

RCMコンバージドコアでのスイッチオーバー問題のトラブルシューティング

内容

[概要](#)

[背景説明](#)

[RCMとは何ですか。](#)

[RCMのコンポーネント](#)

[一般的なRCM導入モデル](#)

[RCM CLIの概要](#)

[UPF管理IPアドレス](#)

[UPFデバイスロールIP](#)

[RCMのトラブルシューティングに役立つCLIコマンド](#)

[RCM OPSセンターからの現在のスタンバイUPFの特定](#)

[CNDP PODのRCM障害によって報告される問題](#)

[解決方法](#)

[回避策](#)

[スイッチオーバーを引き起こすUPF障害時に収集するログ](#)

[RCMオペレーションセンターのログレベル](#)

[ステップバイステップデータ収集](#)

[関連情報](#)

概要

このドキュメントでは、ネットワーク障害イベントの場合にRedundancy Configuration Manager(RCM)でトラブルシューティングを行うための基本的な手順について説明します。

背景説明

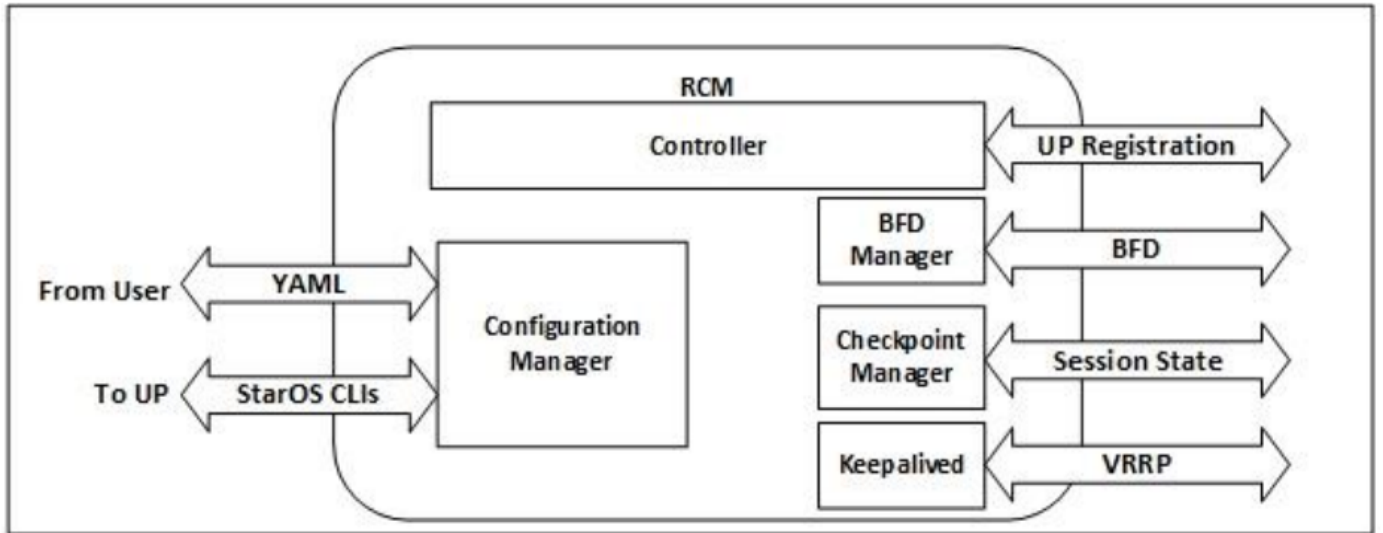
RCMとは何ですか。

RCMは、StarOSベースのユーザプレーン機能(UPF)に冗長性を提供するシスコ独自のノードまたはネットワーク機能(NF)です。

RCMは、UPFのN:Mの冗長性を提供します。NはアクティブUPFの数で10未満、Mは冗長性グループ内のスタンバイUPFの数です。

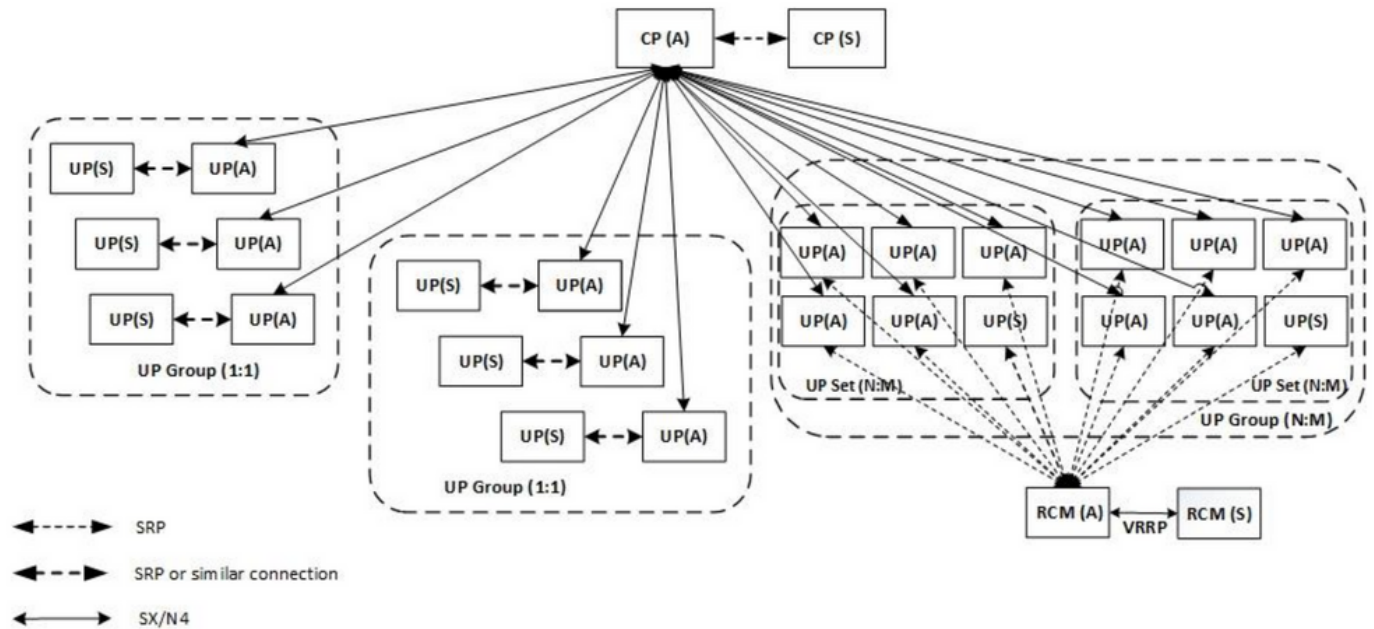
RCMのコンポーネント

RCMは、RCM VMでポッドとして動作するコンポーネントで構成されます。



- コントローラ：イベント固有の決定をRCM内の他のすべてのポッドと通信する
- BFDマネージャ(BFDMgr):BFDプロトコルを使用してデータプレーンの状態を特定する
- 構成マネージャー(ConfigMgr):要求された設定をユーザプレーン(UP)にロードする
- 冗長マネージャ(RedMgr):チェックポイントマネージャとも呼ばれます。チェックポイントデータを保存し、スタンバイUPFに送信する
- キープアライブ：VRRPを使用して、アクティブRCMとスタンバイRCMの間で通信を行います

一般的なRCM導入モデル



RCM CLIの概要

この例では、4つのRCM OPSセンターがあります。どのRCM KubernetesがどのRCM OPS CenterおよびRCM Common Execution Environment(CEE)に対応しているかを確認するには、RCM Kubernetesにログインし、名前空間をリストします。

```
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アドレス

このIPは固有であり、VMまたはUPFに関連付けられています。UPFとRCM間の初期通信に使用され、UPFがRCMに登録され、RCMがUPFを設定し、ルールも割り当てます。このIPを使用して、RCMのCLI出力からUPFを識別できます。

UPFデバイスロールIP

ルールにリンク (アクティブ/スタンバイ) :

このIPアドレスは、スイッチオーバーが発生すると移動します。

RCMのトラブルシューティングに役立つCLIコマンド

RCMオペレーションセンターから、どのRCMグループがUPFであるかを確認できます。Cloud Native Deployment Platform(CNDP)のサンプルを参照してください。

```
[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：ホストIDがUPFホスト名と同じではありません。

ここでは、RCM OPS Centerのステータスを確認できます。

```
[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センターからの現在のスタンバイUPFの特定

RCM OPSから、`rcm show-statistics controller`コマンドを使用して、スタンバイ状態のUPFを特定します。

```

{
  "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"
},

```

UPFにログインし、RCM情報を確認します。

```

[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)

```

RCM OPS Centerのその他の有用な情報を次に示します。

```

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

```

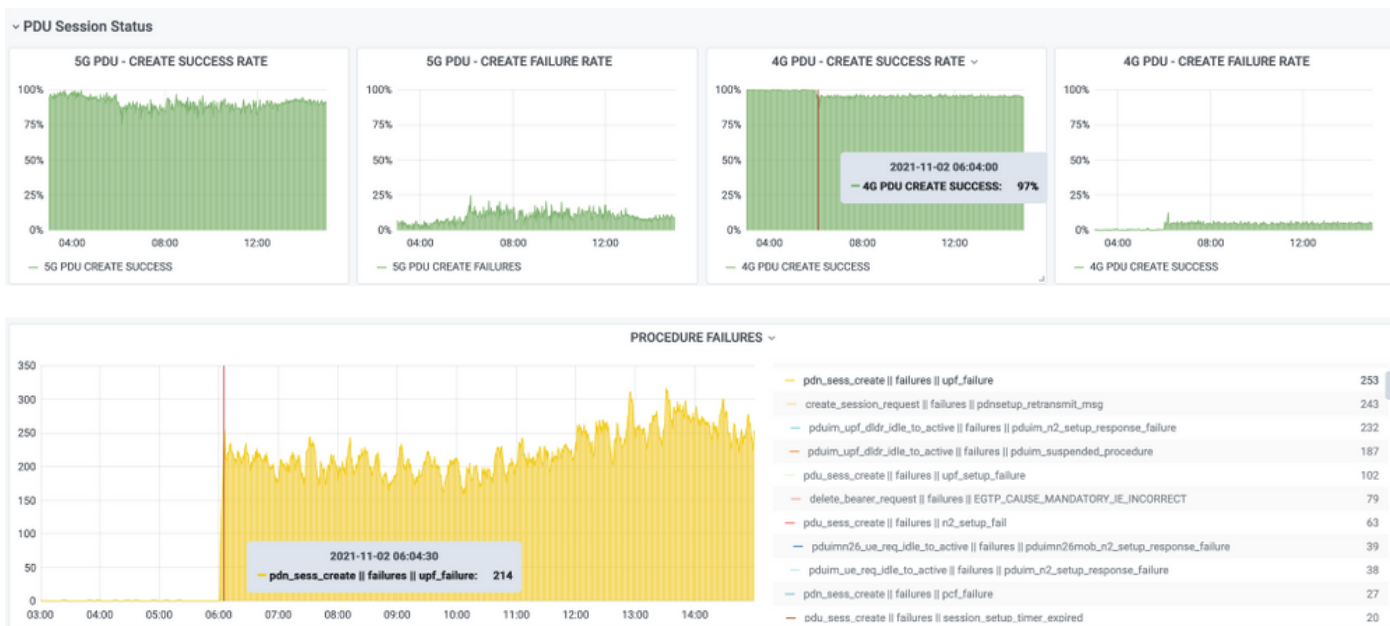
```
configmgr      Show RCM Configmgr Statistics information
controller     Show RCM Controller Statistics information
|             Output modifiers
<cr>
```

リリース21.24の[RCMガイド](#)をダウンロードします。

CNDP PODのRCM障害によって報告される問題

アラートUP_SX_SESS_ESTABLISHMENT_SRに関連するUPFの1つで問題が報告されました。このアラートは、SXインターフェイスのセッション確立成功率が、設定されたしきい値を下回ったことを示します。

Grafanaの統計情報を見ると、切断理由pdn_sess_createにより5G/4Gの劣化が観察されます **エラー || upf_failure:**



これにより、pdn_sess_create **エラー || upf_failure**はUPF419が原因です：

```
[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)
```

SMFでは、UPF設定をチェックできます。この場合、UPF N4 IPアドレスを探す必要があります。

```
[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
```

次に、Grafanaクエリを実行して、最も障害の多いUPF N4アドレスを特定できます。

Grafanaクエリ：

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

ラベル:{{message_name}} || {{status}} || {{peer_info}}

Grafanaは、障害が発生した場所を示す必要があります。この例では、UPF419に関連しています。

システムに接続する際に、セッションマネージャの多くが期待される「Actv Ready」状態にないため、RCMスイッチオーバー後にsessmgrが正しく設定されていないことを確認できます。

```
[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
```

解決方法

これは、Cisco不具合トラッキングシステム(CDETS)[CSCvz9749](#)に関連しています。この修正は21.22.ua4.82694以降に統合されています。

回避策

UPF419で、隠しコマンドtask kill facility sessmgr instance <>を使用してActv Ready状態ではなかったセッションマネージャインスタンスを再起動する必要があります。これにより、この状況が解決します。

```
[local]UPF419# show srp checkpoint statistics verbose
```

```
Wednesday November 03 16:44:57 UTC 2021
```

smgr inst	state	peer conn	recovery records	pre-alloc calls	chk-point full	rcvd micro	chk-point full	sent 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

スイッチオーバーを引き起こすUPF障害時に収集するログ

注：RCMでデバッグ・ログが使用可能であることを確認します（デバッグ・ログを使用可能にする前に承認を要求します）。ロギングの推奨事項を参照してください。

RCMオペレーションセンターのログレベル

```
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
```

ステップバイステップデータ収集

1. 問題の概要：問題の説明は明確でなければなりません。問題のあるノード名/ipを示すと、ログから必要な情報を見つけやすくなります。たとえば、スイッチオーバーの問題の場合、IP x.x.x.xが送信元UPFで、x.x.x.yが宛先UPFであると言及すると役立ちます。

2. 問題を再現する方法が複数ある場合は、それらを挙げてください。
3. RCMバージョン情報：RCM VMからRCM VMを導入する場合は、オペレーションセンターから `cat /etc/smi/rcm-image-versionshow helm` を入手します。RCMの場合は、オペレーションセンターから `show helm` を実行します。
4. 問題の発生時のRCM TacデバッグCNまたはRCMログ。場合によっては、PODが起動した直後からログを要求することもできます。
5. どのRCMがプライマリまたはバックアップであることを示します。CNの場合は、両方のRCMペアの情報を共有します。
6. すべてのインスタンスからRCM ops-centerの実行コンフィギュレーションを共有します。
7. RCM SNMPトラップを収集します。
8. スイッチオーバーの障害に関係なく、アクティブUP SSDとスタンバイUP SSDを1つずつ収集することをお勧めします。
9. 正確なCLIについて言及するには、RCM controller、configmgr、checkpoint manager、switchover、およびswitchover-verbose statisticsコマンドを使用します。
`rcm show-statistics controller`
`rcm show-statistics configmgr`
`rcm show-statistics checkpointmgr`
`rcm show-statistics switchover`
`rcm show-statistics switchover-verbose`
10. UPFまたはRCMのsyslog。
11. スイッチオーバー障害に関連する問題の場合は、新しいアクティブUPF SSDと古いUPFアクティブSSDが必要です。場合によっては、スイッチオーバーが原因で古いアクティブがリブートします。その場合は、問題を再現する必要があります。その直前に、古いアクティブなUP SSDを収集する必要があります。
12. スイッチオーバー障害の場合は、問題の再現時に、vpn、sessmgr、sess-gr、およびsxdemuxのデバッグログを新旧のアクティブから収集することも役立ちます。
`logging filter active facility sxdemux level debug`
`logging filter active facility sessmgr level debug`
`logging filter active facility sess-gr level debug`
`logging filter active facility vpn level debug`
13. Sessmgr/vpnmgrでエラー/問題が発生した場合は、Vpnmgr/Sessmgrコアが必要です。sessmgr_instance_idは、問題が発生したインスタンスです。vpnmgr_instance_idは、RCMコンテキストのコンテキスト番号です。
`タスクコア機能sessmgrインスタンス<sessmgr_instance_id>`
`タスクコアファシリティvpnmgrインスタンス<vpnmgr_instance_id>`
14. RCM HAの問題の場合は、両方のインスタンスからRCM TACのdebug/podログを共有します。

関連情報

- <https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html>
- [テクニカル サポートとドキュメント – Cisco Systems](#)