Risoluzione dei problemi relativi alle connessioni di controllo SD-WAN

Sommario

Introduzione

In questo documento vengono descritte alcune delle possibili cause che hanno causato un problema con le connessioni di controllo e viene spiegato come risolverlo.

Premesse

> **Nota**: la maggior parte degli output del comando presentati in questo documento provengono da router vEdge. Tuttavia, l'approccio è lo stesso per i router con software Cisco IOS® XE SD-WAN. Immettere il **sdwan** per ottenere gli stessi output sul software Cisco IOS XE SD-WAN. Ad esempio, **show sdwan control connections** anziché **show control connections** .

Prima di risolvere il problema, verificare che il server WAN Edge in questione sia stato configurato correttamente.

Esso comprende:

- Certificato valido installato.
- Queste configurazioni sono implementate nell'ambito **system** blocco:
  - System-IP
  - ID sito
  - Nome-organizzazione

- Indirizzo vBond
- Interfaccia di trasporto VPN 0 configurata con l'opzione Tunnel e l'indirizzo IP.
- Orologio di sistema configurato correttamente su vEdge e quelli che corrispondono ad altri dispositivi/controller:

OSPF (Open Shortest Path First) **show clock** conferma l'ora corrente impostata.

Immettere il **clock set** per impostare l'ora corretta sul dispositivo.

Per tutti i casi menzionati in precedenza, verificare che Transport Locator (TLOC) sia attivo. Controllare con il **show control local-properties**

Di seguito è riportato un esempio di output valido:

```
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
```

Nel software vEdge versione 16.3 e successive, l'output presenta alcuni campi aggiuntivi:

```
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
```

Scenari di problema

Errore di connessione DTLS (DCONFAIL)

Questo è uno dei problemi comuni della connettività del controllo che non si presenta. Le possibili cause includono un firewall o altri problemi di connettività.

Potrebbe darsi che alcuni o tutti i pacchetti vengano scartati o filtrati da qualche parte. L'esempio con quelli più grandi è fornito in**tcpdump** qui i risultati.

- Il router dell'hop successivo (NH) non è raggiungibile.
- Il gateway predefinito non è installato nel database RIB (Routing Information Base).
- La porta DTLS (Datagram Transport Layer Security) non è aperta nei controller.

Èpossibile utilizzare i seguenti comandi show:

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

Quando si verifica un errore di connessione DTLS, è possibile visualizzarlo nel **show control connections-history** output del comando.

```
                                                                                                    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
```

Questo è ciò che accade quando i pacchetti di grandi dimensioni non raggiungono vEdge quando si utilizza **tcpdump** , ad esempio sul lato SD-WAN (vSmart):

```
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
```

Di seguito è riportato un esempio del lato vEdge:

```
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
```

> **Nota**: sul software Cisco IOS XE SD-WAN, è possibile usare Embedded Packet Capture (EPC) anziché **tcpdump**.

Èpossibile utilizzare **traceroute** o **nping** , nonché per generare traffico con pacchetti di dimensioni diverse e contrassegni DSCP (Differentiated Services Code Point) per controllare la connettività, in quanto il provider di servizi può avere problemi con la consegna di pacchetti UDP più grandi, pacchetti UDP frammentati (in particolare piccoli frammenti UDP) o pacchetti con contrassegno DSCP. Di seguito è riportato un esempio di **nping** quando la connettività ha esito positivo.

Da vSmart:

```
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
```

Di seguito è riportato un esempio di vEdge:

```
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
```

Ecco un esempio di connettività non riuscita con **traceroute** (eseguito da vShell) su vSmart:

```
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 non riceve pacchetti inviati da vSmart (solo altri tipi di traffico o frammenti):

```
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 disabilitato (DISTLOC)

I trigger per i messaggi TLOC disabilitati possono essere dovuti alle seguenti probabili cause:

- Cancella Connessioni Di Controllo.
- Modificate il colore in TLOC.
- Modifica nell'indirizzo IP del sistema.

Modifica di una qualsiasi delle configurazioni indicate nel blocco di sistema o nelle proprietà del tunnel nella**show control connections-history**output del comando.

```
                                                                                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
```

ID scheda non inizializzato (BIDNTPR)

In una rete altamente instabile, in cui le connessioni di rete si interrompono continuamente, è possibile visualizzare TXCHTOBD - failed to send a challenge to Board ID failed e/o RDSIGFBD - Read Signature from Board ID failed. Inoltre, a volte a causa di problemi di blocco, una richiesta inviata a board-id fallisce e quando ciò accade, reimpostare la board-ID e riprovare. Non capita spesso, e ritarda la forma delle connessioni di controllo. Questo problema è stato risolto nelle versioni successive.

```
                                                                                    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 - Errore firma ID scheda

Ciò indica che il numero-chassis/id-univoco/numero di serie di vEdge viene rifiutato da vBond. Quando ciò si verifica, confermare le informazioni vEdge mostrate nella **show control local-properties** dell'output del comando e confrontarlo con **show orchestrator valid-vedges** sul vBond.

Se non esiste una voce per vEdge, verificare di disporre di:

- vEdge aggiunto allo smart account.
- Il file è stato caricato correttamente in vManage.

Clic **Send to Controllers** sotto **Configuration > Certificates**.

Se il problema persiste, verificare la presenza di voci duplicate nella tabella valid-vEdge e rivolgersi al Cisco Technical Assistance Center (TAC) per risolvere ulteriormente il problema

Bloccato in 'Connect': problemi di routing

Le connessioni di controllo non vengono attivate se vi sono problemi di routing nella rete. Verificare che nella NERVATURA sia presente un percorso valido con NH/TLOC corretto.

Alcuni esempi:

- Un percorso più specifico per vBond nella RIB punta a un NH/TLOC che non viene utilizzato per stabilire connessioni di controllo.
- L'indirizzo IP TLOC è trapelato tra il provider di servizi upstream causando un routing errato.

Immettere i seguenti comandi per la verifica:

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

Cercare il valore della distanza e il protocollo per il prefisso IP.

vEdge tenta di stabilire una connessione di controllo senza successo o le connessioni ai controller continuano a lampeggiare.

Verifica con **show control connections** e/o **show sdwan control connections-history** comandi.

```
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
```

Errori socket (LISFD)

Se nella rete è presente un IP duplicato, le connessioni di controllo non vengono attivate. Viene visualizzata la LISFD - Listener Socket FD Error messaggio. Questo può accadere anche per altri motivi, quali il danneggiamento dei pacchetti, un RESET, una mancata corrispondenza tra vEdge e i controller sulle porte TLS e DTLS, se le porte FW non sono aperte, e così via.

La causa più comune è un IP di trasporto duplicato. Verificare la connettività e assicurarsi che gli indirizzi siano univoci.

```
                                                                          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
```

Problema di timeout peer (VM_TMO)

Una condizione di timeout peer viene attivata quando un vEdge perde la raggiungibilità al controller in questione.

In questo esempio, acquisisce un**vManage Timeout msg (peer VM_TMO)**. Altri includono i timeout peer vBond, vSmart e/o vEdge (**VB_TMO, VP_TMO, VS_TMO**).

Nell'ambito della risoluzione dei problemi, assicurarsi di disporre della connettività al controller.

Utilizzare il protocollo ICMP (Internet Control Message Protocol) e/o **traceroute** all'indirizzo IP in questione. Casi in cui si verificano molte perdite di traffico (la perdita è elevata). Rapido **ping** e assicurarsi che sia buona.

```
                                                                                    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
```

Inoltre, controllare la **show control connections-history detail** per controllare le statistiche dei controlli TX/RX e verificare se ci sono discrepanze significative nei contatori. Si noti nell'output la differenza tra i numeri dei pacchetti hello RX e TX.

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

Numeri di serie non presenti (CRTREJSER, BIDNTVRFD)

Se il numero di serie non è presente sui controller di un determinato dispositivo, le connessioni del controllo avranno esito negativo.

Può essere verificato con **show controllers [valid-vsmarts | valid-vedges]** e ha fissato la maggior parte del tempo. Passa a **Configuration > Certificates > Send to Controllers or Send to vBond** dalle schede vManage. In vBond, selezionare **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts**.

Nei log su vBond si osservano questi messaggi con ragione 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"
```

Quando si risolve un problema di questo tipo, verificare che siano stati configurati il numero di serie e il modello del dispositivo corretti e che sia stato eseguito il provisioning sul portale PnP (software.cisco.com) e su vManage.

Per controllare il numero di chassis e il numero di serie del certificato, questo comando può essere utilizzato sui router vEdge:

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

Su un router con software Cisco IOS XE SD-WAN, immettere questo comando:

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

Oppure questo comando:

```
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
```

Per i problemi con vEdge/vSmart

Ecco come appare l'errore su vEdge/vSmart nel **show control connections-history** output comando:

```
                                                                                    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
```

Su vBond in **show orchestrator connections-history** output comando:

```
                                                                                                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
```

Inoltre, il numero di serie del dispositivo su vBond non è presente nell'elenco dei vEdge validi:

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

Problemi con i controller

Se il file seriale tra i controller non corrisponde, l'errore locale in vBond è il numero di serie non presente rispetto al certificato revocato per vSmarts/vManage.

Su 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
```

Su vSmart/vManage interessato:

```
                                                                                                  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
```

Inoltre, sullo vSmart interessato vengono visualizzati messaggi ORPTMO relativi a vEdge:

```
                                                                                                  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
```

Su vEdge interessato vSmart, nel **show control connections-history** viene visualizzato l'errore "SERNTPRES":

```
                                                                    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
```

Numero-Chassis/Id-Univoco Errato

Èpossibile visualizzare un altro esempio dello stesso errore "CRTREJSER/NOERR" se sul portale PnP viene utilizzato l'ID prodotto (modello) errato. Ad esempio:

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

Tuttavia, il modello reale del dispositivo è diverso (notare che il suffisso "DNA" non è nel nome):

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

Mancata corrispondenza organizzazione (CTORGNMMIS)

Il nome dell'organizzazione è un componente critico per l'attivazione della connessione di controllo. Per una determinata sovrapposizione, il nome dell'organizzazione deve corrispondere tra tutti i controller e i bordi in modo da consentire la connessione dei controlli.

In caso contrario, si verifica un errore di mancata corrispondenza del nome dell'organizzazione del certificato, come mostrato di seguito:

```
                                                                                    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
```

Certificato vEdge/vSmart revocato/non convalidato (VSCRTREV/CRTVERFL)

Nei casi in cui il certificato viene revocato nei controller o il numero di serie di vEdge viene invalidato, viene visualizzato rispettivamente un messaggio di revoca della certificazione vSmart o vEdge.

Di seguito sono riportati alcuni output di esempio dei messaggi di revoca dei certificati vSmart. Questo è il certificato revocato su vSmart:

```
                                                                                      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
```

Allo stesso modo, su un altro vSmart nella stessa sovrapposizione, questo è il modo in cui vede il vSmart il cui certificato è stato revocato:

```
                                                                                  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
```

Ed ecco come vBond la vede:

```
                                                                                    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
```

L'errore di verifica della certificazione si verifica quando non è possibile verificare il certificato con il certificato radice installato:

1. Controllare l'ora con il **show clock** Deve essere compreso almeno nell'intervallo di validità del certificato vBond (verificare con **show orchestrator local-properties**).

2. Il problema può essere dovuto al danneggiamento del certificato radice su vEdge.

Poi **show control connections-history** sul router vEdge restituisce un output simile:

```
                                                                          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
```

In questo caso, vEdge non può convalidare anche il certificato del controller. Per risolvere il problema, è possibile reinstallare la catena di certificati radice. Se viene utilizzata l'autorità di certificazione Symantec, è possibile copiare la catena di certificati root dal file system di sola lettura:

```
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
```

Modello vEdge non collegato in vManage

Al momento dell'accensione del dispositivo se quest'ultimo non è collegato a un modello in vManage, il **NOVMCFG - No Config in vManage for device** viene visualizzato un messaggio.

```
                                                                          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
```

Condizioni transitorie (DISCVBD, SYSIPCHNG)

Di seguito sono riportate alcune condizioni transitorie in cui le connessioni di controllo si interrompono. Essi comprendono:

- System-IP modificato su vEdge.
- Messaggio di cancellazione a vBond (la connessione di controllo a vBond è transitoria).

```
                                                                          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
```

Errore DNS

Quando non vengono rilevati tentativi di connessione nel **show control connection-history** è possibile verificare la presenza di errori di risoluzione DNS verso vBond eseguendo la procedura seguente:

- Ping verso l'indirizzo DNS del vBond.

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

- Eseguire il ping di Google DNS (8.8.8.8) dall'interfaccia di origine per verificare la raggiungibilità di Internet.

```
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 per il traffico DNS sulla porta 53 per verificare il traffico DNS inviato e ricevuto.

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

Documento di riferimento: Embedded Packet Capture.

Avviare l'acquisizione del monitor e lasciarla in esecuzione per un paio di minuti, quindi arrestarla. Esaminare l'acquisizione dei pacchetti per verificare se le query DNS vengono inviate e ricevute.

Informazioni correlate

- Configurare i parametri di base per formare le connessioni dei controlli su cEdge
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).