

SAPC VNF Upgrade by Replacement

Ericsson Service-Aware Policy Controller

Upgrade Instruction

Copyright

©Ericsson España S.A. 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	VNF Upgrade by Replacement Introduction	1
1.1	Prerequisites	1
2	Upgrade Overview	5
2.1	Stages of Upgrade by Replacement	5
2.2	Upgrade Impact in UDC	7
2.3	Upgrade Times	7
2.4	System Downtime	8
2.5	Traffic Loss	8
2.6	Service Disturbance	8
2.7	Network Connectivity	8
3	Upgrade Preparation	13
3.1	Access Management	13
3.2	Network Plan	14
3.3	NFV Infrastructure Resources	14
3.4	SAPC Virtual Delivery Package	15
3.5	Destination SAPC vAPP Descriptor Generation	15
3.6	Upgrade Environment Preparation	15
4	Upgrade Instructions	17
4.1	Instantiation of Destination SAPC vAPP	17
4.2	Upgrade Execution	18
4.3	Decommission of Origin SAPC vAPP	24
5	Post-Upgrade Activities	25
5.1	Update SAPC Version in OSS/ENM	25
5.2	Remove IP Routes	25
5.3	Entities with External Subscriber Repository	25
6	Rollback Procedure	27
6.1	Automatic Rollback	27
6.2	On-Demand Rollback	28
6.3	Execute Rollback Procedure	28
7	Troubleshooting	31





1 VNF Upgrade by Replacement Introduction

This document describes the upgrade by replacement procedure supported for Service-Aware Policy Controller (SAPC) Virtualized Network Function (VNF) deployments.

Benefits of Upgrade by Replacement include:

- All time availability of the Origin SAPC vAPP for a rollback procedure
- The possibility of **babysitting**, which is a control period when the Upgrade Execution can be interrupted after the deployment of the Destination SAPC vAPP is finished. The operator can monitor and evaluate the performance of the Destination SAPC vAPP, and if the redirected traffic is being processed as expected. The operator then can decide to finish the upgrade, or revert the procedure and rollback to the Origin SAPC vAPP in case the system develops unexpected behaviors during the babysitting phase
- Applying some network configuration changes during the upgrade

1.1 Prerequisites

This section describes the prerequisites which must be fulfilled before initiating the SAPC upgrade procedure.

1.1.1 Hardware and Software Requirements

Hardware Requirements	The upgrade procedure requires an external host machine with Linux and glibc version 2.12-1 or higher.
Network Element Version	This instruction applies to the SAPC Network Element CXP 903 0138/7 SAPC 1.3 onwards.
State of Software Configurations	This type of upgrade applies to SAPC VNF deployments from version 1.0 onwards.
Upgrade Deliverable	The SAPC installation package for VNF deployments, which can be obtained from the Ericsson Software Gateway.
NFV Infrastructure Resources	The upgrade procedure requires a Network Function Virtualization (NFV) infrastructure with enough resources, like vCPU, memory, storage, and vNICs to deploy an extra instance of SAPC.



NFV Infrastructure Type	<ul style="list-style-type: none">• VMware vCenter• OpenStack Cloud
Network Plan	This procedure requires the reservation of four new Virtual IP (VIP) addresses in the network plan.

1.1.2 Documents and Tools

The following documents are required to prepare and deploy the new SAPC instance:

- SAPC VNF Deployment Instruction for OpenStack
- SAPC VNF Deployment Instruction for VMware
- SAPC VNF Network Configuration Guide
- Adapt Cluster Tool
- VNF Descriptor Generator Tool

Ensure that the following tools are at your disposal to execute the upgrade procedure and operate the NFV infrastructure:

- OpenStack CLI Server
- VMware vCenter or vCloud Director
- Proper access rights, refer to Section 3.1 on page 13

1.1.3 Conditions

Consider the following conditions during the upgrade procedure:

- No Operation and Maintenance (OAM) actions are allowed to perform during the execution of the upgrade
- The upgrade must be executed during low traffic hours
- Disable any scheduled backup during the upgrade time window
- Ensure the maximum number of backups are properly dimensioned according to [Change Maximum Number of Manual Backups](#)
- The network configured according to Section 2.7 on page 8
- The Destination SAPC vAPP requires the amount of PayLoad (PL) as the Origin SAPC vAPP
- Root credentials enabled to access and log on from the external host to the Origin SAPC vAPP through Secure Shell (SSH) using private and public key



1.1.4 Limitations and Workarounds

No limitations or workarounds.





2 Upgrade Overview

The upgrade by replacement procedure consists of three stages:

2.1 Stages of Upgrade by Replacement

This section describes the phases and order of the Upgrade by Replacement procedure.

2.1.1 Instantiation of Destination SAPC vAPP

This phase includes the following steps:

- Deployment of the Destination SAPC vAPP using the Virtual Delivery Package of the target software version
- Configuration of the external connectivity according to the requirements of the upgrade
- Scale out of the Destination SAPC vAPP instance to have the same amount of PayLoad (PL) as the Origin SAPC vAPP

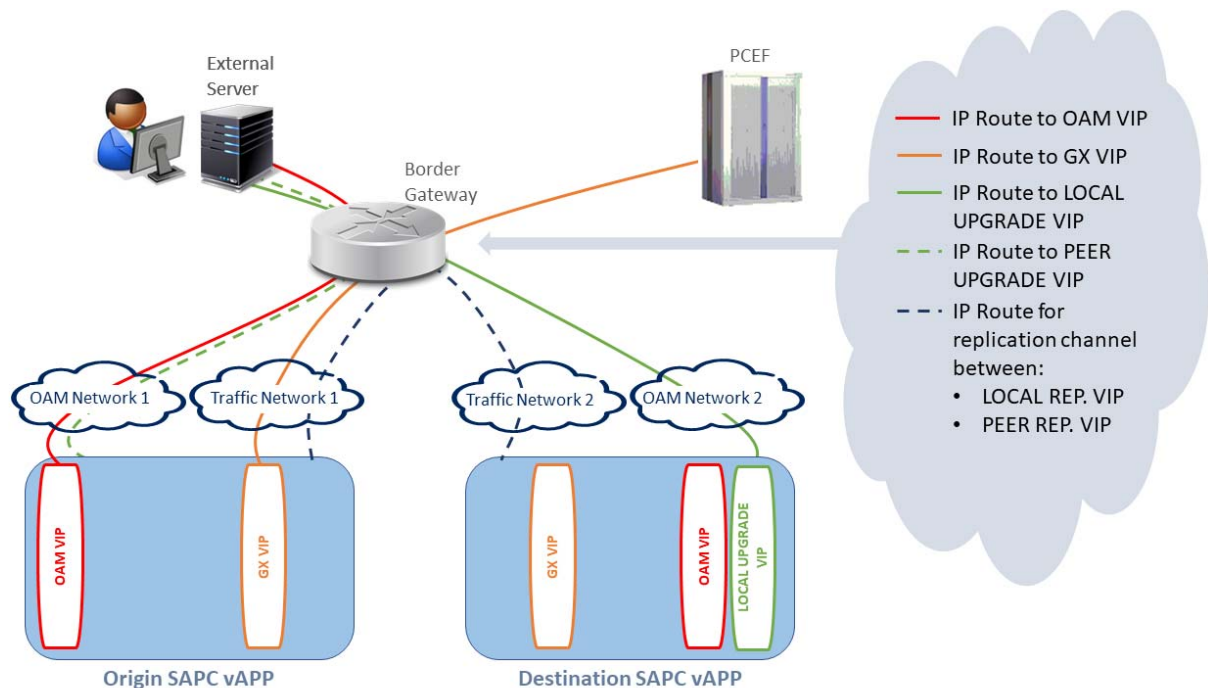


Figure 1 Instantiation of the Destination SAPC vAPP

2.1.2 Upgrade Execution

This phase includes the following steps:

- Migration of the Origin SAPC vAPP configuration and user accounts in use to the Destination SAPC vAPP
- Synchronization of the Destination SAPC vAPP with the session and the provisioned data stored in the Origin SAPC vAPP by means of a replication channel
- Direct the incoming traffic from the Origin SAPC vAPP to the Destination SAPC vAPP according to the Section 2.7.3.3 on page 11
- Migrate the rest of the data files, like counters or log files from the Origin SAPC vAPP to the Destination SAPC vAPP
- Optional babysitting period to monitor the performance of the Destination SAPC vAPP, and rollback to the Origin SAPC vAPP, if needed. See Figure 2 for the babysitting phase
- Consolidation of the Destination SAPC vAPP when the replication channel and configuration settings of the upgrade are removed

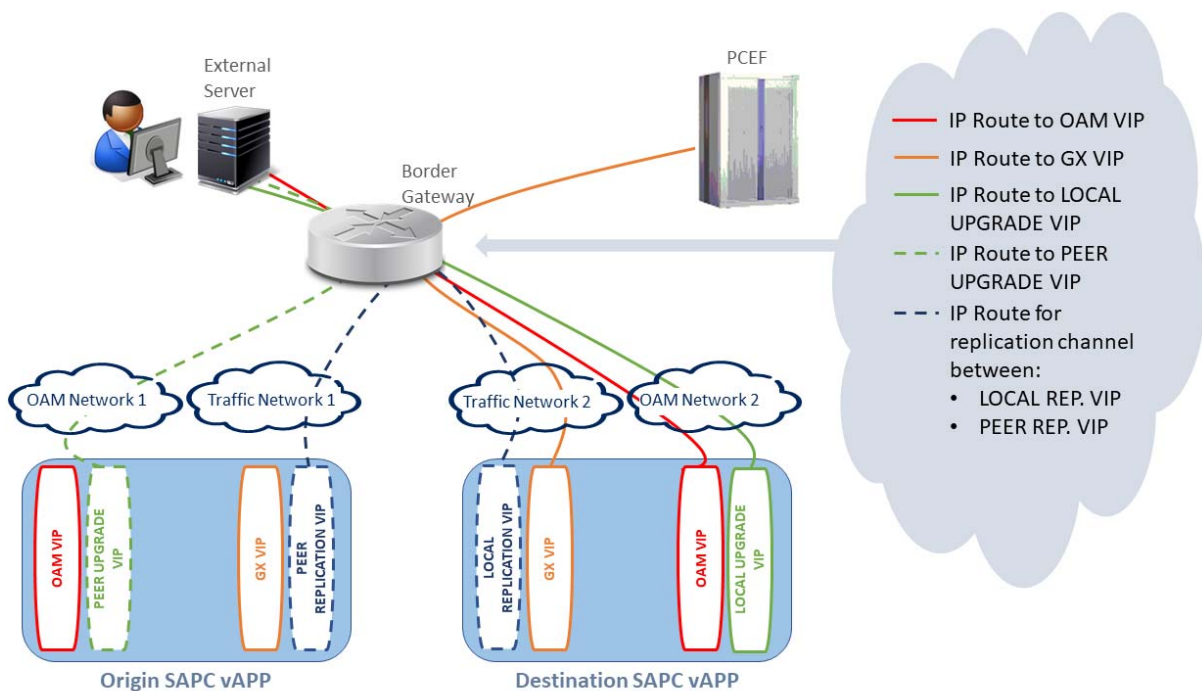


Figure 2 Upgrade Execution

The Upgrade Execution stage includes health-checks of the SAPC vAPP instances to base the decisions to continue the process on the current status, and the creation of system backups at different phases to recover the system in case of failures.



2.1.3 Decommission of Origin SAPC vAPP

This phase includes the following steps:

- Decommission of the Origin SAPC vAPP from NFV infrastructure
- Remove the extra network configuration used during the upgrade by replacement procedure

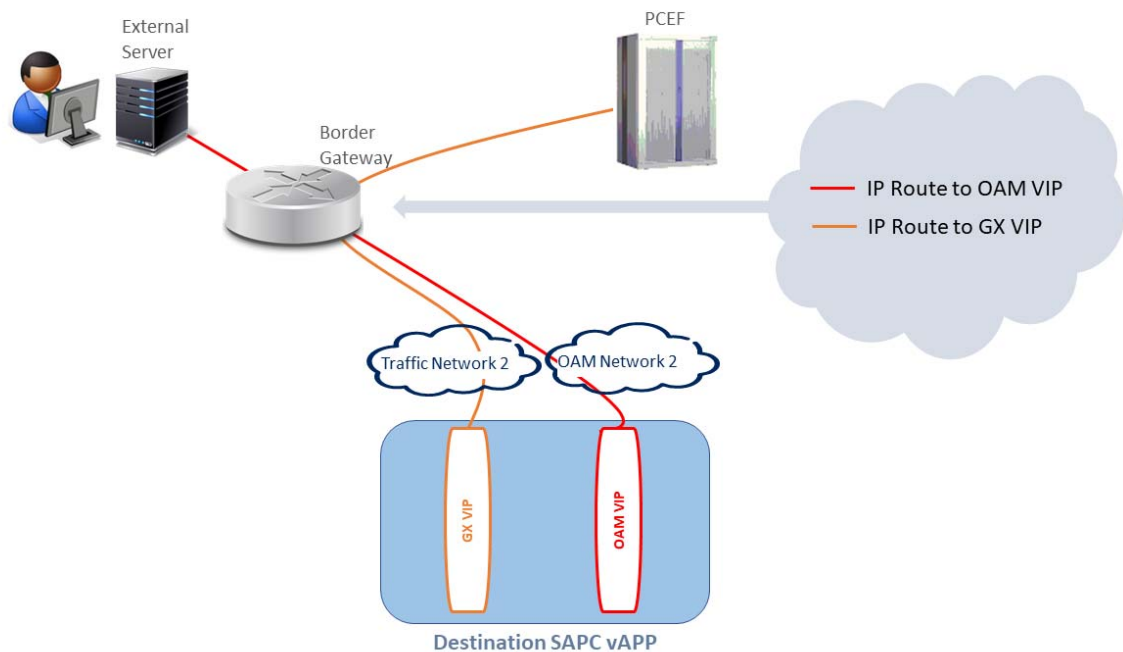


Figure 3 Decommissioning of Origin SAPC vAPP

2.2 Upgrade Impact in UDC

For impacts related to User Data Consolidation (UDC) solution, refer to the Upgrade chapter of SAPC 1 Network Impact Report.

2.3 Upgrade Times

Table 1 shows an estimation of the upgrade procedure lifecycle.

Table 1 Upgrade Times

Upgrade by Replacement Procedure			
SAPC Deployment Layout	Instantiation of Destination SAPC vAPP (min) ⁽¹⁾	Upgrade Execution (min) ⁽²⁾	Decommission of Origin SAPC vAPP (min) ⁽¹⁾
2+2	15	30	1



Table 1 Upgrade Times

2+10	47 ⁽³⁾	30	1
2+34	143 ⁽³⁾	30	1

(1) This process can be executed out of the maintenance window.

(2) This process is executed during the maintenance window is open.

(3) 15+4 per additional PL

Do!

The time of the manual network reconfiguration and the babysitting periods is not considered in the calculations for the Upgrade Execution. Add the estimated figures of these processes to the time defined in the Upgrade Execution column of Table 1.

Consider approximately 2 minutes for the on-demand rollback procedure in case of babysitting, and 10 minutes for the automatic rollback procedure if errors occurred during the Upgrade Execution.

2.4 System Downtime

No system downtime is expected during the upgrade procedure.

2.5 Traffic Loss

Minor traffic loss is expected during the upgrade procedure.

2.6 Service Disturbance

Minor service disturbances can occur after the network reconfiguration, and until the migration of data files, like logs or measurements is completed.

The Performance Data Collector service is disabled in the Destination SAPC vAPP until all measurement files are migrated.

2.7 Network Connectivity

The upgrade by replacement procedure requires additional network configuration related to the Virtual Internet Protocol (VIP) networks and addresses.

For general information about the network configuration and network connectivity, refer to the [SAPC VNF Network Configuration Guide](#).



Warning!

The Destination SAPC vAPP must be instantiated with the same OAM and Traffic VIPs already used in the Origin SAPC vAPP. This chapter is focused on the new VIPs required for the Upgrade by Replacement procedure.

2.7.1 External Networks

This type of upgrade initiates new requirements about External Networks to ensure connectivity to both the Origin and the Destination SAPC vAPP instances, and secure the replication channel to synchronize the data involved during the upgrade procedure.

Table 2 shows the required IP addresses to the affected networks.

Table 2 External Network Impacts

Network Common Name	Upgrade by Replacement Impacts	VIP Requirements
OAM Networks	Provide access to the public virtual IP addresses that are required for the procedure	<ul style="list-style-type: none"> • Destination SAPC vAPP: local upgrade VIP • Origin SAPC vAPP: peer upgrade VIP
Traffic Networks	Provide access to the public virtual IP addresses that are required for the replication channel involved during the procedure	<ul style="list-style-type: none"> • Destination SAPC vAPP: local replication VIP • Origin SAPC vAPP: peer replication VIP

2.7.2 VIP Address Allocation

Virtual IP addresses are required for both the Origin and Destination SAPC vAPP instances to support the upgrade procedure.

The following sections describe the types of virtual IP addresses.

2.7.2.1 Local Upgrade VIP

This is a mandatory IP address corresponding to the VIP that can be accessed through the external OAM network. It is used to manage and maintain the Destination SAPC vAPP during the upgrade procedure.

The IP address is provided by the customer. The allocation of the IP address is done from the customer network plan through the external OAM network on site.



2.7.2.2 Peer Upgrade VIP

This is a mandatory IP address corresponding to the VIP that can be accessed through the external OAM network. It is used to manage and maintain the Origin SAPC vAPP during the upgrade procedure.

The IP address is provided by the customer. The allocation of the IP address is done from the customer network plan through the external OAM network on site.

2.7.2.3 Local Replication VIP

This is a mandatory IP address corresponding to the VIP that can be accessed through the external traffic network from the Destination SAPC vAPP. This VIP is used to send and receive replication data from the Origin SAPC vAPP during the upgrade procedure.

The IP address is provided by the customer. The allocation of the IP address is done from the customer network plan through the external traffic operator network on site.

2.7.2.4 Peer Replication VIP

This is a mandatory IP address corresponding to the VIP that can be accessed through the external traffic network from Origin SAPC vAPP. This VIP is used to send and receive replication data from the Destination SAPC vAPP during the upgrade procedure.

The IP address is provided by the customer. The allocation of the IP address is done from the customer network plan through the external traffic operator network on site.

2.7.3 Gateway Router Configuration

This section describes the configuration of the external networks.

Configuration of additional IP routes is required from both the Origin and the Destination SAPC vAPP instances to access the upgrade VIP addresses apart from the IP routes set in the gateway routers to interoperate with the in-service Origin SAPC vAPP.

The upgrade by replacement procedure also requires a network reconfiguration. During the procedure, all IP routes establishing the incoming traffic to the in-service Origin SAPC vAPP need to be modified to reach the Destination SAPC vAPP. The gateway configuration would be reestablished according to the original IP routes in case of a rollback.

Equal-Cost Multipath (ECMP) is configured for the traffic distribution among the FEE IP addresses for each traffic type.



2.7.3.1 Gateway Router Configuration of Origin SAPC vAPP

This section describes the configuration of additional IP routes in the gateway routers towards the Origin SAPC vAPP to support the upgrade procedure.

Configuration of OAM Gateways

Define static routes for the Front-End Element (FEE) IP addresses in the System Controller (SC) to reach the Peer Upgrade VIP

Configuration of Traffic Gateways

Define static routes for the FEE IP addresses in the PL to reach the Peer Replication VIP

2.7.3.2 Gateway Router Configuration of Destination SAPC vAPP

This section describes the configuration of additional IP routes in the gateway routers towards the Destination SAPC vAPP to support the upgrade procedure.

Configuration of OAM Gateways

Define static routes for the FEE IP addresses in the SC to reach the Local Upgrade VIP

Configuration of Traffic Gateways

Define static routes for the FEE IP addresses in the PL to reach the Local Replication VIP

2.7.3.3 Network Reconfiguration

This section describes the IP routes to reconfigure in the gateway routers during the upgrade procedure.

Reconfiguration of OAM Gateways

Change the static routes of the FEE IP addresses in the SC to reach the OAM VIPs from the Destination SAPC vAPP instead of the Origin SAPC vAPP

Reconfiguration in Traffic Gateways

Change the static routes of the FEE IP addresses in the SC to reach the traffic VIPs from the Destination SAPC vAPP instead of the Origin SAPC vAPP





3 Upgrade Preparation

This section describes the preparations required before initiating the SAPC upgrade by replacement to the SAPC software target version.

The following action points can be done before the upgrade window.

3.1 Access Management

This chapter describes the accesses and credentials needed to execute the upgrade procedure.

3.1.1 Obtain the SAPC Virtual Delivery Package

Access to the SAPC software gateway is required to download the installation package for the Destination SAPC vAPP.

3.1.2 Access to Cloud Orchestration

- Access to OpenStack Command-Line Interface (CLI) server in case of OpenStack
- Access to vCenter or vCloud Director in case of VMware

3.1.3 Access to Origin SAPC vAPP

Access to the Origin SAPC vAPP requires a pair of Public or Private keys for SSH connections. For this to establish, a remote trust relation is required between the root user of the Origin SAPC vAPP and the external host machine.

The following section describes the instructions to set up the credentials and the access.

1. Execute ssh-keygen to generate the pair of keys. Use the default file and no passphrase when asked for.

The keygen to use for the keys:

```
ExternalHostMachine:$ ssh-keygen -t rsa
```

Complete the inquiry to use the default file:

Generating public or private rsa key pair.

Enter file in which to save the key (/user/.ssh/id_rsa):



Created directory '/user/.ssh'.

Enter passphrase (empty for no passphrase):

Your identification has been saved in /user/.ssh/id_rsa.

Your public key has been saved in /user/.ssh/id_rsa.pub.

The key fingerprint is:

2. Assign the public key to the Authorized Keys for root user in the SC from the Origin SAPC vAPP and executes the following command:

```
ExternalHostMachine:$ ssh-copy-id -i root@originsapc oamvip
```

The access to each SC is implemented using the same VIP in a circular order. Repeat this action until you secure the public key added to the SCs.

Verify the content of the default file to complete this step.

/user/.ssh/id_rsa.pub is generated in the first step, and is added to the /root/.ssh/authorized_keys file in both SCs.

3. Verify that the connection is functioning properly and access to the SCs does not require a password. Connect to the Origin SAPC vAPP a couple times.

3.2 Network Plan

The upgrade by replacement procedure requires additional VIPs to be reserved in the customer network. Refer to Section 2.7.2 on page 9.

Local Upgrade VIP	This VIP is created in the Destination SAPC vAPP during the instantiation phase. It must be accessible from the external host machine by means of the OAM network.
Peer Upgrade VIP	This VIP is created in the Origin SAPC vAPP during the Upgrade Execution phase. It must be accessible from the external host machine by means of the OAM network.
Local Replication VIP	This VIP is created in the Destination SAPC vAPP during the Upgrade Execution phase. It must be accessible from the Origin SAPC by means of the Traffic network.
Peer Replication VIP	This VIP is created in the Origin SAPC vAPP during the Upgrade Execution phase. It must be accessible from the Destination SAPC by means of the Traffic network.

3.3 NFV Infrastructure Resources

The upgrade by replacement procedure requires that both the Origin and the Destination SAPC vAPP instances to be online at the same time during the maintenance window. It is important to secure that resources, such as vCPUS,



Memory, or Storage are available in the NFV Infrastructure provided by the customer before starting the procedure.

3.4 SAPC Virtual Delivery Package

The software necessary for the upgrade procedure can be downloaded from the Ericsson Software Gateway through opening a unique ticket number. Refer to Release Notes for specific version information and ticket number.

The Software Package file for the SAPC needs to be available on an external host machine through which the OpenStack CLI server can be accessible.

Software Package	Filename
SAPC Virtual Delivery Package	vdp_sapc_qcow2_cxp9032849_<revision>.tar.gz
SAPC Virtual Delivery Package for VMware	vdp_sapc_qcow2_cxp9032850_<revision>.tar.gz

3.5 Destination SAPC vAPP Descriptor Generation

The SAPC Virtual Delivery Software Package provides adapt cluster configuration templates designed for this kind of upgrade. The templates contain an upgrade section which is mandatory to configure the upgrade VIPs described in Section 2.7.2 on page 9.

The following example shows how to configure the upgrade section in the Adapt Cluster Template configuration file:

```
[Upgrade]
LOCAL_UPGRADE_VIP = 10.58.31.17 ALB_OAM
PEER_UPGRADE_VIP = 10.58.30.17 ALB_OAM
LOCAL_REP_VIP = 10.58.31.107 ALB_TRF
PEER_REP_VIP = 10.58.30.107 ALB_TRF
```

Example 1 Upgrade Section Configuration

For more information, refer to the [Adapt Cluster Tool](#) document.

3.6 Upgrade Environment Preparation

The creation of the environment variable is mandatory to execute the upgrade procedure. Create the variable `UPGRADE_BIN_DIR` to point to the bin directory where the SAPC Virtual Delivery Package has been decompressed in the external host machine. The path is `ExternalHostMachine:$ export UPGRADE_BIN_DIR=<SAPC_VDP_DIR>/bin`



For further details on the content of the SAPC Virtual Delivery Software Package, refer to SAPC VNF Descriptor Generator Tool.



4 Upgrade Instructions

This section describes steps to perform the upgrade procedure, so the Destination SAPC vAPP replaces the Origin SAPC vAPP.

4.1 Instantiation of Destination SAPC vAPP

This instantiation can be performed independently of the maintenance window, since it does not imply any changes in the Origin SAPC vAPP.

4.1.1 SAPC Instance Deployment

The first step is to deploy the new SAPC instance by using the delivery package.

Attention!

Dimension the SCs and PLs from the Destination SAPC vAPP the same way as the Origin SAPC vAPP in terms of vCPUs, memory, and disk.

Include the same VIPs defined and managed in the Origin SAPC vAPP in the Adapt Cluster Template Configuration File used to instantiate the Destination SAPC vAPP. Such VIPs include, but not limited to Traffic, OAM, or PROV.

4.1.2 Connection to External Networks

Connectivity configuration to the external networks is required to ensure the access to the upgrade VIPs from both the Origin and Destination SAPC vAPP instances once the deployment of the Destination SAPC vAPP is completed.

Configuration of the IP routes for the upgrade VIPs from both the Origin and the Destination SAPC vAPP instances in the gateway router is described in Section 2.7.3 on page 10.

After configuring the Gateway Routers, the only VIP available from the external host machine is the Local Upgrade VIP in the Destination SAPC vAPP. This VIP is the one used to operate and manage the Destination SAPC vAPP at this point. The rest of the upgrade VIPs are created according to any other requirements during the Upgrade Execution.



4.1.3 Destination SAPC vAPP Scale-Out

The Destination SAPC vAPP requires to have the same amount of PL as the Origin SAPC vAPP prior to executing the upgrade procedure. If the Origin SAPC vAPP has more than 2 PLs, the Destination SAPC vAPP requires to be scaled out until it reaches the same number of PLs. For scaling out each new PL refer to [Configure Scale Out](#).

4.2 Upgrade Execution

4.2.1 Quickstart

The system gathers the minimum configuration information to execute the upgrade by replacement commands during the quickstart procedure, and creates the workspace on the storage where the commands run.

Attention!

Execution of the quickstart is strictly permitted in an empty directory.

Provide the following details:

- OAM virtual IP of SAPC Origin vAPP deployment
- Local upgrade virtual IP of the Destination SAPC vAPP deployment
- Path of the ssh public key file in the external host machine required to perform the upgrade procedure

Follow the instructions to launch the quickstart process:

1. Create a directory for the upgrade workspace in the external host machine.

```
ExternalHostMachine:$ mkdir upgrade_workspace
```

2. Move it to the workspace directory.

```
ExternalHostMachine:$ cd upgrade_workspace
```

3. Execute the quickstart command within the upgrade workspace:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade quickstart
.
.
.
Enter OAM VIP for origin SAPC deployment: <OAM_VIP>
.
.
```



```

Enter Upgrade VIP for destination SAPC deployment: <LOCAL_UPGRADE_VIP>
.
.
Enter the private-key file path [ ~/.ssh/id_rsa ]: <press enter to use default path>
.
.
The upgrade procedure should stop in babysitting step (y/n) [n]: <select y to set a babysitting period>

```

4. The following files created in the upgrade workspace:

context db	This file contains the configuration information and the progress of the upgrade procedure.
events.log	This file contains a high-level report of the actions and their results executed in the process. This file can be checked any time during the upgrade procedure.
traces.log	This file contains low-level traces that are used to resolve failures occurring at the upgrade procedure.

Execute the following command for more information on quickstart:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade quickstart -h
```

4.2.2 Initiate Execution

This section describes how to start the Upgrade Execution stage, and what actions take place until the incoming traffic towards the Destination SAPC vAPP gets redirected from the Origin SAPC vAPP.

Execute the following command from the upgrade workspace to initiate the execution:



```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade run upgrade
```

STEP	EXECUTION
Setup	SCHEDULED
MigrateConfiguration	SCHEDULED
AddDBReplication	SCHEDULED
PrepareNetworkReconfiguration	SCHEDULED
ReconfigureNetwork	SCHEDULED
ConsolidateNetworkReconfiguration	NOT SCHEDULED
MigrateData	NOT SCHEDULED
StartBabysitting	NOT SCHEDULED
ConsolidateVNF	NOT SCHEDULED

SCHEDULED: Step to be run in this iteration

NOT SCHEDULED: Step not to be run in this iteration

DONE: Step already run

do you want to proceed? (y/n) [y]: <press enter to proceed>

Example 2 Initiate Execution

The scheduled steps of this process are the following:

Setup

This step performs a health check in both SAPC instances, and retrieves information about the upgrade from the Destination SAPC vAPP. It also creates the Peer Upgrade VIP in the Origin SAPC vAPP.

MigrateConfiguration

This step extracts all the configuration information from the Origin SAPC vAPP and set it in the Destination SAPC vAPP according to the new software version.

AddDbReplication

This step creates the Replication VIPs and establishes a replication channel between both the Origin and the Destination SAPC vAPP instances to synchronize provisioning and session data.

PrepareNetworkReconfiguration

This step checks if the OAM and Traffic VIPs are activated in the Destination SAPC vAPP before redirecting the traffic.

ReconfigureNetwork

This step pauses the procedure until the operator completes the reconfiguration of the IP routes in the gateway router, so the incoming traffic can be redirected towards the Destination SAPC vAPP.



If the scheduled steps are executed successfully, the following messages appear on the console output of the external host machine:

```
UPGRADE - Setup (1/5) [SUCCESS] 04s
UPGRADE - MigrateConfiguration (2/5) [SUCCESS] 04s
UPGRADE - AddDBReplication (3/5) [SUCCESS] 04s
UPGRADE - PrepareNetworkReconfiguration (4/5) [SUCCESS] 01s
UPGRADE - ReconfigureNetwork (5/5) [SUCCESS] 04s
```

```
Destination SAPC is ready to process incoming traffic.
Please reconfigure static routes now.
When you are done, execute "upgrade run upgrade --continue"
```

Example 3 Upgrade Execution output message

Warning!

DBS, NR, Network Redundancy with Schema Difference

Once the replication is enabled, this alarm message may appear. No actions are needed. The alarm is normal and will be automatically removed when the upgrade completes.

4.2.3 Reconfigure Network

The Upgrade Execution disrupts the process at the ReconfigureNetwork step as described in Section 4.2.2 on page 19. The Destination SAPC vAPP is ready to process the incoming traffic at this point. The new IP routes are mandatory to be configured in the gateway routers according to Section 2.7.3 on page 10.

If the new IP routes are committed in the gateway routers, all the connection from the neighboring peer nodes is cut and reestablished towards the Destination SAPC vAPP. All traffic is processed by the new SAPC instance at this point.

If the traffic is properly managed by the Destination SAPC vAPP after the reconfiguration, the upgrade procedure can be continued to complete the migration of non-critical information, such as measures or log files from the Origin SAPC vAPP. If the new instance is not able to manage the incoming traffic as expected, the rollback procedure can be initiated to restore the conditions prior to the upgrade.

Execute the following command from the upgrade workspace to continue with the upgrade procedure after the network reconfiguration is successful:



```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade run upgrade --continue
```

STEP	EXECUTION
Setup	DONE
MigrateConfiguration	DONE
AddDBReplication	DONE
PrepareNetworkReconfiguration	DONE
ReconfigureNetwork	DONE
ConsolidateNetworkReconfiguration	SCHEDULED
MigrateData	SCHEDULED
StartBabysitting	SCHEDULED
ConsolidateVNF	NOT SCHEDULED

SCHEDULED: Step to be run in this iteration

NOT SCHEDULED: Step not to be run in this iteration

DONE: Step already run

do you want to proceed? (y/n) [y]: <press enter to proceed>

Example 4 Reconfigure Network

The scheduled steps of this process are the following:

ConsolidateNetworkReconfiguration

This step checks if the OAM VIP is pointing to the correct version of SAPC vAPP after the network reconfiguration.

MigrateData

This step copies data files, measures, and other non-critical information from the Origin SAPC vAPP to the Destination SAPC vAPP.

StartBabysitting

This step pauses the procedure until the operator decides if the upgrade was successful or if a rollback is necessary. This decision is based on performance monitoring of the Destination SAPC vAPP.

If the scheduled steps are executed successfully, the following messages appear on the console output of the external host machine:

```
UPGRADE - ConsolidateNetworkReconfiguration (1/3) [SUCCESS] 04s
UPGRADE - MigrateData (2/3) [SUCCESS] 04s
UPGRADE - StartBabysitting (3/3) [SUCCESS] 01s
```

Destination SAPC is ready to process incoming traffic.
Please reconfigure static routes now.
When you are done, execute "upgrade run upgrade --continue"

Example 5 Network reconfiguration output message



4.2.4 Babysitting

This is an optional step that can be configured at the quickstart.

Execute the following command from the upgrade workspace to complete babysitting phase:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade run upgrade --continue
```

STEP	EXECUTION
=====	=====
Setup	DONE
-----	-----
MigrateConfiguration	DONE
-----	-----
AddDBReplication	DONE
-----	-----
PrepareNetworkReconfiguration	DONE
-----	-----
ReconfigureNetwork	DONE
-----	-----
ConsolidateNetworkReconfiguration	DONE
-----	-----
MigrateData	DONE
-----	-----
StartBabysitting	DONE
-----	-----
ConsolidateVNF	SCHEDULED
-----	-----

```
SCHEDULED: Step to be run in this iteration
NOT SCHEDULED: Step not to be run in this iteration
DONE: Step already run

do you want to proceed? (y/n) [y]: <press enter to proceed>
```

Example 6 Babysitting

The scheduled step of this process is:

ConsolidateVNF This step removes the replication channel between both the Origin and the Destination SAPC vAPP instances and all the extra configuration related to the upgrade procedure in the new instance.

If this step executes successfully, the following messages appear on the console output of the external host machine:

```
UPGRADE - ConsolidateVNF (1/1) [SUCCESS] 04s
    Upgrade successfully completed.
    Congratulations
```

Example 7 Babysitting output message

If the upgrade completes successfully, it is recommended to obtain the upgrade report and check that the events of interest occurred during the procedure, particularly if any warning appeared during the upgrade, since warnings imply manual intervention to resolve the issues in most cases. The Upgrade Execution provides useful information of the errors and warnings in the following files: `traces.log` and `events.log` allocated in the upgrade workspace path.



Execute the following command from the upgrade workspace to get the upgrade report:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade show report
```

```
#####
# UPGRADE STATUS #
#####
```

Start	Elapsed Time	Upgrade Status	Current Step
2018-05-29 09:39:48	1:21:55	UPGRADED	-

```
#####
# UPGRADE REPORT #
#####
```

Upgrade	Status	Start	Elapsed Time
Setup	SUCCESS	2018-05-29 09:39:48	0:02:10
MigrateConfiguration	SUCCESS	2018-05-29 09:41:58	0:12:16
AddDBReplication	SUCCESS	2018-05-29 09:54:14	0:01:47
PrepareNetworkReconfiguration	SUCCESS	2018-05-29 09:56:01	0:00:00
ReconfigureNetwork	SUCCESS	2018-05-29 09:56:02	0:00:00
ConsolidateNetworkReconfiguration	SUCCESS	2018-05-29 10:33:38	0:00:51
MigrateData	SUCCESS	2018-05-29 10:34:30	0:02:46
StartBabysitting	SUCCESS	2018-05-29 10:37:17	0:01:36
ConsolidateVNF	SUCCESS	2018-05-29 10:59:38	0:02:05

```
#####
# EVENTS OF INTEREST #
#####
```

Example 8 Upgrade Workspace

4.3 Decommission of Origin SAPC vAPP

Decommissioning of the Origin SAPC vAPP can be done out of the maintenance window. Refer to [SAPC VNF Decommissioning Instruction for OpenStack](#), and [SAPC VNF Decommissioning Instruction for VMware](#) to perform the decommissioning process.



5 Post-Upgrade Activities

This section describes the tasks to manage after the upgrade is completed.

5.1 Update SAPC Version in OSS/ENM

Update the software version of the Destination SAPC vAPP in Operations Support System (OSS) and Ericsson Network Manager (ENM).

5.2 Remove IP Routes

If the upgrade procedure is completed, remove all the IP routes registered in the gateway routers for the extra VIPs used during the Upgrade Execution, as these are removed automatically from the SAPC vAPP as part of the upgrade by replacement procedure.

5.3 Entities with External Subscriber Repository

Attention!

In external subscriber repository deployments, only when there are new attributes for existing entities, or new entities that are eligible to be configured in an external repository (see [SAPC 1 Network Impact Report](#)), update their `fieldDef` definition and URL as necessary. For detailed information on how to update the `fieldDef` block and the URL, see [Integration in User Data Consolidation and Database Access](#).





6 Rollback Procedure

This section describes the rollback concept and activities necessary to revert to the source SAPC software version in the Origin SAPC vAPP if the upgrade fails. The chapter also includes the description of the different types of rollback that can be invoked during the upgrade by replacement procedure.

Rollback is a process that returns to the Origin SAPC vAPP with the original configuration and performance. This process executes the rollback activities defined for each upgrade step in reverse order. The rollback procedure also stops whenever the intervention of the user is needed.

If a rollback procedure is performed for any reason, decommission the Destination SAPC vAPP before restarting the Upgrade Procedure.

6.1 Automatic Rollback

The upgrade command automatically executes a rollback procedure if an error occurs during the Upgrade Execution. The rollback procedure reverses the actions performed in each of the upgrade steps until the failed step.

Note: The interval of the automatic rollback procedure is approximately 10 minutes.

The following example shows the console output from the external host machine in case an error occurs during the upgrade:

```
UPGRADE - Setup (1/4) [SUCCESS] 04s
UPGRADE - MigrateConfiguration (2/4) [SUCCESS] 04s
UPGRADE - AddDBReplication (3/4) [ERROR] 03s

Upgrade procedure has failed.
Collecting information 02m 38s
Automatically starting rollback procedure.

ROLLBACK - AddDBReplication (1/3) [SUCCESS] 03s
ROLLBACK - MigrateConfiguration (2/3) [SUCCESS] 04s
ROLLBACK - Setup (3/3) [SUCCESS] 04s

Rollback successfully completed
```

Example 9 Upgrade error message

If an automated rollback happens because of an error, the upgrade procedure collects information from both the Origin and the Destination SAPC vAPP instances, and stores the data in the upgrade workspace for troubleshooting purposes.



6.2 On-Demand Rollback

If an issue occurs in the upgrade steps that imply manual interaction, like ReconfigureNetwork or StartBabysitting the upgrade command stops, and requests the operator to intervene and start the rollback procedure.

Note: The interval of the on-demand rollback procedure is approximately 2 minutes.

Instructions follow as:

1. Go to the upgrade workspace.
2. Execute the following command:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade rollback
```

STEP	ROLLBACK
StartBabysitting	SCHEDULED
MigrateData	SCHEDULED
ConsolidateNetworkReconfiguration	SCHEDULED
ReconfigureNetwork	SCHEDULED
PrepareNetworkReconfiguration	NOT SCHEDULED
AddDBReplication	NOT SCHEDULED
MigrateConfiguration	NOT SCHEDULED
Setup	NOT SCHEDULED

```

-----
SCHEDULED: Step to be rolled-back in this iteration
NOT SCHEDULED: Step not to be rolled-back in this iteration

Do you want to proceed? (y/n) [y]:
ROLLBACK - StartBabysitting (1/4) [SUCCESS] 01s
ROLLBACK - MigrateData (2/4) [SUCCESS] 01s
ROLLBACK - ConsolidateNetworkReconfiguration (3/4) [SUCCESS] 01s
ROLLBACK - ReconfigureNetwork (4/4) [SUCCESS] 01s

Origin SAPC is ready to process incoming traffic again.
Please reconfigure static routes now.
When you are done, execute "upgrade run rollback --continue"
```

6.3 Execute Rollback Procedure

The rollback procedure reverses the actions performed step by step. It pauses whenever intervention of the user is needed. For example, manual redirection of the incoming traffic from the Destination SAPC vAPP to the Origin SAPC vAPP is required from the user.

Follow the instructions to resume the rollback:

1. Go to the upgrade workspace.



2. Execute the following command:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade run rollback --continue
```

```

STEP                               ROLLBACK
=====
PrepareNetworkReconfiguration      SCHEDULED
-----
AddDBReplication                   SCHEDULED
-----
MigrateConfiguration               SCHEDULED
-----
Setup                              SCHEDULED
-----
SCHEDULED: Step to be run in this iteration.
NOT SCHEDULED: Step not to be run in this iteration.

Do you want to proceed? (y/n) [y]: y

ROLLBACK - PrepareNetworkReconfiguration (1/4) [SUCCESS] 01s
ROLLBACK - AddDBReplication (2/4) [SUCCESS] 16s
ROLLBACK - MigrateConfiguration (3/4) [SUCCESS] 01s
ROLLBACK - Setup (4/4) [SUCCESS] 05s

```

Rollback successfully finished.

Follow the instructions to continue with the rollback procedure after the IP routes are reestablished to get to the Origin SAPC vAPP again:

```
ExternalHostMachine:$ $UPGRADE_BIN_DIR/upgrade run rollback --continue
```

```

STEP                               ROLLBACK
=====
PrepareNetworkReconfiguration      SCHEDULED
-----
AddDBReplication                   SCHEDULED
-----
MigrateConfiguration               SCHEDULED
-----
Setup                              SCHEDULED
-----
SCHEDULED: Step to be run in this iteration.
NOT SCHEDULED: Step not to be run in this iteration.

Do you want to proceed? (y/n) [y]: y

ROLLBACK - PrepareNetworkReconfiguration (1/4) [SUCCESS] 01s
ROLLBACK - AddDBReplication (2/4) [SUCCESS] 16s
ROLLBACK - MigrateConfiguration (3/4) [SUCCESS] 01s
ROLLBACK - Setup (4/4) [SUCCESS] 05s

```

Rollback successfully finished.

Example 10 Rollback procedure





7 Troubleshooting

The following files are relevant in case of a troubleshooting process:

context db	This file contains the configuration information and the progress of the upgrade procedure.
events.log	This file contains a high-level report of the actions and their results executed during the process. This file can be checked during the upgrade procedure any time.
traces.log	This file contains low-level traces that are used to resolve failures occurring during the upgrade procedure.
origin_sapc_collect_info.tgz and destination_sapc_collect_info.tgz	These files contain SAPC collect information for the Origin and Destination vAPPs compiled just before an automatic rollback error occurs.

There are some unexpected situations that are identified as **warnings** based on the severity of the effect, therefore these do not provoke an automatic rollback. This means that the failure of certain steps is classified as warning instead of error. One example is the failure of the `MigrateData` step, which can cause that some data files, measures, and other non-critical information would not be copied from the Origin SAPC vAPP to the Destination SAPC vAPP.