排除RCM融合核心上的切换故障

目录

简介

本文档介绍在发生网络故障事件时对Redundancy Configuration Manager(RCM)进行故障排除的基本步骤。

背景信息

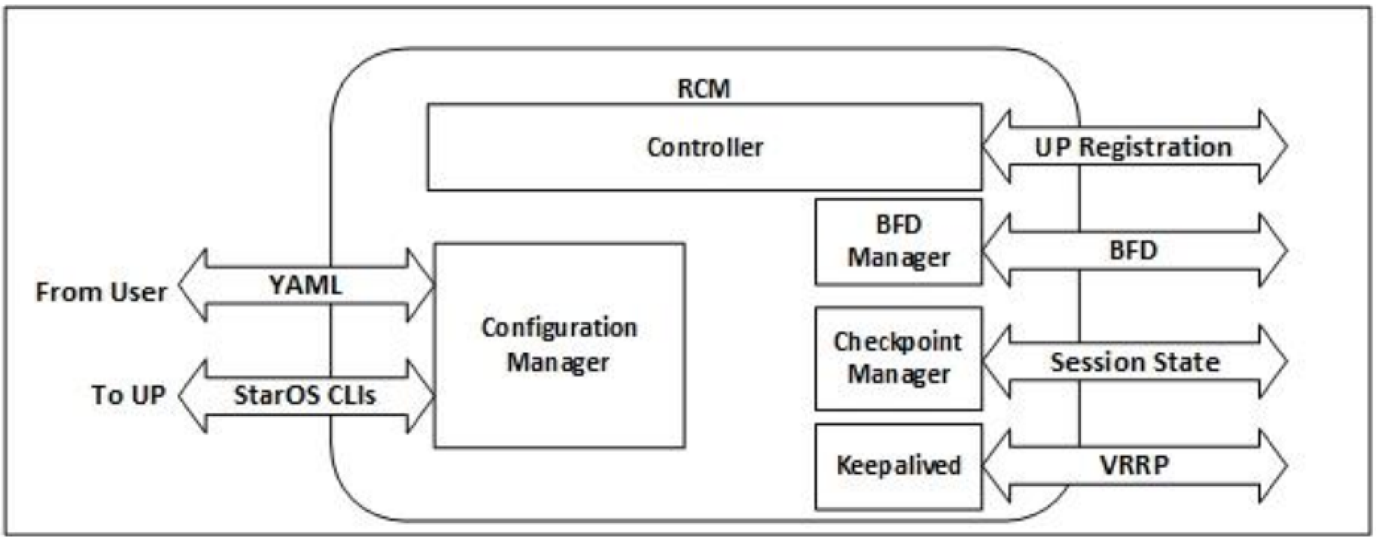
什么是RCM?

RCM是思科专有节点或网络功能(NF)，为基于StarOS的用户平面功能(UPF)提供冗余。

RCM提供UPF的N:M冗余，其中N是多个活动UPF且小于10,M是冗余组中的多个备用UP。

RCM的组件

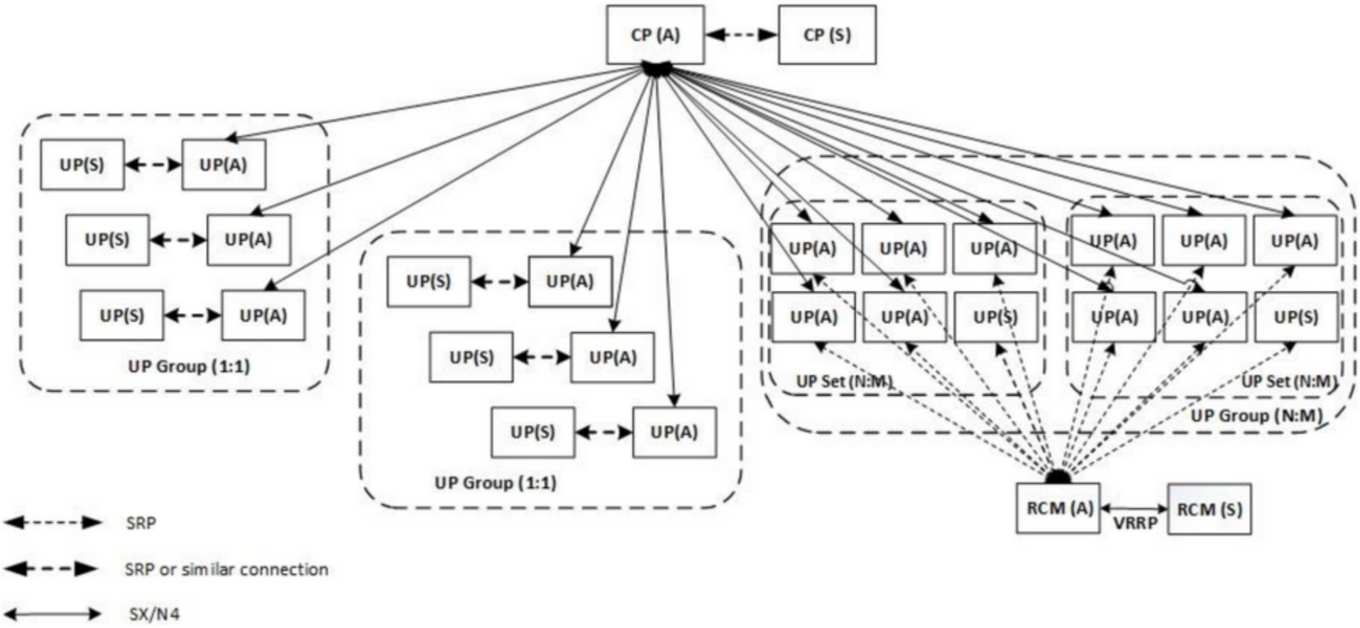
RCM包括在RCM VM中作为Pod运行的组件：



- 控制器：它与RCM中的所有其他Pod传达特定于事件的决策
- BFD管理器(BFDMgr):它使用BFD协议来标识数据平面的状态
- 配置管理器(ConfigMgr):将请求的配置加载到用户平面(UP)
- 冗余管理器(RedMgr):它也称为检查点管理器。它存储检查点数据并将其发送到备用UPF

- 保持连接：它使用VRRP在主用RCM和备用RCM之间通信

典型RCM部署模式



RCM CLI概述

在本例中，有四个RCM OPS中心。为了确认RCM Kubernetes与RCM OPS Center和RCM Common Execution Environment(CEE)对应哪个RCM Kubernetes ，您可以登录到RCM Kubernetes并列出命名空间：

```
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
```

UPF管理IP地址

此IP是特定的，并与VM或UPF关联。它用于UPF和RCM之间的初始通信，其中UPF向RCM和RCM注册，配置UPF并分配角色。您可以使用此IP从RCM CLI输出中标识UPF。

UPF设备角色IP

链接到角色（主用/备用）：

此IP地址会随着切换发生而移动。

RCM故障排除的有用CLI命令

您可以从RCM OPS Center查看哪个RCM组是UPF。从云本地部署平台(CNDP)中查找示例：

```
[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)
```

注意：主机ID与UPF主机名不同。

在此，您可以看到RCM OPS Center的状态：

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

从RCM OPS中心确定当前备用UPF

在RCM OPS中，中心使用rcm show-statistics controller命令识别备用**UPF的状**态：

```
  {
         "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"
       },
```

登录UPF并检查RCM信息：

```
[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)
```

以下是RCM OPS Center的其他有用信息：

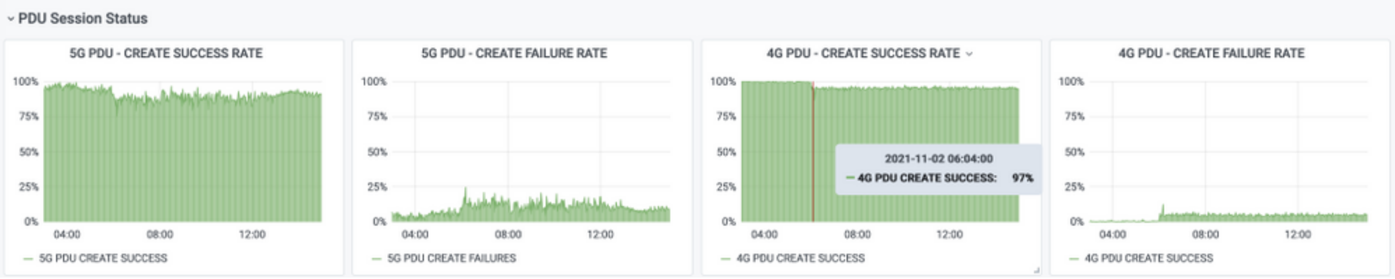
```
[up300-aio-2/rm34] rcm# rcm show-statistics
Possible completions:
 bfdmgr          Show RCM BFDMgr Statistics information
 checkpointmgr   Show RCM Checkpointmgr Statistics information
 configmgr       Show RCM Configmgr Statistics information
 controller      Show RCM Controller Statistics information
 |               Output modifiers
 <cr>
```

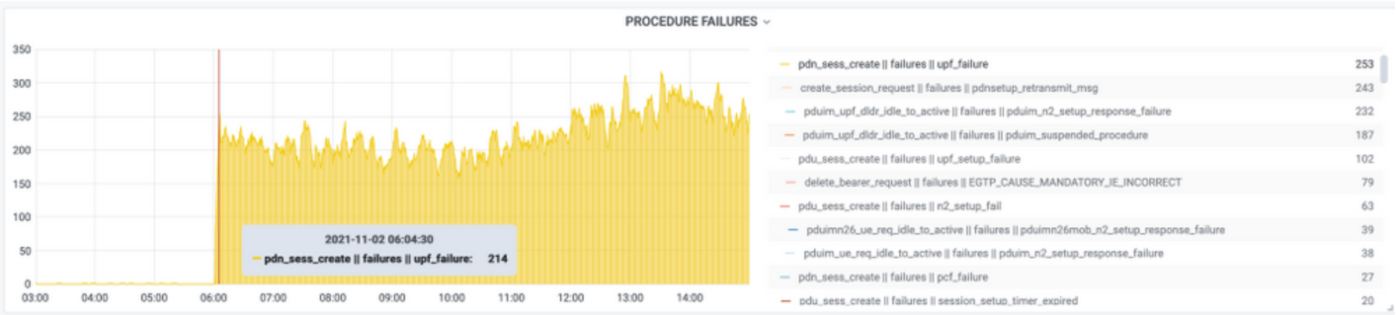
下载版本21.24的RCM指南。

CNDP POD上RCM故障报告的问题

问题报告在与警报UP_SX_SESS_ESTABLISHMENT_SR相关的其中一个UPF上。此警报表示SX接口上的会话建立成功率在配置的阈值以下。

如果查看Grafana统计信息，会发现5G/4G降级是由于断开原因**pdn_sess_create |失败 || upf_failure**:




PROCEDURE FAILURES
350
300
250
200
150
100
50
0
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
2021-11-02 06:04:30
pdn_sess_create || failures || upf_failure: 214
pdn_sess_create || failures || upf_failure 253
create_session_request || failures || pdnsetup_retransmit_msg 243
pduim_upf_dldr_idle_to_active || failures || pduim_n2_setup_response_failure 232
pduim_upf_dldr_idle_to_active || failures || pduim_suspended_procedure 187
pdu_sess_create || failures || upf_setup_failure 102
delete_bearer_request || failures || EGTP_CAUSE_MANDATORY_IE_INCORRECT 79
pdu_sess_create || failures || n2_setup_fail 63
pduimn26_ue_req_idle_to_active || failures || pduimn26mob_n2_setup_response_failure 39
pduim_ue_req_idle_to_active || failures || pduim_n2_setup_response_failure 38
pdn_sess_create || failures || pcf_failure 27
pdu_sess_create || failures || session_setup_timer_expired 20

这确认**pdn_sess_create |失败 || upf_failure**由UPF419引起：

```
[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)
```

在SMF上，您可以检查UPF配置。在这种情况下，您必须查找UPF N4 IP地址：

```
[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
```

然后，您可以执行Grafana查询，以确定哪个UPF N4地址存在最多故障：

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

标签：{{message_name}} || {{status}} || {{peer_info}}

格拉法纳必须显示故障发生的位置。在本例中，它与UPF419相关。

连接到系统时，可以确认在RCM切换后未正确设置sessmgr，因为许多会话管理器未处于预期的“Actv Ready”状态。

```
[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
```

解决方案

这与思科缺陷跟踪系统(CDETS)CSCvz9749相关。修复程序已集成到21.22.ua4.82694及更高版本中。

解决方法

在UPF419上，必须使用隐藏命令task kill facility sessmgr instance <>重新启动未**在Actv Ready中**的会**话管理器实例，这**就解决了问题。

```
[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
```

在UPF故障导致切换时要收集的日志

> **注意：**确保在RCM中启用调试日志（在启用任何调试日志之前请求批准）。请参阅日志记录建议。

RCM运营中心日志记录级别

```
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
```

分步数据收集

1. 问题摘要：问题语句必须清晰。指示有问**题的节点名**称/ip，以便更轻松地从日志中查找必要信息。例如，在发生切换问题时，如果提到IP x.x.x.x是源UPF，x.x.x.y是目标UPF，则很有帮助。
2. 如果有多种方法可以重现问题，请提及这些。
3. RCM版本信息：在从RCM VM部署RCM VM时，从运**营中心部署cat/etc/smi/rcm-image-versionshow** helm。在RCM CN部署中，从运**营中**心显示helm。
4. 发生问题时的RCM Tac调试CN或RCM日志。在某些情况下，您还可以要求从POD刚启动时开始使用日志。
5. 指出哪个RCM是主RCM或备份RCM。对于CN，共享两个RCM对的信息。
6. 从所有实例共享RCM运行中心的运行配置。
7. 收集RCM SNMP陷阱。

8. 无论是否发生切换故障，最好收集一个活动UP SSD和一个备用UP SSD。
9. RCM控制器、configmgr、检查点管理器、切换和switchover-verbose statistics命令用于提及确切的CLI。
   rcm show-statistics controller
   rcm show-statistics configmgr
   rcm show-statistics checkpointmgr
   rcm show-statistics switchover
   rcm show-statistics switchover-verbose
10. UPF或RCM的系统日志。
11. 如果问题与切换故障有关，则需要新的活动UPF SSD和旧的UPF活动SSD。在某些情况下，旧活动会因切换而重新启动。在这种情况下，您必须重现问题，并且在问题发生之前，您需要收集旧的活动UP SSD。
12. 在切换故障情况下，在问题重现时从旧活动和新活动收集vpn、sessmgr、sess-gr和sxdemux调试日志也很有帮助。
    logging filter active facility sxdemux level debug
    logging filter active facility sessmgr level
    logging filter active facility sess-gr level debug
    logging filter active facility vpn level
13. 如果sessmgr/vpnmgr中出现错误/问题，则需要Vpnmgr/Sessmgr核心。
    sessmgr_instance_id是发现问题的实例。**vpnmgr_instance_id**是RCM上下文的上下文编号。
    task core facility sessmgr instance <sessmgr_instance_id
    任务核心设施vpnmgr实例<vpnmgr_instance_id
14. 如果RCM HA出现问题，请从两个实例共享RCM TAC调试/Pod日志。

相关信息

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- 技术支持和文档 - Cisco Systems