Hardware-Wartung in 5G IMS- und Daten-UPF-Knoten

Inhalt

Einleitung

Dieses Dokument beschreibt das Verfahren zur Durchführung von Wartungsaktivitäten an den Knoten IP Multimedia Subsystem (IMS) und Daten User Plane Function (UPF).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 5G-UPF
- Redundanz Configuration Manager (RCM)
- Virtual Packet Core (VPC) - Single Instance (SI)
- Kernel-basierter Virtual Machine (KVM)-Hypervisor

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Subscriber Microservices Infrastructure SMI) 2020.02.2.35
- Star OS 21.22

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Was ist UPF?

Die User Plane Interface (UPF) ist eine der Netzwerkfunktionen (NFs) des 5G-Core-Netzwerks (5GC). Er ist für Paketrouting und -weiterleitung, Paketprüfung, Verarbeitung von QoS und externe PDU-Sitzungen zuständig, um Data Networks (DN) in der 5G-Architektur miteinander zu verbinden.

Was ist VPC-SI?

VPC-SI konsolidiert den Betrieb physischer Cisco ASR 5500-Chassis, die StarOS in einem einzigen virtuellen System (VM) ausführen, das auf kommerziellen Standardservern (COTS) ausgeführt werden kann. Jedes VPC-SI VM agiert als unabhängige StarOS-Instanz und umfasst die Funktionen für Management und Sitzungsprozess eines physischen Chassis.

Was ist KVM Hypervisor?

Kernel-basiertes Virtual Machine (KVM) ist eine in Linux integrierte Open-Source-Virtualisierungstechnologie. Mit KVM können Sie Linux in einen Hypervisor umwandeln, mit dem ein Host-Rechner mehrere, isolierte virtuelle Umgebungen, die als Gäste oder virtuelle Systeme (VMs) bezeichnet werden, ausführen kann.

Was ist ICSR?

Interchassis Session Recovery (ICSR) ist eine lizenzierte Cisco Funktion, die eine separate Lizenz erfordert. Diese Funktion bietet die höchstmögliche Verfügbarkeit für einen kontinuierlichen Anrufprozess ohne Unterbrechung der Teilnehmerdienste. Der ICSR ermöglicht es dem Betreiber, Gateways für Redundanzzwecke zu konfigurieren. Im Falle eines Gateway-Ausfalls ermöglicht ICSR das transparente Routing von Sitzungen um den Ausfall herum, wodurch die Benutzerfreundlichkeit erhalten bleibt. Der ICSR behält auch Sitzungsinformationen und den Status bei.

Problem

Für Hardware-Wartung wie Hardwarefehler oder Software-/Firmware-Upgrades und vieles mehr sind Ausfallzeiten auf den Servern erforderlich. Dieses Verfahren muss befolgt werden, damit Wartungsarbeiten an den UPF-Bare-Metal-Servern durchgeführt werden können und ein sanftes Umschalten der Services möglich ist, um unerwünschte Ausfallzeiten in der UPF-Anwendung zu vermeiden.

Instandhaltungsverfahren

UPF-Knoten sind StarOS-VMs, die im KVM-Hypervisor gehostet werden. Ein KVM-Hypervisor hostet 2 VM-Instanzen. IMS UPF verfügt über eine Redundanz von 1:1. Jede aktive Instanz verfügt über eine Standby-Instanz. Es verwendet ICSR zusammen mit Session Redundancy Protocol (SRP), um Redundanz zu gewährleisten. SRP wird zum Austausch von Hello-

Nachrichten zwischen ICSR-Chassis verwendet. Außerdem werden Sitzungsstatusinformationen zwischen dem aktiven/Standby-Chassis (Prüfpunktinformationen) ausgetauscht. Vollständige Informationen zur Teilnehmersitzung werden vom ACTIVE Chassis in Form eines Call Recovery Record (CRR) über die SRP-Verbindung an das STANDBY-Chassis gesendet.

Melden Sie sich beim KVM-Knoten an, und listen Sie die VM-Instanzen mit dem KVM **virsh-**Befehl auf.

```
cloud-user@podname-upf-ims-kvmnode-1:~$ sudo virsh list --all
Id Name State
----------------------------------------------------
1 imsupf01 running
4 imsupf10 running

cloud-user@podname-upf-ims-kvmnode-1:~$
```

Melden Sie sich bei der UPF-Instanz an, und überprüfen Sie den Chassis-Status.

```
[local]imsupf10# show srp info
Friday July 22 15:50:24 UTC 2022
Service Redundancy Protocol:
------------------------------------------------------------------------------
Context: srp
Local Address: 10.x.x.74
Chassis State: Standby
Chassis Mode: Backup
Chassis Priority: 2
Local Tiebreaker: 02-7E-35-53-F9-F1
Route-Modifier: 9

Peer Remote Address: 10.x.x.73
Peer State: Active
Peer Mode: Primary
Peer Priority: 1
Peer Tiebreaker: 02-11-59-73-87-35
Peer Route-Modifier: 8
Last Hello Message received: Fri Jul 22 15:50:21 2022 (3 seconds ago)
Peer Configuration Validation: Complete
Last Peer Configuration Error: None
Last Peer Configuration Event: Fri Jul 22 15:50:22 2022 (2 seconds ago)
Last Validate Switchover Status: None
Connection State: Connected

[local]imsupf01# show srp info
Friday July 22 15:31:20 UTC 2022
Service Redundancy Protocol:
------------------------------------------------------------------------------
Context: srp
Local Address: 10.x.x.66
Chassis State: Active
Chassis Mode: Backup
Chassis Priority: 2
Local Tiebreaker: 02-7C-1A-62-FA-3C
Route-Modifier: 5

Peer Remote Address: 10.x.x.65
Peer State: Standby
Peer Mode: Primary
Peer Priority: 1
Peer Tiebreaker: 02-87-33-98-6D-08
```

```
Peer Route-Modifier: 6
Last Hello Message received: Fri Jul 22 15:31:20 2022 (1 seconds ago)
Peer Configuration Validation: Complete
Last Peer Configuration Error: None
Last Peer Configuration Event: Fri Jul 22 15:20:13 2022 (668 seconds ago)
Last Validate Switchover Status: None
Connection State: Connected
```

Überprüfen Sie, ob die Anzahl der Leitungen im Aktiv-Standby-ICSR-Paar für IMS UPF identisch ist.

```
Active node
# show configuration | grep -n -E "^end$"
Thursday July 21 07:30:17 UTC 2022
14960:end

Standby Node
# show configuration | grep -n -E "^end$"
Thursday July 21 07:31:02 UTC 2022
14959:end
```

Überprüfen Sie, ob sich die SRP-Sessmgr im Status "Aktiv-verbunden" befindet, bevor die SRP auf aktivem UPF umschaltet, und stellen Sie sicher, dass kein ausstehender Aktiv-Status vorliegt.

```
[local]imsupf01# show srp checkpoint statistics active
Thursday July 21 07:38:04 UTC 2022
Number of Sessmgrs: 20
Sessmgrs in Active-Connected state: 20
Sessmgrs in Standby-Connected state: 0
Sessmgrs in Pending-Active state: 0
```

Überprüfen Sie, ob sich die SRP-Sessmgr im aktiven Verbindungszustand befindet, bevor die SRP auf die Standby-UPF umschaltet, und stellen Sie sicher, dass kein ausstehender Aktiv-Status vorliegt.

```
[local]imsupf02# show srp checkpoint statistics active
Thursday July 21 07:40:03 UTC 2022
Number of Sessmgrs: 20
Sessmgrs in Active-Connected state: 0
Sessmgrs in Standby-Connected state: 20
Sessmgrs in Pending-Active state: 0
```

Wenn sich eine dieser beiden Optionen in einem aktiven Zustand befindet, müssen Sie diese Aufgaben vor dem Switchover ausführen:

```
[upf-ims]# save config /flash/xxx_production.cfg. --> Replace xxx with the desired name of the config
[upf-ims]# srp validate-configuration
[upf-ims]# srp validate-switchover
```

Vor dem Herunterfahren des virtuellen Systems müssen Sie sicherstellen, dass die aktiven Instanzen auf den Standby-Modus umgestellt werden, damit die Teilnehmer ordnungsgemäß umgeschaltet werden. Wenn die Instanz bereits im Standby-Modus ist, ist keine Aktion erforderlich. Wenn die Instanz aktiv ist, überprüfen Sie die hervorgehobenen Werte, und stellen Sie sicher, dass der Standby-Modus aktiviert ist.

Überprüfen Sie die aktuellen Abonnenten in der aktiven UPF-Instanz.

```
[local]imsupf01# show subscribers data-rate summary
Friday July 22 16:01:37 UTC 2022

Total Subscribers : 175024
Active : 175024 Dormant : 0
```

Wechseln Sie die aktive Instanz in den Standby-Modus.

```
[context-name]<hostname># srp initiate-switchover
```

Überprüfen Sie den Status des Standby-Geräts, das inzwischen aktiv geworden wäre, und die Teilnehmersitzungen werden ebenfalls in die neue aktive Instanz verschoben. Da sich nun beide VM-Instanzen im Standby-Modus befinden, können sie für die Serverwartung heruntergefahren werden. Verwenden Sie die angegebenen **virtuellen** Befehle, um die VM-Instanzen zu beenden und den Status zu überprüfen.

```
cloud-user@podname-upf-ims-kvmnode-1:~$ sudo virsh shutdown imsupf01
Domain imsupf01 is being shutdown
cloud-user@podname-upf-ims-kvmnode-1:~$ sudo virsh shutdown imsupf10
Domain imsupf10 is being shutdown
cloud-user@podname-upf-ims-kvmnode-1:~$ sudo virsh list --all
Id Name State
----------------------------------------------------
1 imsupf01 shut off
4 imsupf10 shut off

cloud-user@podname-upf-ims-kvmnode-1:~$
```

Sobald der Server nach der Wartung wieder verfügbar ist, werden die VMs automatisch gestartet. UPF-Instanzen bleiben im Standby-Modus. mit dem angegebenen Befehl überprüfen.

```
[local]imsupf10# show srp info
Friday July 22 15:50:24 UTC 2022
Service Redundancy Protocol:
------------------------------------------------------------------------------
Context: srp
Local Address: 10.x.x.74
Chassis State: Standby
Chassis Mode: Backup
Chassis Priority: 2
Local Tiebreaker: 02-7E-35-53-F9-F1
Route-Modifier: 9

Peer Remote Address: 10.x.x.73
Peer State: Active
Peer Mode: Primary
Peer Priority: 1
Peer Tiebreaker: 02-11-59-73-87-35
Peer Route-Modifier: 8
Last Hello Message received: Fri Jul 22 15:50:21 2022 (3 seconds ago)
Peer Configuration Validation: Complete
Last Peer Configuration Error: None
Last Peer Configuration Event: Fri Jul 22 15:50:22 2022 (2 seconds ago)
Last Validate Switchover Status: None
Connection State: Connected
```

Daten-UPF verwendet RCM mit N:M-Redundanz, wobei N eine Anzahl aktiver UPFs ist und weniger als 10 beträgt, und M eine Anzahl von Standby-UPs in der Redundanzgruppe. Der RCM ist eine proprietäre Knoten- oder Netzwerkfunktion (NF) von Cisco, die Redundanz für StarOS-

basierte User Plane Functions (UPF) bietet. Es speichert oder spiegelt alle erforderlichen Sitzungsinformationen aus allen aktiven UPFs. Bei einem Switchover-Trigger wird ein Standby-UPF ausgewählt, um die entsprechenden Sitzungsdaten vom allgemeinen Standort zu empfangen. Der RCM wird auf einem K3-Cluster auf einer VM ausgeführt. Das Ops Center konfiguriert den RCM-Knoten.

Daten-UPF-Knoten sind auch die gleichen wie IMS UPF-Knoten. Der einzige Unterschied besteht in der RCM-Redundanzverwaltung.

Überprüfen Sie den VM-Status im KVM-Knoten.

```
cloud-user@podname-upf-data-kvmnode-1:~$ sudo virsh list --all
Id Name State
----------------------------------------------------
1 dataupf20 running
2 dataupf11 running

cloud-user@podname-upf-data-kvmnode-1:~$
```

Überprüfen Sie nach der Anmeldung bei der UPF-Instanz den RCM-Redundanzstatus. Wenn die Instanz bereits im Standby-Modus ist, ist keine Aktion erforderlich. Wenn sie aktiv ist, muss sie sanft in den Standby-Modus umgeschaltet werden.

```
[local]dataupf11# show rcm info
Friday July 22 17:23:17 UTC 2022
Redundancy Configuration Module:
------------------------------------------------------------------------------
Context: rcm
Bind Address: 10.x.x.75
Chassis State: Active
Session State: SockActive
Route-Modifier: 26
RCM Controller Address: 10.x.x.163
RCM Controller Port: 9200
RCM Controller Connection State: Connected
Ready To Connect: Yes
Management IP Address: 10.x.x.149
Host ID: DATAUPF15
SSH IP Address: 10.x.x.158 (Activated)
SSH IP Installation: Enabled

[local]dataupf11#
```

Überprüfen Sie, ob sich alle Sessmgr im Status "Aktiv verbunden" befinden.

```
local]dataupf11# show rcm checkpoint statistics active
Thursday July 21 07:47:03 UTC 2022
Number of Sessmgrs: 22
Sessmgrs in Active-Connected state: 22
Sessmgrs in Standby-Connected state: 0
Sessmgrs in Pending-Active state: 0
```

Identifizieren Sie den entsprechenden RCM-Knoten im Customer Information Questionnaire (CIQ), und überprüfen Sie den RCM-Status. Beachten Sie, dass ein RCM-Switchover nur über den Master-Knoten durchgeführt werden kann. Stellen Sie sicher, dass Sie sich beim Master-RCM anmelden.

```
[podname-aio-1/dcrm01] rcm# rcm show-status
message :
{"status":"MASTER"}
[podname-aio-1/dcrm01] rcm#
```

Suchen Sie die aktiven und Standby-UPF-Knoten mit dem angegebenen Befehl (Ausgabe gekürzt):

```
[podname-aio-1/dcrm01] rcm# rcm show-statistics controller
message :
{
"keepalive_version": "e7386cb81b1fefc3396dfd1d528e0d2a27de80d5de6a78364caf938a0d2149b6",
"keepalive_timeout": "20s",
"num_groups": 2,
"groups": [
{
"groupid": 1,
"endpoints_configured": 7,
"standby_configured": 1,
"pause_switchover": false,
"active": 6,
"standby": 1,
"endpoints": [
{
"endpoint": "10.x.x.75",
"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": 26,
"pool_received": true,
"echo_received": 142354,
"management_ip": "10.x.x.149",
"host_id": "DATAUPF15",
"ssh_ip": "10.x.x.158",
"force_nso_registration": false

....

....

{
"endpoint": "10.x.x.77",
"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": 3673,
"management_ip": "10.x.x.153",
"host_id": "",
"ssh_ip": "10.x.x.186",
"force_nso_registration": false
},
```

Melden Sie sich mit der Management-IP bei der Standby-UPF-Instanz an, und überprüfen Sie den Status.

```
[local]dataupf13# show rcm info
Friday July 22 17:36:04 UTC 2022
Redundancy Configuration Module:
-------------------------------------------------------------------------------
Context: rcm
Bind Address: 10.x.x.77
Chassis State: Standby
Session State: SockStandby
Route-Modifier: 50
RCM Controller Address: 10.x.x.163
RCM Controller Port: 9200
RCM Controller Connection State: Connected
Ready To Connect: Yes
Management IP Address: 10.x.x.153
Host ID:
SSH IP Address: 10.x.x.186 (Activated)
SSH IP Installation: Enabled

[local]dataupf13#
```

Schalten Sie nach der Überprüfung vorsichtig in den Standby-Modus um. Stellen Sie sicher, dass die Verwaltungs-IP verwendet wird.

```
[podname-aio-1/dcrm01] rcm# rcm switchover-mgmt-ip source 10.x.x.149 destination 10.x.x.153
```

Anmerkung: Im Falle nach dem Switchover, wenn der neue aktive UP-Sessmgr im **SERVER-**Zustand feststeckt. Wenden Sie sich an den technischen Support von Cisco. Bei problematischen Fällen muss sessmgr beendet werden, sodass die Verbindung mit dem RCM mit dem korrekten CLIENT-Socketstatus wiederhergestellt und wiederhergestellt wird. Alle Sitzungen müssen im **CLIENT-**Zustand sein. Überprüfen Sie es mit dem angegebenen Befehl (im ausgeblendeten Modus).

```
# show session subsystem facility sessmgr all debug-info | grep -E "SessMgr|Mode:"
Thursday July 21 07:56:26 UTC 2022
SessMgr: Instance 5000
Mode: UNKNOWN State: SRP_SESS_STATE_SOCK_ACTIVE
SessMgr Activity Detected: FALSE
SessMgr: Instance 22
Mode: CLIENT State: SRP_SESS_STATE_SOCK_ACTIVE
SessMgr Activity Detected: TRUE
SessMgr: Instance 21
Mode: CLIENT State: SRP_SESS_STATE_SOCK_ACTIVE
SessMgr Activity Detected: TRUE
```

Überprüfen Sie, ob alle Sitzungen aktiv und bereit sind.

```
# show rcm checkpoint statistics verbose
Thursday July 21 07:52:29 UTC 2022
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 1731 68120 3107912 409200665
2 Actv Ready 0 0 1794 70019 3060062 408647685
3 Actv Ready 0 0 1753 68793 3078531 406227415
4 Actv Ready 0 0 1744 67585 3080952 410218643
5 Actv Ready 0 0 1749 69155 3096067 404944553
6 Actv Ready 0 0 1741 68805 3067392 407133464
7 Actv Ready 0 0 1744 67963 3084023 406772101
8 Actv Ready 0 0 1748 68702 3009558 408073589
```

```
9 Actv Ready 0 0 1736 68169 3030624 405679108
10 Actv Ready 0 0 1707 67386 3071592 406000628
11 Actv Ready 0 0 1738 68086 3052899 407991476
12 Actv Ready 0 0 1720 68500 3102045 408803079
13 Actv Ready 0 0 1772 69683 3082235 406426650
14 Actv Ready 0 0 1727 66900 2873736 392352402
15 Actv Ready 0 0 1739 68465 3032395 409603844
16 Actv Ready 0 0 1756 69221 3063447 411445527
17 Actv Ready 0 0 1755 68708 3051573 406333047
18 Actv Ready 0 0 1698 66328 3066983 407320405
19 Actv Ready 0 0 1736 68030 3037073 408215965
20 Actv Ready 0 0 1733 67873 3069116 405634816
21 Actv Ready 0 0 1763 69259 3074942 409802455
22 Actv Ready 0 0 1748 68228 3051222 406470380
```

Überprüfen Sie, ob die Teilnehmer in den neuen Standby-Modus verschoben werden:

```
[local]dataupf11# show subscribers data-rate summary
Friday July 22 17:40:18 UTC 2022

Total Subscribers : 62259
Active : 62259 Dormant : 0
```

Wenn beide Instanzen im Standby-Modus sind, können VMs mithilfe von **virtuellen** Befehlen vom KVM-Switch heruntergefahren werden.

```
cloud-user@podname-upf-data-kvmnode-1:~$ sudo virsh shutdown dataupf20
Domain dataupf20 is being shutdown
cloud-user@podname-upf-data-kvmnode-1:~$ sudo virsh shutdown dataupf11
Domain dataupf11 is being shutdown
cloud-user@podname-upf-data-kvmnode-1:~$ sudo virsh list --all
Id Name State
----------------------------------------------------
1 dataupf20 shut off
4 dataupf11 shut off

cloud-user@podname-upf-data-kvmnode-1:~$
```

Wenn VMs heruntergefahren werden, kann der KVM-Knoten (physischer Server) zur Wartung heruntergefahren werden. Starten Sie den Server nach Abschluss des Vorgangs. VMs werden automatisch aktiviert. UPF-Instanzen werden eigenständig in den Standby-Modus versetzt. Überprüfen Sie dies mit den angegebenen Befehlen.

```
cloud-user@podname-upf-data-kvmnode-1:~$ sudo virsh list --all
Id Name State
----------------------------------------------------
1 dataupf20 running
2 dataupf11 running

cloud-user@podname-upf-data-kvmnode-1:~$

[local]dataupf11# show rcm info
Friday July 22 17:36:04 UTC 2022
Redundancy Configuration Module:
-------------------------------------------------------------------------------
Context: rcm
Bind Address: 10.x.x.77
Chassis State: Standby
Session State: SockStandby
Route-Modifier: 50
```

```
RCM Controller Address: 10.x.x.163
RCM Controller Port: 9200
RCM Controller Connection State: Connected
Ready To Connect: Yes
Management IP Address: 10.x.x.153
Host ID:
SSH IP Address: 10.x.x.186 (Activated)
SSH IP Installation: Enabled

[local]dataupf13#
```

Im RCM-Knoten kann der RCM-Controller den Standby-UPF noch als "ausstehender Standby" anzeigen. Dies kann bis zu 15 bis 20 Minuten in Anspruch nehmen, um in den Standby-Modus umzuwandeln. Überprüfen Sie mit den angegebenen Befehlen das Gleiche (Ausgabe gekürzt):

```
[podname-aio-1/dcrm01] rcm# rcm show-statistics controller
message :
{
"keepalive_version": "e7386cb81b1fefc3396dfd1d528e0d2a27de80d5de6a78364caf938a0d2149b6",
"keepalive_timeout": "20s",
"num_groups": 2,
"groups": [
{
"groupid": 1,
"endpoints_configured": 7,
"standby_configured": 1,
"pause_switchover": false,
"active": 6,
"standby": 1,
"endpoints": [
....
....
{
"endpoint": "10.x.x.77",
"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": 3673,
"management_ip": "10.x.x.153",
"host_id": "",
"ssh_ip": "10.x.x.186",
"force_nso_registration": false
},
```