

Fehlerbehebung bei IP-Chunk-Verlusten in UPF nach einem RCM-ausgelösten Switchover

Inhalt

[Einleitung](#)

[Problem](#)

[Lösung](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung beim Upgrade der Benutzerebenenfunktion (User Plane Function, UPF) nach dem Switchover des Redundancy Configuration Manager (RCM) beschrieben.

Problem

Schritt 1: Im aktiven UPF (RCM-basiert) werden Instanzen fehlender Blöcke beobachtet:

```
<#root>
[local]UPF#
context n6

[n6]UPF#
show ipv6 chunks
```

Failure: This CLI is only for User-plane

 Hinweis: Überprüfen Sie stets, ob [DIMM-/ECC-/UEC-/ADDDC-Fehler](#) auf Quell- und Ziel-UCS-Servern vorliegen, die UPFs hosten, und führen Sie das RCM-TAC-Debugging/ durch.

Schritt 2: Überwachen Sie auf dem aktiven UPF, falls Chunks fehlen, SNMP-Trap-Ereignisse, um den Übergang des UPF-Status von Standby zu Aktiv zu ermöglichen.

```
<#root>
[n6]UPF#
show snmp trap history verbose | grep RCM
```

Tuesday November 14 21:16:45 UTC 2023

```
Mon Oct 13 08:24:42 2023 Internal trap notification 1426 (RCMChassisState) RCM Chassis State: (0) Chassis
Mon Oct 13 08:24:49 2023 Internal trap notification 1414 (RCMServiceStart) Context Name:rcm Service Name:rcm
Mon Oct 13 08:25:04 2023 Internal trap notification 1425 (RCMTCPConnect) Context Name: rcm
Mon Oct 13 08:25:04 2023 Internal trap notification 1421 (RCMConfigPushCompleteSent) Context Name: rcm
Mon Oct 13 08:25:04 2023 Internal trap notification 1426 (RCMChassisState) RCM Chassis State: (2) Chassis
Mon Oct 13 08:33:47 2023 Internal trap notification 1420 (RCMConfigPushCompleteReceived) Context Name:
Mon Oct 13 08:33:47 2023 Internal trap notification 1421 (RCMConfigPushCompleteSent) Context Name: rcm
Mon Oct 13 08:48:10 2023 Internal trap notification 1421 (RCMConfigPushCompleteSent) Context Name: rcm
Mon Oct 13 08:48:10 2023 Internal trap notification 1420 (RCMConfigPushCompleteReceived) Context Name:
Mon Oct 13 08:48:12 2023 Internal trap notification 1426 (RCMChassisState) RCM Chassis State: (1) Chassis
```

Schritt 3: Untersuchen Sie das Syslog auf fehlenden Blöcken im aktiven UPF auf Protokollereignisse, die das Beenden der übrigen (5) sx-demux-Dienste in der entsprechenden Redundanzgruppe (RG-1) anzeigen, während das Standby-UPF in den aktiven Zustand wechselt.

```
Oct 13 08:48:11 UPF evlogd: [local-60sec11.091] [sessctrl 8066 info] [1/0/9050 <sessctrl:0> ctrl_mgrs_c
Oct 13 08:48:11 UPF evlogd: [local-60sec11.483] [sessctrl 8066 info] [1/0/9050 <sessctrl:0> ctrl_mgrs_c
Oct 13 08:48:11 UPF evlogd: [local-60sec11.582] [sessctrl 8066 info] [1/0/9050 <sessctrl:0> ctrl_mgrs_c
Oct 13 08:48:11 UPF evlogd: [local-60sec11.726] [sessctrl 8066 info] [1/0/9050 <sessctrl:0> ctrl_mgrs_c
Oct 13 08:48:18 UPF evlogd: [local-60sec18.749] [sessctrl 8066 info] [1/0/9050 <sessctrl:0> ctrl_mgrs_c
```

Schritt 4: Aktivieren Sie auf dem aktiven UPF mit fehlenden Blöcken den Debug-Modus (cli test-commands password <Kennwort>), und führen Sie den Befehl aus, um Sx DeReg-Transaktionen zu überwachen, die mit dem aktiven UPF-Zeitraum übereinstimmen.

<#root>

[n6]UPF#

show ip pool vpn-sx-transactions

Context: n6

Sx transactions:

sent: 0, received: 0

Failed transactions: 0

Sx Deregistration transactions:

Peer Address

Deregistration Time

```
=====
192.168.1.55      Mon Oct 13 08:48:18 2023
192.168.1.49      Mon Oct 13 08:48:18 2023
192.168.1.49      Mon Oct 13 08:48:18 2023
192.168.2.55      Mon Oct 13 08:48:18 2023
192.168.2.55      Mon Oct 13 08:48:18 2023
192.168.2.49      Mon Oct 13 08:48:18 2023
192.168.2.49      Mon Oct 13 08:48:18 2023
```

[n6]UPF#

Schritt 5: Durchsuchen Sie auf dem aktiven UPF mit fehlenden Blöcken das Syslog nach Protokollen, die in der Nähe des Übergangs des UPF in den aktiven Zustand auftreten.

```
Oct 13 08:48:12 UPF evlogd: [local-60sec12.060] [vpn 5013 error] [1/0/9399 <vpnmgr:3> _cups_ip_pool.c:1
```

Beobachten Sie Protokollereignisse, die kontinuierlich von vpnmgr instance 3 task (vpnmgr:3) kommen.

```
<#root>
```

```
localsystem:$
```

```
less UPF-Destination-UPF-Syslog.log | grep "Pool_name is not present" | head -1
```

```
Oct 13 08:48:18 UPF evlogd: [local-60sec18.811] [vpn 5013 error] [1/0/9399 <vpnmgr:3> vpn_ip_pool.c:274
```

```
localsystem:$
```

```
localsystem:$
```

```
less UPF-Destination-UPF-Syslog.log | grep "Pool_name is not present" | tail -1
```

```
Oct 13 09:29:59 UPF evlogd: [local-60sec59.671] [vpn 5013 error] [1/0/9399 <vpnmgr:3> vpn_ip_pool.c:274
```

```
localsystem:$
```

Lösung

Weitere Informationen hierzu finden Sie im Fehlerbericht: Cisco Bug-ID [CSCwh97931](#)

Die Lösung für dieses Problem besteht in der Verbesserung von SxDemux, um die Bereinigung von IP-Chunks während des Übergangs zur SRP zu verhindern, während gleichzeitig die Protokolldebugfunktionen verbessert werden.

Wenn der erwähnte CDETS-Fix in dem von Ihnen verwendeten UPF-Build noch nicht verfügbar ist, können Sie diese Problemumgehung anwenden:

Ausführen der Standard-N4-Zuordnung Dis-Associate/Associate MOPP innerhalb des MW-Zeitrahmens.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.