Solución de problemas de conmutación en núcleo convergente RCM

Contenido

Introducción

Este documento describe los pasos básicos para resolver problemas en el administrador de configuración redundante (RCM) en caso de un evento de falla de red.

Antecedentes

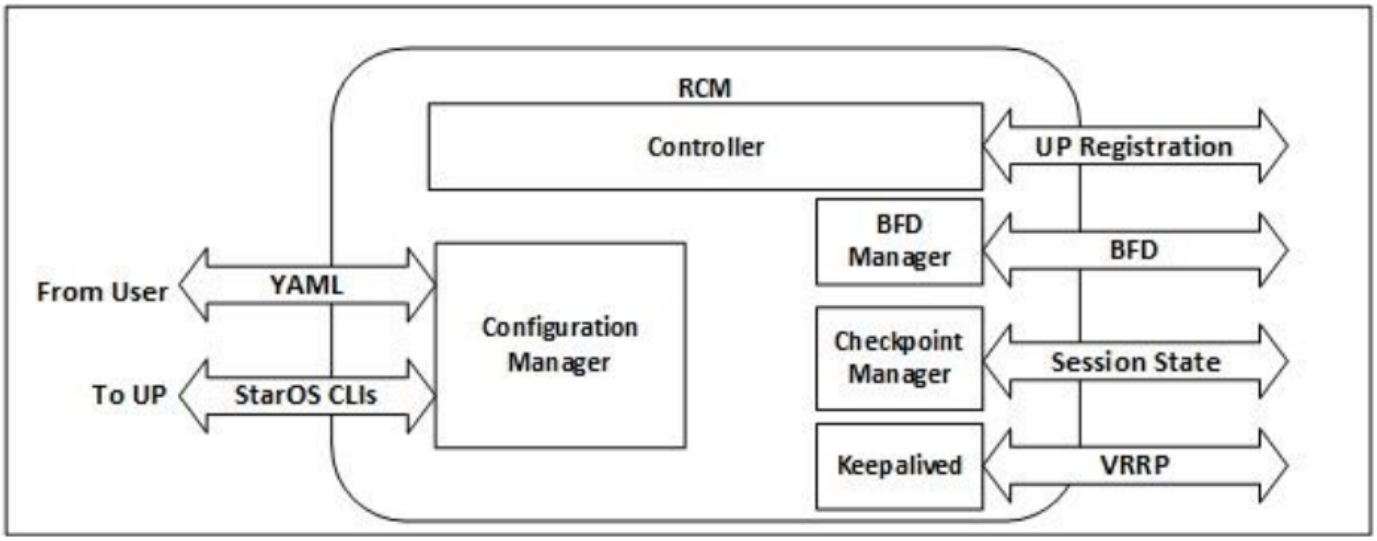
¿Qué es RCM?

El RCM es un nodo propietario de Cisco o una función de red (NF) que proporciona redundancia para las funciones de plano de usuario (UPF) basadas en StarOS.

El RCM proporciona redundancia N:M de UPF donde N es un número de UPF activos y es menor que 10, y M es un número de UP en espera en el grupo de redundancia.

Componentes de RCM

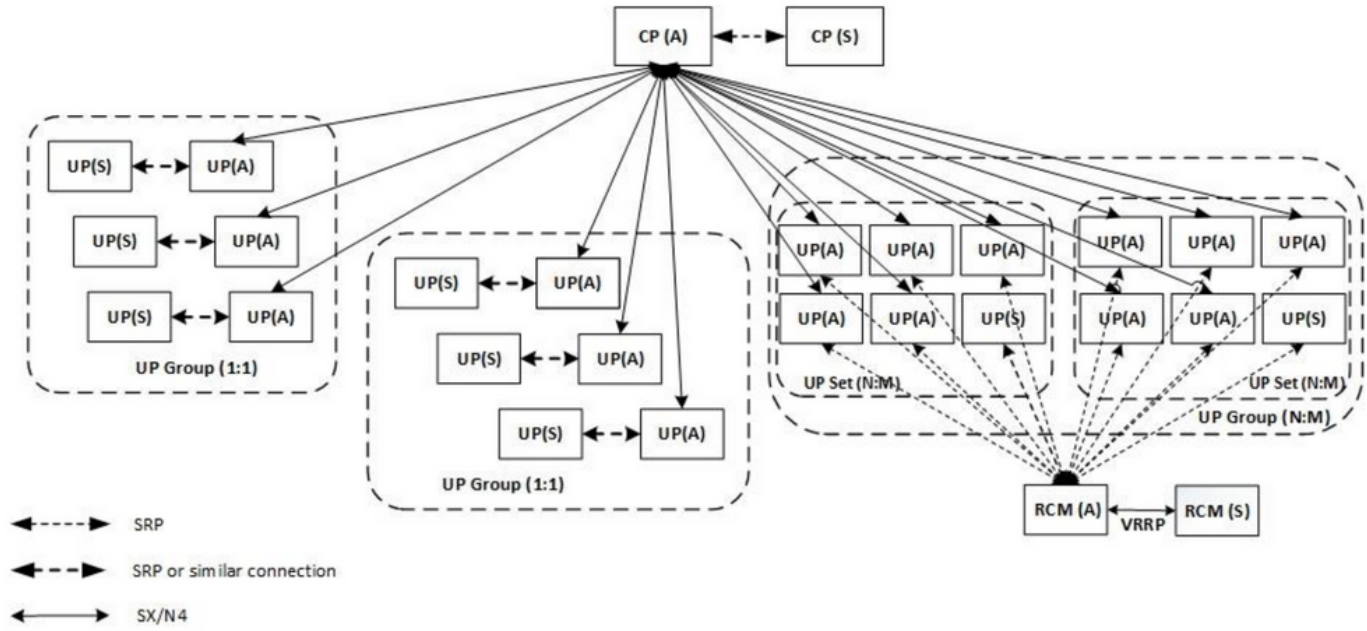
El RCM consta de componentes que se ejecutan como grupos de dispositivos en la VM del RCM:



- Controlador: Comunica las decisiones específicas de los eventos con todos los demás grupos de dispositivos en el RCM
- Administrador de BFD (BFDMgr): Utiliza el protocolo BFD para identificar el estado del plano de datos
- Administrador de configuración (ConfigMgr): Carga la configuración solicitada en los planos de usuario (UP)
- Administrador de redundancia (RedMgr): También se denomina administrador de punto de comprobación. Almacena y envía los datos del punto de control a un UPF en espera

- Mantenimiento: Se comunica entre el RCM Activo y en Espera con el uso de VRRP

Modelo típico de implementación de RCM



Descripción general de RCM CLI

En este ejemplo, hay cuatro centros OPS de RCM. Para confirmar qué RCM Kubernetes corresponde con qué Centro OPS de RCM y Entorno de ejecución común de RCM (CEE) puede iniciar sesión en RCM Kubernetes y enumerar los espacios de nombres:

```
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
```

Dirección IP de administración UPF

Esta IP es específica y está vinculada a VM o UPF. Se utiliza en la comunicación inicial entre UPF y RCM, donde UPF se registra con RCM y RCM configura UPF y también asigna funciones. Puede utilizar esta IP para identificar UPF de los resultados de RCM CLI.

IP de rol de dispositivo UPF

Vinculado a una función (activo/en espera):

Esta dirección IP se mueve a medida que se produce el switchover.

Comandos CLI útiles para la resolución de problemas de RCM

Puede revisar qué grupo RCM es el UPF del Centro OPS de RCM. Busque un ejemplo de la plataforma de implementación nativa en la nube (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: El ID de host no es el mismo que el nombre de host de UPF.

Aquí puede ver el estado en el Centro OPS de RCM:

```
[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"
      }
    ]
  },
```

Identificar UPF en espera actual del centro OPS de RCM

Desde RCM OPS, el Centro identifica el UPF en espera con el 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"
      },
```

Inicie sesión en UPF y verifique la información de 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)
```

Esta es otra información útil del Centro OPS de RCM:

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

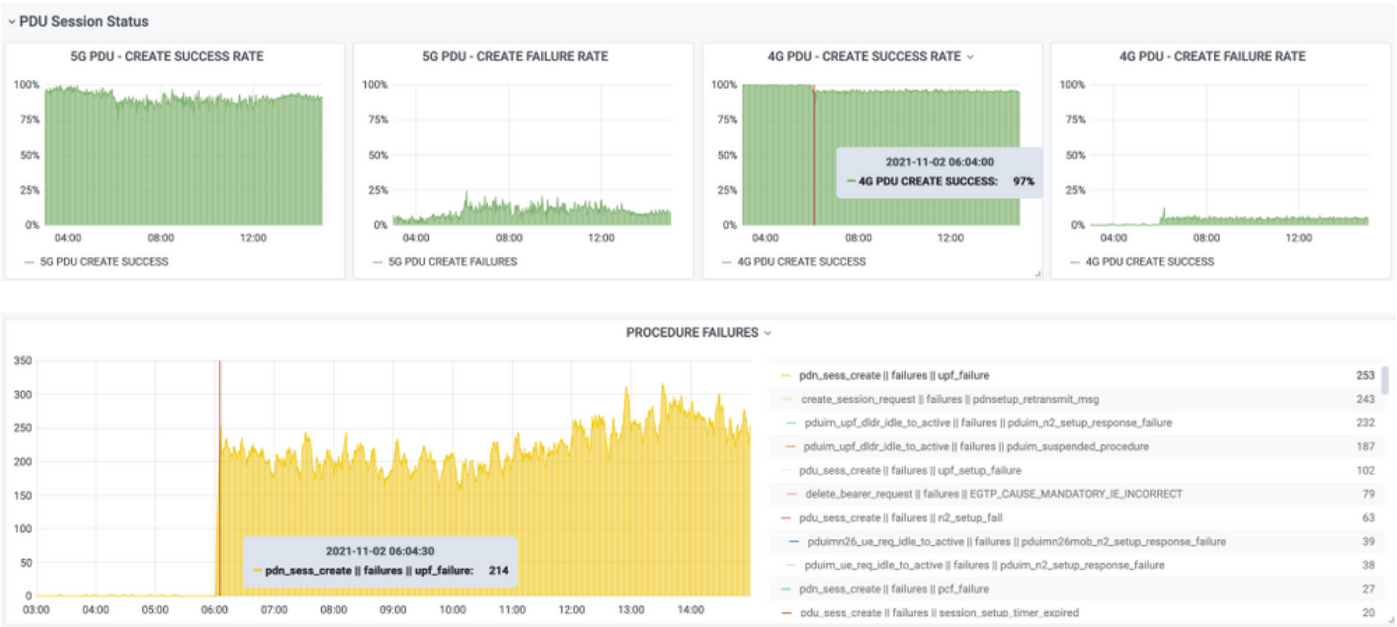
```
checkpointmgr   Show RCM Checkpointmgr Statistics information
configmgr       Show RCM Configmgr Statistics information
controller      Show RCM Controller Statistics information
|               Output modifiers
<cr>
```

Descargue la guía del RCM para la versión 21.24.

Problema notificado por fallas de RCM en PODs CNDP

Se informó del problema en uno de los UPF relacionados con la alerta UP_SX_SESS_ESTABLISHMENT_SR. Esta alerta indica que la tasa de éxito de establecimiento de sesión en la interfaz SX se redujo bajo el umbral configurado.

Si observa las estadísticas de Grafana, se observa una degradación de 5G/4G debido a la razón de desconexión **pdn_sess_create || fallos || upf_failure**:



Esto confirma que **pdn_sess_create || fallos || upf_failure** fueron causados por 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)
```

En SMF puede verificar la configuración de UPF. En este caso, debe buscar la dirección 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
```

Luego puede realizar la consulta Grafana para identificar hacia qué dirección UPF N4 hay más fallas:

Consulta Grafana:
sum(Increase(proto_udp_res_msg_total{espacio de nombres=~"$espacio de nombres", message_name="session_establishment_res", status="no_rsp_received_tx"} [15m]) por (message_name, status, peer_info)

Etiqueta: {{message_name}} || {{status} || {{peer_info}

Grafana debe mostrar dónde ocurren los fracasos. En el ejemplo, está relacionado con UPF419.

Cuando se conecta al sistema, puede confirmar que el sessmgr no se configuró correctamente después del switchover de RCM porque muchos de los administradores de sesión no están en el estado 'Actv Ready' esperado.

```
[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
```

Solución

Esto se relaciona con el Sistema de seguimiento de defectos de Cisco (CDETS) CSCvz9749. La corrección se integró en 21.22.ua4.82694 y posterior.

Solución Aternativa

En UPF419, debe reiniciar las instancias del administrador de sesión que no estaban en **Actv Ready** con el comando oculto **instancia sessmgr de la instalación de habilidades de habilidades <>** y esto resuelve la situación.

```
[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
```

Registros que se recopilarán en caso de fallo de UPF que provoque un Switchover

> **Nota:** Asegúrese de que los registros de depuración estén habilitados en el RCM (solicite la aprobación antes de activar cualquier registro de depuración). Consulte recomendaciones de registro.

Nivel de registro del centro de operaciones de 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
```

Recopilación de datos paso a paso

1. Resumen del problema: La sentencia del problema debe ser clara. Indíquele el **nombre de nodo/ip** problemático para que sea más fácil encontrar la información necesaria de los registros. Por ejemplo, en caso de un problema de switchover, es útil si se menciona que IP x.x.x.x es el origen UPF y x.x.x.y es el destino UPF.
2. Si hay varias formas de reproducir el problema, menciónelas.
3. Información de la versión de RCM: En el caso de la implementación de VM RCM desde la VM RCM, cat **/etc/smi/rcm-image-versionesshow helm** desde el centro de operaciones. En el caso del despliegue de CN de RCM, **mostrar helm** del centro de operaciones.
4. Registros de depuración CN o RCM de Tac RCM en el momento en que se produjo el problema. En algunos casos, también puede requerir registros desde el principio cuando el POD acaba de aparecer.
5. Indique qué RCM es primario o de respaldo. En el caso de CN, comparta la información de ambos pares de RCM.
6. Comparta la configuración en ejecución del centro de operaciones de RCM desde todas las instancias.
7. Recopile las trampas SNMP del RCM.
8. Independientemente de la falla del switchover o no, es mejor recopilar una SSD UP activa y una SSD UP en espera.
9. Los comandos RCM controller, configmgr, checkpoint manager, switchover y switchover-verbose statistics se utilizan para mencionar la CLI exacta.
   RCM show-statistics controller
   rcm show-statistics configmgr
   rcm show-statistics checkpoint mgr
   rcm show-statistics switchover
   rcm show-statistics switchover-verbose
10. Syslogs de UPF o RCM.
11. Si el problema se relaciona con la falla de switchover, se requiere una nueva UPF SSD activa y una UPF SSD activa antigua. En algunos casos, old activa el reinicio debido al switchover. En ese caso, debe reproducir el problema, y justo antes de eso debe recopilar la antigua SSD UP activa.
12. En un caso de falla de switchover, también es útil recopilar los registros de depuración vpn, sessmgr, sess-gr y sxdemux de los actives antiguos y nuevos en la reproducción del problema.
    logging filter active feature sxdemux level debug
    logging filter active facility sessmgr level debug
    logging filter active facility sess-gr level debug
    logging filter active Facility vpn level debug
13. Los núcleos Vpnmgr/Sessmgr son necesarios en caso de error/problema en sessmgr/vpnmgr. El sessmgr_instance_id es la instancia donde se observa el problema. **vpnmgr_instance_id** es el nº de contexto del contexto RCM.
    recurso principal de tarea sessmgr instance <sessmgr_instance_id>
    recurso de núcleo de tarea vpnmgr instance <vpnmgr_instance_id>
14. En caso de problema de HA de RCM, comparta los registros de debug/pod del TAC de RCM de ambas instancias.

Información Relacionada

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- Soporte Técnico y Documentación - Cisco Systems