速な **ping** そして、それが良好であることを確認します。

```
                                                                                PEER
PEER
PEER     PEER     PEER             SITE         DOMAIN      PEER              PRIVATE  PEER
PUBLIC                                 LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID           ID          PRIVATE IP        PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
vmanage  tls      10.0.1.3          3           0           10.0.2.42        23456
203.0.113.124   23456   default          tear_down       VM_TMO     NOERR      21    2019-04-
30T15:59:24+0000
```

さらに、 **show control connections-history detail** コマンド出力を参照して、TX/RX制御の統計情報を調べ、カウンタに重大な不一致があるかどうかを確認します。出力で、RXとTXのHelloパケット番号の違いに注目してください。

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

シリアル番号がない(CRTREJSER、BIDNTVRFD)

特定のデバイスのコントローラにシリアル番号がない場合、コントロールの接続は失敗します。

次のコマンドで確認できます。 **show controllers [valid-vsmarts | valid-vedges]** ほとんどの時間を修正しました。移動先 **Configuration > Certificates > Send to Controllers or Send to vBond** [vManage]タブのボタン vBondで、次を確認します。 **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts.**

vBondのログで、これらのメッセージが理由を持って表示されます ERR_BID_NOT_VERIFIED:

```
messages:local7 info: Dec 21 01:13:31 vBond-1 VBOND[1677]: %Viptela-vBond-1-vbond_0-6-INFO-
1400002: Notification: 12/21/2018 1:13:31 vbond-reject-vedge-connection severit
y-level:major host-name:"vBond-1" system-ip:10.0.1.11 uuid:"11OG301234567" organization-
name:"Example_Orgname" sp-organization-name:"Example_Orgname"" reason:"ERR_BID_NOT_VERIFIED"
```

このような問題のトラブルシューティングを行う際には、正しいシリアル番号とデバイスモデルが設定され、PnPポータル(software.cisco.com)とvManageでプロビジョニングされていることを確認します。

シャーシ番号と証明書のシリアル番号を確認するために、vEdgeルータで次のコマンドを使用できます。

```
vEdge1# show control local-properties | include  "chassis-num|serial-num"
chassis-num/unique-id        11OG528180107
serial-num                   1001247E
```

Cisco IOS XE SD-WANソフトウェアを実行するルータで、次のコマンドを入力します。

```
cEdge1#show sdwan control local-properties | include chassis-num|serial-num
chassis-num/unique-id            C1111-4PLTEEA-FGL223911LK
serial-num                       016E9999
```

または、次のコマンドを使用します。

```
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
```

vEdge/vSmartに関する問題

vEdge/vSmartでのエラーの表示は次のとおりです。 **show control connections-history** コマンド出力:

```
                                                                                                PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
12346   biz-internet     challenge_resp  RXTRDWN    BIDNTVRFD  0     2019-06-01T16:40:16+0200
```

On vBond in the **show orchestrator connections-history** コマンド出力:

```
                                                                                                  PEER
PEER             PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
PEER             PUBLIC                                                      REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
PUBLIC IP        PORT    REMOTE COLOR     STATE              LOCAL/REMOTE    COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0
192.168.10.234   12346   default          tear_down        BIDNTVRFD/NOERR     1     2019-06-
01T18:44:34+0200
```

また、vBondのデバイスのシリアル番号が有効なvEdgeのリストにありません。

```
vbond1# show orchestrator valid-vedges | i 11OG528180107
```

コントローラに関する問題

コントローラ自体の間のシリアルファイルが一致しない場合、vBondのローカルエラーは、存在しないシリアル番号とvSmarts/vManage用に取り消された証明書です。

vBond:

```
                                                                                                  PEER
PEER             PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
PEER             PUBLIC                                                      REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
PUBLIC IP        PORT    REMOTE COLOR     STATE              LOCAL/REMOTE    COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0
192.168.0.229    12346   default          tear_down        SERNTPRES/NOERR     2     2019-06-
01T19:04:51+0200

vbond1# show orchestrator valid-vsmarts

SERIAL
NUMBER  ORG
```

```
-----------------------
0A       SAMPLE - ORGNAME
0B       SAMPLE - ORGNAME
0C       SAMPLE - ORGNAME
0D       SAMPLE - ORGNAME
```

影響を受けるvSmart/vManage:

```
                                                                                      PEER
PEER
         PEER      PEER      PEER              SITE        DOMAIN PEER              PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
INSTANCE TYPE      PROTOCOL SYSTEM IP        ID          ID      PRIVATE IP         PORT     PUBLIC
IP         PORT    REMOTE COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-----------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------
---
0        vbond    dtls     0.0.0.0          0            0       192.168.0.231    12346
192.168.0.231    12346   default           tear_down       CRTREJSER  NOERR       9     2019-06-
01T19:06:32+0200

vsmart# show control local-properties| i serial-num
serial-num                       0F
```

また、vEdgeに関して、影響を受けるvSmartでORPTMOメッセージが表示されます。

```
                                                                                      PEER
PEER
         PEER      PEER      PEER              SITE        DOMAIN PEER              PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
INSTANCE TYPE      PROTOCOL SYSTEM IP        ID          ID      PRIVATE IP         PORT     PUBLIC
IP         PORT    REMOTE COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-----------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------
---
0        unknown  tls      -                0            0       ::                0
192.168.10.238   54850   default           tear_down       ORPTMO     NOERR       0     2019-06-
01T19:18:16+0200
0        unknown  tls      -                0            0       ::                0
192.168.10.238   54850   default           tear_down       ORPTMO     NOERR       0     2019-06-
01T19:18:16+0200
0        unknown  tls      -                0            0       ::                0
198.51.100.100   55374   default           tear_down       ORPTMO     NOERR       0     2019-06-
01T19:18:05+0200
0        unknown  tls      -                0            0       ::                0
198.51.100.100   59076   default           tear_down       ORPTMO     NOERR       0     2019-06-
01T19:18:03+0200
0        unknown  tls      -                0            0       ::                0
192.168.10.240   53478   default           tear_down       ORPTMO     NOERR       0     2019-06-
01T19:18:02+0200
```

vEdgeで影響を受けたvSmartでは、 **show control connections-history** 出力に「SERNTPRES」エラーが表示されます。

```
                                                                             PEER
PEER
PEER      PEER      PEER              SITE        DOMAIN PEER              PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE      PROTOCOL SYSTEM IP         ID          ID      PRIVATE IP         PORT     PUBLIC IP
PORT     LOCAL COLOR       STATE             ERROR      ERROR      COUNT DOWNTIME
-----------------------------------------------------------------------------------------------------
```

```
--------------------------------------------------------------------------------------------
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229
23456   biz-internet     tear_down       SERNTPRES  NOERR      29    2019-06-01T19:18:51+0200
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229
23456   mpls             tear_down       SERNTPRES  NOERR      29    2019-06-01T19:18:32+0200
```

誤ったChassis-Num/Unique-Id

PnPポータルで誤った製品ID（モデル）が使用されている場合、同じエラー「CRTREJSER/NOERR」の別の例が表示されます。以下に、いくつかの例を示します。

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

ただし、実際のデバイスのモデルは異なります（「DNA」の接尾辞部分は名前に含まれていません）。

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

組織の不一致(CTORGNMMIS)

組織名は、制御接続を起動するための重要なコンポーネントです。指定されたオーバーレイに対して、組織名はすべてのコントローラとvEdge間で一致する必要があります。これにより、制御接続が確立されます。

そうでない場合は、次に示すように「Certificate Org. name mismatch」エラーが表示されます。

```
                                                                                PEER
PEER
PEER     PEER     PEER             SITE         DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID           ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
--------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
vbond    dtls     -                0           0      203.0.113.197    12346    203.0.113.197
12346   biz-internet     tear_down       CTORGNMMIS NOERR      14    2019-04-08T00:26:19+0000
vbond    dtls     -                0           0      198.51.100.137   12346    198.51.100.137
12346   biz-internet     tear_down       CTORGNMMIS NOERR      13    2019-04-08T00:26:04+0000
```

vEdge/vSmart証明書の失効/無効化(VSCRTREV/CRTVERFL)

コントローラ上で証明書が失効した場合、またはvEdgeシリアル番号が無効になった場合は、vSmartまたはvEdge Certification revokedメッセージがそれぞれ表示されます。

vSmart証明書の取り消しメッセージの出力例を次に示します。vSmartで失効した証明書を次に示します。

```
                                                                          PEER
PEER
        PEER     PEER     PEER             SITE         DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID           ID     PRIVATE IP       PORT     PUBLIC
```

```
IP         PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
0        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346
192.168.0.231    12346   default          up              RXTRDWN    VSCRTREV   0     2019-06-
01T18:13:22+0200
1        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346
192.168.0.231    12346   default          up              RXTRDWN    VSCRTREV   0     2019-06-
01T18:13:22+0200
```

同様に、同じオーバーレイ内の別のvSmartでは、証明書が失効しているvSmartが次のように表示されます。

```
                                                                        PEER
PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                   LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC
IP         PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
0        vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456
192.168.0.229    23456   default          tear_down       VSCRTREV   NOERR      0     2019-06-
01T18:13:24+0200
```

vBondは次のように考えています。

```
                                                                                  PEER
PEER             PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
PEER             PUBLIC                                                    REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
PUBLIC IP        PORT    REMOTE COLOR     STATE              LOCAL/REMOTE    COUNT DOWNTIME
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
0        vsmart   dtls     10.10.10.229     1           1           192.168.0.229    12346
192.168.0.229    12346   default          tear_down          VSCRTREV/NOERR     0     2019-06-
01T18:13:14+0200
```

証明書検証の失敗は、インストールされたルート証明書で証明書を検証できない場合です。

1.時間を確認するには、 **show clock** コマンドが表示されない場合もあります。少なくともvBond証明書の有効範囲内である必要があります(**show orchestrator local-properties** コマンド)。

2.これは、vEdgeのルート証明書が破損していることが原因である可能性があります。

Then **show control connections-history** コマンドをvEdgeルータで実行すると、次のような出力が表示されます。

```
                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
PUBLIC                                   LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
```

```
vbond    dtls     -                0           0           203.0.113.82     12346
203.0.113.82     12346   default          tear_down       CRTVERFL   NOERR      32    2018-11-
16T23:58:22+0000
vbond    dtls     -                0           0           203.0.113.81     12346
203.0.113.81     12346   default          tear_down       CRTVERFL   NOERR      31    2018-11-
16T23:58:03+0000
```

この場合、vEdgeはコントローラ証明書も検証できません。この問題を解決するには、ルート証明書チェーンを再インストールします。Symantec認証局(CA)を使用している場合は、読み取り専用ファイルシステムからルート証明書チェーンをコピーできます。

```
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にアタッチされていないvEdgeテンプレート

デバイスがvManage上のテンプレートに接続されていない場合、デバイスが起動すると、**NOVMCFG - No Config in vManage for device** 少し時間がかかります（最大 10 分）。

```
                                                                        PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT D                OWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------                ---------
----------
vmanage  dtls     10.0.1.1          1           0      10.0.2.80        12546    203.0.113.128
12546   default          up              RXTRDWN    NOVMCFG    35    2                019-02-
26T12:23:52+0000
```

一時的な状態(DISCVBD、SYSIPCHNG)

コントロール接続がフラップする一時的な状態を次に示します。これには、次のようなルーティング プロトコルが含まれます。

- vEdgeでシステムIPが変更されました。
- vBondへの切断メッセージ（vBondへのコントロール接続は一時的）。

```
                                                                        PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
```

```
vmanage  dtls     10.0.0.1         1           0      198.51.100.92   12646     198.51.100.92
12646   default          tear_down       SYSIPCHNG  NOERR      0     2018-11-02T16:58:00+0000
```

DNS障害

接続の試行が **show control connection-history** コマンドを使用して、vBondに対するDNS解決の失敗を確認するには、次の手順を実行します。

- vBondのDNSアドレスに対してpingを実行します。

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

- 送信元インターフェイスからgoogle DNS(8.8.8.8)にpingを実行し、インターネットの到達可能性を確認します。

```
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:
```

- 送受信されたDNSトラフィックを確認するための、ポート53でのDNSトラフィック用の組み込みパケットキャプチャ。

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

参照文書：組み込みパケットキャプチャ。

モニタのキャプチャを開始し、数分間実行してから、キャプチャを停止します。次に、パケットキャプチャを調べて、DNSクエリが送受信されているかどうかを確認します。

関連情報

- cEdgeでフォームコントロール接続の基本パラメータを設定する
- テクニカル サポートとドキュメント – Cisco Systems

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。