

# RCM 통합 코어의 전환 문제 해결

## 목차

[소개](#)

[배경 정보](#)

[RCM이란 무엇입니까?](#)

[RCM의 구성 요소](#)

[일반적인 RCM 구축 모델](#)

[RCM CLI 개요](#)

[UPF 관리 IP 주소](#)

[UPF 장치 역할 IP](#)

[RCM 트러블슈팅을 위한 유용한 CLI 명령](#)

[RCM OPS 센터에서 현재 대기 UPF 식별](#)

[CNDP POD에서 RCM 장애로 보고된 문제](#)

[솔루션](#)

[해결 방법](#)

[전환을 일으키는 UPF 실패 시 수집할 로그](#)

[RCM 운영 센터 로깅 레벨](#)

[단계별 데이터 수집](#)

[관련 정보](#)

## 소개

이 문서에서는 네트워크 장애 이벤트가 발생할 경우 RCM(Redundancy Configuration Manager)에서 문제를 해결하기 위한 기본 단계에 대해 설명합니다.

## 배경 정보

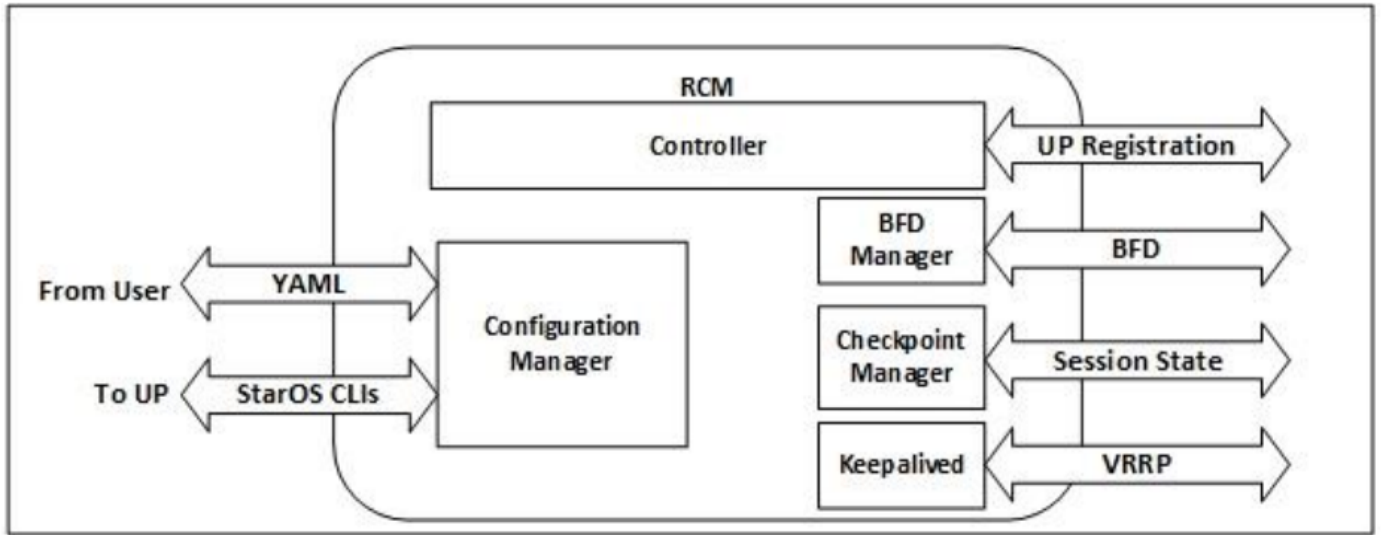
### RCM이란 무엇입니까?

RCM은 StarOS 기반 UPF(User Plane Functions)에 리던던시를 제공하는 Cisco 전용 노드 또는 네트워크 기능(NF)입니다.

RCM은 UPF의 N:M 이중화를 제공합니다. 여기서 N은 활성 UPF의 수이며 10보다 작고 M은 이중화 그룹의 대기 UP의 수입니다.

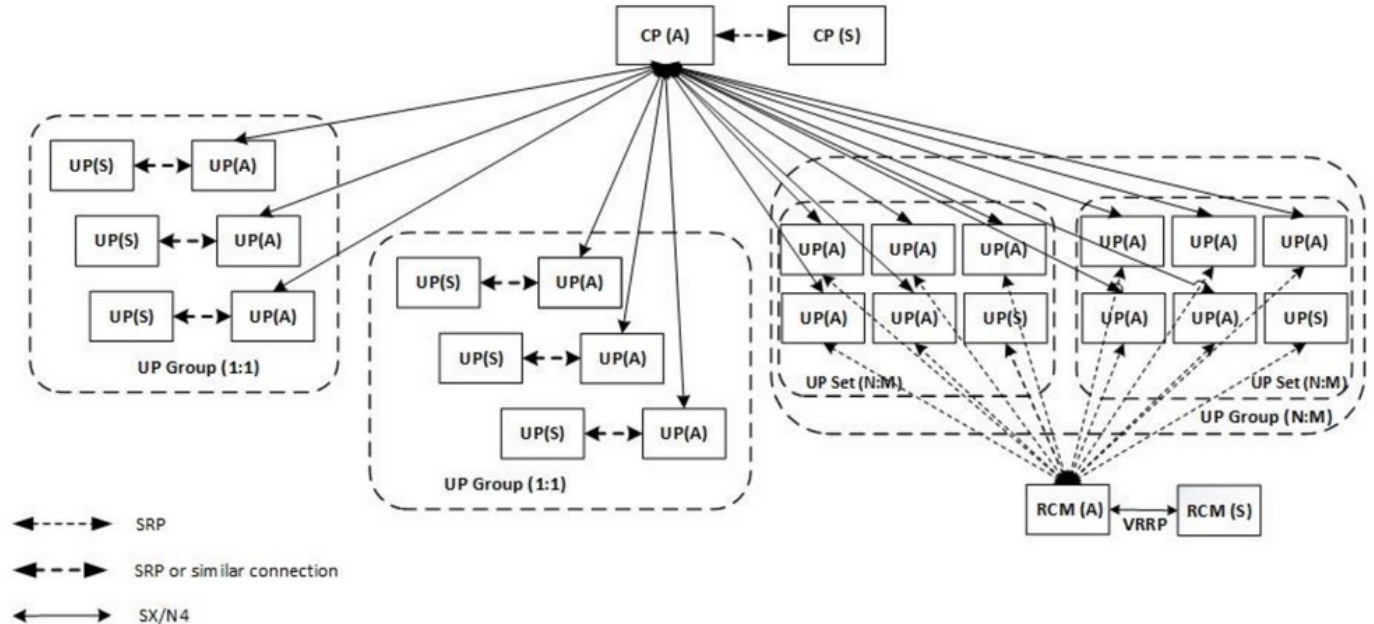
### RCM의 구성 요소

RCM은 RCM VM에서 포드로 실행되는 구성 요소로 구성됩니다.



- 컨트롤러: RCM의 다른 모든 포드와 이벤트 관련 의사 결정을 전달합니다.
- BFD 관리자(BFDMgr): BFD 프로토콜을 사용하여 데이터 플레인의 상태를 식별합니다.
- 구성 관리자(ConfigMgr): 요청된 컨피그레이션을 UP(사용자 플레인)에 로드합니다.
- 이중화 관리자(RedMgr): Checkpoint Manager라고도 합니다. Checkpoint 데이터는 대기 UPF에 저장 및 전송
- 보존: VRRP를 사용하여 액티브 RCM과 스탠바이 RCM 간에 통신합니다.

## 일반적인 RCM 구축 모델



## RCM CLI 개요

이 예에서는 4개의 RCM OPS 센터가 있습니다. 어떤 RCM Kubernetes가 어떤 RCM OPS Center 및 RCM CEE(Common Execution Environment)에 해당하는지 확인하려면 RCM Kubernetes에 로그인하여 네임스페이스를 나열하십시오.

```
cloud-user@up0300-ai0-1-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 관리 IP 주소

이 IP는 VM 또는 UPF에 연결되어 있습니다. UPF와 RCM 간의 초기 통신에 사용됩니다. UPF는 RCM에 등록되고 RCM은 UPF를 구성하고 역할도 할당합니다. 이 IP를 사용하여 RCM CLI 출력에서 UPF를 식별할 수 있습니다.

## UPF 장치 역할 IP

역할에 연결됨(활성/대기):

이 IP 주소는 전환 시 이동합니다.

## RCM 트러블슈팅을 위한 유용한 CLI 명령

RCM OPS Center에서 어떤 RCM 그룹이 UPF인지 검토할 수 있습니다. CNDP(Cloud Native Deployment Platform)에서 샘플을 찾습니다.

```
[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)

**참고:** 호스트 ID가 UPF 호스트 이름과 동일하지 않습니다.

RCM OPS Center의 상태를 확인할 수 있습니다.

```
[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": "BFDDState_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": "BFDDState_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"
  }
]
},

```

## RCM OPS 센터에서 현재 대기 UPF 식별

RCM OPS에서 Center는 `rcm show-statistics controller` 명령을 사용하여 Standby의 UPF를 식별합니다.

```

{
  "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"
},

```

UPF에 로그인하여 RCM 정보를 확인합니다.

```

[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)

```

다음은 RCM OPS Center의 다른 유용한 정보입니다.

```

[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

```

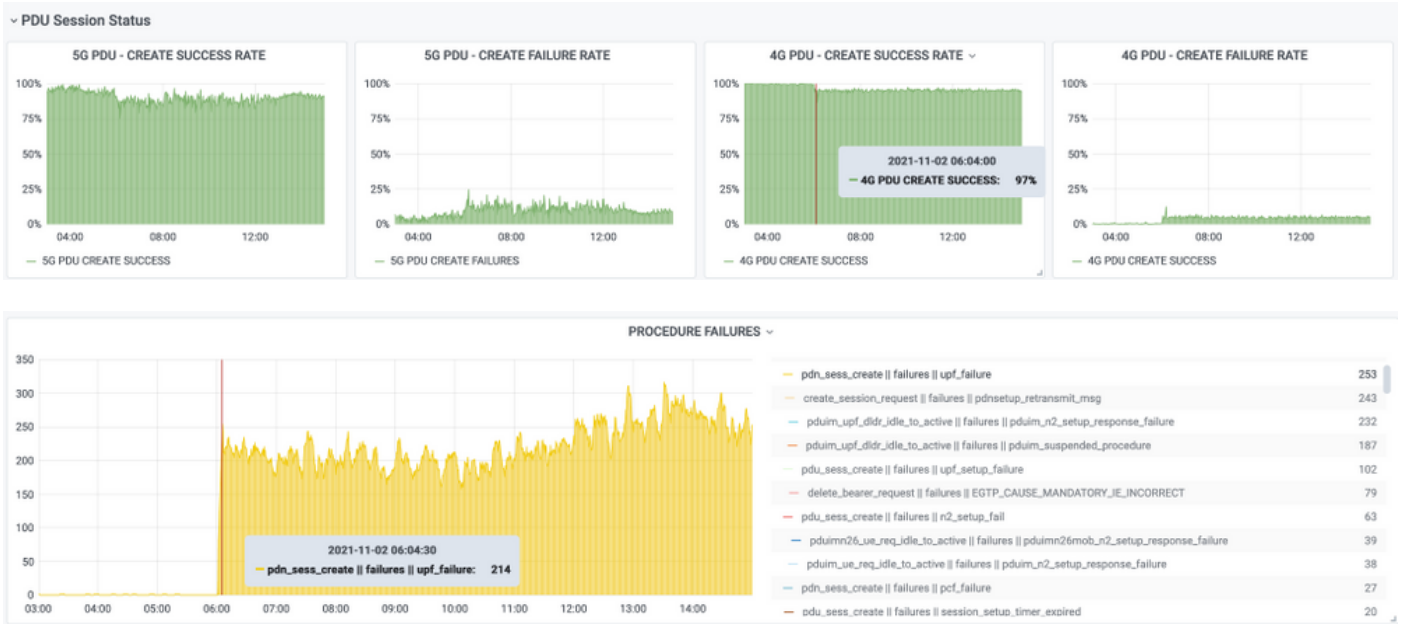
<cr>

릴리스 21.24에 대한 RCM [가이드](#)를 다운로드합니다.

## CNDP POD에서 RCM 장애로 보고된 문제

UP\_SX\_SESS\_ESTABLISHMENT\_SR 알림과 관련된 UPF 중 하나에 문제가 보고되었습니다. 이 알림에 따르면 SX 인터페이스의 세션 설정 성공률이 구성된 임계값 아래로 내려갔습니다.

Grafana 통계를 보면 연결이 끊어진 원인 pdn\_sess\_create로 인해 5G/4G 성능 저하가 관찰됩니다  
**|| 실패 | upf\_failure:**



그러면 pdn\_sess\_create가 **|| 실패 | upf\_failure**는 UPF419에 의해 발생했습니다.

```
[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)
```

SMF에서 UPF 컨피그레이션을 확인할 수 있습니다. 이 경우 UPF N4 IP 주소를 찾아야 합니다.

```
[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

```

그런 다음 Grafana 쿼리를 수행하여 UPF N4 주소에 오류가 가장 많은 주소를 식별할 수 있습니다.

그라파나 쿼리:

```

sum(increase(proto_udp_res_msg_total{namespace=~"$namespace",
message_name="session_estigation_res", status="no_rsp_received_tx"}
[15m]))by(message_name, status, peer_info)

```

레이블: {{message\_name}} || {{status}} || {{peer\_info}}

Grafana는 어디서 장애가 발생하는지 보여 주어야 합니다. 이 예에서는 UPF419와 관련이 있습니다.

시스템에 연결할 때 많은 세션 관리자가 예상 'Actv Ready' 상태가 아니므로 RCM 전환 후 sessmgr이 제대로 설정되지 않았는지 확인할 수 있습니다.

```

[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

```

## 솔루션

이는 CDETS(Cisco Defect Tracking System) CSCvz9749와 관련이 있습니다. 이 수정은 21.22.ua4.82694 이상에서 통합되었습니다.

## 해결 방법



UPF419에서는 Actv Ready에 없는 세션 관리자 인스턴스를 숨겨진 명령 작업으로 작업 중지 기능 `sessmgr` 인스턴스 <>와 함께 다시 시작해야 합니다. 그러면 상황이 해결됩니다.

```
[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
```

## 전환을 일으키는 UPF 실패 시 수집할 로그

참고: 디버그 로그가 RCM에서 활성화되었는지 확인합니다(디버그 로그를 활성화하기 전에 승인 요청). 로깅 권장 사항을 참조하십시오.

### RCM 운영 센터 로깅 레벨

```
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
```

### 단계별 데이터 수집

1. 문제 요약: 문제 설명은 명확해야 합니다. 문제가 있는 **노드 이름/ip**를 표시하여 로그에서 필요한 정보를 쉽게 찾을 수 있도록 합니다. 예를 들어 전환 문제의 경우 IP x.x.x.x가 소스 UPF이고 x.x.x.y가 대상 UPF라고 언급하면 유용합니다.
2. 문제를 재현할 수 있는 여러 가지 방법이 있는 경우 해당 문제를 언급하십시오.
3. RCM 버전 정보: RCM VM에서 RCM VM을 구축하는 경우, 운영 센터에서 `Cat/etc/smi/rcm-image-version`을 Helm으로 표시합니다. RCM CN 구축의 경우 운영 센터에서 키를 보여줍니다.

4. RCM Tac 디버그 CN 또는 RCM 로그는 문제가 발생한 시점에 기록됩니다. 경우에 따라 POD가 방금 작동된 처음부터 로그를 요구할 수도 있습니다.
5. 기본 또는 백업인 RCM을 나타냅니다. CN의 경우 두 RCM 쌍에 대한 정보를 공유합니다.
6. 모든 인스턴스에서 RCM 운영 센터에서 실행 중인 컨피그레이션을 공유합니다.
7. RCM SNMP 트랩을 수집합니다.
8. 전환 실패와 상관없이, 하나의 활성 UP SSD와 하나의 대기 UP SSD를 수집하는 것이 좋습니다.
9. RCM 컨트롤러, configmgr, checkpoint manager, switchover 및 switchover-verbose statistics 명령은 정확한 CLI를 언급하는 데 사용됩니다.  
**rcm show statistics 컨트롤러**  
**rcm show statistics configmgr**  
**rcm show statistics checkpoint mgr**  
**rcm show statistics 전환**  
**rcm show statistics switchover-verbose**
10. UPF 또는 RCM의 Syslog.
11. 이 문제가 전환 실패와 관련된 경우 새로운 활성 UPF SSD 및 기존 UPF 활성 SSD가 필요합니다. 경우에 따라 전환 때문에 이전 작업이 재부팅됩니다. 이 경우 문제를 재현해야 하며, 그 바로 전에 이전 활성 UP SSD를 수집해야 합니다.
12. 전환 실패 사례에서는 문제가 다시 발생할 때 이전 및 새 활동에서 vpn, sessmgr, sess-gr 및 sxdemux 디버그 로그를 수집하는 것도 유용합니다.  
**로깅 필터 활성화 기능 sxdemux 레벨 디버그**  
**로깅 필터 활성화 기능 sessmgr 수준 디버그**  
**로깅 필터 활성화 시설 sess-gr 레벨 디버그**  
**로깅 필터 활성화 협업공간 vpn 레벨 디버그**
13. sessmgr/vpnmgr에서 오류/문제가 발생할 경우 Vpnmgr/Sessmgr 코어가 필요합니다. sessmgr\_instance\_id는 문제가 발견된 인스턴스입니다. vpnmgr\_instance\_id는 RCM 컨텍스트의 컨텍스트 번호입니다.  
**작업 핵심 기능 sessmgr 인스턴스 <sessmgr\_instance\_id>**  
**작업 핵심 기능 vpnmgr 인스턴스 <vpnmgr\_instance\_id>**
14. RCM HA 문제의 경우 두 인스턴스 모두에서 RCM TAC 디버그/포드 로그를 공유합니다.

## 관련 정보

- <https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html>
- [기술 지원 및 문서 - Cisco Systems](#)