Risoluzione dei problemi di switching su RCM Converged Core

Sommario

Introduzione

In questo documento vengono descritti i passaggi di base per risolvere i problemi relativi a Gestione configurazione ridondanza (RCM) in caso di errore di rete.

Premesse

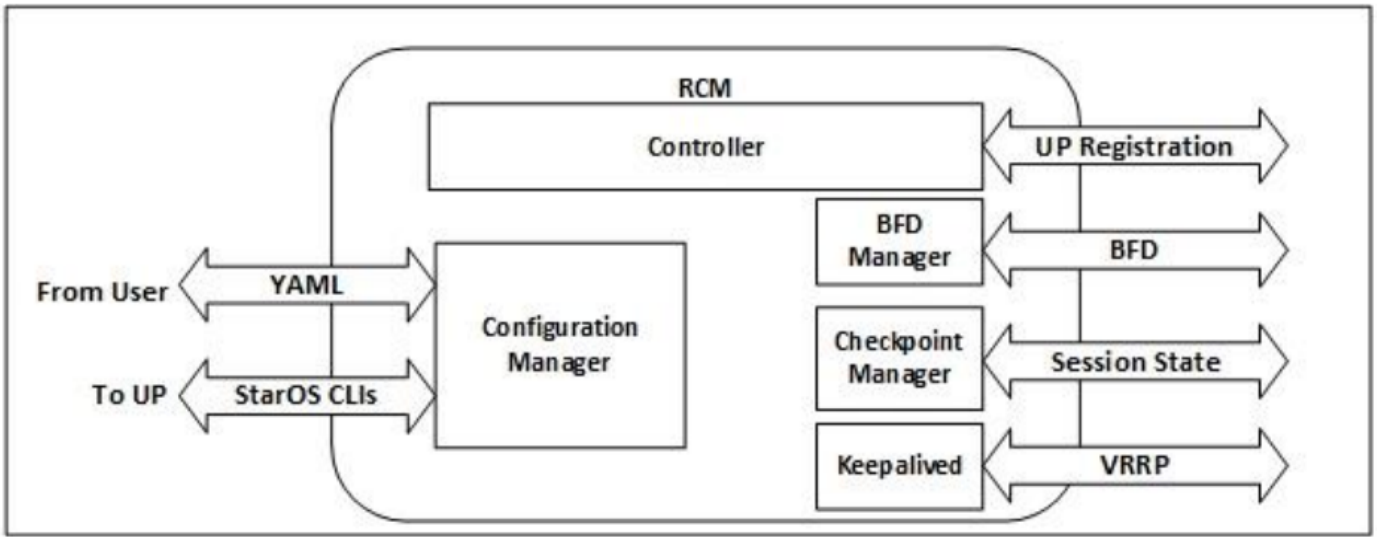
Cos'è RCM?

RCM è un nodo o una funzione di rete (NF) di proprietà di Cisco che fornisce ridondanza per le funzioni UPF (User Plane Functions) basate su StarOS.

RCM fornisce la ridondanza N:M di UPF, dove N è un numero di UPF attivi e è inferiore a 10 e M è un numero di UP standby nel gruppo di ridondanza.

Componenti di RCM

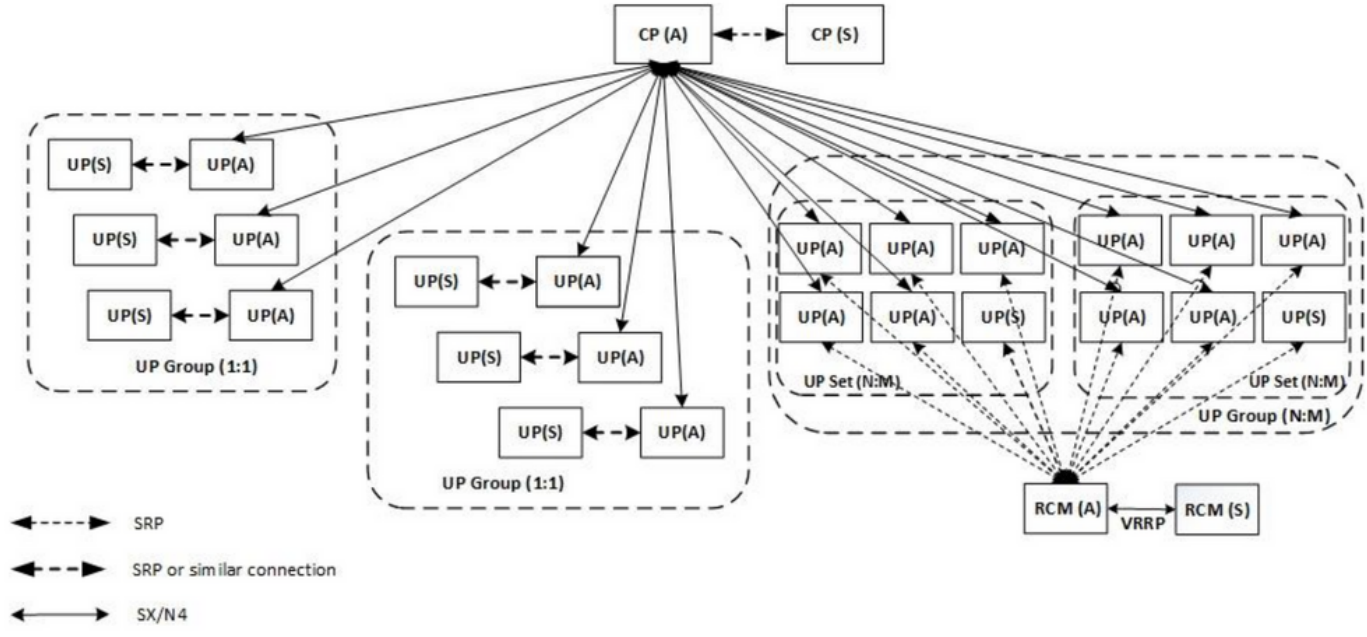
RCM comprende componenti che vengono eseguiti come pod nella VM RCM:



- Controller: Consente di comunicare le decisioni relative agli eventi con tutti gli altri dispositivi di espansione di RCM
- BFD Manager (BFDMgr): Utilizza il protocollo BFD per identificare lo stato del piano dati
- Gestione configurazione (ConfigMgr): Carica la configurazione richiesta nei piani utente (UP)
- Redundancy Manager (RedMgr): È anche denominato Gestione checkpoint. Memorizza e invia i dati del checkpoint a un UPF in standby

- Mantenuti: Comunica tra RCM attivo e in standby utilizzando il protocollo VRRP

Modello di implementazione tipico di RCM



Panoramica di RCM CLI

In questo esempio sono presenti quattro centri RCM OPS. Per verificare la corrispondenza tra RCM Kubernetes e RCM OPS Center e CEE (Common Execution Environment), è possibile accedere a RCM Kubernetes e visualizzare un elenco degli spazi dei nomi:

```
cloud-user@up0300-aio-1-primary-1:~$ kubectl get namespace
NAME              STATUS   AGE
cee-rce31       Active   54d
default           Active   57d
istio-system      Active   57d
kube-node-lease   Active   57d
kube-public       Active   57d
kube-system       Active   57d
nginx-ingress     Active   57d
rcm-rm31        Active   54d
rcm-rm33        Active   54d
registry          Active   57d
smi-certs         Active   57d
smi-node-label    Active   57d
smi-vips          Active   57d

cloud-user@up300-aio-2-primary-1:~$ kubectl get namespace
NAME              STATUS   AGE
cee-rce32         Active   54d
default           Active   57d
istio-system      Active   57d
kube-node-lease   Active   57d
kube-public       Active   57d
kube-system       Active   57d
nginx-ingress     Active   57d
rcm-rm32          Active   54d
rcm-rm34          Active   54d
registry          Active   57d
smi-certs         Active   57d
smi-node-label    Active   57d
smi-vips          Active   57d
```

Indirizzo IP gestione UPF

Questo IP è specifico e legato a VM o UPF. Viene utilizzato nelle comunicazioni iniziali tra UPF e RCM, dove UPF si registra con RCM e RCM configura UPF e assegna il ruolo. È possibile utilizzare questo indirizzo IP per identificare UPF dagli output CLI di RCM.

UPF IP ruolo dispositivo

Collegato a un ruolo (attivo/standby):

Questo indirizzo IP si sposta man mano che si verifica il passaggio.

Comandi CLI utili per la risoluzione dei problemi di RCM

Da RCM OPS Center è possibile verificare quale gruppo di RCM è l'UPF. Trova un esempio da Cloud Native Deployment Platform (CNDP):

```
[local]UPF317# show rcm info
Redundancy Configuration Module:
------------------------------------------------------------------------------
Context:                        rcm
Bind Address:                   10.10.9.81
Chassis State:                  Active
Session State:                  SockActive
Route-Modifier:                 32
RCM Controller Address:         10.10.9.179
```

```
RCM Controller Port:             9200
RCM Controller Connection State: Connected
Ready To Connect:                Yes
Management IP Address:           10.10.14.33
Host ID:                         UPF320
SSH IP Address:                  10.10.14.40 (Activated)
```

Nota: L'ID host è diverso dal nome host UPF.

Qui è possibile visualizzare lo stato su RCM OPS Center:

```
[up300-aio-2/rm34] rcm# rcm show-status
message :
{"status":[" Thu Oct 21 10:45:21 UTC 2021 : State is primary"]}
```

```
[up300-aio-2/rm34] rcm# rcm show-statistics controller
message :
{
 "keepalive_version": "65820a54450f930458c01e4049bd01f207bc6204e598f0ad3184c401174fd448",
 "keepalive_timeout": "2s",
 "num_groups": 2,
 "groups": [
   {
     "groupid": 2,
     "endpoints_configured": 7,
     "standby_configured": 1,
     "pause_switchover": false,
     "active": 6,
     "standby": 1,
     "endpoints": [
       {
         "endpoint": "10.10.9.85",
         "bfd_status": "STATE_UP",
         "upf_registered": true,
         "upf_connected": true,
         "upf_state_received": "UpfMsgState_Active",
         "bfd_state": "BFDState_UP",
         "upf_state": "UPFState_Active",
         "route_modifier": 32,
         "pool_received": true,
         "echo_received": 45359,
         "management_ip": "10.10.14.41",
         "host_id": "UPF322",
         "ssh_ip": "10.10.14.44"
       },
       {
         "endpoint": "10.10.9.86",
         "bfd_status": "STATE_UP",
         "upf_registered": true,
         "upf_connected": true,
         "upf_state_received": "UpfMsgState_Active",
         "bfd_state": "BFDState_UP",
         "upf_state": "UPFState_Active",
         "route_modifier": 32,
         "pool_received": true,
         "echo_received": 4518,
         "management_ip": "10.10.14.43",
         "host_id": "UPF317",
         "ssh_ip": "10.10.14.34"
       },
```

```
{
  "endpoint": "10.10.9.94",
  "bfd_status": "STATE_UP",
  "upf_registered": true,
  "upf_connected": true,
  "upf_state_received": "UpfMsgState_Active",
  "bfd_state": "BFDState_UP",
  "upf_state": "UPFState_Active",
  "route_modifier": 32,
  "pool_received": true,
  "echo_received": 4518,
  "management_ip": "10.10.14.59",
  "host_id": "UPF318",
  "ssh_ip": "10.10.14.36"
},
{
  "endpoint": "10.10.9.81",
  "bfd_status": "STATE_UP",
  "upf_registered": true,
  "upf_connected": true,
  "upf_state_received": "UpfMsgState_Active",
  "bfd_state": "BFDState_UP",
  "upf_state": "UPFState_Active",
  "route_modifier": 32,
  "pool_received": true,
  "echo_received": 45359,
  "management_ip": "10.10.14.33",
  "host_id": "UPF320",
  "ssh_ip": "10.10.14.40"
},
{
  "endpoint": "10.10.9.82",
  "bfd_status": "STATE_UP",
  "upf_registered": true,
  "upf_connected": true,
  "upf_state_received": "UpfMsgState_Standby",
  "bfd_state": "BFDState_UP",
  "upf_state": "UPFState_Standby",
  "route_modifier": 50,
  "pool_received": false,
  "echo_received": 4505,
  "management_ip": "10.10.14.35",
  "host_id": "",
  "ssh_ip": "10.10.14.60"
},
{
  "endpoint": "10.10.9.83",
  "bfd_status": "STATE_UP",
  "upf_registered": true,
  "upf_connected": true,
  "upf_state_received": "UpfMsgState_Active",
  "bfd_state": "BFDState_UP",
  "upf_state": "UPFState_Active",
  "route_modifier": 30,
  "pool_received": true,
  "echo_received": 4518,
  "management_ip": "10.10.14.37",
  "host_id": "UPF319",
  "ssh_ip": "10.10.14.38"
},
{
  "endpoint": "10.10.9.84",
  "bfd_status": "STATE_UP",
  "upf_registered": true,
```

```
        "upf_connected": true,
        "upf_state_received": "UpfMsgState_Active",
        "bfd_state": "BFDState_UP",
        "upf_state": "UPFState_Active",
        "route_modifier": 32,
        "pool_received": true,
        "echo_received": 4518,
        "management_ip": "10.10.14.39",
        "host_id": "UPF321",
        "ssh_ip": "10.10.14.42"
      }
    ]
  },
```

Individuazione UPF standby corrente da RCM OPS Center

Da RCM OPS, il Centro identifica l'UPF in Standby con l'uso del comando **rcm show-statistics controller**:

```
  {
        "endpoint": "10.10.9.82",
        "bfd_status": "STATE_UP",
        "upf_registered": true,
        "upf_connected": true,
        "upf_state_received": "UpfMsgState_Standby",
        "bfd_state": "BFDState_UP",
        "upf_state": "UPFState_Standby",
        "route_modifier": 50,
        "pool_received": false,
        "echo_received": 4505,
        "management_ip": "10.10.14.35",
        "host_id": "",
       "ssh_ip": "10.10.14.60"
      },
```

Accedere a UPF e verificare le informazioni di RCM:

```
[local]UPF318# show rcm info
Saturday November 06 13:29:59 UTC 2021
Redundancy Configuration Module:
------------------------------------------------------------------------------
Context:                          rcm
Bind Address:                     10.10.9.82
Chassis State:                    Standby
Session State:                    SockStandby
Route-Modifier:                   50
RCM Controller Address:           10.10.9.179
RCM Controller Port:              9200
RCM Controller Connection State: Connected
Ready To Connect:                 Yes
Management IP Address:            10.10.14.35
Host ID:
SSH IP Address:                   10.10.14.60 (Activated)
```

Di seguito sono riportate altre informazioni utili fornite da RCM OPS Center:

```
[up300-aio-2/rm34] rcm# rcm show-statistics
Possible completions:
 bfdmgr          Show RCM BFDMgr Statistics information
 checkpointmgr   Show RCM Checkpointmgr Statistics information
```

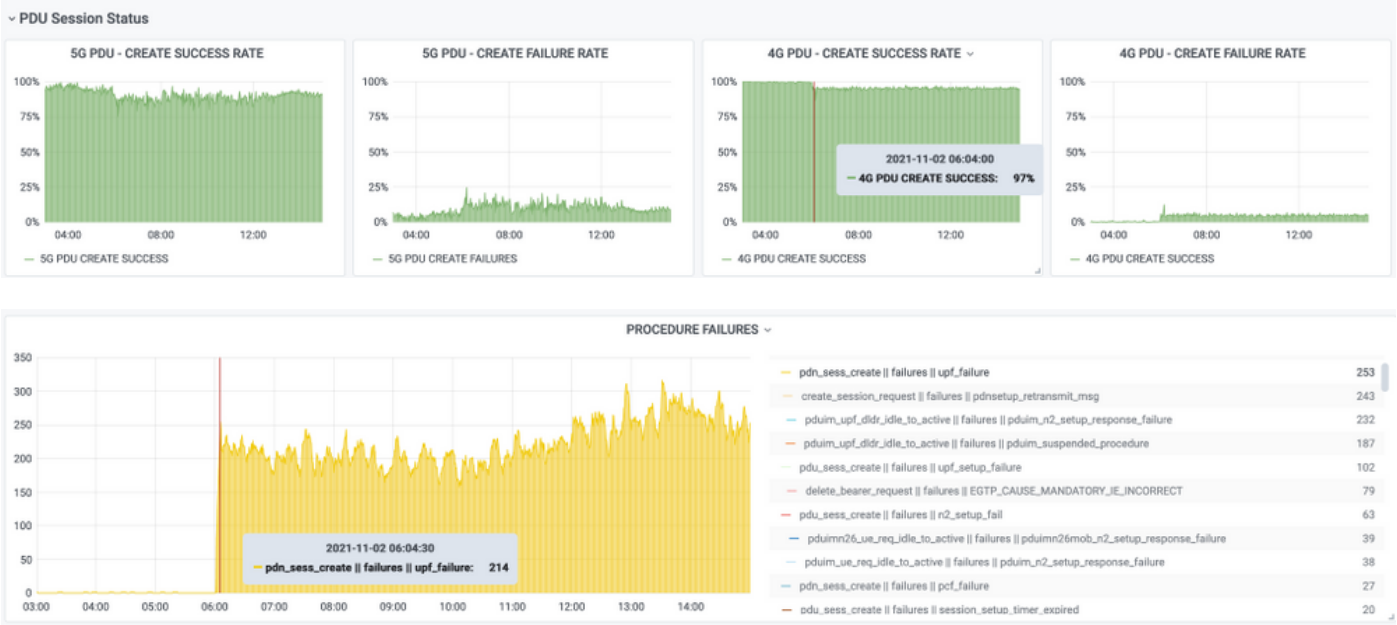
```
configmgr       Show RCM Configmgr Statistics information
controller      Show RCM Controller Statistics information
|               Output modifiers
<cr>
```

Scaricare il [manuale di RCM](#) per la versione 21.24.

Problema segnalato da errori RCM su POD CNDP

Il problema è stato segnalato su uno degli UPF relativi all'avviso UP_SX_SESS_CREATION_SR. Questo avviso indica che la percentuale di successo della creazione della sessione sull'interfaccia SX è scesa sotto la soglia configurata.

Se si osservano le statistiche di Grafana, si osserva una degradazione di 5G/4G a causa del motivo di disconnessione **pdn_sess_create || errori || errore_upf**:



Ciò conferma che il **comando pdn_sess_create || errori || errore_upf** causato da UPF419:

```
[local]UPF419# show rcm info
Saturday November 06 14:01:30 UTC 2021
Redundancy Configuration Module:
--------------------------------------------------------------------------------
Context:                          rcm
Bind Address:                     10.10.11.83
Chassis State:                    Active
Session State:                    SockActive
Route-Modifier:                   30
RCM Controller Address:           10.10.11.179
RCM Controller Port:              9200
RCM Controller Connection State: Connected
Ready To Connect:                 Yes
Management IP Address:            10.10.14.165
Host ID:                          DNUD0417
SSH IP Address:                   10.10.14.162 (Activated)
```

Su SMF è possibile controllare la configurazione UPF. In questo caso, cercare l'indirizzo IP UPF N4:

```
[smf/smf2] smf# show running-config profile network-element upf node-id n4-peer-UPF417
profile network-element upf upf19
 node-id           n4-peer-UPF417
 n4-peer-address ipv4 10.10.10.17
 n4-peer-port      8805
 upf-group-profile upf-group1
 dnn-list          [ internet ]
 capacity          10
 priority          1
exit
```

Quindi è possibile eseguire la query Grafana per identificare verso quale indirizzo UPF N4 si verificano più errori:

Query Grafana:
sum(growth(proto_udp_res_msg_total{namespace=~"$namespace", message_name="session_establishment_res", status="no_rsp_received_tx"} [15m])) da (message_name, status, peer_info)

Etichetta: {{nome_messaggio}} || {{stato}} || {{info_peer}}

Grafana deve mostrare dove avvengono i fallimenti. Nell'esempio, questo attributo è correlato a UPF419.

Quando ci si connette al sistema, è possibile verificare che sessmgr non sia stato impostato correttamente dopo il passaggio a RCM perché molti dei gestori della sessione non sono nello stato 'Attivo pronto' previsto.

```
[local]UPF419# show srp checkpoint statistics verbose
Tuesday November 02 17:24:01 UTC 2021
 smgr     state  peer    recovery  pre-alloc  chk-point rcvd   chk-point sent
 inst            conn    records   calls      full     micro   full     micro
 ----   -------  -----   -------   --------   -----    -----   -----     ----
    1      Actv Ready         0          0    1108    34001   14721   1200158
    2      Actv Ready         0          0    1086    33879   17563   1347298
    3      Actv Ready         0          0    1114    34491   15622   1222592
     4       Actv  Conn         0          0       5      923       0         0
    5      Actv Ready         0          0    1106    34406   13872   1134403
     6       Actv  Conn         0          0       5      917       0         0
     7       Actv  Conn         0          0       5      920       0         0
     8       Actv  Conn         0          0       1      905       0         0
     9       Actv  Conn         0          0       5      916       0         0
    10       Actv  Conn         0          0       5      917       0         0
   11      Actv Ready         0          0    1099    34442   13821   1167011
    12       Actv  Conn         0          0       5      916       0         0
    13       Actv  Conn         0          0       5      917       0         0
   14      Actv Ready         0          0    1085    33831   13910   1162759
   15      Actv Ready         0          0    1085    33360   13367   1081370
    16       Actv  Conn         0          0       4      921       0         0
   17      Actv Ready         0          0    1100    35009   13789   1138089
   18      Actv Ready         0          0    1092    33953   13980   1126028
    19       Actv  Conn         0          0       5      916       0         0
    20       Actv  Conn         0          0       5      918       0         0
   21      Actv Ready         0          0    1098    33521   13636   1108875
   22      Actv Ready         0          0    1090    34464   14529   1263419
```

Soluzione

Questo problema è correlato al Cisco Defect Tracking System (CDETS) CSCvz9749. La correzione è stata integrata nella versione 21.22.ua4.82694 e successive.

Soluzione alternativa

Con l'UPF419, è necessario riavviare le istanze del gestore di sessione che non erano in **Active Ready** con l'**istanza di sessmgr <>**nascosta dell'**operazione di interruzione dell'attività del** comando e questo risolve il problema.

```
[local]UPF419# show srp checkpoint statistics verbose
Wednesday November 03 16:44:57 UTC 2021
 smgr     state  peer    recovery  pre-alloc  chk-point rcvd   chk-point sent
 inst            conn    records   calls      full     micro   full     micro
 ----   -------  -----   -------   --------   -----    -----   -----     ----
    1      Actv Ready         0          0    1108    34001   38319   2267162
    2      Actv Ready         0          0    1086    33879   40524   2428315
    3      Actv Ready         0          0    1114    34491   39893   2335889
    4      Actv Ready         0          0       0        0   12275   1049616
    5      Actv Ready         0          0    1106    34406   37240   2172748
    6      Actv Ready         0          0       0        0   13302   1040480
    7      Actv Ready         0          0       0        0   12636   1062146
    8      Actv Ready         0          0       0        0   11446   976169
    9      Actv Ready         0          0       0        0   11647   972715
   10      Actv Ready         0          0       0        0   11131   950436
   11      Actv Ready         0          0    1099    34442   36696   2225847
   12      Actv Ready         0          0       0        0   10739   919316
   13      Actv Ready         0          0       0        0   11140   970384
   14      Actv Ready         0          0    1085    33831   37206   2226049
   15      Actv Ready         0          0    1085    33360   38135   2225816
   16      Actv Ready         0          0       0        0   11159   946364
   17      Actv Ready         0          0    1100    35009   37775   2242427
   18      Actv Ready         0          0    1092    33953   37469   2181043
   19      Actv Ready         0          0       0        0   13066   1055662
   20      Actv Ready         0          0       0        0   10441   938350
   21      Actv Ready         0          0    1098    33521   37238   2165185
   22      Actv Ready         0          0    1090    34464   38227   2399415
```

Registri da raccogliere in caso di errore UPF che causa un passaggio

> **Nota:** Verificare che i registri di debug siano abilitati in RCM (richiedere l'approvazione prima di abilitare i registri di debug). Consultare le raccomandazioni per la registrazione.

Livello registrazione ops-center RCM

```
logging level application debug
logging level transaction debug
logging level tracing off
logging name infra.config.core level application warn
logging name infra.config.core level transaction warn
logging name infra.resource_monitor.core level application warn
logging name infra.resource_monitor.core level transaction warn
```

Raccolta di dati dettagliata

1. Sintesi del problema: La descrizione del problema deve essere chiara. Indicare il **nome del nodo o l'indirizzo ip** problematico in modo che sia più facile trovare le informazioni necessarie dai log. Ad esempio, in caso di un problema di switchover, è utile ricordare che IP x.x.x.x è l'origine di UPF e x.x.x.y è la destinazione di UPF.
2. Se esistono più modi per riprodurre il problema, menzionare quelli.
3. Informazioni sulla versione di RCM: In caso di installazione di RCM VM da RCM VM, cat **/etc/smi/rcm-image-versionshow helm** dal centro operativo. In caso di installazione di RCM CN, **mostrare il timone** dal centro operativo.
4. Registri CN o RCM di debug Tac di RCM al momento in cui si è verificato il problema. In alcuni casi, è anche possibile richiedere i registri dall'inizio quando il POD è appena arrivato.
5. Indicare l'RCM principale o di backup. Nel caso di CN, condividere le informazioni per entrambe le coppie di RCM.
6. Condividere la configurazione in esecuzione da RCM ops-center da tutte le istanze.
7. Raccogliere le trap SNMP di RCM.
8. Indipendentemente dall'errore di switchover o meno, è preferibile raccogliere una unità SSD UP attiva e una unità SSD UP in standby.
9. I comandi RCM controller, configmgr, checkpoint manager, switchover e switchover-verbose statistics vengono utilizzati per indicare l'esatta CLI.
   rcm show-statistics controller
   rcm show-statistics configmgr
   rcm show-statistics checkpointmgr
   rcm show-statistics switchover
   rcm show-statistics switchover-verbose
10. Syslog di UPF o RCM.
11. Se il problema è relativo a un errore di switchover, è necessario un nuovo UPF SSD attivo e un vecchio UPF SSD attivo. In alcuni casi, il riavvio viene attivato a causa del passaggio. In tal caso, è necessario riprodurre il problema e prima di questo è necessario raccogliere la vecchia unità SSD UP attiva.
12. In un caso di errore di switchover, è anche utile raccogliere i log di debug vpn, sessmgr, sess-gr e sxdemux da attività vecchie e nuove alla riproduzione del problema.
    debug filtro registrazione funzionalità attiva a livello sxdemux
    debug livello sessmgr filtro di registrazione attivo
    debug livello sess-gr filtro di registrazione attivo
    debug filtro registrazione funzionalità attiva a livello vpn
13. I core di Vpnmgr/Sessmgr sono necessari in caso di errore/problema in sessmgr/vpnmgr. sessmgr_instance_id è l'istanza in cui viene rilevato il problema. **vpnmgr_instance_id** è il numero di contesto del contesto RCM.
    istanza sessmgr struttura di base dell'attività <sessmgr_instance_id>
    istanza vpnmgr struttura di base dell'attività <vpnmgr_instance_id>
14. In caso di problema relativo a RCM HA, condividere i registri di debug/pod di RCM TAC da entrambe le istanze.

Informazioni correlate

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- Documentazione e supporto tecnico – Cisco Systems