Fehlerbehebung beim Switchover auf dem RCM Converged Core

Inhalt

Einleitung

Dieses Dokument beschreibt die grundlegenden Schritte zur Fehlerbehebung im Redundanz Configuration Manager (RCM) bei einem Netzwerkfehler.

Hintergrundinformationen

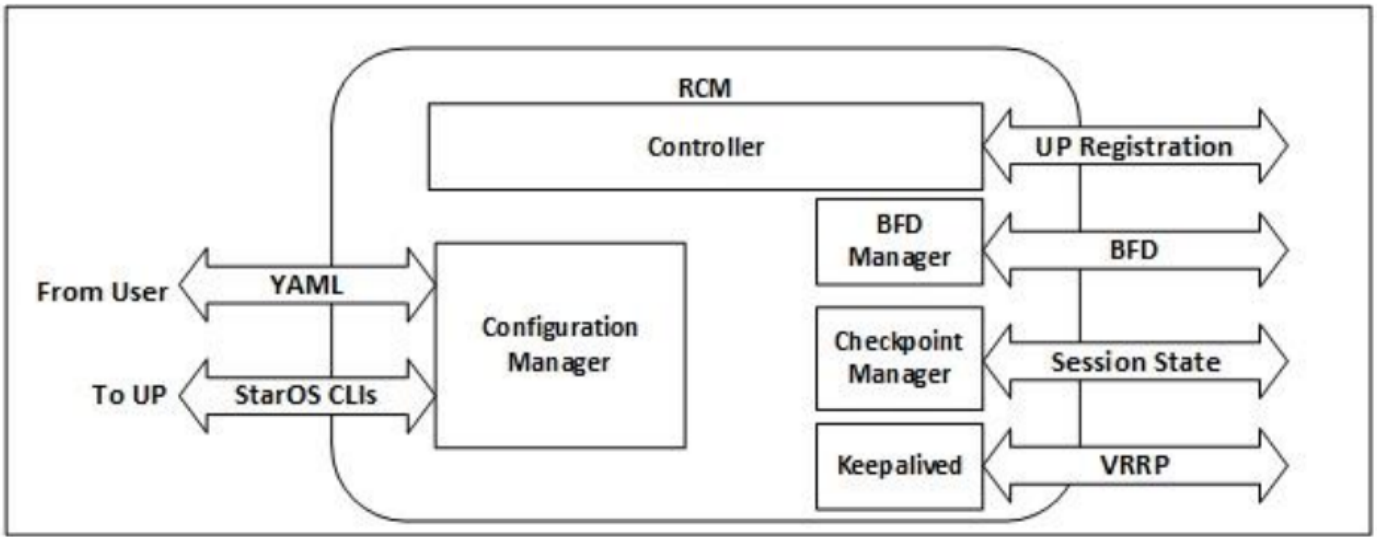
Was ist RCM?

Der RCM ist ein Cisco proprietärer Knoten oder eine Netzwerkfunktion (NF), die Redundanz für StarOS-basierte User Plane Functions (UPF) bietet.

Der RCM bietet eine N:M-Redundanz für UPF, wobei N eine Anzahl aktiver UPFs ist und weniger als 10 ist und M eine Anzahl von Standby-UPs in der Redundanzgruppe.

Komponenten des RCM

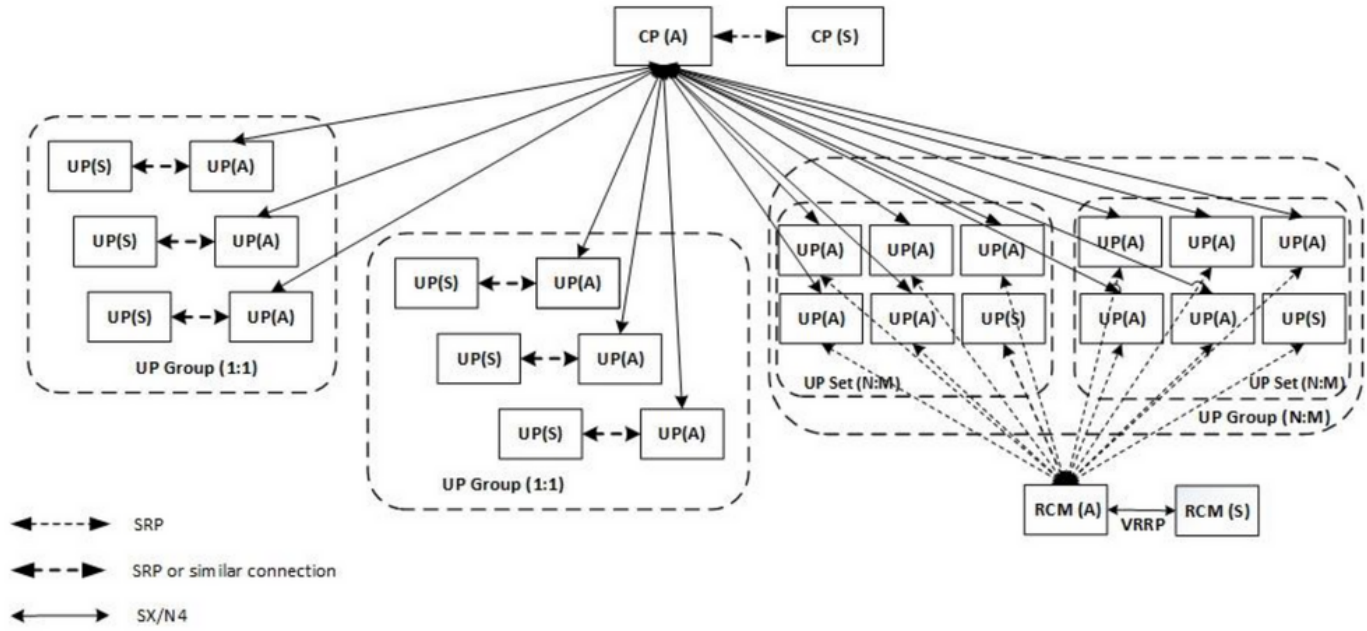
Der RCM umfasst Komponenten, die als PODs im RCM VM ausgeführt werden:



- Controller: Es kommuniziert ereignisspezifische Entscheidungen mit allen anderen PODs im RCM
- BFD-Manager (BFDMgr): Er identifiziert mithilfe des BFD-Protokolls den Zustand der Datenebene.
- Configuration Manager (ConfigMgr): Die angeforderte Konfiguration wird auf die Benutzerebenen (User Plates, UPs) geladen.
- Redundanz Manager (RedMgr): Er wird auch Checkpoint Manager genannt. Es speichert und sendet Kontrollpunktdaten an einen Standby-UPF.

- Keepalives: Es kommuniziert zwischen dem aktiven und dem Standby-RCM über VRRP.

Typisches RCM-Bereitstellungsmodell



RCM CLI - Übersicht

In diesem Beispiel gibt es vier RCM OPS-Zentren. Um zu bestätigen, welche RCM Kuberrot zu welcher RCM OPS Center- und RCM Common Execution Environment (CEE) gehören, können Sie sich beim RCM Kubernetes anmelden und die Namespaces auflisten:

```
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-Management-IP-Adresse

Diese IP-Adresse ist spezifisch und an VM oder UPF gebunden. Es wird bei der Erstkommunikation zwischen UPF und RCM verwendet, bei der UPF bei RCM und RCM registriert wird und außerdem die UPF konfiguriert und Rollen zuweist. Sie können diese IP verwenden, um UPF von RCM CLI-Ausgaben zu identifizieren.

UPF-Geräterolle - IP

Mit einer Rolle verknüpft (aktiv/Standby):

Diese IP-Adresse wird bei einem Switchover verschoben.

Nützliche CLI-Befehle für die RCM-Fehlerbehebung

Sie können prüfen, welche RCM-Gruppe der UPF ist, vom RCM OPS Center. Hier finden Sie ein Beispiel für die 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)
```

Anmerkung: Die Host-ID entspricht nicht dem UPF-Hostnamen.

Hier sehen Sie den Status auf 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"
      }
    ]
  },
```

Aktuelle Standby-UPF vom RCM OPS Center identifizieren

Das Center identifiziert im RCM OPS das UPF im Standby-Modus mithilfe des Befehls **show-statistics (RCM-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"
      },
```

Melden Sie sich bei UPF an, und überprüfen Sie die RCM-Informationen:

```
[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)
```

Hier sind weitere nützliche Informationen aus dem RCM OPS Center:

```
[up300-aio-2/rm34] rcm# rcm show-statistics
Possible completions:
```

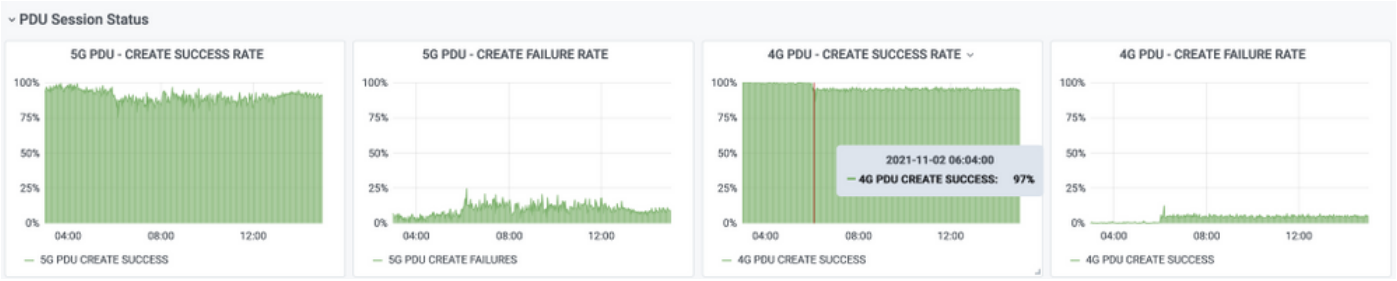
```
bfdmgr          Show RCM BFDMgr Statistics information
checkpointmgr   Show RCM Checkpointmgr Statistics information
configmgr       Show RCM Configmgr Statistics information
controller      Show RCM Controller Statistics information
|               Output modifiers
<cr>
```

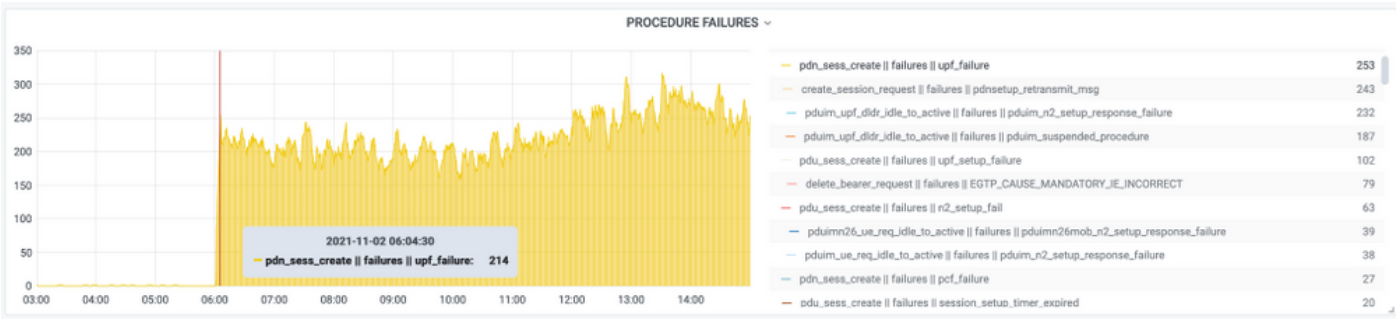
Laden Sie das RCM Handbuch für Version 21.24 herunter.

Probleme gemeldet durch RCM-Fehler auf CNDP PODs

Das Problem wurde bei einem der UPFs für die Warnung UP_SX_SESS_ESTABLISHMENT_SR gemeldet. Diese Warnung besagt, dass die Erfolgsrate der Sitzungseinrichtung für die SX-Schnittstelle unter den konfigurierten Grenzwert gefallen ist.

Wenn Sie sich die Statistiken von Grafana ansehen, wird ein 5G/4G-Abfall beobachtet, weil die Verbindung getrennt wurde, **pdn_sess_create | | Fehler | upf_failure**:





Damit wird bestätigt, dass **pdn_sess_create | | Fehler | upf_failure** wurde durch UPF419 verursacht:

```
[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)
```

Auf SMF können Sie die UPF-Konfiguration überprüfen. In diesem Fall müssen Sie nach der UPF

N4-IP-Adresse suchen:

```
[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
```

Anschließend können Sie mithilfe der Grafana-Abfrage ermitteln, welche UPF N4-Adresse die meisten Fehler aufweist:

Grafana-Abfrage:
sum(increase(proto_udp_res_msg_total{namespace=~"$namespace", message_name="session_einrichtung_res", status="no_rsp_received_tx"} [15 m])) von (message_name, status, peer_info)

Beschriftung: {{message_name}} || {{status}} || {{peer_info}}

Grafana muss zeigen, wo Versäumnisse auftreten. Im Beispiel bezieht sich dies auf UPF419.

Wenn Sie eine Verbindung zum System herstellen, können Sie bestätigen, dass die Sessmgr nach dem RCM-Switchover nicht richtig eingestellt wurde, da sich viele der Sitzungsmanager nicht im erwarteten "aktiven Bereit"-Zustand befinden.

```
[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
```

Lösung

Dies bezieht sich auf das Cisco Defect Tracking System (CDETS) CSCvz9749. Die Behebung wurde in 21.22.ua4.82694 und höher integriert.

Problemumgehung

Unter UPF419 müssen Sie die Instanzen des Sitzungsmanagers neu starten, die sich nicht in **Actv Ready** mit der **Sessmgr-Instanz für** versteckte Befehlsbefehle **<>** befanden, und dies löst die Situation.

```
[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
```

Protokolle, die bei UPF-Ausfällen gesammelt werden müssen, die einen Switchover verursachen

> **Anmerkung:** Stellen Sie sicher, dass Debug-Protokolle im RCM aktiviert sind (fordern Sie eine Genehmigung an, bevor Sie ein Debug-Protokoll aktivieren). Weitere Informationen finden Sie in den Protokollempfehlungen.

Protokollierungsebene für den RCM-Betrieb im Zentrum

```
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
```

Schrittweise Datensammlung

1. Zusammenfassung des Problems: Die Problemaussage muss klar sein. Geben Sie den problematischen **Node-Namen/die IP-Adresse an**, damit die erforderlichen Informationen aus den Protokollen leichter gefunden werden können. Bei einem Switchover-Problem ist es beispielsweise hilfreich, wenn erwähnt wird, dass IP x.x.x.x die Quelle für UPF ist und x.x.x.y die Ziel-UPF.
2. Wenn es mehrere Möglichkeiten gibt, das Problem zu reproduzieren, nennen Sie diese.
3. Informationen zur RCM-Version: Im Fall einer RCM VM-Bereitstellung vom RCM VM, cat **/etc/smi/rcm-image-version-show hubm** vom Ops-Center. Bei RCM **wird** die CN-Bereitstellung vom Operations Center aus **angezeigt**.
4. Der RCM kann zum Zeitpunkt des Auftretens des Problems CN- oder RCM-Debug-Protokolle verwenden. In einigen Fällen können Sie auch Protokolle von Beginn an benötigen, wenn der POD gerade gestartet wurde.
5. Gibt an, welcher RCM primär oder Backup ist. Bei CN: Geben Sie die Informationen für beide RCM-Paare frei.
6. Geben Sie die aktuelle Konfiguration von allen Instanzen aus dem RCM Operations Center frei.
7. Erfassen Sie die SNMP-Traps des RCM.
8. Unabhängig davon, ob ein Switchover ausfällt oder nicht, ist es besser, einen aktiven UP-SSD und einen Standby-UP-SSD zu sammeln.
9. Die genaue CLI wird mit den Befehlen RCM Controller, Configuration Manager, Checkpoint Manager, Switchover und Switchover-Ausführse Statistics angezeigt.
   RCM Anzeigestatistikcontroller
   rcm show-statistics config mgr
   rcm-Kontrollpunkt für die Anzeigestatistik
   RCM-Switchover mit Anzeigestatistik
   rcm show-statistics switchover-verbose
10. Syslogs von UPF oder RCM.
11. Wenn das Problem mit Switchover-Fehlern zusammenhängt, sind ein neues aktives UPF-SSD und ein altes UPF-aktives SSD erforderlich. In einigen Fällen werden alte Aktivisten durch Switchover neu gestartet. In diesem Fall müssen Sie das Problem reproduzieren, und zwar unmittelbar bevor Sie die alte aktive UP-SSD sammeln müssen.
12. Bei einem Switchover-Fehler ist es außerdem hilfreich, die Debug-Protokolle vpn, sessmgr, sess-gr und sxdemux von alten und neuen Aktivierungen bei der Problemwiedergabe zu erfassen.
    Protokollierungsfilter aktiv Einrichtung sxdemux-Ebene Debugging
    Protokollierungsfilter - Debugging auf Ebene der aktiven Einrichtung
    Protokollierungsfilter Active Facility Sess-gr-Level Debugging
    Protokollierungsfilter - Debugging auf VPN-Ebene
13. Vpnmgr/Sessmgr-Kerne werden im Fehlerfall/Problem in sessmgr/vpnmgr benötigt. Die sessmgr_instance_id ist die Instanz, in der das Problem festgestellt wird.
    vpnmgr_instance_id ist die Kontextnummer des RCM-Kontexts.
    CSCM-Instanz <sessmgr_instance_id>
    vpnmgr instance <vpnmgr_instance_id>

14. Bei HA-Problemen des RCM können Sie die RCM TAC-Debug-/POD-Protokolle von beiden Instanzen freigeben.

Zugehörige Informationen

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- Technischer Support und Dokumentation für Cisco Systeme