Identificar e Solucionar Problemas de Switchover no Núcleo Convergente do RCM

Contents

Introduction

Este documento descreve as etapas básicas para solucionar problemas no RCM (Redundancy Configuration Manager, Gerenciador de Configuração de Redundância) no caso de um evento de falha de rede.

Informações de Apoio

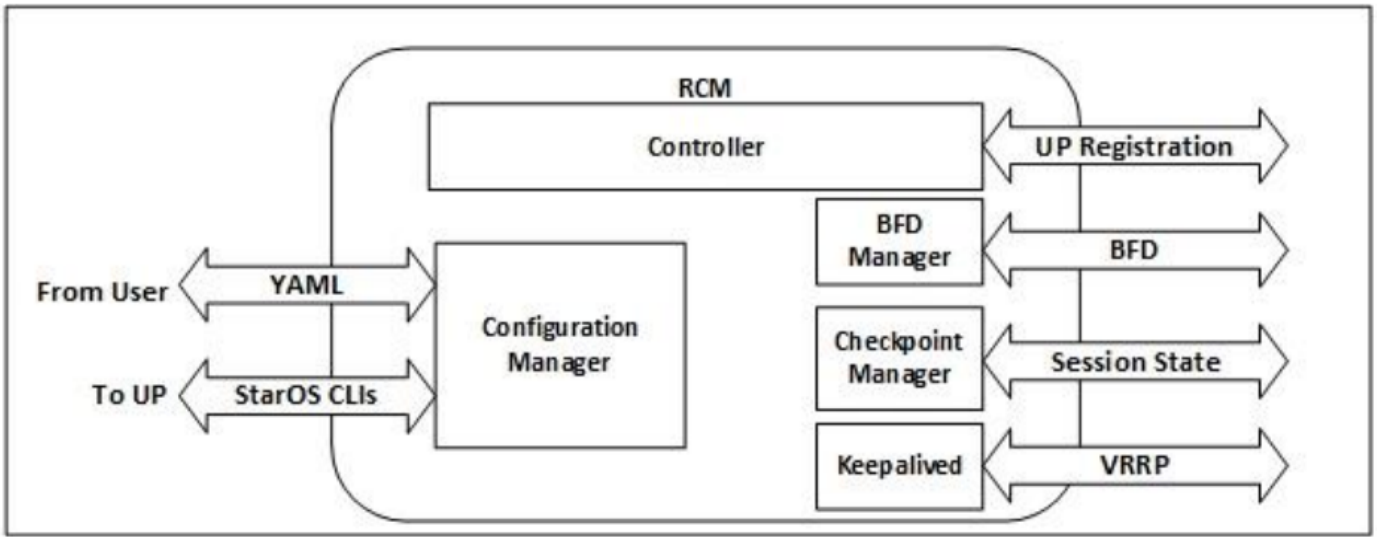
O que é o RCM?

O RCM é um nó proprietário da Cisco ou função de rede (NF) que fornece redundância para funções de plano do usuário (UPF) baseadas em StarOS.

O RCM fornece redundância N:M de UPF em que N é um número de UPFs Ativas e é inferior a 10, e M é um número de UPs em standby no grupo de redundância.

Componentes do RCM

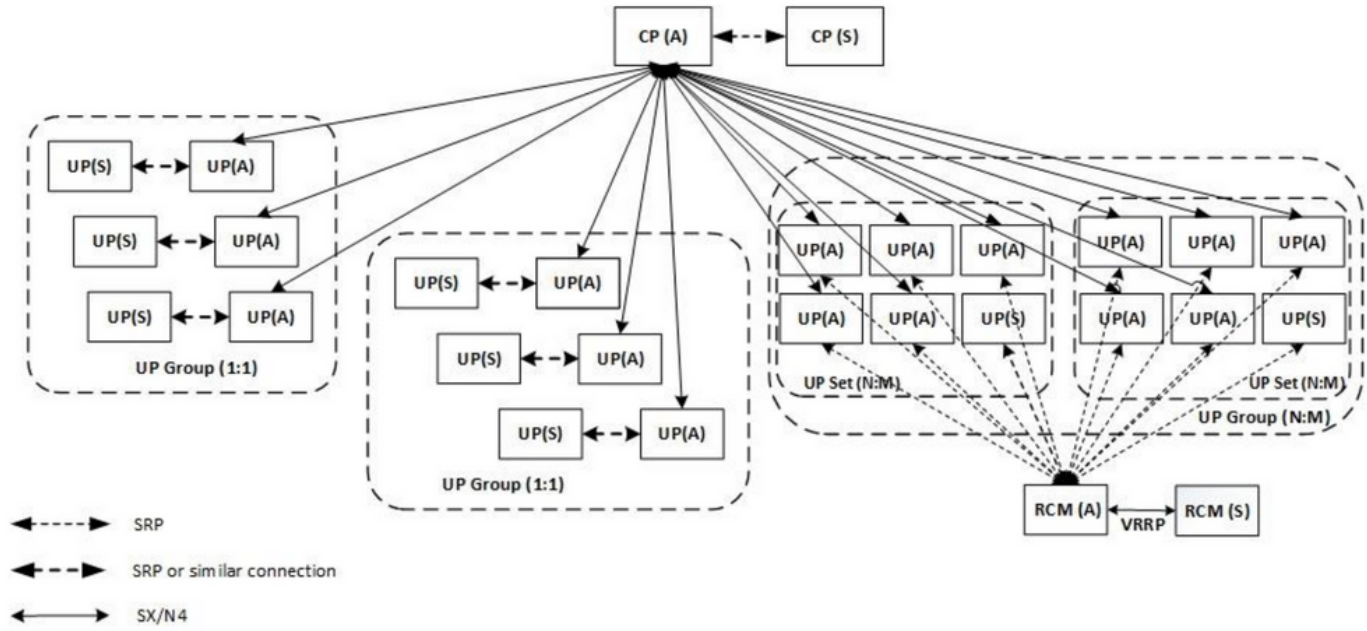
O RCM compreende componentes que funcionam como pods na VM do RCM:



- Controlador: Comunica as decisões específicas dos eventos com todos os outros pods no RCM
- Gerenciador BFD (BFDMgr): Ele usa o protocolo BFD para identificar o estado do plano de dados
- Gerenciador de configuração (ConfigMgr): Carrega a configuração solicitada para os planos do usuário (UPs)
- Gerenciador de redundância (RedMgr): Também é chamado de Checkpoint Manager. Ele armazena e envia os dados do ponto de verificação para um UPF em standby

- Manutenção de atividade: Comunica-se entre o RCM Ativo e Standby com o uso do VRRP

Modelo de Implementação do RCM típico



Visão geral da CLI do RCM

Neste exemplo, há quatro centros de OPS RCM. Para confirmar quais os Kubernetes do RCM correspondentes ao Centro de OPS do RCM e ao Ambiente de Execução Comum do RCM (CEE), pode iniciar sessão nos Kubernetes do RCM e listar os namespaces:

```
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
```

Endereço IP de gerenciamento UPF

Esse IP é específico e está vinculado à VM ou UPF. É utilizado na comunicação inicial entre UPF e RCM, em que a UPF registra com o RCM e o RCM configura a UPF e também atribui funções. Você pode usar este IP para identificar UPF das saídas CLI do RCM.

IP da função do dispositivo UPF

Vinculado a uma função (ativo/standby):

Esse endereço IP se move conforme o switchover acontece.

Comandos CLI úteis para resolução de problemas do RCM

Você pode rever qual grupo do RCM é o UPF do Centro de OPS do RCM. Encontre um exemplo da Plataforma de implantação nativa de nuvem (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)
```

Note: O ID do host não é igual ao nome do host UPF.

Aqui você pode ver o status no Centro de OPS do 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 em Standby Atual a Partir do Centro de OPS do RCM

No RCM OPS, o Centro identifica o UPF em Standby com a utilização do 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"
      },
```

Efetue login no UPF e verifique as informações do 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)
```

Aqui estão outras informações úteis do Centro de OPS do RCM:

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

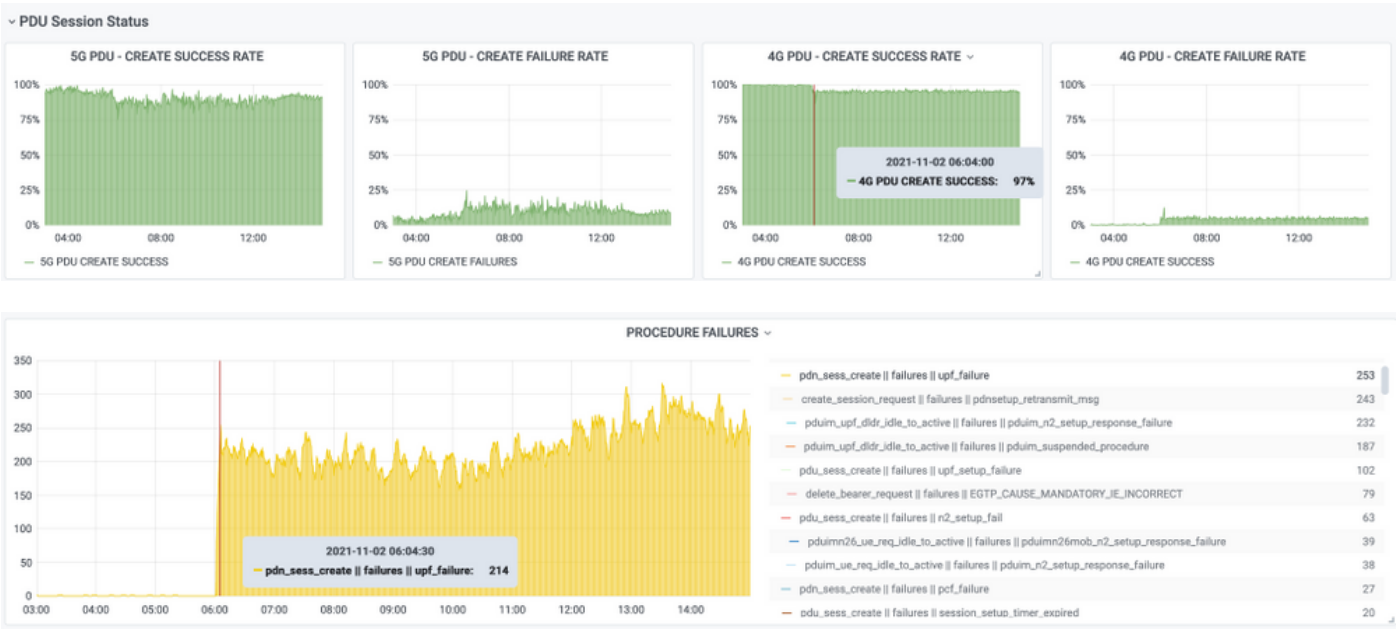
```
checkpointmgr   Show RCM Checkpointmgr Statistics information
configmgr       Show RCM Configmgr Statistics information
controller      Show RCM Controller Statistics information
|               Output modifiers
<cr>
```

Faça o download do guia RCM para a versão 21.24.

Problema Relatado por Falhas do RCM em PODs CNDP

O problema foi relatado em uma das UPFs relacionadas ao alerta UP_SX_SESS_ESTABLISHMENT_SR. Este alerta diz que a taxa de sucesso do estabelecimento da sessão na interface SX caiu abaixo do limite configurado.

Se você observar as estatísticas do Grafana, uma degradação de 5G/4G é observada devido ao motivo da desconexão **pdn_sess_create | Falhas | upf_failure**:



Isso confirma que o **pdn_sess_create | Falhas | upf_failure** causado 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)
```

No SMF, você pode verificar a configuração de UPF. Nesse caso, você deve procurar o endereço IP N4 do UPF:

```
[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
```

Em seguida, você pode executar a consulta Grafana para identificar para qual endereço N4 do UPF há a maioria das falhas:

Consulta Grafana:
sum(growth(proto_udp_res_msg_total{namespace=~"$namespace", message_name="session_established_res", status="no_rsp_receive_tx"} [15m]) por (message_name, status, peer_info)

Rótulo: {{message_name}} | {{status}} | {{peer_info}}

Grafana deve mostrar onde as falhas acontecem. No exemplo, está relacionado ao UPF419.

Quando se liga ao sistema, pode confirmar que o sessmgr não foi corretamente definido após a comutação do RCM, porque muitos dos gerentes de sessão não estão no estado "Pronto para Ativa" 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
```

Solução

Isso está relacionado ao Cisco Defect Tracking System (CDETS) CSCvz9749. A correção foi integrada em 21.22.ua4.82694 e posterior.

Solução

No UPF419, você deve reiniciar as instâncias do gerenciador de sessão que não estavam no **Actv Ready** com **instância do sessmgr do recurso de eliminação de tarefas de comando oculto** e isso resolve a situação.

```
[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 a serem coletados em caso de falha de UPF que causa um switchover

> **Note**: Certifique-se de que os registros de depuração estejam ativados no RCM (solicite aprovação antes de ativar qualquer registro de depuração). Consulte recomendações de registro.

Nível de registro do centro de operações do 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
```

Coleta de dados passo a passo

1. Resumo do problema: A instrução do problema deve ser clara. Indique o **nome/ip do nó** problemático para que seja mais fácil encontrar as informações necessárias dos registros. Por exemplo, no caso de um problema de switchover, é útil se for mencionado que o IP x.x.x.x é o UPF de origem e x.x.x.y é o UPF de destino.
2. Se houver várias maneiras de reproduzir o problema, mencione-as.
3. Informações sobre a versão do RCM: No caso da implantação de VM RCM a partir da VM RCM, cat **/etc/smi/rcm-image-versionshow helm** a partir do centro de operações. No caso da implantação do RCM CN, **mostrar helm** do centro de operações.
4. O RCM Tac debug CN ou RCM registra os registros no momento da ocorrência do problema. Em alguns casos, você também pode exigir registros desde o início quando o POD acabou de aparecer.
5. Indique qual RCM é primário ou de backup. No caso da NC, partilhar as informações relativas a ambos os pares do RCM.
6. Compartilhe a configuração atual do centro de operações do RCM a partir de todas as instâncias.
7. Colete as armadilhas SNMP do RCM.
8. Independentemente da falha de switchover ou não, é melhor coletar um SSD UP ativo e um SSD UP em standby.
9. Controlador RCM, configmgr, gerenciador de ponto de verificação, switchover e comandos de estatística switchover-verbose são usados para mencionar a CLI exata.
   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 ou RCM.
11. Se o problema estiver relacionado à falha de switchover, um novo SSD UPF ativo e um SSD ativo UPF antigo serão necessários. Em alguns casos, os ativos antigos são reinicializados devido ao switchover. Nesse caso, você deve reproduzir o problema e, logo antes disso, precisa coletar a antiga SSD UP ativa.
12. Em um caso de falha de switchover, também é útil coletar os logs de depuração de vpn, sessmgr, sess-gr e sxdemux de antigos e novos ativos na reprodução do problema.
    logging filter ative facility sxdemux level debug
    logging filter ative facility sessmgr level debug
    logging filter ative facility sess-gr level debug
    logging filter ative facility vpn level debug
13. Os núcleos do Vpnmgr/Sessmgr são necessários em caso de erro/problema no sessmgr/vpnmgr. O sessmgr_instance_id é a instância onde o problema é notado.
    vpnmgr_instance_id é o contexto # do contexto do RCM.
    task core facility sessmgr instance <sessmgr_instance_id>
    task core facility vpnmgr instance <vpnmgr_instance_id>
14. Em caso de problema de HA do RCM, compartilhe os registros de depuração/pod do TAC do RCM de ambas as instâncias.

Informações Relacionadas

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