Dépannage du problème de commutation sur le coeur convergent RCM

Contenu

Introduction

Ce document décrit les étapes de base du dépannage sur Redundancy Configuration Manager (RCM) en cas d'événement de panne réseau.

Informations générales

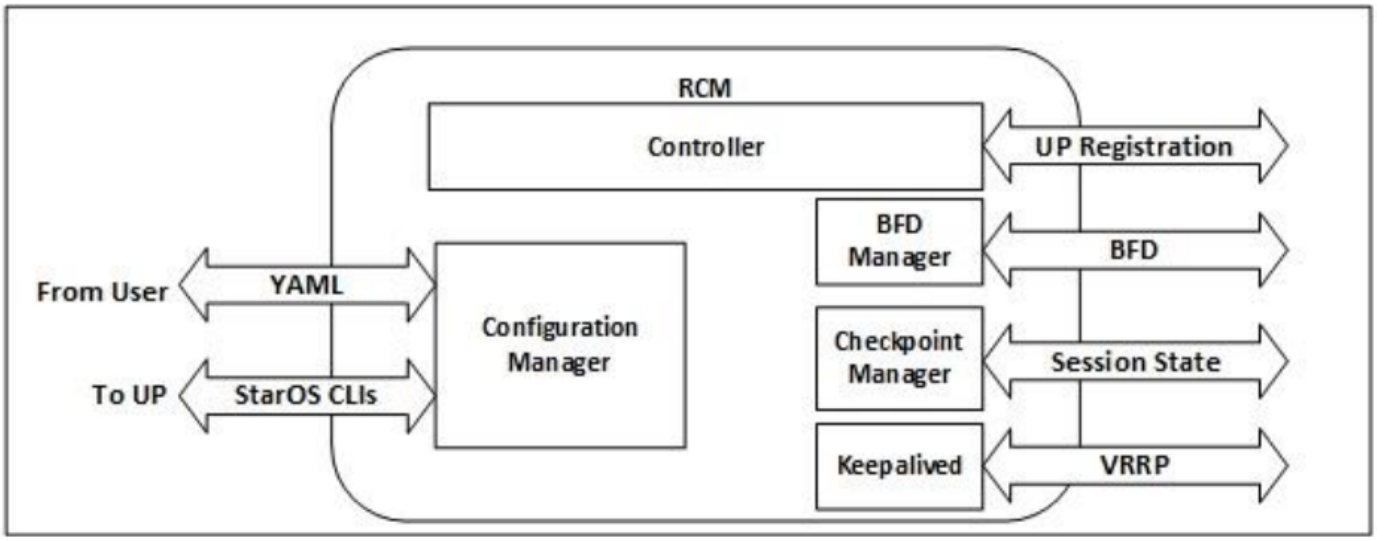
Qu'est-ce que RCM ?

Le RCM est un noeud propriétaire Cisco ou une fonction réseau (NF) qui fournit une redondance pour les fonctions de plan utilisateur basées sur StarOS (UPF).

Le RCM fournit la redondance N : M de l'UPF où N est un nombre d'UPF actifs et est inférieur à 10, et M un nombre d'UP de secours dans le groupe de redondance.

Composants de RCM

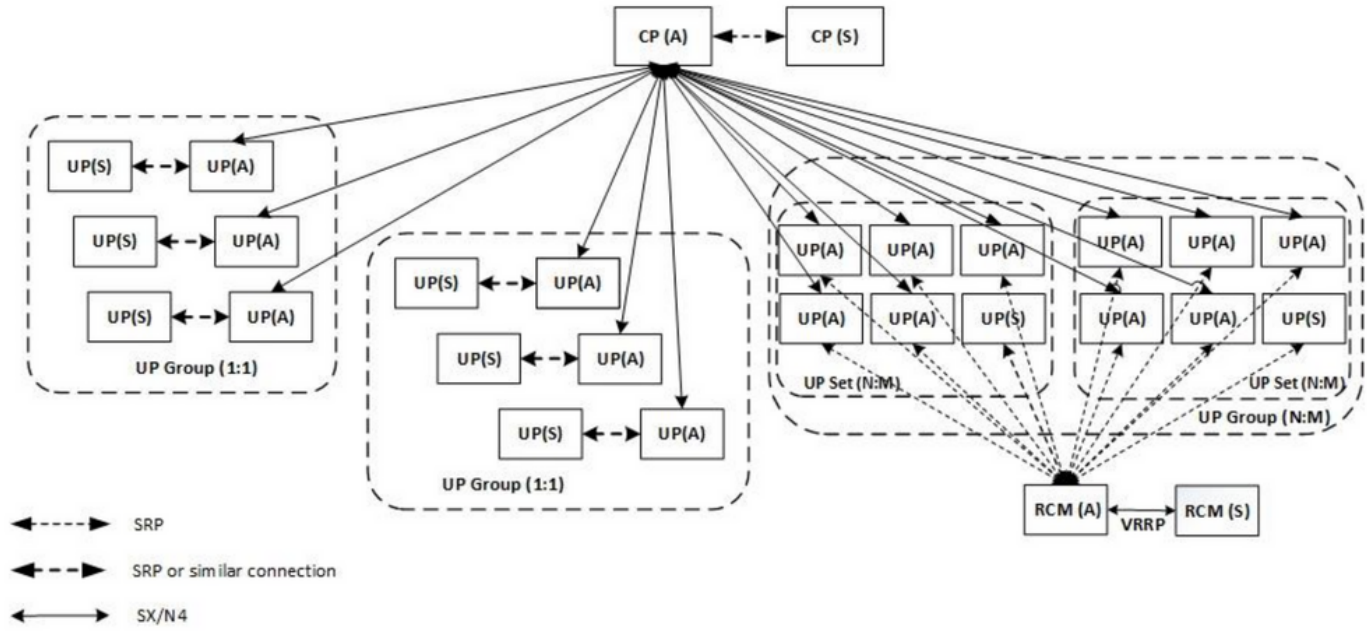
Le RCM comprend des composants qui s'exécutent en tant que pods dans la machine virtuelle du RCM :



- Contrôleur : Il communique les décisions spécifiques à un événement avec tous les autres modules du RCM.
- Gestionnaire BFD (BFDMgr) : Il utilise le protocole BFD pour identifier l'état du plan de données
- Gestionnaire de configuration (ConfigMgr) : Il charge la configuration demandée sur les plans utilisateur (UP)
- Gestionnaire de redondance (RedMgr) : Il est également appelé Checkpoint Manager. Il stocke et envoie les données du point de contrôle à un UPF de secours.

- Conservé : Il communique entre le RCM actif et le RCM de secours avec l'utilisation du VRRP

Modèle de déploiement RCM type



Présentation de l'interface CLI RCM

Dans cet exemple, il existe quatre centres d'OPS RCM. Afin de confirmer quels Kubernetes RCM correspondent à quel Centre OPS RCM et Environnement d'exécution commun RCM (CEE) vous pouvez vous connecter aux Kubernetes RCM et répertorier les espaces de noms :

```
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
```

Adresse IP de gestion UPF

Cette adresse IP est spécifique et liée à la machine virtuelle ou au protocole UPF. Il est utilisé dans la communication initiale entre UPF et RCM, où UPF s'enregistre avec RCM et RCM configure UPF et attribue également un rôle. Vous pouvez utiliser cette adresse IP pour identifier UPF à partir des sorties CLI de RCM.

IP de rôle de périphérique UPF

Lié à un rôle (actif/en veille) :

Cette adresse IP se déplace au fur et à mesure de la commutation.

Commandes CLI utiles pour le dépannage de RCM

Vous pouvez vérifier quel groupe RCM est l'UPF à partir de RCM OPS Center. Trouvez un exemple à partir de la plate-forme de déploiement natif cloud (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: L'ID d'hôte n'est pas le même que le nom d'hôte UPF.

Ici, vous pouvez voir l'état sur 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"
      }
    ]
  },
```

Identifier l'UPF de secours actuel à partir du centre d'opération RCM

Àpartir de RCM OPS, le centre identifie l'UPF en veille à l'aide de la commande **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"
      },
```

Connectez-vous à UPF et vérifiez les informations 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)
```

Voici les autres informations utiles du Centre OPS de RCM :

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

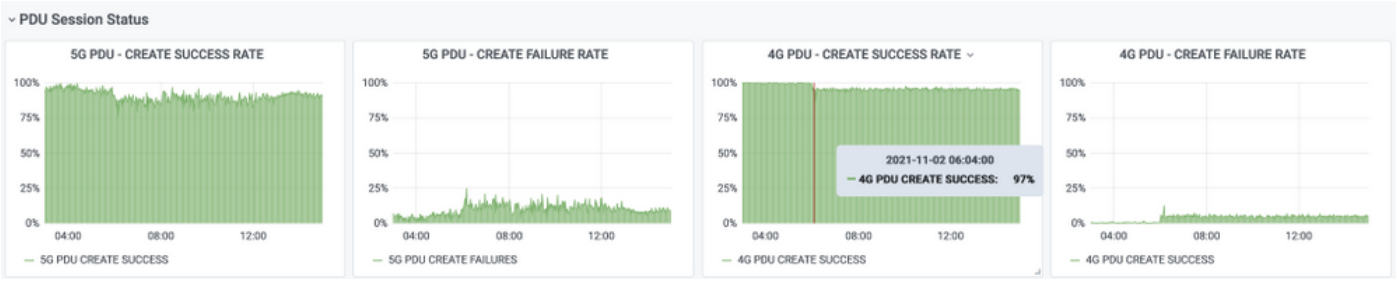
```
bfdmgr          Show RCM BFDMgr Statistics information
checkpointmgr   Show RCM Checkpointmgr Statistics information
configmgr       Show RCM Configmgr Statistics information
controller      Show RCM Controller Statistics information
|               Output modifiers
<cr>
```

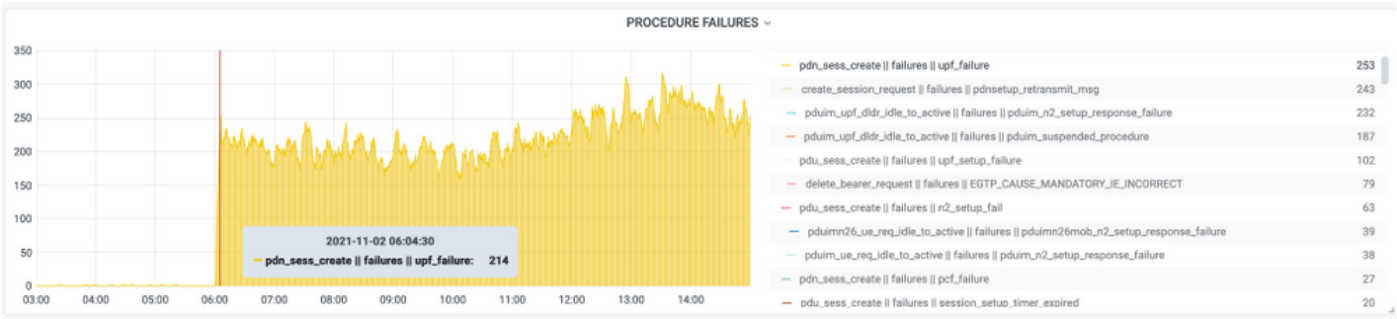
Téléchargez le guide du RCM pour la version 21.24.

Problème signalé par des défaillances RCM sur des POD CNDP

Le problème a été signalé sur l'un des UPF lié à l'alerte UP_SX_SESS_ESTABLISHMENT_SR. Cette alerte indique que le taux de réussite de l'établissement de session sur l'interface SX a baissé sous le seuil configuré.

Si vous regardez les statistiques Grafana, une dégradation 5G/4G est observée en raison de la raison de déconnexion **pdn_sess_create | Échecs| | upf_fail** :





Ceci confirme que le **pdn_sess_create | Échecs| | upf_fail** a été causé par 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)
```

Sur SMF, vous pouvez vérifier la configuration UPF. Dans ce cas, vous devez rechercher l'adresse IP N4 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
```

Ensuite, vous pouvez exécuter la requête Grafana pour identifier l'adresse UPF N4 qui présente le plus d'échecs :

Requête Grafana :
sum(expand(proto_udp_res_msg_total{namespace=~"$namespace », message_name=« session_establishment_res », status=« no_rsp_ived_tx »} [15m])) par (nom_message, état, peer_info)

Étiquette : {{nom_message}} || {{status}} || {{peer_info}}

Grafana doit montrer où les échecs se produisent. Dans l'exemple, il est lié à UPF419.

Lorsque vous vous connectez au système, vous pouvez confirmer que le sessmgr n'a pas été correctement défini après la commutation RCM, car de nombreux gestionnaires de session ne sont pas dans l'état 'Actv Ready' attendu.

```
[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
```

Solution

Ceci est lié à Cisco Defect Tracking System (CDETS) CSCvz9749. Le correctif a été intégré dans 21.22.ua4.82694 et versions ultérieures.

Solution de contournement

Sur UPF419, vous devez redémarrer les instances du gestionnaire de session qui n'étaient pas dans **Actv Ready** avec **instance sessmgr** masquée de l'**utilitaire de suppression de tâche de** commande **<>** et cela résout la 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
```

Journaux à collecter en cas de défaillance d'UPF qui provoque un basculement

> **Note**: Assurez-vous que les journaux de débogage sont activés dans RCM (demandez l'approbation avant d'activer un journal de débogage). Reportez-vous aux recommandations de journalisation.

Niveau de journalisation des centres d'opération 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
```

Collecte de données étape par étape

1. Résumé de la question : L'énoncé du problème doit être clair. Indiquez le **nom/adresse IP** du **noeud** problématique afin qu'il soit plus facile de trouver les informations nécessaires à partir des journaux. Par exemple, en cas de problème de commutation, il est utile de mentionner qu'IP x.x.x.x est l'UPF source et x.x.x.y est l'UPF de destination.
2. S'il existe plusieurs façons de reproduire le problème, mentionnez-les.
3. Informations de version RCM : Dans le cas d'un déploiement de MV RCM à partir de MV RCM, chat **/etc/smi/rcm-image-version show helm** à partir du centre d'opération. Dans le cas du déploiement du RCM CN, **montrer** la **barre** depuis le centre des opérations.
4. RCM Tac débogue les journaux CN ou RCM au moment de l'occurrence du problème. Dans certains cas, vous pouvez également demander des journaux dès le début lorsque le POD vient d'être lancé.
5. Indiquez quel RCM est principal ou de secours. Dans le cas du CN, partagez l'information pour les deux paires RCM.
6. Partagez la configuration en cours à partir de RCM ops-center à partir de toutes les instances.
7. Collectez les interruptions SNMP du RCM.
8. Quelle que soit la panne de commutation, il est préférable de collecter un SSD UP actif et un SSD UP de secours.
9. Les commandes RCM controller, configmgr, checkpoint manager, switchover et switchover-verbose statistics sont utilisées pour mentionner l'interface de ligne de commande exacte.
   rcm show-statistics controller
   rcm show-statistics configmgr
   rcm show-statistics checkpointmgr
   rcm show-statistics switchover
   rcm show-statistics switchover-verbose
10. Syslogs de UPF ou RCM.
11. Si le problème est lié à une panne de commutation, un nouveau SSD UPF actif et un ancien SSD actif UPF sont requis. Dans certains cas, les actifs anciens redémarrent en raison de la commutation. Dans ce cas, vous devez reproduire le problème, et juste avant cela vous devez collecter l'ancien SSD UP actif.
12. Dans un cas d'échec de commutation, il est également utile de collecter les journaux de débogage vpn, sessmgr, sess-gr et sxdemux des anciens et des nouveaux actifs lors de la reproduction du problème.
    logging filter active installation sxdemux level debug
    logging filter active installation sessmgr level debug
    logging filter active, installation sess-gr level debug
    logging filter active Facility vpn level debug
13. Les coeurs Vpnmgr/Sessmgr sont nécessaires en cas d'erreur/problème dans sessmgr/vpnmgr. Sessmgr_instance_id est l'instance où le problème est détecté.
    vpnmgr_instance_id est le numéro de contexte du contexte RCM.
    tâche principale installation instance sessmgr <id_instance_sessmgr>
    tâche principale installation instance vpnmgr <vpnmgr_instance_id>
14. En cas de problème de HA RCM, partagez les journaux de débogage/pod du centre d'assistance technique RCM des deux instances.

Informations connexes

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- Support et documentation techniques - Cisco Systems