Software Management Operations

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in This Release:	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2022.01.2

Overview

5G UPF supports backward compatibility of software releases on the SMF and the UPF. The feature allows seamless upgrade/downgrade of the software from/to one previous release (N-1). The functionality includes support for the following:

- N-1 compatibility of software releases on two UPFs in ICSR mode—allows seamless upgrade of UPFs from one version to another in UPF 1:1 redundancy scenario.
- N-1 compatibility of software releases between SMF and UPF—allows seamless upgrade of the associated SMF or UPF from one version to another.
- N-1 compatibility of software releases between SMF and UPF with multi-Sx—allows seamless upgrade of the associated SMF or UPF from one version to another in multi-Sx scenario.

Important Contact your Cisco Account representative for procedural assistance prior to upgrading or downgrading your software versions.

Version Exchange between SMF and UPF

Version/release information is exchanged when SMF and UPF pairs. The release information exchange also occurs when the UPF pairs with a Standby UPF (in 1:1 redundancy scenario) through the heart beat message exchanged between Active and Standby.

When incompatible releases are paired, an Alarm (SNMP trap) is raised. For details, see SNMP Traps section.

To indicate the peer version during the exchange of release information, the following new IE is included in the association request and heartbeat request messages.

Information Elements	P	Condition / Comment								IE Length	IE ID
Peer Version	O	Used to specify the peer GR/PFCP version and StarOS version								4 bytes	245
		Bits									
	Octets	8	7	6	5	4	3	2	1		
	1 to 2	Peer Version IE Type = 245 (decimal)									
	3 to 4	Length = n bytes									
	5 to 8	Peer GR/PFCP Version									
	9 to 12	StarOS GR Version									
	13 to 13	StarOS Version String Length									
	Variable Length	StarOS Version String Value									

SNMP Traps

The following SNMP traps are raised when pairing is done with an incompatible release.

SNMP Trap	Description
SRPPeerUnsupportedVersion	The Active/Standby UPF in higher version raises the SNMP trap when the peer is in a version lower than N-1.
SRPPeerUnsupportedVersionClear	The Active/Standby UPF in higher version raises the SNMP trap to clear the SRPPeerUnsupportedVersion.
SxPeerUnsupportedVersion	The UPF in higher version raises the SNMP trap when the peer is in a version lower than N-1.
SxPeerUnsupportedVersionClear	The UPF in higher version raises an SNMP trap to clear the SxPeerUnsupportedVersion.

Limitations

The following are the known limitations of the feature:

- When the peer version is determined to be lower than the supported N-1 version, the association/pairing is allowed. However, functional aspect of the same isn't guaranteed.

Caution Don't attempt to upgrade from incompatible versions. Contact your Cisco Account representative for the upgrade path and steps.

- Few CLI commands may not be supported in N+1 version.
- The SMF version must be compatible with the UPF version.
- The hardware configuration must be similar in both Active and Standby UPFs.
- SNMP traps are raised by the node on the latest version with respect to the StarOS version. For details, see the SNMP Traps section of this chapter.
- From release 2022.01.2, RCM is checkpoint agnostic to enable support for future UPF releases. Currently RCM supports only N-1 compatibility.

Health Checks

Perform the following health checks after every operation of upgrade, downgrade, or reload of chassis.

1. Check the Service Redundancy Protocol (SRP) information on the Active chassis to avoid issues during an SRP switchover and decide if proactive analysis must be done before the SRP switchover. Use the following CLI commands:
   - **srp validate-configuration**

- **srp validate-switchover**
- **show srp info**

The following is a sample output.

```
Peer Configuration Validation: Complete
Last Peer Configuration Error: None
Last Peer Configuration Event: Wed Mar 18 15:34:02 2022  (1602 seconds ago)
Last Validate Switchover Status: None
Connection State: Connected
```

Check the following parameters:

- **Peer Configuration Validation: Complete**—If it shows "In Progress," you must wait and then execute the **show srp info** CLI command again after 15 seconds (approximately).
- **Last Peer Configuration Error: None**—If you see "Peer Checksum Validation Failure," then it indicates that there are configuration differences between Active and Standby chassis that must be fixed.

Note If you see any error in **Last Peer Configuration Error**, validate the configuration using the **show configuration srp** CLI command on both the Active and Standby UPFs.

- **Last Validate Switchover Status: None**—The output must show as "None." Also, the output must be *Remote Chassis - Ready for Switchover (XX seconds ago)* when the **srp validate-configuration** and **srp validate-switchover** CLI commands are triggered.
- **Connection State: Connected**—The output must show as "Connected."

2. Check subscriber count on both Active and Standby chassis.

   After sessions are up, execute the **show subscribers summary | grep Total** CLI command in the Active chassis. The following is a sample output.

   ```
   show subscribers summary | grep Total
      Total Subscribers:  100
   ```

   On the Standby chassis, execute the **show srp checkpoint statistics | grep allocated** CLI command. The following is a sample output.

   ```
   show srp checkpoint statistics | grep allocated
      Current pre-allocated calls:  100
   ```

3. Check the status of the license by executing the **show license information** CLI command. It must be in "Good (Redundant)" and not in "Expired" state.
4. Check the Session Recovery Status by executing the **show session recovery status verbose** CLI command. The following is a sample output.

   ```
   Session Recovery Status:
     Overall Status        : Ready For Recovery
     Last Status Update    : 7 seconds ago

                 ----sessmgr---  ----aaamgr----  demux
    cpu state    active standby  active standby  active  status
   1/0  Active     8      1        8      1        17     Good
   ```

5. Verify if all the SessMgrs are in Standby-Connected state on the Standby chassis by executing the **show srp checkpoint statistics | grep Sessmgrs** CLI command. The following is a sample output.

```
Number of Sessmgrs:        1
Sessmgrs in Active-Connected state:  0
Sessmgrs in Standby-Connected state: 8
Sessmgrs in Pending-Active state:    0
```

6. Verify the status of all the cards to see if they are in Active or Standby state. The following is a sample output.

```
show card table

Slot          Card Type              Oper State  SPOF  Attach
----------- ---------------------- ----------- ----- ------
1: VC        5-Port Virtual Card     Active        -
```

7. Execute the **show task resources | grep -v good** CLI command, and its output must only display the total number of SessMgrs and sessions.
8. Execute the **show crash list** CLI command to check if there are any new crashes.
9. Execute the **show service all** CLI command to verify that the state is displayed as "Started" and not "Initialized."

Build Upgrade

Backup Configuration

1. Back up the current configuration—Save the current configuration that is used in case of downgrade/upgrade, which probably has all the features and configuration present until now.
2. Collect the **show support details** on both Active and Standby chassis before making any changes or upgrade.
3. Perform Health Checks.

Upgrade Procedure

1. Perform chassis Health Checks on both the nodes.
2. On the secondary chassis (ICSR), which is in Standby state, change boot priority with N+1 build.
3. Reload to the latest build version.
4. Do the new configuration change on Standby chassis (For example, any new CLI, license, or configuration changes).
5. Perform Health Check on the reloaded chassis. Check for any crashes or errors.

Perform Switchover

1. Before SRP switchover from Active to Standby on both chassis, check:
   a. On Active chassis: **show subscriber summary | grep Total**

b. On Standby chassis: **show srp checkpoint statistics | grep allocated**

Note The count must be same for both chassis.

c. On Active and Standby chassis: **show sx peer**

For example:

```
|||||  Sx Service                                                    No of
|||||  ID                                                                Restart
|||||  |                                                 Recovery              |
Current    Max        Peer
vvvvv  v     Group Name    Node ID         Peer ID     Timestamp             v
Sessions   Sessions   State
----- ---- ----------------- ------------------------- ------------------- ------
--------- --------- --------
CAAXD  22    CPGROUP21   209.165.200.225   50331649    2021-03-17:02:33:55    0
    0          0      NONE

Total Peers:    1
```

Note Peer state must be Active and associated. Peer ID must match on both the chassis.

d. On Standby chassis: **show srp checkpoint statistics | grep Sessmgrs**

Note "Number of Sessmgrs" must be equal to the "Sessmgrs in Standby-Connected state".

e. On Active chassis:

1. **srp validate-configuration**: This CLI command initiates a configuration validation check in the Active chassis. If the validation doesn't have any error, the output of this CLI command is blank.
2. **srp validate-switchover**: Validates if both Active and Standby chassis are ready for a planned SRP switchover. If the chassis is ready for switchover, then the output of this CLI command is blank.
3. **show srp info | grep "Last Validate Switchover Status"** : Output of this CLI command must be as follows.

   ```
   Last Validate Switchover Status: Remote Chassis - Ready for Switchover
   ```

4. **show srp info debug**: Active and Standby chassis must have the same output.

2. On Active chassis: **srp initiate-switchover**
   a. Perform chassis Health Checks on both the nodes. Also check Step 1a and Step 1c under the *Perform Switchover* section. There can be a difference of 5%.
   b. Perform call testing since new sessions are serviced on the new Active chassis.
   c. Upgrade the old Active as mentioned in Step 2 through Step 5 under the *Upgrade Procedure* section.

UPF Upgrade

This section describes the procedure for UPF upgrade.

1. Perform Health Check procedure on both the UPF nodes as mentioned in the Health Checks, on page 3 section.
2. Perform Upgrade on Standby UPF as mentioned in the Build Upgrade, on page 5 section.
3. Do "sx-peer configuration" on the upgraded Standby chassis.
4. Perform Health Check on both the UPF nodes, and then do UPF switchover.
5. Upgrade the new Standby UPF as mentioned in the Build Upgrade, on page 5 section.

UPF Downgrade

Perform the following steps to downgrade the UPF:

1. Perform Health Check on the UPF.
2. Change boot priority to the N-1 build on the Standby UPF. Reload the Standby UPF.
3. Do "sx-peer configuration" on the downgraded Standby UPF.
4. Perform Health Check on both the UPF nodes and then do UPF switchover.
5. Perform Step 1 to Step 3 on the new Standby UPF.