

System Upgrade to Ericsson Dynamic Activation 1

Ericsson Dynamic Activation 1

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017. 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	Introduction	1
1.1	Purpose and Scope	1
1.2	Target Group	1
1.3	Typographic Conventions	1
1.4	Prerequisites	1
1.5	Pre-Upgrade Checklist (Native Deployment)	3
2	General Upgrade Information	5
2.1	Hardware Migration	5
2.2	Upgrade Paths	5
2.2.1	From Native Deployment	5
2.2.2	From Virtual Multi Activation Deployment	9
3	Upgrading from Native Multi Activation 16.0 Using SCXB2, NWI-E, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Keeping the GEP3 Blades	11
3.1	General Upgrade Process	11
3.2	Generate License Key Values	13
3.3	Backup	14
3.3.1	System Backup	14
3.3.2	Hardware Configuration Backup	15
3.3.3	SSL Certificate Backup (Optional)	17
3.4	Upgrade Procedure	17
3.4.1	Upgrade Preparations	17
3.4.2	Adapt cluster.conf, and evip.xml for Dynamic Activation 1	17
3.4.3	BSP 8100 Installation and Configuration	18
3.4.4	Network Setup Check	20
3.4.5	Dynamic Activation Upgrade Instructions	20
3.5	Upgrade Cassandra	23
3.6	Creating Administrative Users	24
3.7	Rollback to Multi Activation 16.0 on Native Deployment, using SCXB2, NWI-E, GEP3, and DMX 3.1	24
3.7.1	Rollback Cassandra	24
3.7.2	Rollback the Multi Activation Software	24
3.7.3	Rollback cluster.conf and evip.xml	25
3.7.4	Hardware Replacement	26
3.7.5	Health Check	26



4	Upgrading from Native Multi Activation 16.0 Using SCXB2, NWI-E, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Upgrading to GEP5 Blades	27
4.1	General Upgrade Process	27
4.2	Migrate/Backup	29
4.2.1	Migrate/Backup Configuration from existing Multi Activation 16.0 System	29
4.2.2	System Backup	29
4.2.3	Hardware Configuration Backup	29
4.2.4	SSL Certificate Backup (Optional)	31
4.3	Hardware Configuration	31
4.3.1	CMXB3, SCXB3, and GEP5 Hardware	31
4.4	Software Installation	33
4.5	Restore Configuration	33
4.6	Rollback to Multi Activation 16.0 on Native Deployment, using SCXB2, NWI-E, GEP3 (downgrading from GEP5 to GEP3 Blades), and DMX 3.1	33
5	Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Keeping the GEP3 Blades	35
5.1	General Upgrade Process	35
5.2	Backup	37
5.2.1	System Backup	37
5.2.2	Hardware Configuration Backup	38
5.3	Upgrade Procedure	39
5.3.1	Upgrade Preparations	39
5.3.2	Adapt cluster.conf, and evip.xml for Dynamic Activation 1	39
5.3.3	BSP 8100 Installation and Configuration	40
5.3.4	Network Setup Check	41
5.3.5	Dynamic Activation Upgrade Instructions	42
5.4	Upgrade Cassandra	45
5.5	Creating Administrative Users	46
5.6	Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP3, and DMX 3.1	46
5.6.1	Rollback Cassandra	46
5.6.2	Rollback the Multi Activation Software	46
5.6.3	Rollback cluster.conf and evip.xml	47
5.6.4	Hardware Replacement	47
5.6.5	Restore DMX	48
5.6.6	Health Check	48
6	Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Upgrading to GEP5 Blades	49
6.1	General Upgrade Process	49



6.2	Migrate/Backup	51
6.2.1	Migrate/Backup Configuration from existing Multi Activation 16.0 System	51
6.2.2	System Backup	51
6.2.3	Hardware Configuration Backup	51
6.2.4	SSL Certificate Backup (Optional)	52
6.3	Hardware Configuration	53
6.3.1	CMXB3, SCXB3, and GEP5 Hardware	53
6.4	Software Installation	54
6.5	Restore Configuration	54
6.6	Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP3 (downgrading from GEP5 to GEP3 Blades), and DMX 3.1	55
6.6.1	Hardware Replacement	55
6.6.2	Restore DMX	55
7	Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP5, and DMX 3.1, to Native Dynamic Activation 1, Keeping the GEP5 Blades	57
7.1	General Upgrade Process	57
7.2	Backup	59
7.2.1	System Backup	59
7.2.2	Hardware Configuration Backup	60
7.3	Upgrade Procedure	61
7.3.1	Upgrade Preparations	61
7.3.2	Adapt cluster.conf, and evip.xml for Dynamic Activation 1	61
7.3.3	BSP 8100 Installation and Configuration	62
7.3.4	Network Setup Check	64
7.3.5	Dynamic Activation Upgrade Instructions	64
7.4	Upgrade Cassandra	67
7.5	Creating Administrative Users	68
7.6	Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP5, and DMX 3.1	68
7.6.1	Rollback Cassandra	68
7.6.2	Rollback the Multi Activation Software	68
7.6.3	Rollback cluster.conf and evip.xml	69
7.6.4	Hardware Replacement	70
7.6.5	Restore DMX	70
7.6.6	Health Check	70
8	Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP5, and BSP 8100, to Native Dynamic Activation 1, Keeping the GEP5 Blades	71
8.1	General Upgrade Process	71
8.2	Backup	73
8.2.1	System Backup	73



8.2.2	Backup of evip.xml	74
8.3	Upgrade Procedure	74
8.3.1	Upgrade Preparations	74
8.3.2	BSP 8100 Upgrade Instructions	76
8.3.3	Dynamic Activation Upgrade Instructions	76
8.4	Network Setup Check	80
8.5	Upgrade Cassandra	81
8.6	Creating Administrative Users	81
8.7	Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP5, and BSP 8100	81
8.7.1	Rollback Cassandra	82
8.7.2	Rollback the Multi Activation Software	82
8.7.3	Health Check	82
9	Upgrading from Native Multi Activation 16.1 or 16.2 Using SCXB3, CMXB3, GEP3/GEP5, and BSP 8100, to Native Multi Activation 1, Keeping the GEP3/GEP5 Blades	85
9.1	General Upgrade Process	85
9.2	Backup	86
9.2.1	System Backup	86
9.2.2	Backup of evip.xml	87
9.3	Upgrade Procedure	87
9.3.1	Upgrade Preparations	87
9.3.2	BSP 8100 Upgrade Instructions	89
9.3.3	Dynamic Activation Upgrade Instructions	89
9.4	Creating Administrative Users	93
9.5	Rollback to Multi Activation 16.1 or 16.2 on Native Deployment, using SCXB3, CMXB3, GEP3/GEP5, and BSP 8100	94
9.5.1	Health Check	94
10	Cassandra Upgrade (Alternative 1)	97
10.1	Cassandra System File-Backup (Optional - Downtime)	98
10.2	Upgrade to Cassandra 2.1.13	100
10.2.1	Logconsolidation Data Retention	100
10.2.2	Upgrade Cassandra to Version 2.1.13 (Without Downtime)	101
10.3	Preparation of Upgrade to Cassandra 2.2.5	103
10.3.1	Logconsolidation Data Retention	104
10.3.2	Upgrade Cassandra (Without Downtime)	105
11	Cassandra Upgrade (Alternative 2)	107
11.1	Remove all Processing Logs in Cassandra	108
11.2	Upgrade Cassandra to Version 2.1.13	110
11.2.1	Upgrade to Cassandra 2.1.13	110



11.3	Upgrade Cassandra to Cassandra 2.2.5	111
11.3.1	Upgrade to Cassandra 2.2.5	112
12	Rollback Cassandra With Processing Logs Backup	113
13	Rollback Cassandra Without Processing Logs Backup	115
14	Upgrading from Virtual Multi Activation 16.0, 16.1 or 16.2 to Virtual Dynamic Activation 1	117
14.1	Prerequisites	117
14.2	General Upgrade Process	118
14.3	Upgrade Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1	118
14.3.1	Data Migration	120
14.3.2	Upgrade Process	120
14.3.3	Creating Administrative Users	126
15	Upgrading from CEE Multi Activation 16.2 to CEE Dynamic Activation 1	127
15.1	Prerequisites	127
15.2	General Upgrade Process	127
15.3	Upgrade Multi Activation 16.2 to Dynamic Activation 1	128
15.3.1	Data Migration	129
15.3.2	Upgrade Process	129
15.3.3	Creating Administrative Users	133
16	Configuration Data Migration	135
16.1	Migrate Configuration	135
16.2	Restore Configuration	136
16.3	CUDB Configuration	137
17	Generate Sentinel License Key Values	139
	Reference List	141





1 Introduction

This document contains instructions regarding how to upgrade to Ericsson Dynamic Activation (EDA) 1.

1.1 Purpose and Scope

The purpose of this document is to provide the readers information on how to upgrade the system from Ericsson Multi Activation (EMA) 16.0, 16.1, or 16.2. to Ericsson Dynamic Activation (EDA) 1.

Note: Upgrade is not supported for Multi Activation 7.1, 7.2 or 15.0 to EDA 1. Instead a maiden installation is required using new hardware.

1.2 Target Group

The following are included in the target group for this document:

- System Administrator
- Network Administrator

For information about the different target groups, see *Library Overview*, Reference [2].

1.3 Typographic Conventions

Typographic conventions are described in the document *Library Overview*, Reference [2].

For information about abbreviations used throughout this document, see *Glossary of Terms and Acronyms*, Reference [1].

1.4 Prerequisites

The following are the prerequisites for upgrading Dynamic Activation and to make full use of this document:

- Make sure to check the Delivery Report before using this document. The Delivery Report contains information about known problems, limitations and exceptions related to the system software that will be upgraded. It can contain complementary instructions and information, that may prevent system failure and damage.



- All hardening applied on the system, for example the LDE etc-overlay-framework rpm, must be removed before proceeding with a system upgrade. Not removing hardening can cause the upgrade to fail, and bring the system in irreversible failed state. In such scenario, a maiden installation is necessary.
- Knowledge about Dynamic Activation.
- Knowledge about Linux™ Distribution Extensions with SUSE (LDEwS) operating system.
- Knowledge about RedHat Enterprise Linux (RHEL) operation system.
- Knowledge about Ericsson Cloud Execution Environment (ECEE)
- Knowledge about Kernel Based Virtualized Machine (KVM)
- Knowledge about VMware
- Knowledge about OpenStack
- Before upgrading to the latest main release, the target system needs to be updated with the latest correction package of the current release. For example, if the target system currently is on Multi Activation 16.2, it needs to have the latest CP package (including EPs) for 16.2 installed, prior to upgrading to Dynamic Activation 1.

Note: Make sure a backup of the system has been performed before starting the upgrade procedure.

- Make sure that all specific system adaptations, modules, and customizations are noted, and add them again after system upgrading.
- Make sure to have a valid Dynamic Activation 1 license in Ericsson License Information System (ELIS).
- Make sure to have all Dynamic Activation 1 related software available.
- Make sure that all configuration templates for Dynamic Activation 1 are prepared before starting the upgrade. (Applies only for Native deployments).

Note: When upgrading from Multi Activation 16.0, 16.1 or 16.2, using SCXB3, CMXB3, GEP3/GEP5 hardware, and BSP 8100 Network Software, only the `evip.xml` file needs to be prepared.

- If Putty is used as terminal, the keyboard should be set to Xterm R6 to get `F<x>` buttons to work to enter GEP3/GEP5 IMPI. (Applies only for Native deployments).



1.5 Pre-Upgrade Checklist (Native Deployment)

This section includes information about what is needed to have in place before conducting an upgrade. Use the table below as a check, prior and during the upgrade.

Table 1 Pre-Upgrade Checklist

	Type	System	SCXB2, NWI-E, GEP3 (Yes)	SCXB3, CMXB3, GEP3 (Yes)	SCXB3, CMXB3, GEP5 (Yes)
Prior Upgrade	Console access	NWI-E RO-00		N/A	N/A
		NWI-E RO-01		N/A	N/A
		SCX-0-0			
		SCX-0-25			
		SC-XX			
		PL-XX			
	Old Software (in case of restore)	NWI-E ⁽¹⁾		N/A	N/A
		DMX/BSP			
		LOTG/LDE			
		Multi Activation			
	New Software	BSP 8100			
		LOTG/LDE			
		Dynamic Activation			
	New Configura tion File	BSP 8100			
		LOTG/LDE			
		eVIP			
	License	Multi Activation ⁽²⁾			
		Dynamic Activation ⁽³⁾			



During Upgrade	Backup (Old system)	NWI-E RO-00		N/A	N/A
		NWI-E RO-01		N/A	N/A
		DMX/BSP			
		vipconfig.xml/ evip.xml			
		cluster.conf			
		Multi Activation ⁽⁴⁾			
		Cabling	Take note of the old cabling	Take note of the old cabling	Take note of the old cabling
		Blade Position	Take note of the old blade position	Take note of the old blade position	Take note of the old blade position

(1) Including ssh module

(2) Old version will be gathered during upgrade

(3) New version

(4) NFS, Zookeeper and config (migrate) backups



2 General Upgrade Information

This section contains general information on configuration data migration and upgrade paths.

Upgrade of Dynamic Activation is done as user `root`.

2.1 Hardware Migration

- **GEP3, CMXB3, SCXB3**

If conducting the installation on a not previously used Dynamic Activation GEP3 system, for example newly purchased one (including subrack, power and fan-modules), perform a maiden installation according to *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6], *Network Description and Configuration for Native Deployment*, Reference [9] and *Software Installation for Native Deployment*, Reference [17].

- **GEP5, CMXB3, SCXB3**

If conducting the installation on a newly purchased Dynamic Activation GEP5 system, for example newly purchased one (including subrack, power and fan-modules), perform a maiden installation according to *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7], *Network Description and Configuration for Native Deployment*, Reference [9] and *Software Installation for Native Deployment*, Reference [17].

Migrate and restore the configuration according to the instructions in Section 16.1 on page 135, and Section 16.2 on page 136. All other sections can be ignored.

2.2 Upgrade Paths

This section contains information about the different upgrade paths supported in Dynamic Activation, both for Native, Virtual, and Cloud deployments.

Note: Cloud deployments consist of both ECEE and OpenStack.

2.2.1 From Native Deployment

Table 2 shows possible upgrade paths between the different Native Dynamic Activation releases.



Attention!

Since DMX 3.1 and SCXB2 are end of support, the only upgrade possible from older Multi Activation version to Dynamic Activation 1, is to upgrade to SCXB3, CMXB3, GEP3/GEP5 hardware, and BSP 8100 network software.

This means that:

- Upgrading from Native Multi Activation 16.0

- Using (SCXB2, NWI-E, GEP3, and DMX 3.1) to Dynamic Activation 1 requires an exchange of SCXB2, NWI-E to SCXB3 and CMXB3, an exchange of the DMX software to BSP 8100 software and configuration, and change of `evip.xml`, and `cluster.conf` files. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.

Upgrade of Cassandra to version 2.2.5.

Note: If this deployment is used, and the GEP3 blades are exchanged to GEP5 blades, migration of processing log data is not supported.

- Using (SCXB3, CMXB3, GEP3, and DMX 3.1) to Dynamic Activation 1 requires an exchange of the DMX software to BSP 8100 software and configuration, and change of `evip.xml`, and `cluster.conf` files. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.

Upgrade of Cassandra to version 2.2.5.

Note: If this deployment is used, and the GEP3 blades are exchanged to GEP5 blades, migration of processing log data is not supported.

- Using (SCXB3, CMXB3, GEP5, and DMX 3.1) to Dynamic Activation 1 requires an exchange of the DMX software to BSP 8100 software and configuration, and change of `evip.xml`, and `cluster.conf` files. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.

Upgrade of Cassandra to version 2.2.5.

- Using (SCXB3, CMXB3, GEP5, and BSP 8100 software and configuration) to Dynamic Activation 1 requires an upgrade of the BSP 8100 software (to latest version), and change of `evip.xml` file. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.

Upgrade of Cassandra to version 2.2.5.



- Upgrading from Native Multi Activation 16.1
 - Using (SCXB3, CMXB3, GEP3, and BSP 8100 software and configuration) to Dynamic Activation 1 requires an upgrade of the BSP 8100 software (to latest version), and change of `evip.xml` file. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.
 - Using (SCXB3, CMXB3, GEP5, and BSP 8100 software and configuration) to Dynamic Activation 1 requires an upgrade of the BSP 8100 software (to latest version), and change of `evip.xml` file. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.
- Upgrading from Native Multi Activation 16.2
 - Using (SCXB3, CMXB3, GEP3, and BSP 8100 software and configuration) to Dynamic Activation 1 requires an upgrade of the BSP 8100 software (to latest version), and change of `evip.xml` file. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.
 - Using (SCXB3, CMXB3, GEP5, and BSP 8100 software and configuration) to Dynamic Activation 1 requires an upgrade of the BSP 8100 software (to latest version), and change of `evip.xml` file. Upgrade of LDE, eVIP, and Multi Activation is handled by the `ema_upgrade` script.
- Upgrading from Native Multi Activation deployment to Virtual or Cloud Dynamic Activation deployment, requires a maiden installation, and data migration.
 - Upgrade from a Native Multi Activation 15.0, 16.0, 16.1 or 16.2 deployment to Virtual or Cloud Dynamic Activation 1 is not supported. However, it is possible to migrate data from a Native Multi Activation deployment to a Virtual Dynamic Activation deployment. To migrate and restore the configuration follow the instructions in Section 16.1 on page 135, and Section 16.2 on page 136.

To install a Virtual Dynamic Activation deployment, follow the instructions in *Software Installation for Virtual and Cloud Deployment*, Reference [16].

Table-explanation:

Find current hardware deployment in the **Existing Deployment** column. Continue to the right to find the target deployment, Network impact and Software impact.



Table 2 Upgrade Paths to Dynamic Activation 1

Release	Existing Deployment		Target Deployment SCXB3, CMXB3, (GEP3/GEP5)			Impact						
						Network			Software/Data			
	HW	SW	GEP 3 (Current)	New	Current	Re-use HW	Network change	Re-cable	Network SW)	Dynamic Activation SW	User/Customizer data	Processing Log Data Cassandra
MA 16.0	SCXB 2, NWI-E	DMX 3.1	x			Yes, GEP3 only.	Yes	Yes	Yes	Upgrade	(1)	(2)
				x		No	Yes	Yes	Yes	Maiden Installation	Migration	(3)
	SCXB 3, CMXB 3	DMX 3.1	x			Yes	Yes	Yes	Yes	Upgrade	(1)	(2)
				x		Yes, New purchased GEP5 only.	Yes	Yes	Yes	Maiden Installation	Migration	(3)
		BSP SW			x	Yes	No	No	Yes, BSP SW upgrade	Upgrade	(1)	(2)
MA 16.1	SCXB 3, CMXB 3	BSP SW	x			Yes	No	No	Yes, BSP SW upgrade	Upgrade	(1)	(2)
					x	Yes	No	No	Yes, BSP SW upgrade	Upgrade	(1)	(2)
MA 16.2	SCXB 3, CMXB 3	BSP SW	x			Yes	No	No	Yes, BSP SW upgrade	Upgrade	(1)	(2)
					x	Yes	No	No	Yes, BSP SW upgrade	Upgrade	(1)	(2)

(1) Userdata handled by the ema_upgrade script.

(2) Migration of processing log data is supported.

(3) Migration of processing log data is not supported.

- **If coming from Native Multi Activation 7.1, 7.2 or 15.0:**

- It will require a maiden installation with newly purchased hardware. Data migration is applicable though according to instructions in Section 16 on page 135. If deciding to reuse old GEP3/GEP5 hardware, rollback is not possible to perform.

- **Upgrading from Native Multi Activation 16.0:**



- Using SCXB2, NWI-E, GEP3, and DMX 3.1, to Native Dynamic Activation 1, and keeping the GEP3 Blades, refer to Section 3 on page 11.
- Using SCXB2, NWI-E, GEP3, and DMX 3.1, to Native Dynamic Activation 1, and upgrading to GEP5 Blades, refer to Section 4 on page 27.
- Using SCXB3, CMXB3, GEP3, and DMX 3.1, to Native Dynamic Activation 1, and keeping the GEP3 Blades, refer to Section 5 on page 35.
- Using SCXB3, CMXB3, GEP3, and DMX 3.1, to Native Dynamic Activation 1, and upgrading to GEP5 Blades, refer to Section 6 on page 49.
- Using SCXB3, CMXB3, GEP5, and DMX 3.1, to Native Dynamic Activation 1, and keeping the GEP5 Blades, refer to Section 7 on page 57.
- Using SCXB3, CMXB3, GEP5, and BSP 8100, to Native Dynamic Activation 1, and keeping the GEP5 Blades, refer to Section 8 on page 71.
- **Upgrading from Native Multi Activation 16.1:**
 - Using SCXB3, CMXB3, GEP3, and 8100, to Native Dynamic Activation 1, and keeping the GEP3 Blades, refer to Section 9 on page 85.
 - Using SCXB3, CMXB3, GEP5, and 8100, to Native Dynamic Activation 1, and keeping the GEP5 Blades, also refer to Section 9 on page 85.
- **Upgrading from Native Multi Activation 16.2:**
 - Using SCXB3, CMXB3, GEP3, and 8100, to Native Dynamic Activation 1, and keeping the GEP3 Blades, refer to Section 9 on page 85.
 - Using SCXB3, CMXB3, GEP5, and 8100, to Native Dynamic Activation 1, and keeping the GEP5 Blades, also refer to Section 9 on page 85.

2.2.2

From Virtual Multi Activation Deployment

- If upgrading from Virtual Multi Activation 7.2 or 15.0 to Virtual or Cloud Dynamic Activation 1, only data migration is applicable, refer to Section 16 on page 135.
- If upgrading from Virtual Multi Activation 15.0, 16.0, 16.1 or 16.2 to Cloud Dynamic Activation 1, only data migration is applicable, refer to Section 16 on page 135.
- If upgrading from Virtual Multi Activation 16.0, 16.1 or 16.2 to Virtual Dynamic Activation 1, refer to Section 14 on page 117.



- If upgrading from CEE Multi Activation 16.2 to CEE Dynamic Activation 1, refer to Section 15 on page 127.
- If upgrading from CEE Multi Activation 16.2 to OpenStack, only data migration is applicable, refer to Section 16 on page 135.



3 Upgrading from Native Multi Activation 16.0 Using SCXB2, NWI-E, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Keeping the GEP3 Blades

This section contains information on how to upgrade from a Native Multi Activation 16.0 system, using SCXB2, NWI-E, GEP3, and DMX 3.1, to Dynamic Activation 1, and keeping the GEP3 Blades.

3.1 General Upgrade Process

An upgrade from Multi Activation 16.0 to Dynamic Activation 1 consists of either one or four maintenance windows, as shown in Figure 1. This depends whether wanting to keep the processing logs in the Cassandra database or not. If keeping the processing logs in the Cassandra database, follow alternative 1 (four maintenance windows), if not keeping the processing logs in the Cassandra database, follow alternative 2.

Note: For alternative 2 there is a possibility to keep the processing logs, by exporting them by use of the Processing Log Admin Tool. This must however be done outside the maintenance window, and before starting the upgrade process.

An import of the exported processing log is not supported.

Choosing Alternative 2 and not keeping the processing logs in the Cassandra database, will impact the **Log Management** feature to not be able to handle those exported logs.

For information on how to export processing log files, refer to section **Processing Log Admin Tool** in *System Administrators Guide for Native Deployment*, Reference [12]



Upgrade Process

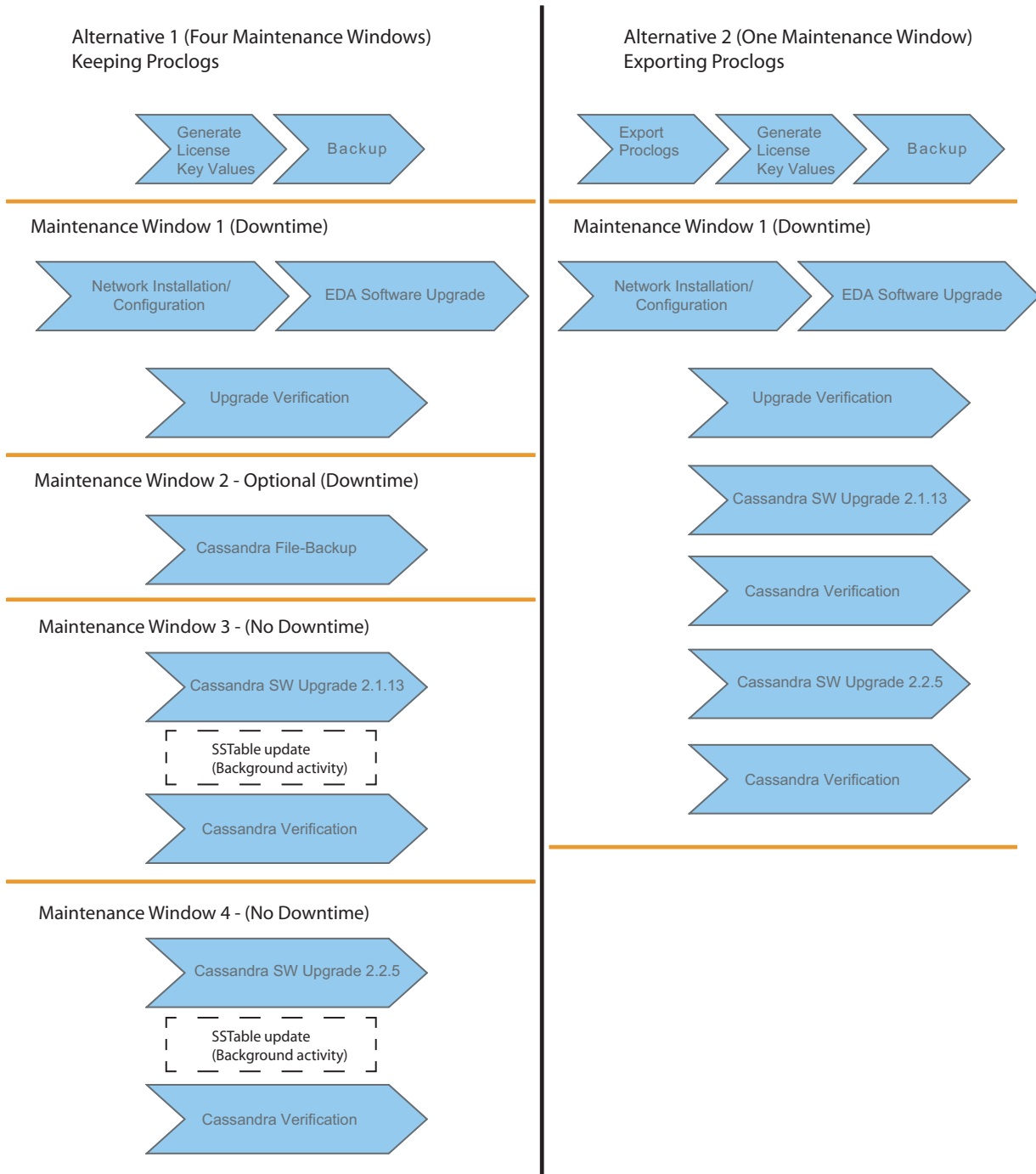


Figure 1 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from Multi Activation 16.0.



An upgrade is an upgrade of all RPMs (including LDE and eVIP), and modules on the current system to a newer software version.

The upgrade and rollback is proceeded with all nodes at once, with downtime. If any previously modified configuration files are affected by the upgrade, they may need to be modified again.

To see if a configuration file is replaced in platform RPMs, look in the `/home/actadm/config/log/config.log` file. Lines with correct date/time containing `Replacing` and `Backing up` are files that have been replaced. The backed up files are located in `/home/actadm/config/backup/<file><date>`

To see if a configuration file is replaced in the modules, look in the `/home/actadm/config/module_config_files/log/config.log` file. Lines with correct date/time containing `<config file> replaced due to new original file`, old file renamed to `<config file>.save` are files that has been replaced. The backed up files are located in `/home/actadm/config/module_config_files/<module>/<config file>.save`

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

Any modules that have been manually added before the upgrade will be removed. After the upgrade, such modules need to be added again (manually).

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters) will be migrated during the upgrade.
- Proclogs

The Proclog migration is handled separately (only applicable if using alternative 1). For details, see Section 10 on page 97.

3.2 Generate License Key Values

This section describes how to prepare a license file for upgrade. This file will be used by the upgrade scrip to install all license files automatically.

On SC-1:

1. Transfer the Dynamic Activation software to the `/var/log/installfiles` directory on SC-1.
2. Change directory:

```
# cd /var/log/installfiles/
```
3. Untar the software (EDA System Base SW):



```
# tar -zxf <Software_Package>.tar.gz
```

4. Obtain the license locking codes for the system.

```
# /var/log/installfiles/<Prod_Number>-<Version>/ema_upgrade generateLicenseInformation
```

Output:

```
INFO - *** Locking codes for <SC-1>:
```

```
INFO - ***
```

```
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Information
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1 : 2008-*1NE URGH T85R V4K4
Locking Code 1 (Old Style) : 2008-292BD
```

```
INFO - *** Locking codes for <SC-2>:
```

```
INFO - ***
```

```
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Information
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1 : 2008-*1PW 65F3 8ABD KJET
Locking Code 1 (Old Style) : 2008-66063
```

5. Provide all Locking Code for the Ericsson License Information System (ELIS) and get the license file.
6. Transfer (SFTP) the license file to the /var/log/installfiles/ directory on SC1, and rename the file to license.txt.

During the upgrade process, the upgrade scrip will use the license.txt file to install all license files.

3.3 Backup

This section contains information on how to perform a backup.

3.3.1 System Backup

Before initiating a system upgrade, a full backup should be performed. Table 3 shows the documentation references for each Multi Activation version.



Table 3 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.0	See specific chapters in Reference [3].

Note: Make sure to have everything in place before the upgrade, according to the *Pre-Upgrade Checklist* in Table 1.

3.3.2 Hardware Configuration Backup

To perform a complete hardware configuration backup, the following backups are needed:

Table 4 Scenario Mapping, Backup

Hardware	DMX, NWI-E, RO-00, and RO-01 configurations	cluster.conf, evip.xml, and Multi Activation license	HSS Validator Plugin (optional)
SCXB2, NWI-E, GEP3	x	x	x

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.

3.3.2.1 Backup of NWI-E, RO-00, and RO-01

Perform a backup of the active configuration, both locally and to a remote Trivial File Transfer Protocol (TFTP) server, on RO-00 and RO-01 respectively. Use VR-Mgmt if the management interface is used for accessing the TFTP server, otherwise use VR-Default.

The `<RO-00-primary>-12_6_1_3` and `<RO-01-primary>-12_6_1_3` file names must match the name of the file stored on the tftp server. Therefore, make sure that there is a file on the tftp server with this name.

1. Save the configuration locally on RO-00:

```
# save configuration <RO-00/01-primary>-12_6_1_3
```

```
Do you want to save configuration to
<RO-00/01-primary>-12_6_1_3.cfg? (y/N)
```

Enter **y** and press **Return**.

```
Saving configuration on master ..... done!
```



Configuration saved to <RO-00/01-primary>-12_6_1_3.cfg successfully.

The current selected default configuration database to boot up the system (primary.cfg) is different than the one just saved (<RO-00/01-primary>-12_6_1_3.cfg).

Do you want to make <RO-00/01-primary>-12_6_1_3.cfg the default database? (y/N)

Enter **n** and press **Return**.

Default configuration database selection cancelled.

2. Save the configuration to a remote TFTP server:

```
# upload configuration <TFTPSEVER> <RO-00/01-primary>-12_6_1_3.cfg vr [VR-Mgmt/VR-Default]
```

3. Repeat step 1 and step 2 for RO-01.

3.3.2.2 Backup of DMX Configuration

Perform a backup of the current configuration and export it to a remote server:

1. Login to the DMXC remote using the <SYSOAM-CNB-IP> on port 2024:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

2. Create a configuration backup:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 save
```

3. Export the configuration backup file to a remote server:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 export filename </path/filename>.bup ipAddress <ip address> username <username>
```

```
password: ****
```

3.3.2.3 Backup cluster.conf, evip.xml, license file, and HSS Validator

Perform a backup of the cluster.conf, evip.xml, HSS Validator Plugin, and applicable license files by transferring them to a remote server.

The cluster.conf file resides in the /cluster/etc directory.

The evip.xml file resides in the /storage/system/config/evip-apr9010467 directory.



The license file `lservrc` resides in the `/home/dveadm/licenses` directory.

The HSS Validator Plugin resides in the `/home/bootloader/repository` directory.

3.3.3 SSL Certificate Backup (Optional)

If an SSL connection has been used, save the certificate keystore to a secure storage.

The keystore file is found in the `/home/asuser/nodes/<nodeId>/domains/dve-domain/config` directory on the PL nodes.

3.4 Upgrade Procedure

This section contains information on how to install and configure BSP 8100, and how to upgrade to the Dynamic Activation software.

Time requirements for installing and configuring BSP 8100 and upgrading to the Dynamic Activation software, if all templates are filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration of BSP 8100 software, and Dynamic Activation software	285 (when all templates are filled in and updated, with downtime)

3.4.1 Upgrade Preparations

- Make sure to have all templates prepared, according to instruction in sections *Accessing Hardware Specific Information* and *Preparing Deployment Artifacts* in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.
- Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

3.4.2 Adapt `cluster.conf`, and `evip.xml` for Dynamic Activation 1

This section contains information on how to adapt the `cluster.conf`, and `evip.xml` files to the BSP 8100 network setup.

Follow the step-list:

1. Go to the `/cluster/etc` directory, back up the old `cluster.conf` file and then remove the file:

```
# cd /cluster/etc
```



```
# cp cluster.conf cluster.conf.ebs
```

```
# rm cluster.conf
```

The backup file `cluster.conf.ebs` can be used for faster rollback if necessary.

2. Create a new `cluster.conf` file, using the template prepared in Section 3.4.1 on page 17.

```
# vi /cluster/etc/cluster.conf
```

3. Reload the `cluster.conf` file on all nodes in the cluster:

```
# cluster config -r -a
```

4. Go to the `/storage/system/config/evip-apr9010467` directory, back up the old `evip.xml` file and then remove the file:

```
# cd /storage/system/config/evip-apr9010467
```

```
# cp evip.xml evip.xml.ebs
```

```
# rm evip.xml
```

The backup file `evip.xml.ebs` can be used for faster rollback if necessary.

5. Create a new `evip.xml` file, using the template prepared in Section 3.4.1 on page 17. This file is to be used later, when upgrading the software.

```
# vi /storage/system/config/evip-apr9010467/evip.xml
```

6. Copy the new `evip.xml` file to the `/var/log/installfiles/` directory. This file is to be used later, when upgrading the software.

```
# cp /storage/system/config/evip-apr9010467/evip.xml  
/var/log/installfiles/evip.xml
```

3.4.3 BSP 8100 Installation and Configuration

This section describes how to install and configure the BSP 8100 software, when upgrading to Dynamic Activation 1. Follow the step-list:

1. Login to the DMXC (remote using the `<SYSOAM-CNB-IP>` on port 2024), and lock all GEP blades in the cluster:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```



Attention!

From now on, all provisioning traffic is down.

2. Power off all GEP blades in the cluster:

DMX 3.1

```
> configure
```

```
% set ManagedElement 1 Equipment 1 Shelf 0 Slot <slot  
position> Blade 1 administrativeState locked
```

```
% commit
```

The *<slot position>* variable corresponds to the slot position of the GEP blade.

3. Replace the SCXB2 and NWI-E blades with the new SCXB3 and CMXB3 blades according to section **Hardware Installation** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.

Attention!

Take note of the position of each blade, in case of a rollback they need to be positioned on the exact position they were extracted from.

Take notice of how the cabling on the current system is setup. In case of a rollback.

4. Re-cable the system according to instructions in section **Cabling and Wiring** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.
5. When the re-cabling is done, continue with the instructions in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.

Start with section **Installation Tools Preparation**, it is not mandatory to perform the **GEP BIOS Settings** section, this section should already have been performed in the first installation of the cluster. Continue with the instructions throughout section **BSP Configuration**.



Attention!

Do not proceed with the **LDEwS Installation**, and the next coming sections. After finishing the **BSP Configuration** section, return to this document and continue with Section 3.4.4 on page 20.

3.4.4 Network Setup Check

Check the network setup according to instructions in **Network Setup Check**, *System Administrators Guide for Native Deployment*, Reference [12].

After the network setup check, continue with the upgrade instructions, see Section 3.4.5 on page 20.

3.4.5 Dynamic Activation Upgrade Instructions

Upgrade to Dynamic Activation 1 only supports **All nodes with downtime**. The upgrade sequence will upgrade LDE, eVIP, and the Dynamic Activation system.

Caution!

Before starting the upgrade procedure, make sure the new value package licenses are ordered for the new EDA 1 system.

3.4.5.1 Dynamic Activation Upgrade Preparations

A provisioning client with `Full` authorities for the Configuration Management Authorities is needed during the upgrade. Add one if not already available. The provisioning client is added in the old Multi Activation GUI, **Access Control>Users** tab. For instructions, refer to section **Access Control** in Reference [24].

On SC-1:

1. Transfer the Dynamic Activation software to the `/var/log/installfiles` directory on SC-1.
2. Change directory:

```
# cd /var/log/installfiles/
```
3. Untar the software (EDA System Base SW):



```
# tar -zxf <Software_Package>.tar.gz
```

3.4.5.2

Dynamic Activation Software Upgrade

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The upgrade needs to be performed as user `root`, and SC-1.

The `ema_upgrade` script will upgrade LDE, eVIP, and issue a reboot. After the reboot, the script will automatically continue to upgrade the Dynamic Activation system and install the new licenses.

1. Upgrade the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema_upgrade upgrade
```

Note: Only **Resource Activation** (in 16.0 - 16.2 called Subscriber Activation (SA)) will be installed.

The following is prompted:

```
All ongoing provisioning will fail during upgrade.  
Are you sure you want to continue with upgrade? (y/n)
```

Enter **y** and press **Enter**

Note: If error message:

```
ERROR - *** IP addresses for OSPF areas differs  
in  
running evip and CMX, must use the same IP  
addresses.  
, check the Delivery Report for current release and add required  
software package.
```

The following is prompted:

```
Please enter provisioning client user name:
```

Enter name of a provisioning user with Full authorities and press **Enter**.

The following is prompted:



```
INFO - *** Please enter your provisioning client
password.
Password:
```

Enter password and press **Enter**.

2. To know when the upgrade is finished, after the reboot, login as user `root` on SC-1, and perform a tail on the `/var/log/ema/ema.log` file:

```
# tail -f /var/log/ema/ema.log
```

When the following is prompted, continue with the next step in the step-list:

```
- upgradehandler - INFO - *** Upgrade finished

- ema - DEBUG - INPUT: /var/log/installfiles/<Prod_Number>-<Version>/ema post_upgrade: Duration: xx seconds
```

3. Check the `/home/actadm/config/log/config.log` and `/home/bootloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.
4. Log out and log in again to receive all the updated environment variables.
5. Check the result of the latest system status.

Run the following command:

```
# healthcheck.py show -d
```

Note: If any problems appear, check any created logs during the upgrade phase:

- Before reboot:

```
/var/log/ema/ema_upgrade.log
```

- After reboot:

```
/var/log/ema/ema_post_upgrade-console.log
```

```
/var/log/ema/ema.log
```

- Installation of new modules after reboot:

```
/var/log/bootloader/bootloader.log
```

6. Run CAI3G test traffic.

Run test traffic on ports (8080, 8181) to verify the updated nodes.



Note: In UDC specific solution, make sure that the HSS validator plug-in is installed or upgraded correctly. For more information, refer to refer to *System Administrators Guide for Native Deployment*, Reference [12].

Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.

Caution!

After the Dynamic Activation software upgrade is finished, it is important not to remove the `/var/log/installfiles` directory. Some files in this directory are used for rollback purposes.

Continue with the Cassandra upgrade, see Section 3.5 on page 23.

3.5 Upgrade Cassandra

Attention!

Before continuing with the upgrade of Cassandra, make sure the system works as expected. If proceeding with the Cassandra upgrade, it is not possible to perform a complete restore of the Dynamic Activation application.

If alternative 1 has been chosen (keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 10 on page 97.

If alternative 2 has been chosen (not keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 11 on page 107.

After the upgrade procedure is finished, verify the Cassandra upgrade as follows:

1. Fetch several proclogs to check if they are stored properly.
2. Check Cassandra status and performance by using `nodetool` commands. For command details, refer to *System Administrators Guide for Native Deployment*, Reference [12].
3. Run CAI3G test traffic.



Run test traffic on ports (8080, 8181) to verify the updated nodes.

Note: In UDC specific solution, make sure that the HSS validator plug-in is installed or upgraded correctly. For more information, refer to *System Administrators Guide for Native Deployment*, Reference [12].

Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.

3.6 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users > Create Administrative User** in *System Administrators Guide for Native Deployment*, Reference [12].

3.7 Rollback to Multi Activation 16.0 on Native Deployment, using SCXB2, NWI-E, GEP3, and DMX 3.1

This section contains information on how to perform a rollback from Dynamic Activation 1 to Multi Activation 16.0 on Native Deployment, using SCXB2, NWI-E, GEP3 hardware, and DMX 3.1 network software.

To perform a rollback, follow the subsections.

3.7.1 Rollback Cassandra

Attention!

To be able to perform a software rollback to Multi Activation 16.0, Cassandra needs to be in revision 2.0.15. If a Cassandra upgrade has been performed, roll back Cassandra according to Section 12 on page 113 or Section 13 on page 115 before proceeding with the instructions in Section 3.7.2 on page 24.

3.7.2 Rollback the Multi Activation Software

To perform a rollback of the Dynamic Activation software, follow the step-list:

1. Rollback the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```




```
# ./ema rollback
```

The following is prompted:

```
All ongoing provisioning will fail during rollback.  
Are you sure you want to continue with rollback? (y/n)
```

Enter **y** and press **Enter**

2. The `ema` script will roll back LDE, eVIP, and the Dynamic Activation system, and issue a reboot.

Login as user `root` on SC-1, and wait for the system to be fully installed.

Check system status by running `bootloader.py` and `3ppmon` commands.

3. Check the `/home/dveadm/config/log/config.log` and `/home/bootloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.

3.7.3

Rollback `cluster.conf` and `evip.xml`

This section contains information on how to rollback the `cluster.conf` and `evip.xml` files to the previous network setup.

Follow the step-list:

1. Go to the `/cluster/etc` directory, and remove the `cluster.conf` file:

```
# cd /cluster/etc
```

```
# rm cluster.conf
```

2. Restore the old `cluster.conf` file. Use the `cluster.conf` file that was backed up before the upgrade.

```
# vi /cluster/etc/cluster.conf
```

3. Reload the `cluster.conf` file on all nodes in the cluster:

```
# cluster config -r -a
```

4. Go to the `/storage/system/config/evip-apr9010467/` directory, and remove the `evip.xml` file:

```
# cd /storage/system/config/evip-apr9010467/
```

```
# rm evip.xml
```

5. Restore the old `evip.xml` file. Use the `evip.xml` file that was backed up before the upgrade.

```
# vi /storage/system/config/evip-apr9010467/evip.xml
```



6. Power off the subrack.

3.7.4 Hardware Replacement

1. Replace the SCXB3, and CMXB3 blades with the old SCXB2, and NWI-E blades. Insert the old blades in the exact position as they were before the upgrade.
2. Reset the cables to the exact position as they were before the upgrade.
3. Power on the subrack.

3.7.5 Health Check

Perform a health-check according to instructions in the step-list below.

1. Run the complete health-checks according to instructions in sections **Health Check on Multi Activation Common** and **Health Check on Multi Activation EBS 1.0 HW with DMX 3.1** in Reference [20].
2. Run CAI3G test traffic.

Run test traffic on test ports (8080, 8181) to verify the rolled back nodes.



4 Upgrading from Native Multi Activation 16.0 Using SCXB2, NWI-E, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Upgrading to GEP5 Blades

This section contains information on how to upgrade from Native Multi Activation 16.0 (using SCXB2, NWI-E, GEP3, and DMX 3.1), to Dynamic Activation 1, and upgrading to GEP5 Blades.

4.1 General Upgrade Process

An upgrade of Multi Activation consists of one maintenance window, as shown in Figure 2.

Upgrade Process

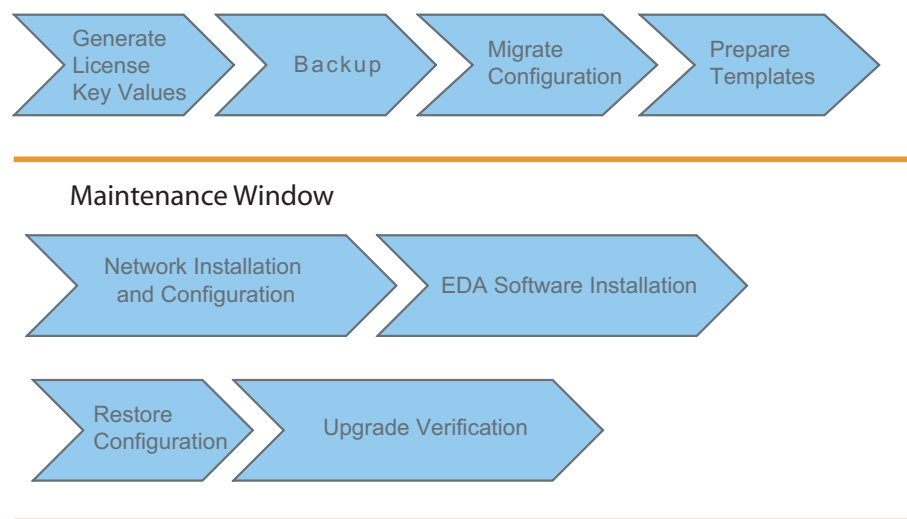


Figure 2 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from a previous Multi Activation version:

- The Linux Distribution Extensions (LDE), and the evolved Virtual Internet Protocol (eVIP) solutions require a maiden installation with data migration to be performed.



- Due to the new LDE features and the re-partitioning of the file structure, the cluster nfs partition that prior to the upgrade was approximately 80 GB, will decrease to a storage area of approximately 40 GB.

The following parts are migrated in the upgrade process:

- Multi Activation configuration (application users, network elements, license counters)

The following parts are not migrated in the migration process:

- ESA configuration files

See *System Administrators Guide for Native Deployment*, Reference [12] for information on how to configure trap destination. If any other customer specific configuration has been done, this needs to be migrated, see **Migration Methods in ESA Upgrade Instruction** Reference [13].

- Proclogs
- Customized changes in system level files, for example Linux users, groups, and crontab.

This means, for example, that all crontab jobs are removed and recreated according to default setup for the latest target Multi Activation version.

Linux users related to the Multi Activation application are recreated as part of the upgrade procedure. If any other customer specific Linux users have been created, these are not migrated. To recreate specific Linux users, see chapter **User and Group Management** in Reference [10].

The following parts are not migrated in the migration process but backed up in the tar file `pgconfigbackup-*.tar.gz`:

- Other Multi Activation configuration files, `log4j.xml`, `cli.properties`, `core.properties` and `iptables-rules-custom.cfg`.
- The Centralized User Database (CUDB) configuration files.

For example `CUDBConfig_HLRAUC.xml`

- All present notification rules files (`NotificationRulesDae.xml`, `NotificationRulesIms.xml`, `NotificationRulesEps.xml`)

Limitations:

- Changes performed after completing the backup on the old system are not migrated, for example license counters.



4.2 Migrate/Backup

This section contains information on how to perform a backup and data migration.

4.2.1 Migrate/Backup Configuration from existing Multi Activation 16.0 System

To migrate/backup existing configuration to be used on the upgraded Dynamic Activation 1 system, follow the instructions in Section 16.1 on page 135.

Note: This backup will later be used to restore existing configuration on the upgraded Dynamic Activation 1 system

4.2.2 System Backup

Before initiating a system upgrade, a full backup should be performed. Table 5 shows the documentation references for each Multi Activation version. These backups will be used if the upgrade fails, and a rollback needs to be performed

Table 5 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.0	See specific chapters in Reference [3].

4.2.3 Hardware Configuration Backup

To perform a complete hardware configuration backup, the following backups are needed:

Table 6 Scenario Mapping, Backup

Hardware/Controller	DMX, NWI-E, RO-00, and RO-01 configurations	cluster.conf, vipconfig.xml /evip.xml, and Multi Activation license	HSS Validator Plugin (optional)
SCXB2, NWI-E/DMXC	x	x	x

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.



4.2.3.1 Backup of NWI-E, RO-00, and RO-01

Perform a backup of the active configuration, both locally and to a remote Trivial File Transfer Protocol (TFTP) server, on RO-00 and RO-01 respectively. Use VR-Mgmt if the management interface is used for accessing the TFTP server, otherwise use VR-Default.

The `<RO-00-primary>-12_6_1_3` and `<RO-01-primary>-12_6_1_3` file names must match the name of the file stored on the tftp server. Therefore, make sure that there is a file on the tftp server with this name.

1. Save the configuration locally on RO-00:

```
# save configuration <RO-00/01-primary>-12_6_1_3
```

```
Do you want to save configuration to
<RO-00/01-primary>-12_6_1_3.cfg? (y/N)
```

Enter **y** and press **Return**.

```
Saving configuration on master ..... done!
```

```
Configuration saved to <RO-00/01-primary>-12_6_1_3.cfg
successfully.
```

```
The current selected default configuration database to
boot up the system
(primary.cfg) is different than the one just saved
(<RO-00/01-primary>-12_6_1_3.cfg).
```

```
Do you want to make <RO-00/01-primary>-12_6_1_3.cfg the
default database? (y/N)
```

Enter **n** and press **Return**.

```
Default configuration database selection cancelled.
```

2. Save the configuration to a remote TFTP server:

```
# upload configuration <TFTPSERVER> <RO-00/01-primary>-12
_6_1_3.cfg vr [VR-Mgmt/VR-Default]
```

3. Repeat step 1 and step 2 for RO-01.

4.2.3.2 Backup of DMX Configuration

Perform a backup of the current configuration and export it to a remote server:

1. Login to the DMXC remote using the `<SYSOAM-CNB-IP>` on port 2024:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

2. Create a configuration backup:



```
> request ManagedElement 1 DmxFunctions 1 SoftwareManag  
ement 1 ConfigurationBackup 1 save
```

3. Export the configuration backup file to a remote server:

```
> request ManagedElement 1 DmxFunctions 1 Software  
Management 1 ConfigurationBackup 1 export filename  
</path/filename>.bup ipAddress <ip address> username  
<username>
```

```
password: ****
```

4.2.3.3 Backup cluster.conf, evip.xml, License file, and HSS Validator for Multi Activation 16.0

Perform a backup of the `cluster.conf`, `evip.xml`, HSS Validator Plugin, and applicable license files by transferring them to a remote server.

The `cluster.conf` file resides in the `/cluster/etc` directory.

The `evip.xml` file resides in the `/storage/system/config/evip-apr9010467` directory.

The license file `lservrc` resides in the `/home/dveadm/licenses` directory.

The HSS Validator Plugin resides in the `/home/bootloader/repository` directory.

4.2.4 SSL Certificate Backup (Optional)

If an SSL connection has been used, save the certificate `keystore` to a secure storage.

The `keystore` file is found in the `/home/asuser/nodes/<nodeId>/domains/dve-domain/config` directory on the PL nodes.

4.3 Hardware Configuration

This section describes how to configure the hardware when upgrading to Dynamic Activation 1.

4.3.1 CMXB3, SCXB3, and GEP5 Hardware

This section describes how to install and configure CMXB3 routers, SCXB3 switches and GEP5 Blades.

1. Make sure to have all templates prepared, according to instructions in sections *Accessing Hardware Specific Information* and *Preparing*



Deployment Artifacts in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.

2. Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

Time requirements for upgrading if all templates are filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration	300 (when all templates are filled in and updated, with downtime)

4.3.1.1

Cabling

1. Login to the DMXC (remote using the `<SYSOAM-CNB-IP>` on port 2024), and lock all the GEP blades in the cluster:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

Attention!

From now on, all provisioning traffic is down.

2. Power off all GEP blades in the cluster:

DMX 3.1

```
> configure
```

```
% set ManagedElement 1 Equipment 1 Shelf 0 Slot <slot position> Blade 1 administrativeState locked
```

```
% commit
```

The `<slot position>` variable corresponds to the slot position of the GEP blade.

3. Replace the SCXB2, NWI-E, and GEP3 blades with the new SCXB3, CMXB3, and GEP5 blades according to section **Hardware Installation** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.



Attention!

Take note of the position of each blade, in case of a rollback they need to be positioned on the exact position they were extracted from.

Take notice of how the cabling on the current system is setup. In case of a rollback.

4. Re-cable the system according to instructions in section **Cabling and Wiring** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.
5. When the re-cabling is done, continue with the instructions in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.

Start with section **Installation Tools Preparation**.

Continue with the instructions throughout the whole document.

Continue with the Software installation according to Section 4.4 on page 33.

4.4 Software Installation

Perform a Dynamic Activation 1 installation according to instructions in *Software Installation for Native Deployment*, Reference [17].

Note: Section **Configurations** in the *Software Installation for Native Deployment*, Reference [17] document is replaced by Section 16.2 on page 136 (Restore Configuration).

Continue with Section 4.5 on page 33.

4.5 Restore Configuration

Follow the instructions in Section 16.2 on page 136.

4.6 Rollback to Multi Activation 16.0 on Native Deployment, using SCXB2, NWI-E, GEP3 (downgrading from GEP5 to GEP3 Blades), and DMX 3.1

This section contains information on how to perform a rollback from Dynamic Activation 1 to Multi Activation 16.0 on Native Deployment, using SCXB2,



NWI-E, GEP3 (downgrading from GEP5 to GEP3 Blades) hardware, and DMX 3.1 network software.

To perform a rollback, follow the step-list.

1. Replace the SCXB3, CMXB3 and GEP5 blades with the old SCXB2, NWI-E, and GEP3 blades. Insert the old blades in the exact position as they were before the upgrade.
2. Reset the cables to the exact position as they were before the upgrade.
3. Set the GEP3 BIOS Settings according to instructions in section **GEP3 BIOS Settings** in Reference [8].



5 Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Keeping the GEP3 Blades

This section contains information on how to upgrade from a Native Multi Activation 16.0 system, using SCXB3, CMXB3, GEP3, and DMX 3.1, to Dynamic Activation 1, and keeping the GEP3 Blades.

5.1 General Upgrade Process

An upgrade from Multi Activation 16.0 to Dynamic Activation 1 consists of either one or four maintenance windows, as shown in Figure 3. This depends whether wanting to keep the processing logs in the Cassandra database or not. If keeping the processing logs in the Cassandra database, follow alternative 1 (four maintenance windows), if not keeping the processing logs in the Cassandra database, follow alternative 2.

Note: For alternative 2 there is a possibility to keep the processing logs, by exporting them by use of the Processing Log Admin Tool. This must however be done outside the maintenance window, and before starting the upgrade process.

An import of the exported processing log is not supported.

Choosing Alternative 2 and not keeping the processing logs in the Cassandra database, will impact the **Log Management** feature to not be able to handle those exported logs.

For information on how to export processing log files, refer to section **Processing Log Admin Tool** in *System Administrators Guide for Native Deployment*, Reference [12]



Upgrade Process

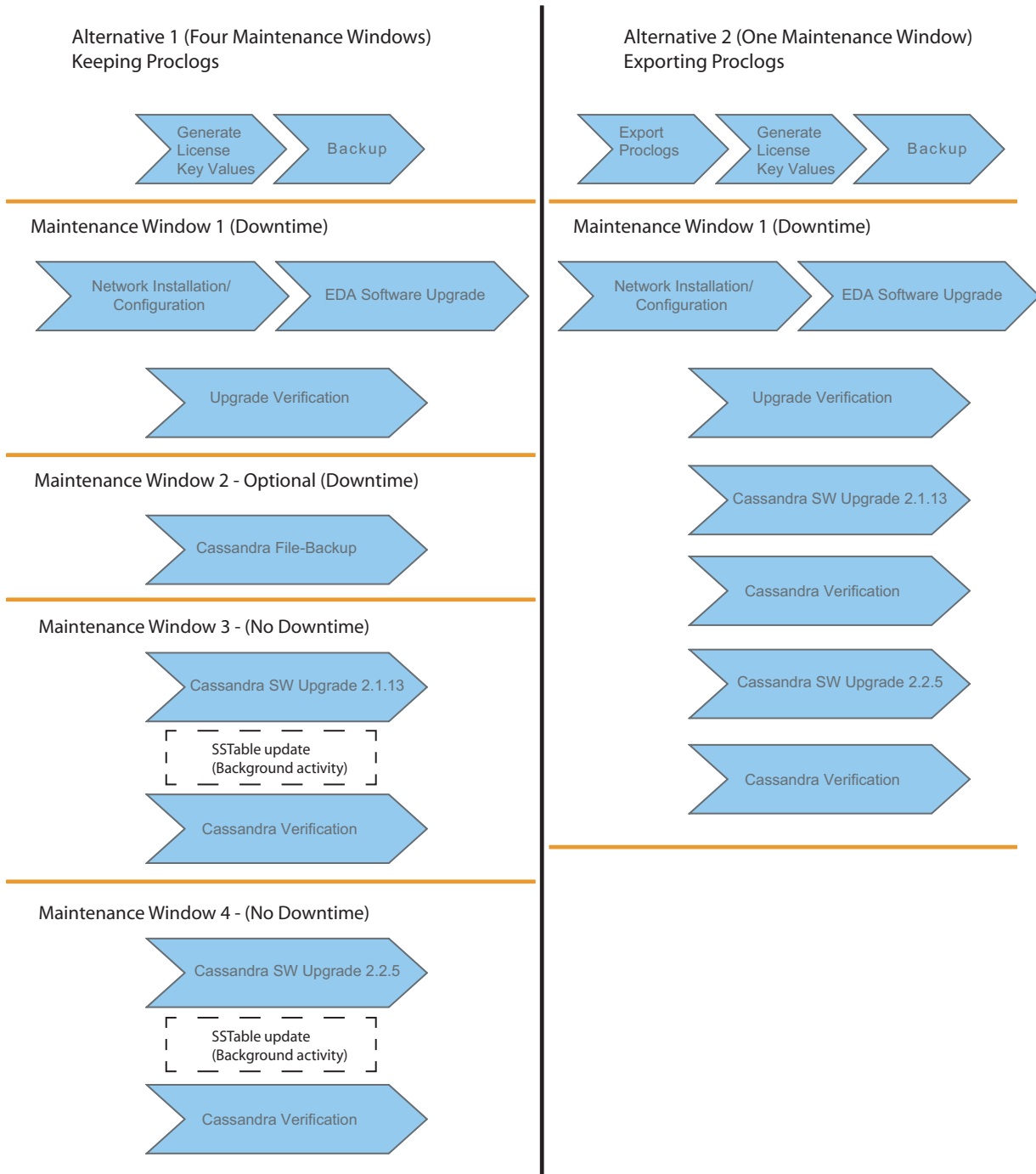


Figure 3 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from Multi Activation 16.0.



An upgrade is an upgrade of all RPMs (including LDE and eVIP), and modules on the current system to a newer software version.

The upgrade and rollback is proceeded with all nodes at once, with downtime. If any previously modified configuration files are affected by the upgrade, they may need to be modified again.

To see if a configuration file is replaced in platform RPMs, look in the `/home/actadm/config/log/config.log` file. Lines with correct date/time containing Replacing and Backing up are files that have been replaced. The backed up files are located in `/home/actadm/config/backup/<file><date>`

To see if a configuration file is replaced in the modules, look in the `/home/actadm/config/module_config_files/log/config.log` file. Lines with correct date/time containing `<config file>` replaced due to new original file, old file renamed to `<config file>.save` are files that has been replaced. The backed up files are located in `/home/actadm/config/module_config_files/<module>/<config file>.save`

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

Any modules that have been manually added before the upgrade will be removed. After the upgrade, such modules need to be added again (manually).

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters) will be migrated during the upgrade.
- Proclogs

The Proclog migration is handled separately (only applicable if using alternative 1). For details, see Section 10 on page 97.

5.2 Backup

This section contains information on how to perform a backup.

5.2.1 System Backup

Before initiating a system upgrade, a full system backup should be performed. Table 7 shows the documentation references for each Multi Activation version.

Table 7 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.0	See section Multi Activation Backup and Restore in Reference [3].



Note: Make sure to have everything in place before the upgrade, according to the *Pre-Upgrade Checklist* in Table 1.

5.2.2 Hardware Configuration Backup

To perform a complete hardware configuration backup, the following backups are needed:

Table 8 Scenario Mapping, Backup

Hardware	DMX Configuration	cluster.conf, and evip.xml
SCXB3, CMXB3, GEP3	x	x

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.

5.2.2.1 Backup of DMX Configuration

Perform a backup of the current configuration and export it to a remote server:

1. Login to the DMXC remote using the `<SYSOAM-CNB-IP>` on port 2024:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

2. Save the configuration:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 cmx_save_config
```

3. Create a configuration backup:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 save
```

4. Export the configuration backup file to a remote server:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 export filename </path/filename>.bup ipAddress <ip address> username <username>
```

```
password: ****
```



5.2.2.2 Backup of evip.xml and cluster.conf

Perform a backup of the `cluster.conf` and `evip.xml` files by transferring (copying) them to a remote server.

The `cluster.conf` file resides in the `/cluster/etc` directory.

The `evip.xml` file resides in the `/storage/system/config/evip-apr9010467/` directory.

Note: Do not rename origin `evip.xml` or `cluster.conf` files, keep the same name.

5.3 Upgrade Procedure

This section contains information on how to install and configure BSP 8100, and how to upgrade to the Dynamic Activation software.

Time requirements for installing and configuring BSP 8100 and upgrading to the Dynamic Activation software, if all templates are filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration of BSP 8100 software, and Dynamic Activation software	240 (when all templates are filled in and updated, with downtime)

5.3.1 Upgrade Preparations

- Make sure to have all the templates prepared, according to instructions in sections *Accessing Hardware Specific Information* and *Preparing Deployment Artifacts* in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.
- Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

5.3.2 Adapt cluster.conf, and evip.xml for Dynamic Activation 1

This section contains information on how to adapt the `cluster.conf`, and `evip.xml` files to the BSP 8100 network setup.

Follow the step-list:

1. Go to the `/cluster/etc` directory, and remove the old `cluster.conf` file:

```
# cd /cluster/etc
```

```
# rm cluster.conf
```



2. Create a new `cluster.conf` file, using the template prepared in Section 5.3.1 on page 39.

```
# vi /cluster/etc/cluster.conf
```

3. Reload the `cluster.conf` file on all nodes in the cluster:

```
# cluster config -r -a
```

4. Go to the `/storage/system/config/evip-apr9010467` directory, and remove the old `evip.xml` file:

```
# cd /storage/system/config/evip-apr9010467
```

```
# rm evip.xml
```

5. Create a new `evip.xml` file, using the template prepared in Section 5.3.1 on page 39. This file is to be used later, when upgrading the software.

```
# vi /storage/system/config/evip-apr9010467/evip.xml
```

Note: All blades in the cluster need to be configured, regardless if fewer of them are to be installed. This, to make it easier for future cluster expansion.

6. Copy the new `evip.xml` file to the `/var/log/installfiles/` directory. This file is to be used later, when upgrading the software.

```
# cp /storage/system/config/evip-apr9010467/evip.xml  
/var/log/installfiles/evip.xml
```

5.3.3

BSP 8100 Installation and Configuration

This section describes how to install and configure the BSP 8100 software, when upgrading to Dynamic Activation 1. Follow the step-list:

1. Login to the DMXC (remote using the `<SYSOAM-CNB-IP>` on port 2024), and lock all GEP blades in the cluster:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

Attention!

From now on, all provisioning traffic is down.

2. Power off all GEP blades in the cluster:

```
> configure
```




```
% set ManagedElement 1 Equipment 1 Shelf 0 Slot <slot  
position> Blade 1 administrativeState locked
```

```
% commit
```

The *<slot position>* variable corresponds to the slot position of the GEP blade.

3. Re-cable the system according to instructions in section **Cabling and Wiring** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.

4. When the re-cabling is done, continue with the instructions in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [6] document.

Start with section **Installation Tools Preparation**, it is not mandatory to perform the **GEP BIOS Settings** section, this section should already have been performed in the first installation of the cluster. Continue with the instructions throughout section **BSP Configuration**.

Attention!

Do not proceed with the **LDEwS Installation**, and the next coming sections. After finishing the **BSP Configuration** section, return to this document and continue with Section 5.3.4 on page 41.

5.3.4 Network Setup Check

Check the network setup according to instructions in **Network Setup Check**, *System Administrators Guide for Native Deployment*, Reference [12].

After the network setup check, continue with the upgrade instructions, see Section 5.3.5 on page 41.



5.3.5 Dynamic Activation Upgrade Instructions

Upgrade to Dynamic Activation 1 only supports **All nodes with downtime**. The upgrade sequence will upgrade LDE, eVIP, and the Multi Activation system.

Caution!

Before starting the upgrade procedure, make sure the new value package licenses are ordered for the new EDA 1 system.

5.3.5.1 Dynamic Activation Upgrade Preparations

A provisioning client with `Full` authorities for the Configuration Management Authorities is needed during the upgrade. Add one if not already available. The provisioning client is added in the old Multi Activation GUI, **Access Control>Users** tab. For instructions, refer to section **Access Control** in Reference [24].

On SC-1:

1. Transfer the Dynamic Activation software to the `/var/log/installfiles` directory on SC-1.

2. Change directory:

```
# cd /var/log/installfiles/
```

3. Untar the software (EDA System Base SW):

```
# tar -zxf <Software_Package>.tar.gz
```

5.3.5.2 Dynamic Activation Software Upgrade

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The upgrade needs to be performed as user `root`, and from SC-1.

The `ema_upgrade` script will upgrade LDE, eVIP, and issue a reboot. After the reboot, the script will automatically continue to upgrade the Dynamic Activation system and install the new licenses.

1. Obtain the license locking codes for the system.



From SC-1:

```
# /var/log/installfiles/<Prod_Number>-<Version>/ema_upgrade generateLicenseInformation
```

Output:

```
INFO - *** Locking codes for <SC-1>:
INFO - ***
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Information
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1NE URGH T85R V4K4
Locking Code 1 (Old Style) : 2008-292BD
```

```
INFO - *** Locking codes for <SC-2>:
INFO - ***
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Information
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1PW 65F3 8ABD KJET
Locking Code 1 (Old Style) : 2008-66063
```

2. Provide all Locking Code for the Ericsson License Information System (ELIS) and get the license file.
3. Transfer (SFTP) the license file to the /var/log/installfiles/ directory on SC1, and rename the file to license.txt. This will automatically install all license files when running the ./ema_upgrade upgrade script.
4. Upgrade the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema_upgrade upgrade
```

Note: Only **Resource Activation** (in 16.0 - 16.2 called Subscriber Activation (SA)) will be installed.

The following is prompted:

```
All ongoing provisioning will fail during upgrade.
Are you sure you want to continue with upgrade? (y/n)
```

Enter **y** and press **Enter**



Note: If error message:

```
ERROR - *** IP addresses for OSPF areas differs
in
running evip and CMX, must use the same IP
addresses.
, check the Delivery Report for current release and add required
software package.
```

The following is prompted:

Please enter provisioning client user name:

Enter name of a provisioning user with Full authorities and press **Enter**.

The following is prompted:

```
INFO - *** Please enter your provisioning client
password.
Password:
```

Enter password and press **Enter**.

5. To know when the upgrade is finished, after the reboot, login as user `root` on SC-1, and perform a tail on the `/var/log/ema/ema.log` file:

```
# tail -f /var/log/ema/ema.log
```

When the following is prompted, continue with the next step in the step-list:

```
- upgradehandler - INFO - *** Upgrade finished

- ema - DEBUG - INPUT: /var/log/installfiles/<Prod_Number>-<Version>/ema post_upgrade: Duration: xx seconds
```

6. Check the `/home/actadm/config/log/config.log` and `/home/boottloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.
7. Log out and log in again to receive all the updated environment variables.
8. Check the result of the latest system status.

Run the following command:

```
# healthcheck.py show -d
```



Note: If any problems appear, check any created logs during the upgrade phase:

- Before reboot:

`/var/log/ema/ema_upgrade.log`

- After reboot:

`/var/log/ema/ema_post_upgrade-console.log`

`/var/log/ema/ema.log`

- Installation of new modules after reboot:

`/var/log/bootloader/bootloader.log`

9. Run CAI3G test traffic.

Run test traffic on ports (8080, 8181) to verify the updated nodes.

Note: Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.

Caution!

After the Dynamic Activation software upgrade is finished, it is important not to remove the `/var/log/installfiles` directory. Some files in this directory are used for rollback purposes.

Continue with the Cassandra upgrade, see Section 5.4 on page 45.

5.4 Upgrade Cassandra

Attention!

Before continuing with the upgrade of Cassandra, make sure the system works as expected. If proceeding with the Cassandra upgrade, it is not possible to perform a complete restore of the Dynamic Activation application.



If alternative 1 has been chosen (keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 10 on page 97.

If alternative 2 has been chosen (not keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 11 on page 107.

5.5 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users > Create Administrative User** in *System Administrators Guide for Native Deployment*, Reference [12].

5.6 Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP3, and DMX 3.1

This section contains information on how to perform a rollback from Dynamic Activation 1 to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP3 hardware, and DMX 3.1 network software.

To perform a rollback, follow the subsections.

5.6.1 Rollback Cassandra

Attention!

To be able to perform a Dynamic Activation software rollback to Multi Activation 16.0, Cassandra needs to be in revision 2.0.15. If a Cassandra upgrade has been performed, roll back Cassandra according to Section 12 on page 113 before proceeding with the instructions in Section 5.6.2 on page 46.

5.6.2 Rollback the Multi Activation Software

To perform a rollback of the Dynamic Activation software, follow the step-list:

1. Rollback the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema rollback
```



The following is prompted:

```
All ongoing provisioning will fail during rollback.  
Are you sure you want to continue with rollback? (y/n)
```

Enter **y** and press **Enter**

2. The `ema` script will roll back LDE, eVIP, and the Dynamic Activation system, and issue a reboot.

Login as user `root` on SC-1, and wait for the system to be fully installed.

3. Check the `/home/dveadm/config/log/config.log` and `/home/boottloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.

5.6.3 Rollback `cluster.conf` and `evip.xml`

This section contains information on how to rollback the `cluster.conf` and `evip.xml` files to the previous network setup.

Follow the step-list:

1. Go to the `/cluster/etc` directory, and remove the `cluster.conf` file:

```
# cd /cluster/etc  
  
# rm cluster.conf
```
2. Restore the old `cluster.conf` file. Use the `cluster.conf` file that was backed up before the upgrade.

```
# vi /cluster/etc/cluster.conf
```
3. Reload the `cluster.conf` file on all nodes in the cluster:

```
# cluster config -r -a
```
4. Go to the `/storage/system/config/evip-apr9010467/` directory, and remove the `evip.xml` file:

```
# cd /storage/system/config/evip-apr9010467/  
  
# rm evip.xml
```
5. Restore the old `evip.xml` file. Use the `evip.xml` file that was backed up before the upgrade.

```
# vi /storage/system/config/evip-apr9010467/evip.xml
```

5.6.4 Hardware Replacement

1. Reset the cables to the exact position as they were before the upgrade.



5.6.5 Restore DMX

1. Install the DMX 3.1 software as described in *DMX Jumpstart Instruction*, Reference [15].

Note: The default SCX root user password is: `tre,14`

The default DMX expert user password is: `expert`

2. Follow the chapter *Importing Configuration Backup* in *DMX Software Management*, Reference [14].
3. Follow chapter *Restoring Configuration Backup* in *DMX Software Management*, Reference [14].

Note: In this step a console needs to be used, this to be able to logon to the DMX as user `expert`.

5.6.6 Health Check

Perform a health-check according to instructions in the step-list below.

1. Run the complete health-checks according to instructions in sections **Health Check on Multi Activation Common** and **Health Check on Multi Activation EBS 2.0 HW with DMX 3.1** in Reference [20].
2. Run CAI3G test traffic.

Run test traffic on test ports (8080, 8181) to verify the rolled back nodes.



6 Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP3, and DMX 3.1, to Native Dynamic Activation 1, Upgrading to GEP5 Blades

This section contains information on how to upgrade from Native Multi Activation 16.0 (using SCXB3, CMXB3, GEP3, and DMX 3.1), to Dynamic Activation 1, and upgrading to GEP5 Blades.

6.1 General Upgrade Process

An upgrade of Multi Activation consists of one maintenance window, as shown in Figure 4.

Upgrade Process

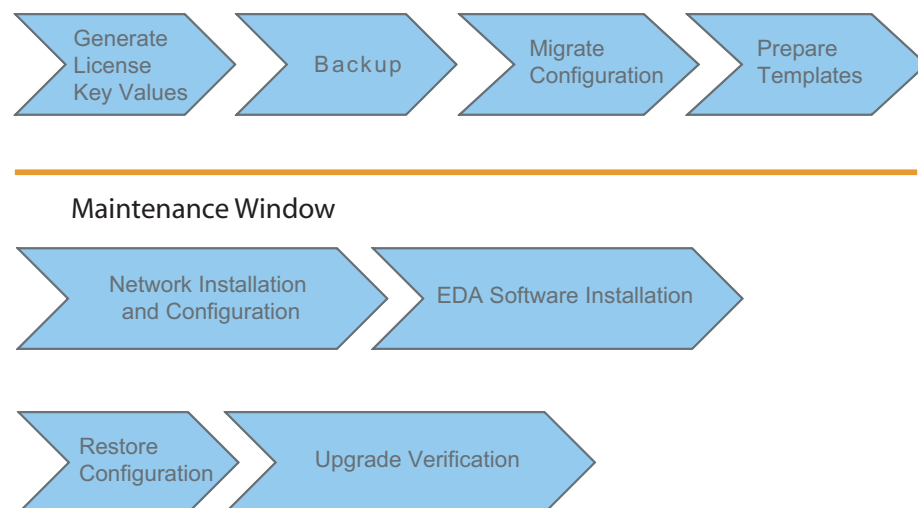


Figure 4 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from a previous Multi Activation version:



- The Linux Distribution Extensions (LDE), and the evolved Virtual Internet Protocol (eVIP) solutions require a maiden installation with data migration to be performed.
- Due to the new LDE features and the re-partitioning of the file structure, the cluster nfs partition that prior to the upgrade was approximately 80 GB, will decrease to a storage area of approximately 40 GB.

The following parts are migrated in the upgrade process:

- Multi Activation configuration (application users, network elements, license counters)

The following parts are not migrated in the migration process:

- ESA configuration files

See *System Administrators Guide for Native Deployment*, Reference [12] for information on how to configure trap destination. If any other customer specific configuration has been done, this needs to be migrated, see **Migration Methods in ESA Upgrade Instruction** Reference [13].

- Proclogs
- Customized changes in system level files, for example Linux users, groups, and crontab.

This means, for example, that all crontab jobs are removed and recreated according to default setup for the latest target Multi Activation version.

Linux users related to the Multi Activation application are recreated as part of the upgrade procedure. If any other customer specific Linux users have been created, these are not migrated. To recreate specific Linux users, see chapter **User and Group Management** in Reference [10].

The following parts are not migrated in the migration process but backed up in the tar file `pgconfigbackup-*.tar.gz`:

- Other Multi Activation configuration files, `log4j.xml`, `cli.properties`, `core.properties` and `iptables-rules-custom.cfg`.
- The Centralized User Database (CUDb) configuration files.

For example `CUDbConfig_HLRAUC.xml`

- All present notification rules files (`NotificationRulesDae.xml`, `NotificationRulesIms.xml`, `NotificationRulesEps.xml`)

Limitations:

- Changes performed after completing the backup on the old system are not migrated, for example license counters.



6.2 Migrate/Backup

This section contains information on how to perform a backup and data migration.

6.2.1 Migrate/Backup Configuration from existing Multi Activation 16.0 System

To migrate/backup existing configuration to be used on the upgraded Dynamic Activation 1 system, follow the instructions in Section 16.1 on page 135.

Note: This backup will later be used to restore existing configuration on the upgraded Dynamic Activation 1 system.

6.2.2 System Backup

Before initiating a system upgrade, a full backup should be performed. Table 9 shows the documentation references for each Multi Activation version. These backups will be used if the upgrade fails, and a rollback needs to be performed

Table 9 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.0	See specific chapters in Reference [3].

6.2.3 Hardware Configuration Backup

To perform a complete hardware configuration backup, the following backups are needed:

Table 10 Scenario Mapping, Backup

Hardware	DMX configuration	cluster.conf, vipconfig.xml /evip.xml, and Multi Activation license	HSS Validator Plugin (optional)
SCXB3, CMXB3, GEP3	x	x	x

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.



6.2.3.1 Backup of DMX Configuration

Perform a backup of the current configuration and export it to a remote server:

1. Login to the DMXC remote using the `<SYSOAM-CNB-IP>` on port 2024:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

2. Save the DMX configuration:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 cmx_save_config
```

3. Create a configuration backup:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 save
```

4. Export the configuration backup file to a remote server:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 export filename
</path/filename>.bup ipAddress <ip address> username
<username>
```

```
password: ****
```

6.2.3.2 Backup cluster.conf, evip.xml, License file, and HSS Validator for Multi Activation 16.0

Note: This section is only valid for Multi Activation 16.0.

Perform a backup of the `cluster.conf`, `evip.xml`, HSS Validator Plugin, and applicable license files by transferring them to a remote server.

The `cluster.conf` file resides in the `/cluster/etc` directory.

The `evip.xml` file resides in the `/storage/system/config/evip-apr9010467` directory.

The license file `lservrc` resides in the `/home/dveadm/licenses` directory.

The HSS Validator Plugin resides in the `/home/bootloader/repository` directory.

6.2.4 SSL Certificate Backup (Optional)

If an SSL connection has been used, save the certificate keystore to a secure storage.

The keystore file is found in the `/home/asuser/nodes/<nodeId>/domains/dve-domain/config` directory on the PL nodes.



6.3 Hardware Configuration

This section describes how to configure the hardware when upgrading to Dynamic Activation 1.

6.3.1 CMXB3, SCXB3, and GEP5 Hardware

This section describes how to install and configure CMXB3 routers, SCXB3 switches and GEP5 Blades.

1. Make sure to have all templates prepared, according to instructions in sections *Accessing Hardware Specific Information* and *Preparing Deployment Artifacts* in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.
2. Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

Time requirements for upgrading if all templates are filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration	285 (when all templates are filled in and updated, with downtime)

6.3.1.1 Cabling

1. Login to the DMXC (remote using the `<SYSOAM-CNB-IP>` on port 2024), and lock all the GEP blades in the cluster:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

Attention!

From now on, all provisioning traffic is down.

2. Enter configuration mode:

```
> configure
```

3. Power off all GEP blades in the cluster:

```
% set ManagedElement 1 Equipment 1 Shelf 0 Slot <slot  
position> Blade 1 administrativeState locked  
  
% commit
```

The `<slot position>` variable corresponds to the slot position of the GEP blade.

4. Replace the GEP3 blades with the new GEP5 blades according to section **Hardware Installation** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.

Attention!

Take note of the position of each blade, in case of a rollback they need to be positioned on the exact position they were extracted from.

Take notice of how the cabling on the current system is setup. In case of a rollback.

-
-
5. Re-cable the system according to instructions in section **Cabling and Wiring** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.
 6. When the re-cabling is done, continue with the instructions in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.

Start with section **Installation Tools Preparation**.

Continue with the instructions throughout the whole document.

Continue with the Software installation according to Section 6.4 on page 54.

6.4 Software Installation

Perform a Dynamic Activation 1 installation according to instructions in *Software Installation for Native Deployment*, Reference [17].

Note: Section **Configurations** in the *Software Installation for Native Deployment*, Reference [17] document is replaced by Section 16.2 on page 136 (Restore Configuration).

Continue with Section 6.5 on page 54.

6.5 Restore Configuration

Follow the instructions in Section 16.2 on page 136.



6.6 Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP3 (downgrading from GEP5 to GEP3 Blades), and DMX 3.1

This section contains information on how to perform a rollback from Dynamic Activation 1 to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP3 (downgrading from GEP5 to GEP3 Blades) hardware, and DMX 3.1 network software.

To perform a rollback, follow the subsections.

6.6.1 Hardware Replacement

1. Replace the GEP5 blades with the old GEP3 blades. Insert the old blades in the exact position as they were before the upgrade.
2. Reset the console cable to the GEP3 blade.
3. Set the GEP3 BIOS Settings according to instructions in section **GEP3 BIOS Settings** in Reference [8].

6.6.2 Restore DMX

1. Install the DMX 3.1 software as described in *DMX Jumpstart Instruction*, Reference [15].

Note: The default SCX root user password is: `tre,14`

The default DMX expert user password is: `expert`

2. Follow the chapter *Importing Configuration Backup* in *DMX Software Management*, Reference [14].
3. Follow chapter *Restoring Configuration Backup* in *DMX Software Management*, Reference [14].

Note: In this step a console needs to be used, this to be able to logon to the DMX as user `expert`.





7 Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP5, and DMX 3.1, to Native Dynamic Activation 1, Keeping the GEP5 Blades

This section contains information on how to upgrade from a Native Multi Activation 16.0 system, using SCXB3, CMXB3, GEP3, and DMX 3.1, to Dynamic Activation 1, and keeping the GEP5 Blades.

7.1 General Upgrade Process

An upgrade from Multi Activation 16.0 to Dynamic Activation 1 consists of either one or four maintenance windows, as shown in Figure 5. This depends whether wanting to keep the processing logs in the Cassandra database or not. If keeping the processing logs in the Cassandra database, follow alternative 1 (four maintenance windows), if not keeping the processing logs in the Cassandra database, follow alternative 2.

Note: For alternative 2 there is a possibility to keep the processing logs, by exporting them by use of the Processing Log Admin Tool. This must however be done outside the maintenance window, and before starting the upgrade process.

An import of the exported processing log is not supported.

Choosing Alternative 2 and not keeping the processing logs in the Cassandra database, will impact the **Log Management** feature to not be able to handle those exported logs.

For information on how to export processing log files, refer to section **Processing Log Admin Tool** in *System Administrators Guide for Native Deployment*, Reference [12]



Upgrade Process

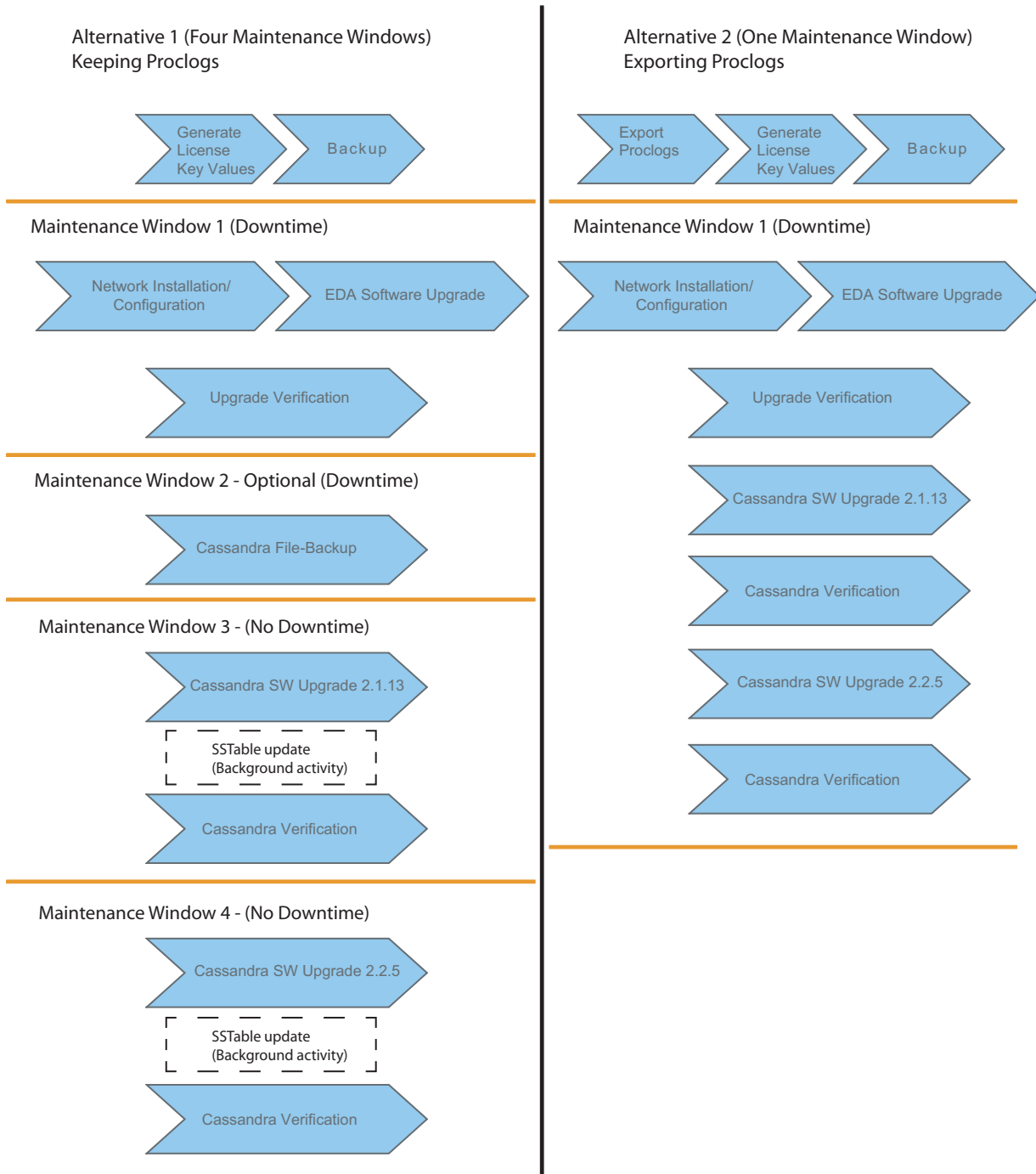


Figure 5 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from Multi Activation 16.0.



An upgrade is an upgrade of all RPMs (including LDE and eVIP), and modules on the current system to a newer software version.

The upgrade and rollback is proceeded with all nodes at once, with downtime. If any previously modified configuration files are affected by the upgrade, they may need to be modified again.

To see if a configuration file is replaced in platform RPMs, look in the `/home/actadm/config/log/config.log` file. Lines with correct date/time containing Replacing and Backing up are files that have been replaced. The backed up files are located in `/home/actadm/config/backup/<file><date>`

To see if a configuration file is replaced in the modules, look in the `/home/actadm/config/module_config_files/log/config.log` file. Lines with correct date/time containing `<config file>` replaced due to new original file, old file renamed to `<config file>.save` are files that has been replaced. The backed up files are located in `/home/actadm/config/module_config_files/<module>/<config file>.save`

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

Any modules that have been manually added before the upgrade will be removed. After the upgrade, such modules need to be added again (manually).

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters) will be migrated during the upgrade.
- Proclogs

The Proclog migration is handled separately (only applicable if using alternative 1). For details, see Section 10 on page 97.

7.2 Backup

This section contains information on how to perform a backup.

7.2.1 System Backup

Before initiating a system upgrade, a full system backup should be performed. Table 11 shows the documentation references for each Multi Activation version.

Table 11 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.0	See section Multi Activation Backup and Restore in Reference [3].



Note: Make sure to have everything in place before the upgrade, according to the *Pre-Upgrade Checklist* in Table 1.

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.

7.2.2 Hardware Configuration Backup

To perform a complete hardware configuration backup, the following backups are needed:

Table 12 Scenario Mapping, Backup

Hardware	DMX Configuration	cluster.conf, and evip.xml
SCXB3, CMXB3, GEP3	x	x

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.

7.2.2.1 Backup of DMX Configuration

Perform a backup of the current configuration and export it to a remote server:

1. Login to the DMXC remote using the `<SYSOAM-CNB-IP>` on port 2024:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```

2. Save the configuration:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 cmx_save_config
```

3. Create a configuration backup:

```
> request ManagedElement 1 DmxFunctions 1 SoftwareManagement 1 ConfigurationBackup 1 save
```

4. Export the configuration backup file to a remote server:



```
> request ManagedElement 1 DmxFunctions 1 Software
Management 1 ConfigurationBackup 1 export filename
</path/filename>.bup ipAddress <ip address> username
<username>
```

```
password: ****
```

7.2.2.2 Backup of evip.xml and cluster.conf

Perform a backup of the `cluster.conf` and `evip.xml` files by transferring (copying) them to a remote server.

The `cluster.conf` file resides in the `/cluster/etc` directory.

The `evip.xml` file resides in the `/storage/system/config/evip-apr 9010467/` directory.

Note: Do not rename origin `evip.xml` or `cluster.conf` files, keep the same name.

7.3 Upgrade Procedure

This section contains information on how to install and configure BSP 8100, and how to upgrade to the Dynamic Activation software.

Time requirements for installing and configuring BSP 8100 and upgrading to the Dynamic Activation software, if all templates are filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration of BSP 8100 software, and Dynamic Activation software	240 (when all templates are filled in and updated, with downtime)

7.3.1 Upgrade Preparations

- Make sure to have all the templates prepared, according to instructions in sections *Accessing Hardware Specific Information* and *Preparing Deployment Artifacts* in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7].
- Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

7.3.2 Adapt cluster.conf, and evip.xml for Dynamic Activation 1

This section contains information on how to adapt the `cluster.conf`, and `evip.xml` files to the BSP 8100 network setup.

Follow the step-list:



1. Go to the `/cluster/etc` directory, and remove the old `cluster.conf` file:

```
# cd /cluster/etc  
  
# rm cluster.conf
```

2. Create a new `cluster.conf` file, using the template prepared in Section 7.3.1 on page 61.

```
# vi /cluster/etc/cluster.conf
```

3. Reload the `cluster.conf` file on all nodes in the cluster:

```
# cluster config -r -a
```

4. Go to the `/storage/system/config/evip-apr9010467` directory, and remove the old `evip.xml` file:

```
# cd /storage/system/config/evip-apr9010467  
  
# rm evip.xml
```

5. Create a new `evip.xml` file, using the template prepared in Section 7.3.1 on page 61. This file is to be used later, when upgrading the software.

```
# vi /storage/system/config/evip-apr9010467/evip.xml
```

Note: All blades in the cluster need to be configured, regardless if fewer of them are to be installed. This, to make it easier for future cluster expansion.

6. Copy the new `evip.xml` file to the `/var/log/installfiles/` directory. This file is to be used later, when upgrading the software.

```
# cp /storage/system/config/evip-apr9010467/evip.xml  
/var/log/installfiles/evip.xml
```

7.3.3 BSP 8100 Installation and Configuration

This section describes how to install and configure the BSP 8100 software, when upgrading to Dynamic Activation 1. Follow the step-list:

1. Login to the DMXC (remote using the `<SYSOAM-CNB-IP>` on port 2024), and lock all GEP blades in the cluster:

```
# ssh -p 2024 expert@<SYSOAM-CNB-IP>
```



Attention!

From now on, all provisioning traffic is down.

2. Power off all GEP blades in the cluster:

```
> configure
```

```
% set ManagedElement 1 Equipment 1 Shelf 0 Slot <slot  
position> Blade 1 administrativeState locked
```

```
% commit
```

The *<slot position>* variable corresponds to the slot position of the GEP blade.

3. Re-cable the system according to instructions in section **Cabling and Wiring** in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.

Attention!

Take notice of how the cabling on the current system is setup. In case of a rollback.

4. When the re-cabling is done, continue with the instructions in the *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [7] document.

Start with section **Installation Tools Preparation**, it is not mandatory to perform the **GEP BIOS Settings** section, this section should already have been performed in the first installation of the cluster. Continue with the instructions throughout section **BSP Configuration**.

Attention!

Do not proceed with the **LDEwS Installation**, and the next coming sections. After finishing the **BSP Configuration** section, return to this document and continue with Section 7.3.4 on page 63.



7.3.4 Network Setup Check

Check the network setup according to instructions in **Network Setup Check**, *System Administrators Guide for Native Deployment*, Reference [12].

After the network setup check, continue with the upgrade instructions, see Section 7.3.5 on page 64.

7.3.5 Dynamic Activation Upgrade Instructions

Upgrade to Dynamic Activation 1 only supports **All nodes with downtime**. The upgrade sequence will upgrade LDE, eVIP, and the Multi Activation system.

Caution!

Before starting the upgrade procedure, make sure the new value package licenses are ordered for the new EDA 1 system.

7.3.5.1 Dynamic Activation Upgrade Preparations

A provisioning client with `Full` authorities for the Configuration Management Authorities is needed during the upgrade. Add one if not already available. The provisioning client is added in the old Multi Activation GUI, **Access Control>Users** tab. For instructions, refer to section **Access Control** in Reference [24].

On SC-1:

1. Transfer the Dynamic Activation software to the `/var/log/installfiles` directory on SC-1.

2. Change directory:

```
# cd /var/log/installfiles/
```

3. Untar the software (EDA System Base SW):

```
# tar -zxf <Software_Package>.tar.gz
```

7.3.5.2 Dynamic Activation Software Upgrade

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.



Note: The upgrade needs to be performed as user `root`, and from SC-1.

The `ema_upgrade` script will upgrade LDE, eVIP, and issue a reboot. After the reboot, the script will automatically continue to upgrade the Dynamic Activation system and install the new licenses.

1. Obtain the license locking codes for the system.

From SC-1:

```
# /var/log/installfiles/<Prod_Number>-<Version>/ema_upgrade generateLicenseInformation
```

Output:

```
INFO - *** Locking codes for <SC-1>:
INFO - ***
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Information
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1          : 2008-*1NE URGH T85R V4K4
Locking Code 1 (Old Style) : 2008-292BD
```

```
INFO - *** Locking codes for <SC-2>:
INFO - ***
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Information
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1          : 2008-*1PW 65F3 8ABD KJET
Locking Code 1 (Old Style) : 2008-66063
```

2. Provide all Locking Code for the Ericsson License Information System (ELIS) and get the license file.
3. Transfer (SFTP) the license file to the `/var/log/installfiles/` directory on SC1, and rename the file to `license.txt`. This will automatically install all license files when running the `./ema_upgrade upgrade` script.
4. Upgrade the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema_upgrade upgrade
```

Note: Only **Resource Activation** (in 16.0 - 16.2 called Subscriber Activation (SA)) will be installed.



The following is prompted:

```
All ongoing provisioning will fail during upgrade.  
Are you sure you want to continue with upgrade? (y/n)
```

Enter **y** and press **Enter**

Note: If error message:

```
ERROR - *** IP addresses for OSPF areas differs  
in  
running evip and CMX, must use the same IP  
addresses.  
, check the Delivery Report for current release and add required  
software package.
```

The following is prompted:

```
Please enter provisioning client user name:
```

Enter name of a provisioning user with Full authorities and press **Enter**.

The following is prompted:

```
INFO - *** Please enter your provisioning client  
password.  
Password:
```

Enter password and press **Enter**.

5. To know when the upgrade is finished, after the reboot, login as user `root` on SC-1, and perform a tail on the `/var/log/ema/ema.log` file:

```
# tail -f /var/log/ema/ema.log
```

When the following is prompted, continue with the next step in the step-list:

```
- upgradehandler - INFO - *** Upgrade finished  
  
- ema - DEBUG - INPUT: /var/log/installfiles/<Prod_Number>-<Version>/ema post_upgrade: Duration: xx seconds
```

6. Check the `/home/actadm/config/log/config.log` and `/home/boottloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.
7. Log out and log in again to receive all the updated environment variables.
8. Check the result of the latest system status.

Run the following command:



```
# healthcheck.py show -d
```

Note: If any problems appear, check any created logs during the upgrade phase:

- Before reboot:

```
/var/log/ema/ema_upgrade.log
```

- After reboot:

```
/var/log/ema/ema_post_upgrade-console.log
```

```
/var/log/ema/ema.log
```

- Installation of new modules after reboot:

```
/var/log/bootloader/bootloader.log
```

9. Run CAI3G test traffic.

Run test traffic on ports (8080, 8181) to verify the updated nodes.

Note: Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.

Caution!

After the Dynamic Activation software upgrade is finished, it is important not to remove the `/var/log/installfiles` directory. Some files in this directory are used for rollback purposes.

Continue with the Cassandra upgrade, see Section 7.4 on page 67.

7.4 Upgrade Cassandra

Attention!

Before continuing with the upgrade of Cassandra, make sure the system works as expected. If proceeding with the Cassandra upgrade, it is not possible to perform a complete restore of the Dynamic Activation application.



If alternative 1 has been chosen (keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 10 on page 97.

If alternative 2 has been chosen (not keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 11 on page 107.

7.5 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users > Create Administrative User** in *System Administrators Guide for Native Deployment*, Reference [12].

7.6 Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP5, and DMX 3.1

This section contains information on how to perform a rollback from Dynamic Activation 1 to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP5 hardware, and DMX 3.1 network software.

To perform a rollback, follow the subsections.

7.6.1 Rollback Cassandra

Attention!

To be able to perform a Dynamic Activation software rollback to Multi Activation 16.0, Cassandra needs to be in revision 2.0.15. If a Cassandra upgrade has been performed, roll back Cassandra according to Section 12 on page 113 before proceeding with the instructions in Section 7.6.2 on page 68.

7.6.2 Rollback the Multi Activation Software

To perform a rollback of the Dynamic Activation software, follow the step-list:

1. Rollback the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema rollback
```



The following is prompted:

```
All ongoing provisioning will fail during rollback.  
Are you sure you want to continue with rollback? (y/n)
```

Enter **y** and press **Enter**

2. The `ema` script will roll back LDE, eVIP, and the Dynamic Activation system, and issue a reboot.

Login as user `root` on SC-1, and wait for the system to be fully installed.

3. Check the `/home/dveadm/config/log/config.log` and `/home/boottloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.

7.6.3 Rollback `cluster.conf` and `evip.xml`

This section contains information on how to rollback the `cluster.conf` and `evip.xml` files to the previous network setup.

Follow the step-list:

1. Go to the `/cluster/etc` directory, and remove the `cluster.conf` file:

```
# cd /cluster/etc
```

```
# rm cluster.conf
```

2. Restore the old `cluster.conf` file. Use the `cluster.conf` file that was backed up before the upgrade.

```
# vi /cluster/etc/cluster.conf
```

3. Reload the `cluster.conf` file on all nodes in the cluster:

```
# cluster config -r -a
```

4. Go to the `/storage/system/config/evip-apr9010467/` directory, and remove the `evip.xml` file:

```
# cd /storage/system/config/evip-apr9010467/
```

```
# rm evip.xml
```

5. Restore the old `evip.xml` file. Use the `evip.xml` file that was backed up before the upgrade.

```
# vi /storage/system/config/evip-apr9010467/evip.xml
```

6. Reboot the cluster

```
# cluster reboot -a
```



Note: It takes a few minutes before all environment variables and commands to be effective after reboot. If any variable or command (`3ppmon` for example) is not available, log out from the system and log on again later.

7.6.4 Hardware Replacement

1. Reset the cables to the exact position as they were before the upgrade.

7.6.5 Restore DMX

1. Install the DMX 3.1 software as described in *DMX Jumpstart Instruction*, Reference [15].

Note: The default SCX root user password is: `tre,14`

The default DMX expert user password is: `expert`

2. Follow the chapter *Importing Configuration Backup* in *DMX Software Management*, Reference [14].
3. Follow chapter *Restoring Configuration Backup* in *DMX Software Management*, Reference [14].

Note: In this step a console needs to be used, this to be able to logon to the DMX as user `expert`.

7.6.6 Health Check

Perform a health-check according to instructions in the step-list below.

1. Run the complete health-checks according to instructions in sections **Health Check on Multi Activation Common** and **Health Check on Multi Activation EBS 2.0 HW with DMX 3.1** in Reference [20].
2. Run CAI3G test traffic.

Run test traffic on test ports (8080, 8181) to verify the rolled back nodes.



8 Upgrading from Native Multi Activation 16.0 Using SCXB3, CMXB3, GEP5, and BSP 8100, to Native Dynamic Activation 1, Keeping the GEP5 Blades

This section contains information on how to upgrade from a Native Multi Activation 16.0 system, using SCXB3, CMXB3, GEP5, and BSP 8100 network software, to Dynamic Activation 1, and keeping the GEP5 Blades.

8.1 General Upgrade Process

An upgrade from Multi Activation 16.0 to Dynamic Activation 1 consists of either one or four maintenance windows, as shown in Figure 6. This depends whether wanting to keep the processing logs in the Cassandra database or not. If keeping the processing logs in the Cassandra database, follow alternative 1 (four maintenance windows), if not keeping the processing logs in the Cassandra database, follow alternative 2.

Note: For alternative 2 there is a possibility to keep the processing logs, by exporting them by use of the Processing Log Admin Tool. This must however be done outside the maintenance window, and before starting the upgrade process.

An import of the exported processing log is not supported.

Choosing Alternative 2 and not keeping the processing logs in the Cassandra database, will impact the **Log Management** feature to not be able to handle those exported logs.

For information on how to export processing log files, refer to section **Processing Log Admin Tool** in *System Administrators Guide for Native Deployment*, Reference [12]



Upgrade Process

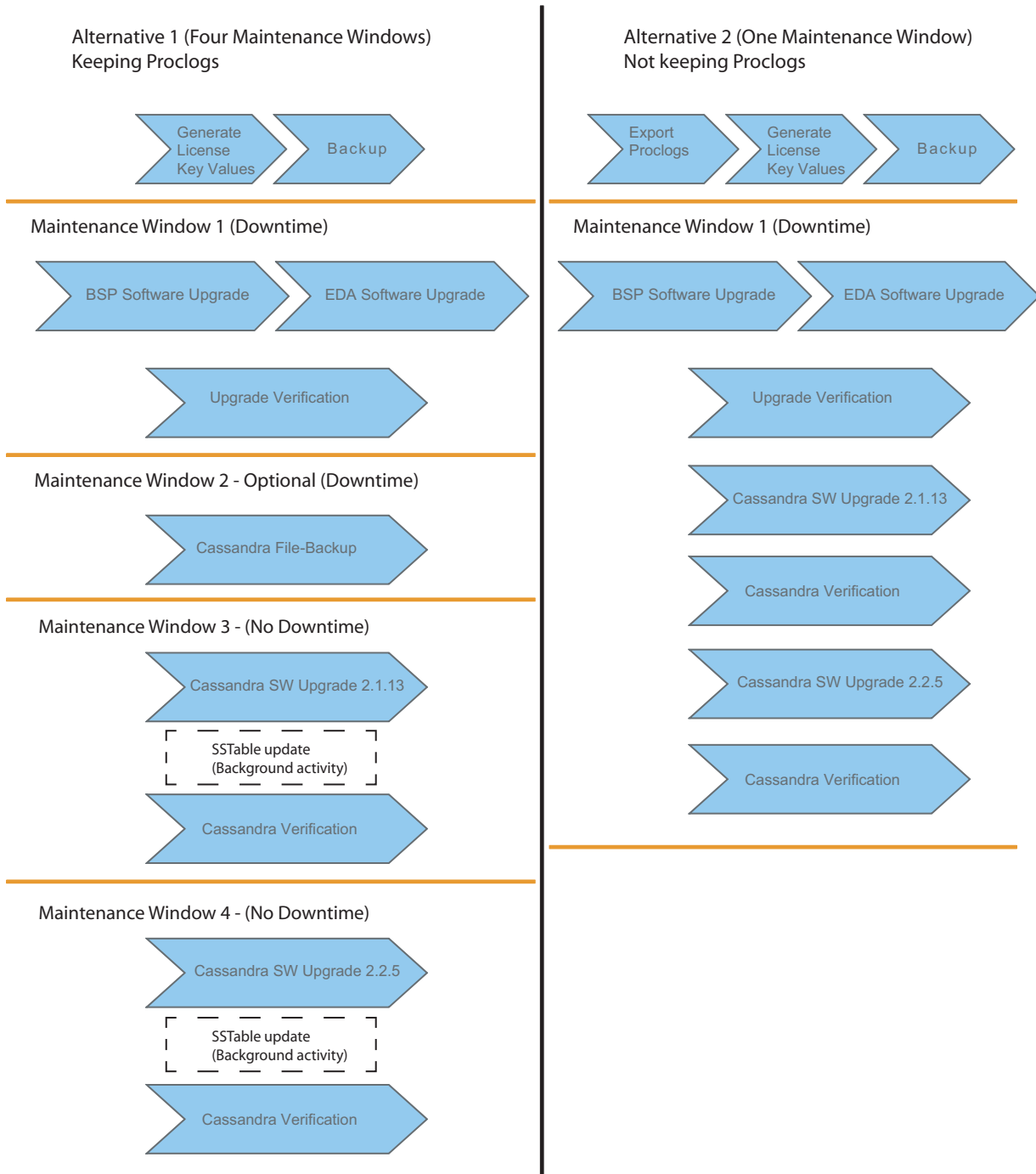


Figure 6 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from Multi Activation 16.0.



An upgrade is an upgrade of all RPMs (including LDE and eVIP), and modules on the current system to a newer software version.

The upgrade and rollback is proceeded with all nodes at once, with downtime. If any previously modified configuration files are affected by the upgrade, they may need to be modified again.

To see if a configuration file is replaced in platform RPMs, look in the `/home/actadm/config/log/config.log` file. Lines with correct date/time containing Replacing and Backing up are files that have been replaced. The backed up files are located in `/home/actadm/config/backup/<file><date>`

To see if a configuration file is replaced in the modules, look in the `/home/actadm/config/module_config_files/log/config.log` file. Lines with correct date/time containing `<config file>` replaced due to new original file, old file renamed to `<config file>.save` are files that has been replaced. The backed up files are located in `/home/actadm/config/module_config_files/<module>/<config file>.save`

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

Any modules that have been manually added before the upgrade will be removed. After the upgrade, such modules need to be added again (manually).

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters) will be migrated during the upgrade.
- Proclogs

The Proclog migration is handled separately (only applicable if using alternative 1). For details, see Section 10 on page 97.

8.2 Backup

This section contains information on how to perform a backup.

8.2.1 System Backup

Before initiating a system upgrade, a full system backup should be performed. Table 13 shows the documentation references for each Multi Activation version.

Table 13 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.0	See section Multi Activation Backup and Restore in Reference [3].



Note: Make sure to have everything in place before the upgrade, according to the *Pre-Upgrade Checklist* in Table 1.

8.2.2 Backup of evip.xml

Perform a backup of the `evip.xml` file by transferring (copy) it to a remote server.

The `evip.xml` file resides in the `/storage/system/config/evip-apr9010467/` directory.

Note: Do not rename origin `evip.xml` file, keep the same name.

8.3 Upgrade Procedure

This section contains information on how to upgrade the BSP 8100 software, and how to upgrade to the Dynamic Activation 1 software.

Time requirements for installing and configuring BSP 8100 and upgrading to the Dynamic Activation software, if `evip.xml` template is filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration of BSP 8100 software, and Dynamic Activation software	150 (when <code>evip.xml</code> template is filled in and updated, with downtime)

8.3.1 Upgrade Preparations

Follow the instructions in the step-list to create a new `evip.xml` file:

1. Download the EDA Native BSP8100 Config Generator tool:
 - Save the zip file, [EDA Native BSP8100 Config Generator.zip](#) to, for example a local area on a local machine
 - Unpack the zip file.
2. Start the EDA Native BSP8100 Config Generator tool by double-clicking the `Activation_ConfigGen.jar` file, located in the folder where the tool was unzipped.

Note: Requires Oracle's JAVA version 1.8.0_71 or higher.

3. Fill in the required values, according to the figure below (see red boxes):



General Parameters

Time Zone: Europe/Stockholm

Hardware: GEP5

DNS-Server-1-IP: 10.64.2.226

DNS-Server-2-IP: 10.64.2.227

NTP-Server-1-IP:

NTP-Server-2-IP:

OSS-IP: 10.216.129.81

VIP-OAM-IP: 10.64.26.246

VIP-TRAFFIC-IP: 10.64.26.245

Uplink Redundancy: VRRP

PG_OM_SP1	BSP_NBI	PROV_OM_CN	OM_CN_SP
Netmask			/29
VLAN ID			184
PG_OM_SP1_NW			10.44.186.64
PG_OM_SP1_VRRP_IP			10.44.186.65
PG_OM_SP1_CMx_0_26_IP			10.44.186.66
PG_OM_SP1_CMx_0_28_IP			10.44.186.67
PG_OM_SP1_SC_1_IP			10.44.186.68
PG_OM_SP1_SC_2_IP			10.44.186.69

Node Hostnames

Number Blades: 4

Hostname Prefix: CL15

HOSTNAME-SC-1: CL15-SC-1

HOSTNAME-SC-2: CL15-SC-2

HOSTNAME-PL-3: CL15-PL-3

HOSTNAME-PL-4: CL15-PL-4

HOSTNAME-PL-5: CL15-PL-5

HOSTNAME-PL-6: CL15-PL-6

HOSTNAME-PL-7: CL15-PL-7

HOSTNAME-PL-8: CL15-PL-8

HOSTNAME-PL-9: CL15-PL-9

HOSTNAME-PL-10: CL15-PL-10

HOSTNAME-PL-11: CL15-PL-11

HOSTNAME-PL-12: CL15-PL-12

First MAC address-SC-1:

MAC address for ext. PXE Boot:

First MAC address-SC-2:

First MAC address-PL-3:

First MAC address-PL-4:

First MAC address-PL-5:

First MAC address-PL-6:

First MAC address-PL-7:

First MAC address-PL-8:

First MAC address-PL-9:

First MAC address-PL-10:

First MAC address-PL-11:

Generate Artifacts

Figure 7 EDA Config Generator Tool

Attention!

Make sure the names of the hosts (HOSTNAME-SC-1, HOSTNAME-SC-2, HOSTNAME-PL-3, HOSTNAME-PL-x) match the names that are currently present in the running `cluster.conf` file.

Make sure the DNS IP Addresses match (amount and IP address) the current, running `cluster.conf` file settings.

- When all values are filled in, click on the **Generate Artifacts** button and choose **evip.xml** in the prompted **Selection** window:



Selection

Only evip.xml or all artifacts?

evip.xml All Cancel

5. Save the generated `evip.xml` file on the local machine.
6. Create a new `evip.xml` file using the newly generated `evip.xml` file in Step 5, to `/var/log/installfiles/` on SC-1:

```
# vi /var/log/installfiles/evip.xml
```

Note: Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

8.3.2

BSP 8100 Upgrade Instructions

1. Upgrade to the latest BSP software Release (BSP R<X>), and follow the BSP Upgrade Instruction found in Ericsson Blade Server Platform (BSP) catalog, in <http://calstore.internal.ericsson.com/alex>

Note: The default SCX root user password is `tre,14`

The default SCX advanced user password is `ett,30`

The default CMX root user password is `tre,14`

The default CMX advanced user password is `ett,30`

Continue with Section 8.3.3 on page 76.

8.3.3

Dynamic Activation Upgrade Instructions

Upgrade to Dynamic Activation 1 only supports **All nodes with downtime**. The upgrade sequence will upgrade LDE, eVIP, and the Dynamic Activation system.

Caution!

Before starting the upgrade procedure, make sure the new value package licenses are ordered for the new EDA 1 system.



8.3.3.1 Dynamic Activation Upgrade Preparations

A provisioning client with Full authorities for the Configuration Management Authorities is needed during the upgrade. Add one if not already available. The provisioning client is added in the old Multi Activation GUI, **Access Control>Users** tab. For instructions, refer to section **Access Control** in Reference [24].

On SC-1:

1. Transfer the Dynamic Activation software to the `/var/log/installfiles` directory on SC-1.

2. Change directory:

```
# cd /var/log/installfiles/
```

3. Untar the software (EDA System Base SW):

```
# tar -zxvf <Software_Package>.tar.gz
```

8.3.3.2 Dynamic Activation Software Upgrade

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The upgrade needs to be performed as user `root`, and from SC-1.

The `ema_upgrade` script will upgrade LDE, eVIP, and issue a reboot. After the reboot, the script will automatically continue to upgrade the Dynamic Activation system and install the new licenses.

1. Obtain the license locking codes for the system.

From SC-1:

```
# /var/log/installfiles/<Prod_Number>-<Version>/ema_upgrade generateLicenseInformation
```

Output:



```
INFO - *** Locking codes for <SC-1>:
INFO - ***
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Inform
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1NE URGH T85R V4K4
Locking Code 1 (Old Style) : 2008-292BD
```

```
INFO - *** Locking codes for <SC-2>:
INFO - ***
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Inform
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1PW 65F3 8ABD KJET
Locking Code 1 (Old Style) : 2008-66063
```

2. Provide all Locking Code for the Ericsson License Information System (ELIS) and get the license file.
3. Transfer (SFTP) the license file to the /var/log/installfiles/ directory on SC1, and rename the file to license.txt. This will automatically install all license files when running the ./ema_upgrade upgrade script.
4. Upgrade the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema_upgrade upgrade
```

Note: Only **Resource Activation** (in 16.0 called Subscriber Activation (SA)) will be installed.

The following is prompted:

```
All ongoing provisioning will fail during upgrade.
Are you sure you want to continue with upgrade? (y/n)
```

Enter **y** and press **Enter**



Note: If error message:

```
ERROR - *** IP addresses for OSPF areas differs  
in  
running evip and CMX, must use the same IP  
addresses.  
, check the Delivery Report for current release and add required  
software package.
```

The following is prompted:

Please enter provisioning client user name:

Enter name of a provisioning user with Full authorities and press **Enter**.

The following is prompted:

```
INFO - *** Please enter your provisioning client  
password.  
Password:
```

Enter password and press **Enter**.

5. To know when the upgrade is finished, after the reboot, login as user root on SC-1, and perform a tail on the `/var/log/ema/ema.log` file:

```
# tail -f /var/log/ema/ema.log
```

When the following is prompted, the upgrade is finished.

```
- upgraderhandler - INFO - *** Upgrade finished
```

```
- ema - DEBUG - INPUT: /var/log/installfiles/<Prod_Numbe  
r>-<Version>/ema post_upgrade: Duration: xx seconds
```

6. Check the `/home/actadm/config/log/config.log` and `/home/bootloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.
7. Log out and log in again to receive all the updated environment variables.
8. Check the result of the latest system status.

Run the following command:

```
# healthcheck.py show -d
```



Note: If any problems appear, check any created logs during the upgrade phase:

- Before reboot:

`/var/log/ema/ema_upgrade.log`

- After reboot:

`/var/log/ema/ema_post_upgrade-console.log`

`/var/log/ema/ema.log`

- Installation of new modules after reboot:

`/var/log/bootloader/bootloader.log`

9. Run CAI3G test traffic.

Run test traffic on ports (8080, 8181) to verify the updated nodes.

Note: Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.

Caution!

After the Dynamic Activation software upgrade is finished, it is important not to remove the `/var/log/installfiles` directory. Some files in this directory are used for rollback purposes.

Continue with the system health check, refer to Section 8.4 on page 80.

8.4 Network Setup Check

Check the network setup according to instructions in **Network Setup Check**, *System Administrators Guide for Native Deployment*, Reference [12].

After system health check, continue with the Cassandra upgrade, see Section 8.5 on page 80.



8.5 Upgrade Cassandra

Attention!

Before continuing with the upgrade of Cassandra, make sure the system works as expected. If proceeding with the Cassandra upgrade, it is not possible to perform a complete restore of the Dynamic Activation application.

If alternative 1 has been chosen (keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 10 on page 97.

If alternative 2 has been chosen (not keeping the processing logs in the Cassandra database), upgrade Cassandra according to instructions in Section 11 on page 107.

8.6 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users > Create Administrative User** in *System Administrators Guide for Native Deployment*, Reference [12].

8.7 Rollback to Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP5, and BSP 8100

This section contains information on how to perform a rollback from Dynamic Activation 1 to a Multi Activation 16.0 on Native Deployment, using SCXB3, CMXB3, GEP5 hardware and BSP 8100 network software.

To perform a rollback, follow the subsections:

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The rollback needs to be performed as user `root`, and from SC-1.



8.7.1 Rollback Cassandra

Attention!

To be able to perform a Dynamic Activation software rollback to Multi Activation 16.0, Cassandra needs to be in revision 2.0.15. If a Cassandra upgrade has been performed, roll back Cassandra according to Section 12 on page 113 before proceeding with the instructions in Section 8.7.2 on page 82.

8.7.2 Rollback the Multi Activation Software

To perform a rollback of the Dynamic Activation software, follow the step-list:

1. Rollback the network software:

For a network rollback, refer to the latest BSP R<x> Upgrade Instruction, found in the Ericsson Blade Server Platform (BSP) > BSP Rx catalog, in <http://calstore.internal.ericsson.com/alex>.

2. Rollback the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema rollback
```

The following is prompted:

```
All ongoing provisioning will fail during rollback.
Are you sure you want to continue with rollback? (y/n)
```

Enter **y** and press **Enter**

3. The `ema` script will roll back LDE, eVIP, and the Dynamic Activation system, and issue a reboot.

Login as user `root` on SC-1, and wait for the system to be fully installed.

4. Check the `/home/dveadm/config/log/config.log` and `/home/boottloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.

8.7.3 Health Check

Perform a health-check according to instructions in the step-list below.

1. Run the complete health-checks according to instructions in sections **Health Check on Multi Activation Common** and **Health Check on Multi Activation BSP 1.0 HW with BSP 8100** in Reference [20].



2. Run CAI3G test traffic.

Run test traffic on test ports (8080, 8181) to verify the rolled back nodes.





9 Upgrading from Native Multi Activation 16.1 or 16.2 Using SCXB3, CMXB3, GEP3/GEP5, and BSP 8100, to Native Multi Activation 1, Keeping the GEP3/GEP5 Blades

This section contains information on how to upgrade from a Native Multi Activation 16.1 or 16.2 system, using SCXB3, CMXB3, GEP3/GEP5, and BSP 8100 network software, to Dynamic Activation 1, and keeping the GEP3/GEP5 Blades.

9.1 General Upgrade Process

An upgrade from Multi Activation 16.1 or 16.2 to Dynamic Activation 1 consists of one maintenance window, as shown in Figure 8.

Upgrade Process

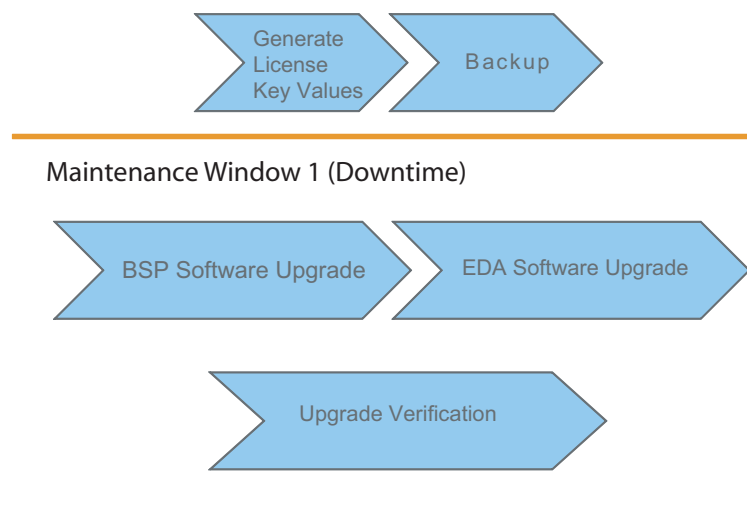


Figure 8 Upgrade Process

The following is noticeable and valuable information prior to performing the upgrade procedure from Multi Activation 16.1 or 16.2.

An upgrade is an upgrade of all RPMs (including LDE and eVIP), and modules on the current system to a newer software version.



The upgrade and rollback is proceeded with all nodes at once, with downtime. If any previously modified configuration files are affected by the upgrade, they may need to be modified again.

To see if a configuration file is replaced in platform RPMs, look in the `/home/actadm/config/log/config.log` file. Lines with correct date/time containing `Replacing` and `Backing up` are files that have been replaced. The backed up files are located in `/home/actadm/config/backup/<file><date>`

To see if a configuration file is replaced in the modules, look in the `/home/actadm/config/module_config_files/log/config.log` file. Lines with correct date/time containing `<config file> replaced due to new original file, old file renamed to <config file>.save` are files that has been replaced. The backed up files are located in `/home/actadm/config/module_config_files/<module>/<config_file>.save`

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

Any modules that have been manually added before the upgrade will be removed. After the upgrade, such modules need to be added again (manually).

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters) will be migrated during the upgrade.
- Proclogs

9.2 Backup

This section contains information on how to perform a backup.

9.2.1 System Backup

Before initiating a system upgrade, a full system backup should be performed. Table 13 shows the documentation references for each Multi Activation version.

Table 14 Full Backup References

Multi Activation Version	Reference
Multi Activation 16.1	See section Multi Activation Backup and Restore in Reference [4].
Multi Activation 16.2	See section Multi Activation Backup and Restore in Reference [5].

Note: Make sure to have everything in place before the upgrade, according to the *Pre-Upgrade Checklist* in Table 1.



9.2.2 Backup of evip.xml

Perform a backup of the `evip.xml` file by transferring (copy) it to a remote server.

The `evip.xml` file resides in the `/storage/system/config/evip-apr9010467/` directory.

Note: Do not rename origin `evip.xml` file, keep the same name.

9.3 Upgrade Procedure

This section contains information on how to upgrade the BSP 8100 software, and how to upgrade to the Dynamic Activation 1 software.

Time requirements for installing and configuring BSP 8100 and upgrading to the Dynamic Activation software, if `evip.xml` template is filled in and ready (with downtime):

Upgrade Step	Time Estimation (minutes)
Installation and configuration of BSP 8100 software, and Dynamic Activation software	105 (when <code>evip.xml</code> template is filled in and updated, with downtime)

9.3.1 Upgrade Preparations

Follow the instructions in the step-list to create a new `evip.xml` file:

1. Download the EDA Native BSP8100 Config Generator tool:
 - Save the zip file, [EDA Native BSP8100 Config Generator.zip](#) to, for example a local area on a local machine
 - Unpack the zip file.
2. Start the EDA Native BSP8100 Config Generator tool by double-clicking the `Activation_ConfigGen.jar` file, located in the folder where the tool was unzipped.

Note: Requires Oracle's JAVA version 1.8.0_71 or higher.

3. Fill in the required values, according to the figure below (see red boxes):

Figure 9 EDA Config Generator Tool

Attention!

Make sure the names of the hosts (HOSTNAME-SC-1, HOSTNAME-SC-2, HOSTNAME-PL-3, HOSTNAME-PL-x) match the names that are currently present in the running `cluster.conf` file.

Make sure the DNS IP Addresses match (Amount and IP address) the current, running `cluster.conf` file settings.

- When all values are filled in, click on the **Generate Artifacts** button and choose **evip.xml** in the prompted **Selection** window:



Selection

Only evip.xml or all artifacts?

5. Save the generated `evip.xml` file on the local machine.
6. Create a new `evip.xml` file using the newly generated `evip.xml` file in Step 5, to `/var/log/installfiles/` on SC-1:

```
# vi /var/log/installfiles/evip.xml
```

Note: Make sure to have everything in place, according to the *Pre-Upgrade Checklist* in Table 1.

9.3.2

BSP 8100 Upgrade Instructions

1. Upgrade to the latest BSP software Release (BSP R_{<X>}), and follow the BSP Upgrade Instruction found in Ericsson Blade Server Platform (BSP) catalog, in <http://calstore.internal.ericsson.com/alex>

Note: The default SCX root user password is `tre,14`

The default SCX advanced user password is `ett,30`

The default CMX root user password is `tre,14`

The default CMX advanced user password is `ett,30`

Continue with Section 9.3.3 on page 89.

9.3.3

Dynamic Activation Upgrade Instructions

Upgrade to Dynamic Activation 1 only supports **All nodes with downtime**. The upgrade sequence will upgrade LDE, eVIP, and the Dynamic Activation system.

Caution!

Before starting the upgrade procedure, make sure the new value package licenses are ordered for the new EDA 1 system.



9.3.3.1 Dynamic Activation Upgrade Preparations

A provisioning client with `Full` authorities for the Configuration Management Authorities is needed during the upgrade. Add one if not already available. The provisioning client is added in the old Multi Activation GUI, **Access Control>Users** tab. For instructions, refer to section **Access Control** in Reference [25] if using Multi Activation 16.1, or Reference [26] if using Multi Activation 16.2.

On SC-1:

1. Transfer the Dynamic Activation software to the `/var/log/installfiles` directory on SC-1.

2. Change directory:

```
# cd /var/log/installfiles/
```

3. Untar the software (EDA System Base SW):

```
# tar -zxf <Software_Package>.tar.gz
```

9.3.3.2 Dynamic Activation Software Upgrade

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The upgrade needs to be performed as user `root`, and from SC-1.

The `ema_upgrade` script will upgrade LDE, eVIP, and issue a reboot. After the reboot, the script will automatically continue to upgrade the Dynamic Activation system and install the new licenses.

1. Obtain the license locking codes for the system.

From SC-1:

```
# /var/log/installfiles/<Prod_Number>-<Version>/ema  
licenseCodes
```

Output:



```
INFO - *** Locking codes for <SC-1>:
INFO - ***
      Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Info
      Copyright (C) 2015 SafeNet, Inc.
```

```
      Locking Code 1      : 2008-*1NE URGH T85R V4K4
      Locking Code 1 (Old Style) : 2008-292BD
```

```
INFO - *** Locking codes for <SC-2>:
INFO - ***
      Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Info
      Copyright (C) 2015 SafeNet, Inc.
```

```
      Locking Code 1      : 2008-*1PW 65F3 8ABD KJET
      Locking Code 1 (Old Style) : 2008-66063
```

2. Provide all Locking Code for the Ericsson License Information System (ELIS) and get the license file.
3. Transfer (SFTP) the license file to the `/var/log/installfiles/` directory on SC1, and rename the file to `license.txt`. This will automatically install all license files when running the `./ema_upgrade` upgrade script.
4. Upgrade the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema_upgrade upgrade
```

Note: Only **Resource Activation** (in 16.0 - 16.2 called Subscriber Activation (SA)) will be installed.

The following is prompted:

```
All ongoing provisioning will fail during upgrade.
Are you sure you want to continue with upgrade? (y/n)
```

Enter **y** and press **Enter**



Note: If error message:

```
ERROR - *** IP addresses for OSPF areas differs
in
running evip and CMX, must use the same IP
addresses.
, check the Delivery Report for current release and add required
software package.
```

The following is prompted:

Please enter provisioning client user name:

Enter name of a provisioning user with Full authorities and press **Enter**.

The following is prompted:

```
INFO - *** Please enter your provisioning client
password.
Password:
```

Enter password and press **Enter**.

5. To know when the upgrade is finished, after the reboot, login as user `root` on SC-1, and perform a tail on the `/var/log/ema/ema.log` file:

```
# tail -f /var/log/ema/ema.log
```

When the following is prompted, continue with the next step in the step-list:

```
- upgradehandler - INFO - *** Upgrade finished

- ema - DEBUG - INPUT: /var/log/installfiles/<Prod_Number>-<Version>/ema post_upgrade: Duration: xx seconds
```

6. Check the `/home/actadm/config/log/config.log` and `/home/boottloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.
7. Log out and log in again to receive all the updated environment variables.
8. Check the result of the latest system status.

Run the following command:

```
# healthcheck.py show -d
```



Note: If any problems appear, check any created logs during the upgrade phase:

- Before reboot:

`/var/log/ema/ema_upgrade.log`

- After reboot:

`/var/log/ema/ema_post_upgrade-console.log`

`/var/log/ema/ema.log`

- Installation of new modules after reboot:

`/var/log/bootloader/bootloader.log`

9. Run CAI3G test traffic.

Run test traffic on ports (8080, 8181) to verify the updated nodes.

10. Check the network setup according to instructions in **Network Setup Check**, *System Administrators Guide for Native Deployment*, Reference [12].

The upgrade is finished.

Caution!

After the Dynamic Activation software upgrade is finished, it is important not to remove the `/var/log/installfiles` directory. Some files in this directory are used for rollback purposes.

9.4 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users > Create Administrative User** in *System Administrators Guide for Native Deployment*, Reference [12].



9.5 Rollback to Multi Activation 16.1 or 16.2 on Native Deployment, using SCXB3, CMXB3, GEP3/GEP5, and BSP 8100

This section contains information on how to perform a rollback from Dynamic Activation 1 to a Multi Activation 16.1 or 16.2 on Native Deployment, using SCXB3, CMXB3, GEP3/GEP5 hardware and BSP 8100 network software.

To perform a rollback, follow the step-list:

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The rollback needs to be performed as user `root`, and from SC-1.

1. Rollback the network software:

For a network rollback, refer to the latest BSP R<x> Upgrade Instruction, found in the Ericsson Blade Server Platform (BSP) > BSP Rx catalog, in <http://calstore.internal.ericsson.com/alex>.

2. Rollback the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema rollback
```

The following is prompted:

```
All ongoing provisioning will fail during rollback.  
Are you sure you want to continue with rollback? (y/n)
```

Enter **y** and press **Enter**

3. The `ema` script will roll back LDE, eVIP, and the Dynamic Activation system, and issue a reboot.

Login as user `root` on SC-1, and wait for the system to be fully installed.

4. Check the `/home/actadm/config/log/config.log` and `/home/actadm/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured.

9.5.1 Health Check

Perform a health-check according to instructions in the step-list below.



1. Run the complete health-checks according to instructions in section **Health Check on Multi Activation**.

For Multi Activation 16.1, refer to Reference [21].

For Multi Activation 16.2, refer to Reference [22].

2. Run CAI3G test traffic.

Run test traffic on test ports (8080, 8181) to verify the rolled back nodes.

Note: Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.





10 Cassandra Upgrade (Alternative 1)

This section contains information on how to upgrade the Cassandra database, and keeping the processing logs. That is, the processing logs will follow the upgrade and be kept in the Cassandra database.

Attention!

If a System File-Backup of the Cassandra database is not performed, it will not be possible to restore any processing logs in case of a Cassandra rollback. A Cassandra rollback is supported though.

The Cassandra upgrade is only applicable for Native upgrade from Multi Activation 16.0 to Dynamic Activation 1. It does not apply if upgrading from Multi Activation 16.1 or 16.2, Cassandra does not need to be upgraded in these cases.

The following chart depicts the Cassandra upgrade procedure:

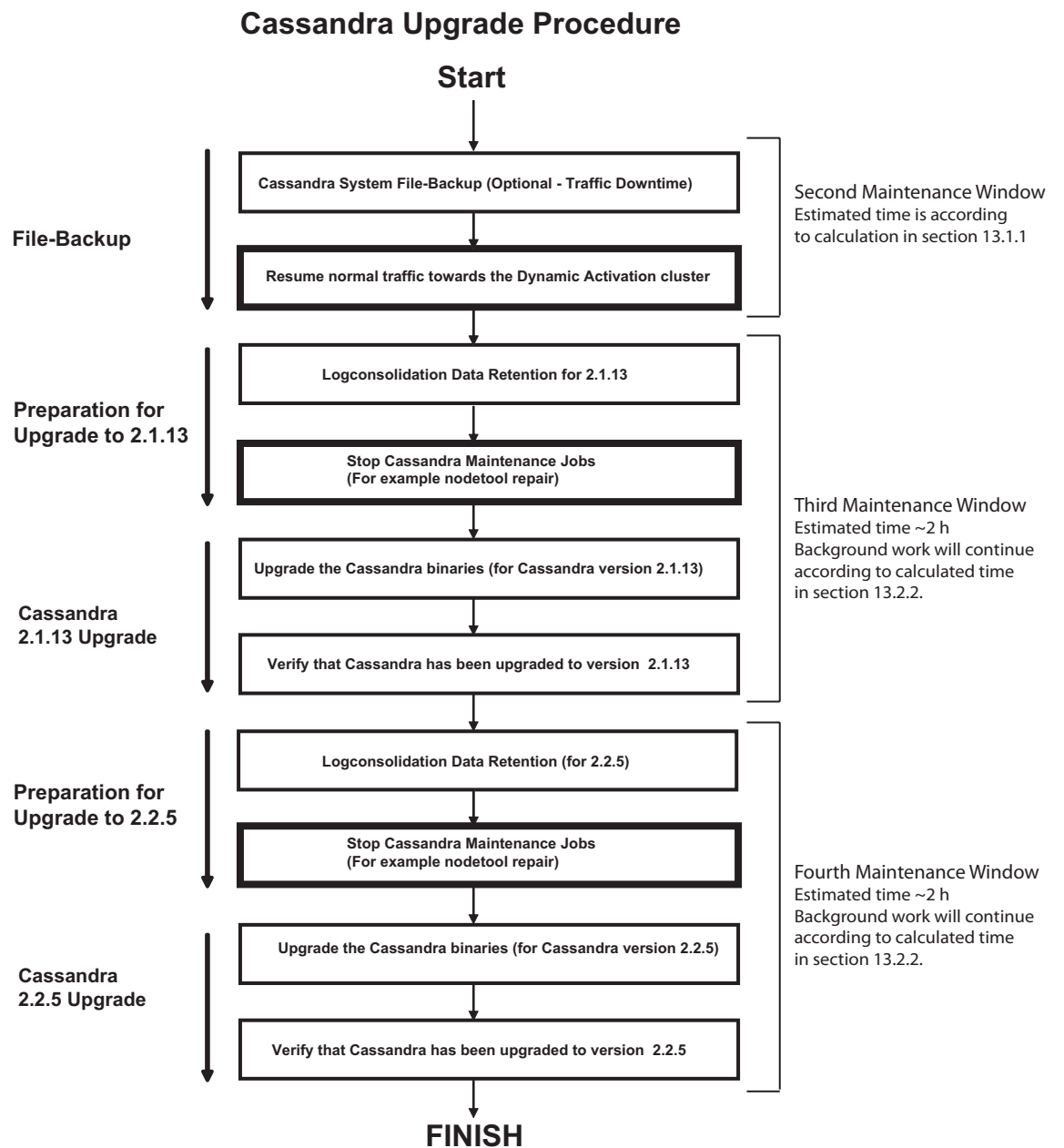


Figure 10 Cassandra Upgrade Procedure Overview

10.1 Cassandra System File-Backup (Optional - Downtime)

Start of second maintenance window



Attention!

To be able to perform a rollback of the Cassandra database (with data), a system file-backup is needed. Though, due to the large amount of time a system file-backup will take, this procedure is optional.

Time Estimation Example:

Elapsed time for this backup, and the corresponding downtime for traffic, depend on the amount of data that is persisted in Cassandra.

This time will also depend on the network speed and disk speed of the backup location.

With a large amount of data, a backup operation will take a considerable amount of time to complete.

As an example, if using a connection speed of 1 GB/s, and 100 GB of data in `/var/cassandra` is to be transferred from the cluster to a remote location, the backup will take approximately 15 minutes.

Note: This must be done for all nodes in the cluster.

Attention!

This procedure will cause traffic downtime until a complete Cassandra backup has been performed.

If this procedure is not performed, in case of a rollback, it is not possible to restore the Cassandra data.

To perform a system file-backup, follow the step-list:

1. Stop all traffic going towards the Dynamic Activation cluster.
2. Stop all processes. Run the following commands on SC1:

```
# bootloader.py node stop -H all
```

```
# 3ppmon stopcassandra -H all
```

3. For each node in the cluster, backup the `/var/cassandra/` directory to an external storage.

Note: Make sure to keep track of each nodes content.



On the backup location, create the backup directory:

```
# mkdir -p /<backup_location_nodeId>/cassandra
```

Run the following command:

```
# scp -r /var/cassandra/ <user>@<remote_host>:<backup_location_nodeId>
```

Time Estimation Example:

Connection Speed (Cluster)	Data Size (Cluster)	Time (Cluster)
1 GB/s	100 GB	15 minutes

4. When all node-data is backed up, start all processes on all nodes in the cluster. Run the following commands on SC1:

```
# 3ppmon startcassandra -H all
```

```
# bootloader.py node start -H all
```

5. Check the status on the cluster:

```
# healthcheck.py run -n Activation_all_Native
```

6. Resume normal traffic towards the Dynamic Activation cluster.

End of second maintenance window

Continue with the third maintenance window, see Preparation of Upgrade procedure in the sub-sections below.

10.2 Upgrade to Cassandra 2.1.13

Start of third maintenance window

This section includes information on how to upgrade Cassandra to version 2.1.13.

10.2.1 Logconsolidation Data Retention

Note: Due to the time constraints of a Dynamic Activation upgrade, combined with the time impact of upgrading Cassandra when considerable amount of data is present, the amount of how many logconsolidation days of proclogs that should follow to the upgrade Dynamic Activation 1 system, must be considered.

The Cassandra upgrade time will depend on the amount of proclogs according to the following formula: $t = d / t_r$, where t = time in minutes, d = amount of data in bytes, and t_r = transfer-rate constant, which by default is 215000000.



Follow the instruction in the step-list to retain the desired data:

1. With the $t = d / tr$ formula, calculate how long an upgrade would take with the current amount of data in the existing cluster.

To get the amount of data in bytes, run the following command from an SC node:

```
# du -hbc /var/cassandra/data/ | grep total
```

Printout example:

193273528320 total, meaning there is a total amount of 193273528320 bytes of data.

If calculating with the above printout, the formula gives us, t (time in minutes) = $193273528320 / 215000000 = 899$ minutes.

If the calculated time is acceptable, continue with the upgrade, refer to Section 10.2.2 on page 101.

If the calculated time is not acceptable, continue with the next step.

2. Delete a day from the database by running the following command.

Login as user `root` and run the following commands:

```
# cd /usr/local/pgngn/admin-tool-<version>/bin
```

```
# sudo -u actadm ./proclog-admin-tool.sh -ro
```

Note: The `sudo -u actadm ./proclog-admin-tool.sh -ro` command will irreversibly delete the data for the last day in the database.

3. Recalculate the amount of data to reduce. Again, use the formula, $t = d / tr$.

If the target time is not reached, perform Step 2 - Step 3 repeatedly to reach the target time.

Note: Check the total amount of data after each time the `sudo -u actadm ./proclog-admin-tool.sh -ro` command is run.

10.2.2 Upgrade Cassandra to Version 2.1.13 (Without Downtime)

This chapter describes how to upgrade Cassandra to 2.1.13 (needed intermediate upgrade).

Note: To be able to perform a rollback of the Cassandra data, the optional system file-backup needs to be in place, see Section 10.1 on page 98.



To upgrade Cassandra from version 2.0.x to version 2.1.13, follow the procedure in the step-lists below.

Caution!

Do not run any Cassandra maintenance jobs such as `nodetool repair` during the Cassandra upgrade. It is possible, if any existing maintenance jobs are needed, to temporary start those, AFTER the Cassandra upgrade to version 2.1.13 is completed (including SSTables background job).

Do not perform any database schema changes on Cassandra during the upgrade procedure.

Regardless of the Cassandra version that operates on the current system, the script will automatically upgrade to the next Cassandra version. The version order is as follows: `2.0.x > 2.1.13 > 2.2.5`. This means that the Cassandra upgrade script will have to run twice for the system to be fully upgraded.

10.2.2.1 Upgrade to Cassandra 2.1.13 (Without Downtime)

1. Log in as user `root` and run the following command on each Dynamic Activation node, one by one, to verify that all nodes are UP and Normal:

```
# nodetool status logconsolidation
```

All nodes in the printout should have status UP and state Normal, UN.

2. Upgrade of the Cassandra binaries on all Dynamic Activation nodes, and start of SSTables background job.

On SC-1, and run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema cassandra --upgrade
```

3. Run the following command to check the status of the SSTables background job:

```
# ./ema cassandra --upgrade --status
```



Attention!

The SSTables job will continue in the background. The time for this job to finish will be according to the calculated estimate in Section 10.2.1 on page 100.

This background job must finish before the upgrade of Cassandra version 2.2.5 can start (fourth maintenance window).

The command will show the status per node, in percentage, of the SSTables progress:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.0.15 to 2.1.13
INFO - *** Node 1's upgrade is 76% left
INFO - *** Node 2's upgrade is 75% left
INFO - *** Node 3's upgrade is 73% left
INFO - *** Node 4's upgrade is 75% left
```

When the following is prompted, all SSTables are upgraded:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.0.15 to 2.1.13
INFO - *** Node 1's upgrade has completed
INFO - *** Node 2's upgrade has completed
INFO - *** Node 3's upgrade has completed
INFO - *** Node 4's upgrade has completed
```

End of third maintenance window

The Cassandra upgrade to version 2.1.13 is now completed.

10.3 Preparation of Upgrade to Cassandra 2.2.5

Start of fourth maintenance window

This section includes information on how to upgrade Cassandra to version 2.2.5.



10.3.1 Logconsolidation Data Retention

Note: Due to the time constraints of a Dynamic Activation upgrade, combined with the time impact of upgrading Cassandra when considerable amount of data is present, the amount of how many logconsolidation days of proclogs that should follow to the upgraded Dynamic Activation1 system, must be considered.

The Cassandra upgrade time will depend on the amount of proclogs according to the following formula: $t = d / tr$, where t = time in minutes, d = amount of data in bytes, and tr = transfer-rate constant, which by default is 169000000.

Follow the instruction in the step-list to retain the desired data:

1. With the $t = d / tr$ formula, calculate how long an upgrade would take with the current amount of data in the existing cluster.

To get the amount of data in bytes, run the following command from an SC node:

```
# du -hbc /var/cassandra/data/ | grep total
```

Printout example:

193273528320 total, meaning there is a total amount of 193273528320 bytes of data.

If calculating with the above printout, the formula gives us, t (time in minutes) = $193273528320 / 169000000 = 1144$ minutes.

If the calculated time is acceptable, continue with the upgrade, refer to Section 10.2.2 on page 101.

If the calculated time is not acceptable, continue with the next step.

2. Delete a day from the database by running the following command:

Login as user `root` and run the following commands:

```
# cd /usr/local/pgngn/admin-tool-<version>/bin
```

```
# sudo -u actadm ./proclog-admin-tool.sh -ro
```

Note: The `sudo -u actadm ./proclog-admin-tool.sh -ro` command will irreversibly delete the data for the last day in the database.

3. Recalculate the amount of data to reduce. Again, use the formula, $t = d / tr$.

If the target time is not reached, perform Step 2 - Step 3 repeatedly to reach the target time.



Note: Check the total amount of data after each time the `sudo -u actadm ./proclog-admin-tool.sh -ro` command is run.

10.3.2 Upgrade Cassandra (Without Downtime)

This chapter describes how to upgrade Cassandra to 2.2.5.

To fully upgrade Cassandra from version 2.1.13 to version 2.2.5, follow the procedure below.

Caution!

Do not run any Cassandra maintenance jobs such as `nodetool repair` during the Cassandra upgrade. It is possible, if any existing maintenance jobs are needed, to start those, AFTER the Cassandra upgrade to version 2.2.5 is completed (including SSTables background job).

Do not perform any database schema changes on Cassandra during the upgrade procedure.

10.3.2.1 Upgrade to Cassandra 2.2.5 (Without Downtime)

1. Log in as user `root` and run the following command on each Dynamic Activation node, one by one, to verify that all nodes are UP and Normal:

```
# nodetool status logconsolidation
```

All nodes in the printout should have status UP and state Normal, UN.

2. Upgrade of the Cassandra binaries on all Dynamic Activation nodes, and start of SSTables background job.

On SC-1, and run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema cassandra --upgrade
```

3. Run the following command to check the status of the SSTables background job:

```
# ./ema cassandra --upgrade --status
```



Attention!

The SSTables job will continue in the background. The time for this job to finish will be according to the calculated estimate in Section 10.3.1 on page 103.

The command will show the status per node, in percentage, of the SSTables progress:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.1.13 to 2.2.5
INFO - *** Node 1's upgrade is 90% left
INFO - *** Node 2's upgrade is 87% left
INFO - *** Node 3's upgrade is 82% left
INFO - *** Node 4's upgrade is 68% left
```

When the following is prompted, all SSTables are upgraded:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.1.13 to 2.2.5
INFO - *** Node 1's upgrade has completed
INFO - *** Node 2's upgrade has completed
INFO - *** Node 3's upgrade has completed
INFO - *** Node 4's upgrade has completed
```

End of fourth maintenance window

The Cassandra upgrade to version 2.2.5 is now completed.



11 Cassandra Upgrade (Alternative 2)

This section contains information on how to upgrade the Cassandra database, but not keeping the processing logs. That is, the processing logs will not follow the upgrade.

Attention!

If this alternative is chosen, it will not be possible to restore any processing logs in case of a Cassandra rollback. A Cassandra rollback is supported though.

The Cassandra upgrade is only applicable for Native upgrade from Multi Activation 16.0 to Dynamic Activation 1. It does not apply if upgrading from Multi Activation 16.1 or 16.2. Cassandra does not need to be upgraded in this case.

The following chart depicts the Cassandra upgrade procedure:

Cassandra Upgrade Procedure - Exportingt the Proclogs (Alternative 2)

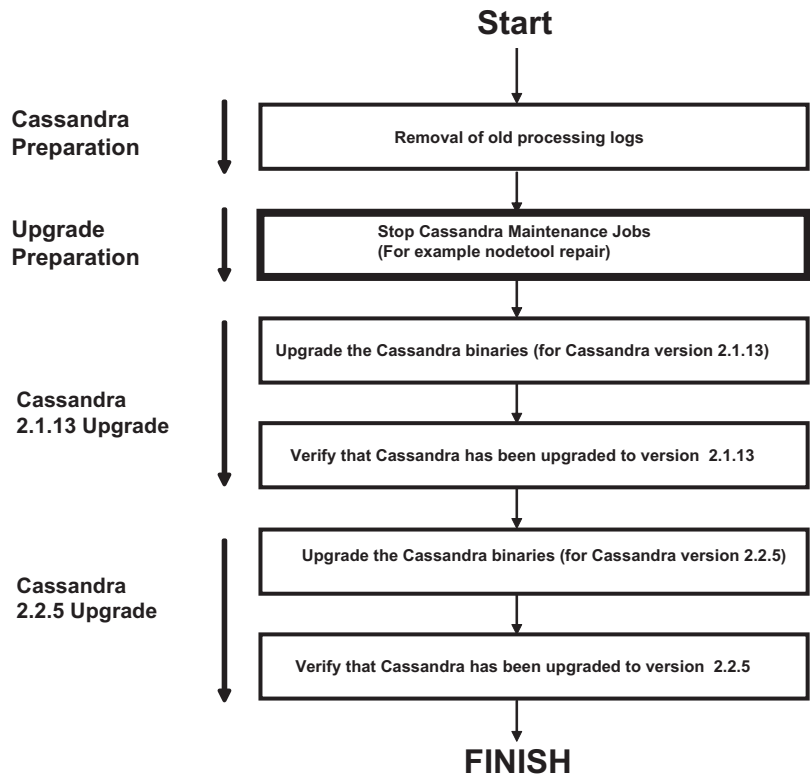


Figure 11 Cassandra Upgrade Procedure (Alternative 2) Overview



11.1 Remove all Processing Logs in Cassandra

To be able to perform a Cassandra upgrade in one maintenance window, it needs to be done without keeping any processing logs.

To remove the processing logs, follow the step-list:

Attention!

From Step 3 throughout Step 7, all processing logs will be deleted.

1. Log in as user `root` to SC-1.
2. Run the following command to extract the number of days the current system keeps proclogs:

```
# bootloader.py config list -A | grep CASSANDRA_NUMBER_OF_DAYS_STORED
```

Example printout:

```
system configured: @CASSANDRA_NUMBER_OF_DAYS_STORED@ = 30
```

Attention!

Take a note of the existing number of stored days. This will be used when restoring the `@CASSANDRA_NUMBER_OF_DAYS_STORED@` parameter, after upgrading Cassandra.

3. Set the `@CASSANDRA_NUMBER_OF_DAYS_STORED@` parameter to 1:

```
# bootloader.py config set --parameter @CASSANDRA_NUMBER_OF_DAYS_STORED@ --value 1
```

This will keep one days of stored processing logs in the system.

The following is printed:

```
INFO - *** @CASSANDRA_NUMBER_OF_DAYS_STORED@=<Same as in step 2> a
INFO - *** @CASSANDRA_NUMBER_OF_DAYS_STORED@=1 inserted in user co
INFO - *** To activate the changed parameter, execute
"bootloader.py node activate --host <hostname>" command
```



4. Verify that the @CASSANDRA_NUMBER_OF_DAYS_STORED@ parameter is set to 1 before activating the change:

```
# bootloader.py config list -A | grep CASSANDRA_NUMBER_OF_DAYS_STORED
```

Expected printout:

```
system configured: @CASSANDRA_NUMBER_OF_DAYS_STORED@ = 1
```

5. Run the following command to activate the change on all nodes:

Note: Running this script, activating all nodes at once will cause downtime. An alternative to avoid downtime is to run the command node by node.

```
# bootloader.py node activate --host all
```

6. The following command will remove all old processing logs, except for the last one:

```
# sudo -u actadm /usr/local/pgngn/admin-tool-*/bin/proc-log-retain-maximum-days.sh
```

7. Run the following command to remove the last stored processing log day:

```
# sudo -u actadm /usr/local/pgngn/admin-tool-*/bin/proc-log-admin-tool.sh -ro
```

8. Check that the processing logs are removed:

```
# sudo -u actadm /usr/local/pgngn/admin-tool-*/bin/proc-log-admin-tool.sh -l
```

Only the current day and the day after should be listed.

9. Reconfigure the @CASSANDRA_NUMBER_OF_DAYS_STORED@ parameter to the same value as extracted in Step 2:

```
# bootloader.py config set --parameter @CASSANDRA_NUMBER_OF_DAYS_STORED@ --value <Same_as_Step2>
```

The following is printed:

```
INFO - *** @CASSANDRA_NUMBER_OF_DAYS_STORED@=1 already exist, wi
INFO - *** @CASSANDRA_NUMBER_OF_DAYS_STORED@=<Same as in step 2>
INFO - *** To activate the changed parameter, execute
"bootloader.py node activate --host <hostname>" command
```

10. Run the following command to activate the change on all nodes:



Note: Running this script, activating all nodes at once will cause downtime. An alternative to avoid downtime is to run the command node by node.

```
# bootloader.py node activate --host all
```

Continue with the next section to upgrade Cassandra to 2.1.13.

11.2 Upgrade Cassandra to Version 2.1.13

This chapter describes how to upgrade Cassandra to 2.1.13 (needed intermediate upgrade).

To upgrade Cassandra from version 2.0.x to version 2.1.13, follow the procedure in the step-lists below.

Caution!

Do not run any Cassandra maintenance jobs such as `nodetool repair` during the Cassandra upgrade. It is possible, if any existing maintenance jobs are needed, to temporary start those, AFTER the Cassandra upgrade to version 2.1.13 is completed (including SSTables background job).

Do not perform any database schema changes on Cassandra during the upgrade procedure.

Regardless of the Cassandra version that operates on the current system, the script will automatically upgrade to the next Cassandra version. The version order is as follows: 2.0.x > 2.1.13 > 2.2.5. This means that the Cassandra upgrade script will have to run twice for the system to be fully upgraded.

11.2.1 Upgrade to Cassandra 2.1.13

1. Log in as user `root` and run the following command on each Dynamic Activation node, one by one, to verify that all nodes are UP and Normal:

```
# nodetool status logconsolidation
```

All nodes in the printout should have status UP and state Normal, UN.

2. Upgrade of the Cassandra binaries on all Dynamic Activation nodes, and start of SSTables background job.

On SC-1, and run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```



```
# ./ema cassandra --upgrade
```

3. Run the following command to check the status of the SSTables background job:

```
# ./ema cassandra --upgrade --status
```

The command will show the status per node, in percentage, of the SSTables progress:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.0.15 to 2.1.13
INFO - *** Node 1's upgrade is 76% left
INFO - *** Node 2's upgrade is 75% left
INFO - *** Node 3's upgrade is 73% left
INFO - *** Node 4's upgrade is 75% left
```

When the following is prompted, all SSTables are upgraded:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.0.15 to 2.1.13
INFO - *** Node 1's upgrade has completed
INFO - *** Node 2's upgrade has completed
INFO - *** Node 3's upgrade has completed
INFO - *** Node 4's upgrade has completed
```

The Cassandra upgrade to version 2.1.13 is now completed.

Continue with the next section to upgrade Cassandra to 2.2.5.

11.3 Upgrade Cassandra to Cassandra 2.2.5

This chapter describes how to upgrade Cassandra to 2.2.5.

To fully upgrade Cassandra from version 2.1.13 to version 2.2.5, follow the procedure below.

Caution!

Do not run any Cassandra maintenance jobs such as `nodetool repair` during the Cassandra upgrade. It is possible, if any existing maintenance jobs are needed, to start those, AFTER the Cassandra upgrade to version 2.2.5 is completed (including SSTables background job).

Do not perform any database schema changes on Cassandra during the upgrade procedure.



11.3.1 Upgrade to Cassandra 2.2.5

1. Log in as user `root` and run the following command on each Dynamic Activation node, one by one, to verify that all nodes are UP and Normal:

```
# nodetool status logconsolidation
```

All nodes in the printout should have status UP and state Normal, UN.

2. Upgrade of the Cassandra binaries on all Dynamic Activation nodes, and start of SSTables background job.

On SC-1, and run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema cassandra --upgrade
```

3. Run the following command to check the status of the SSTables background job:

```
# ./ema cassandra --upgrade --status
```

The command will show the status per node, in percentage, of the SSTables progress:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.1.13 to 2.2.5
INFO - *** Node 1's upgrade is 90% left
INFO - *** Node 2's upgrade is 87% left
INFO - *** Node 3's upgrade is 82% left
INFO - *** Node 4's upgrade is 68% left
```

When the following is prompted, all SSTables are upgraded:

Printout Example:

```
INFO - *** Checking status for Cassandra upgrade from 2.1.13 to 2.2.5
INFO - *** Node 1's upgrade has completed
INFO - *** Node 2's upgrade has completed
INFO - *** Node 3's upgrade has completed
INFO - *** Node 4's upgrade has completed
```

4. Check the Cassandra performance after fully upgrade.

```
# nodetool status logconsolidation
```

All nodes in the printout should have status UP and state Normal, UN.

The Cassandra upgrade to version 2.2.5 is now completed.



12 Rollback Cassandra With Processing Logs Backup

In the event of an upgrade Cassandra failure, a rollback of the Cassandra database can be performed by following the step-list below.

Prerequisites:

- File-Backup of Cassandra data has been performed according to Section 10.1 on page 98.

Note: This part is only applicable for Alternative 1, and if wanting to rollback all Cassandra processing log data.

- Cassandra upgrade to either version 2.1.13 or 2.2.5 is completed.

Note: It is only possible to rollback to the original Cassandra version 2.0.15, regardless if rolling back from version 2.1.13 or 2.2.5.

- Stop all traffic going towards the Dynamic Activation cluster.
- Log in as user `root` and run the following command on SC-1:

```
# zkCli.sh -server 0:6181 set /system/cassandra/version 2.0.15
```

- Verify that the Cassandra version is set to 2.0.15.

```
# zkCli.sh -server 0:6181 get /system/cassandra/version
```

- Stop all processes. Run the following commands on SC1:

```
# bootloader.py node stop -H all
```

```
# 3ppmon stopcassandra -H all
```

- From SC-1, run the following command, for each node in the cluster, one by one, to downgrade the Cassandra RPM:

```
# cluster rpm --upgrade cassandra-2.0.15.rpm -n <nodeId>
```

Note: <nodeId> is:

<nodeId>	1	2	3	4	...
node	SC-1	SC-2	PL-3	PL-4	...

- Remove current Cassandra data. Run the following commands on all nodes in the cluster:



```
# rm -rf /var/cassandra
```

The following is printed:

```
rm: cannot remove '/var/cassandra/data': Device or resource busy
rm: cannot remove '/var/cassandra/commitlog': Device or resource busy
```

Note: The printout is as it should since `/var/cassandra/data`, and `/var/cassandra/commitlog` are mount-points.

7. From SC-1, run the following command to remove `casadm`:

```
# rm -rf /home/casadm/nodes/*/cassandra
```

8. For each node in the cluster, restore the `/var/cassandra/` directory from an external storage.

Note: Make sure to keep track of each nodes content.

Run the following command:

```
# scp -r <user>@<remote_host>:<backup_location_nodeId>/cassandra /var
```

Time Estimation Example:

Connection Speed (Cluster)	Data Size (Cluster)	Time (Cluster)
1 GB/s	100 GB	15 minutes

9. Reboot the cluster. Run the following command on SC1:

```
# cluster reboot -a
```

10. Start all processes. Run the following command on SC1:

```
# bootloader.py node start -H all
```

11. Check the status on the cluster.

Run the following commands:

```
# 3ppmon status --host all
```

```
# bootloader.py node status --host all
```

If the status is OK, all processes should be UP and running, resume normal traffic towards the Dynamic Activation cluster.

The Cassandra rollback is completed.



13 Rollback Cassandra Without Processing Logs Backup

In the event of an upgrade Cassandra failure, a rollback of the Cassandra database can be performed by following the step-list below.

Prerequisites:

- File-Backup of Cassandra processing log data has not been performed.
- Cassandra upgrade to either version 2.1.13 or 2.2.5 is completed.

Note: It is only possible to rollback to the original Cassandra version 2.0.15, regardless if rolling back from version 2.1.13 or 2.2.5.

1. Stop all traffic going towards the Dynamic Activation cluster.
2. Log in as user `root` and run the following command on SC-1:

```
# zkCli.sh -server 0:6181 set /system/cassandra/version 2.0.15
```

3. Verify that the Cassandra version is set to 2.0.15.

```
# zkCli.sh -server 0:6181 get /system/cassandra/version
```

4. Stop all processes. Run the following commands on SC1:

```
# bootloader.py node stop -H all
```

```
# 3ppmon stopcassandra -H all
```

5. From SC-1, run the following command, for each node in the cluster, one by one, to downgrade the Cassandra RPM:

```
# cluster rpm --upgrade cassandra-2.0.15.rpm -n <nodeId>
```

Note: <nodeId> is:

<nodeId>	1	2	3	4	...
node	SC-1	SC-2	PL-3	PL-4	...

6. Remove current Cassandra data. Run the following commands on all nodes in the cluster:

```
# rm -rf /var/cassandra
```

The following is printed:



```
rm: cannot remove '/var/cassandra/data': Device or resource busy
rm: cannot remove '/var/cassandra/commitlog': Device or resource busy
```

Note: The printout is as it should since `/var/cassandra/data`, and `/var/cassandra/commitlog` are mount-points.

7. From SC-1, run the following command to remove `casadm`:

```
# rm -rf /home/casadm/nodes/*/cassandra
```

8. Reboot the cluster. Run the following command on SC1:

```
# cluster reboot -a
```

9. Start all processes. Run the following command on SC1:

```
# bootloader.py node start -H all
```

10. From SC-1, run the following commands to restore the data models:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/data
-model
```

```
# tar -zxf datamodel-cassandra-<Version>.tar.gz
```

```
# /var/log/installfiles/<Prod_Number>-<Version>/data-model
l/install-datamodels.sh <SC1_hostname> 6160
```

```
# bootloader.py node activate --host all
```

11. Check the status on the cluster.

Run the following commands:

```
# 3ppmon status --host all
```

```
# bootloader.py node status --host all
```

If the status is OK, all processes should be `UP` and running, resume normal traffic towards the Dynamic Activation cluster.

The Cassandra rollback is completed.



14 Upgrading from Virtual Multi Activation 16.0, 16.1 or 16.2 to Virtual Dynamic Activation 1

This section contains information on how to upgrade from a Virtual Multi Activation 16.0, 16.1 or 16.2 system to a Virtual Dynamic Activation 1 system.

It does also include rollback information on various scenarios, see applicable steps in Section 14.3.2 on page 120.

14.1 Prerequisites

To be able to upgrade from Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1, a set of prerequisites needs to be followed.

Before starting the upgrade procedure, make sure:

- To check the Delivery Report before proceeding with this part of the document. The Delivery Report contains information about known problems, limitations and exceptions related to the system software that will be upgraded. It can contain complementary instructions and information, that may prevent system failure and damage.
- That the external block storage is in place for the new Dynamic Activation 1 deployment. For instructions on how to setup external block storage, see section **Set Up Persistent Block Storage on VMs (KVM/VMware)** in *System Administrators Guide for Virtual and Cloud Deployment*, Reference [11].
- That the host system meets the latest prerequisites described in *Requirements on Virtualization and Cloud Infrastructure*, Reference [19].
- That new license keys are ordered for the new Dynamic Activation 1 cluster.
- That the current 16.0, 16.1 or 16.2 cluster is running on latest CP release.
- That the old `.ds` file for the deployment tool is available or recreated.
- That the latest Dynamic Activation 1 Ericsson Deployment Manager (EDM) tool is available, refer to *Software Installation for Virtual and Cloud Deployment*, Reference [16].
- That new test ports 9995, and 9996 are opened in the firewall towards the current Multi Activation 16.0, 16.1 or 16.2 cluster.
- The new Dynamic Activation 1 cluster needs to have the private/internal IP addresses in the same subnet as the old Multi Activation 16.0, 16.1 or 16.2 cluster.



14.2 General Upgrade Process

An upgrade from Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1 consists of one maintenance window.

During the upgrade, the old Multi Activation 16.0, 16.1 or 16.2 cluster is left intact as it is, in case of rollback scenario, and a new Dynamic Activation 1 cluster is installed.

Note: During the upgrade process, the new Dynamic Activation 1 cluster must be accessed through serial interface (console).

A new license must be ordered for the new Dynamic Activation 1 cluster.

The external VIP addresses are reused from the old Multi Activation 16.0, 16.1 or 16.2 cluster.

If upgrading from Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1, see Section 14.3 on page 118.

Any modules or adaptations that have been manually added to this specific system before the upgrade will be removed. After the upgrade, such modules or adaptations need to be added again (manually).

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

14.3 Upgrade Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1

The following chart depicts the upgrade procedure from Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1, see Figure 12.



Upgrade MA 16.0, 16.1 or 16.2 to EDA 1

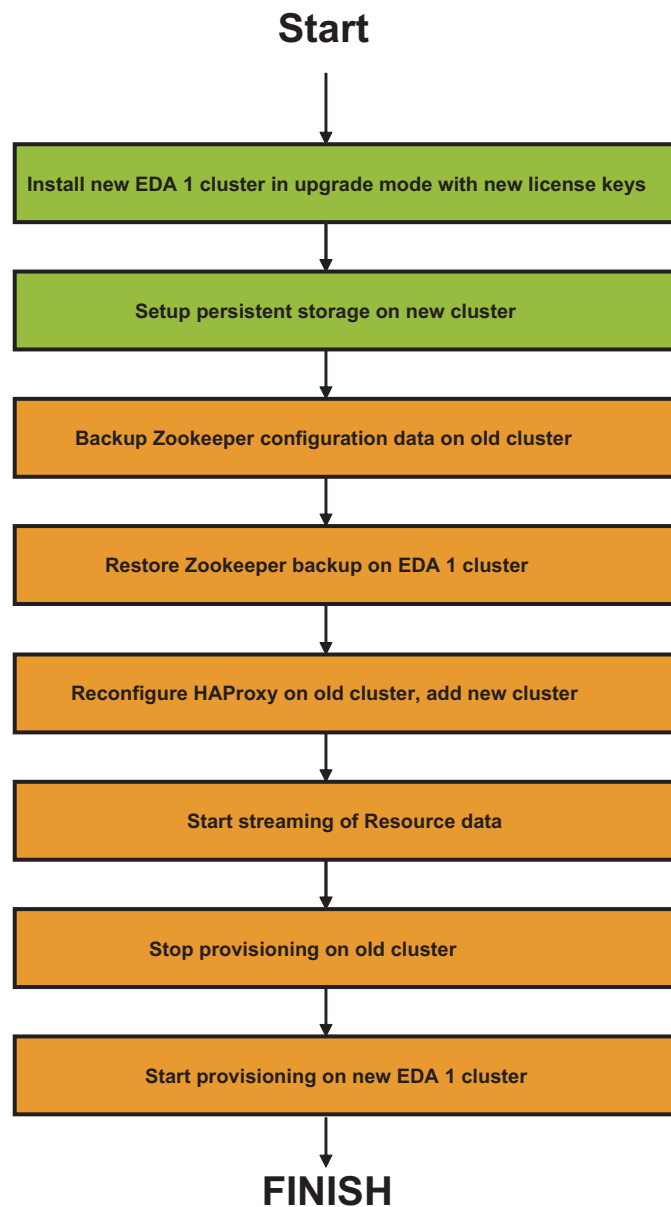


Figure 12 Upgrade Multi Activation 16.0, 16.1 or 16.2 to Dynamic Activation 1



14.3.1 Data Migration

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters).
- Customer adaptations that are stored in `/home/bootloader/CArepository` are copied to the new cluster. They are however not auto-deployed, which is something that has to be done as a post-upgrade task.

The following parts are not migrated in the upgrade process:

- Proclogs are stored on the external block storage and will be persisted in the upgrade process, and accessible on the old cluster for 30 days.

Note: This means, for example, that all crontab jobs are removed and recreated according to default setup for the latest target Dynamic Activation version.

14.3.2 Upgrade Process

1. Start the version of the `EDA Deployment Manager` tool that came with the Dynamic Activation 1 delivery (not the one from Multi Activation 16.0, 16.1 or 16.2).

For the latest tool version, refer to *Software Installation for Virtual and Cloud Deployment*, Reference [16].

2. Load the `.ds` file that was used during the deployment of the system from where the upgrade is performed.

Alternatively, create a new `.ds` file by use of the Dynamic Activation 1 version of the `EDA Deployment Manager` tool, where all values, (except for the VM specific ones, which must be omitted or cleared), match the system from where the upgrade is performed.

See figure below on what values to keep as is in the old 16.0, 16.1 or 16.2 cluster:



Deployment Schema Help **The values within the blue box must be the same as in the MA 16.0, 16.1 or 16.2 cluster**

Cluster Mode	Cluster	O&M Netmask (combined = incl.traffic)	255.255.255.192
Load-balancer	EDA provided	Traffic Netmask	255.255.255.192
Target Hypervisor	KVM/libvirt	Private Netmask	255.255.255.0
Separate traffic and O&M	Yes	Virtual Router ID	84
Time Zone	Europe/Stockholm	OSS IP (optional)	
O&M VIPv4 (combined = incl. traffic)	10.216.129.203	Domain (optional)	
-----> IPv6 (optional)	2001:1b70:82a7:1283:10:216:129:146	VM Default Values	
Traffic VIPv4	10.216.129.203	Number of vCPUs per VM	2
-----> IPv6 (optional)	2001:1b70:82a7:1283:10:216:129:203	Amount of RAM (GB)	10
Private VIPv4	192.168.0.6	List of VM hosts	
-----> IPv6 (optional)	2001:10::6	▼ dl380x1948	
DNS Primary IP	10.64.2.226	CL84-1 (node-1)	
DNS Secondary IP (optional)	10.64.2.227	CL84-4 (node-4)	
NTP Primary IP	10.64.2.226	▼ dl380x1949	
NTP Secondary IP (optional)	10.64.2.227	CL84-2 (node-2)	
O&M Bridge (combined = incl. traffic)		▼ dl380x2382	
Traffic Bridge		CL84-3 (node-3)	
Private Bridge			
O&M Gateway IPv4	10.216.129.129		
-----> IPv6 (optional)	2001:1b70:82a7:1283:0:0:0:1		
Traffic Gateway IPv4	10.216.129.193		
-----> IPv6 (optional)	2001:1b70:82a7:1347:0:0:0:1		

Generate Hypervisor Artifacts

- In the EDA Deployment Manager tool, fill in the VM-specific data. It is possible to use the same host names as in the old system, but use new IP addresses, intended for the upgraded system.

Note: The IP addresses must be unique. Do not use existing IP addresses.

See figures below on how to fill in the VM-specific data values.

VM IDs must be unique and different from the MA 16.0, 16.1 or 16.2 cluster

IP address that must be unique from the MA 16.0, 16.1, or 16.2 system

▼ List of VM hosts

▼ dl380x1948

CL84-1 (node-1)

CL84-4 (node-4)

▼ dl3801949

CL84-2 (node-2)

▼ dl380x2382

CL84-3 (node-3)

VM ID

CL84-1

VM Host Name

Cl 84-host-1

of vCPUs (0 = default)

0

Amount of RAM (GB) (0 = default)

0

O&M IPv4 (combined = incl. traffic)

10.216.129.204

-----> IPv6 (optional)

2001:1b70:82a7:1347:10:216:129:147/6

Traffic IPv4

10.216.129.204

-----> IPv6 (optional)

2001:1b70:82a7:1347:10:216:129:204/6

Private IPv4

192.168.0.7

-----> IPv6 (optional)

2001:10::7/64

- Follow the section **Preparing Deployment Artifacts** in *Software Installation for Virtual and Cloud Deployment*, Reference [16].

Note: When prompted, Upgrade or maiden installation? (during the step Generate Hypervisor artifact), press **Upgrade**.



Selection

Upgrade or maiden installation?

Upgrade

Maiden

Cancel

- Deploy the Dynamic Activation 1 Virtual Machines (VMs) according to instructions in section **Deploying Hypervisor Artifacts - KVM** (only), or section **Deploying Hypervisor Artifacts - VMware** (only) in *Software Installation for Virtual and Cloud Deployment*, Reference [16].
- Activate Dynamic Activation according to instructions in section **Activating Dynamic Activation** (only) in *Software Installation for Virtual and Cloud Deployment*, Reference [16].



Note: When running the command `3ppmon status --host all` before installing Dynamic Activation, it should return `LVS down` on node-1 and node-2.

During the upgrade process, the new Dynamic Activation 1 cluster must be accessed through serial interface (console).

7. Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.

Note: Any files that are to be transferred to the new cluster must first be transferred to the old cluster, and then by use of internal IP addresses transferred to the new cluster.

Attention!

From this point on, and until the end of this step-list (not including any rollback action as stated in the last step), it is not allowed to run the `bootloader.py activate` command. No node in the cluster is allowed to be activated.

8. On the new system (Dynamic Activation 1), from node-1, run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py setuplb
```

Note: The commands will open port 9995, and 9996 in the firewall on the old 16.0, 16.1 or 16.2 cluster to enable access to the new cluster.

Traffic disturbance can occur when HAProxy is reloaded.

Note: During the upgrade, the following is prompted:

```
Are you sure you want to continue connecting?
```

The password (for the old cluster) will need to be inserted several times depending on how many instances that are running on the old cluster.

9. After the first migration, verify that the new Dynamic Activation GUI is working by logging in to:

```
https://<VIP-OAM-IP>:9995
```

Note: It is important to clear the browser cache when switching between the old GUI and the new Dynamic Activation GUI.



10. In the new Dynamic Activation 1 GUI, add a user with full Configuration Management Authorities in the **Access Control>User** tab. Then apply the changes.
11. If the GUI is not working, a rollback can be performed after running migrate setuplb. To rollback at this point, run the following commands through a console on node-1:


```
# cd /var/log/installfiles/<Prod_Number>-<Version>/  
  
# ./virtUpgradeMigration.py rollback -t loadbalancer
```
12. On the new system (Dynamic Activation 1), from node-1, run the following commands:


```
# cd /var/log/installfiles/<Prod_Number>-<Version>/  
  
# ./virtUpgradeMigration.py migrate -t full -user <user  
created in the GUI>
```
13. Run CAI3G test traffic towards the new Dynamic Activation 1 cluster, through the vip-tfr:9996 address (if traffic separation is used), or vip-oam:9996 address.

Attention!

Traffic outage will occur during the delta migration and the enableTraffic script. This outage depends on how many new configurations that have been executed since the Resource Configuration data migration script was run in Step 8.

During the switch to the new cluster, traffic IP will be inaccessible for up to a minute. It is important that the Keepalived and HAProxy processes are not enabled on both clusters at the same time, since they will share the same IP address. Since external IP will be switched during the delta migration and the enableTraffic script, it is required to be logged in to node-1 on both the old cluster and the new cluster through a serial interface (console).

14. If the GUI or test traffic is not working a rollback can be performed after the zookeeper and Cassandra migration.

To rollback at this point run the following commands through a console on node-1:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/  
  
# ./virtUpgradeMigration.py rollback -t migration
```



15. On the new system (Dynamic Activation 1) from node-1, run the following commands through a console on node-1 to start the delta migration:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py migrate -t delta
```

Note: This delta migration will run much faster than the full migration. During this step the traffic is stopped on the old cluster.

16. If the delta migration fails a rollback can be performed.

To rollback at this point run the following commands through a console on node-1:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py rollback -t delta
```

17. Activate VIP addresses on the new cluster by running the following commands through a console on node-1:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py enableTraffic
```

The following is prompted:

Please enter the internal IP address for the node-1 on old cluster:

Add the *<Internal IP Address>* and press **Enter**

Note: Running the `./virtUpgradeMigration.py enableTraffic` script will enable and start the Keepalived and HAProxy processes on node-1 and node-2 on the new cluster. It will also reconfigure HAProxy to enable access to the old Multi Activation 16.0, 16.1 or 16.2 cluster, on port 9995 (OAM), and port 9996 (traffic).

18. If the `./virtUpgradeMigration.py enableTraffic` script fails, a rollback can be performed.

To rollback at this point, use a console and run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py rollback
```

When the above is completed, run the following command:

```
# systemctl restart haproxy.service
```



14.3.3 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users >Create Administrative User** in *System Administrators Guide for Virtual and Cloud Deployment*, Reference [11].



15 Upgrading from CEE Multi Activation 16.2 to CEE Dynamic Activation 1

This section contains information on how to upgrade from a CEE based Multi activation 16.2 system to a CEE based Dynamic Activation 1 system.

It does also include rollback information, see applicable steps in Section 15.3.2 on page 129.

15.1 Prerequisites

To be able to upgrade from CEE based Multi Activation 16.2 to CEE based Dynamic Activation 1, a set of prerequisites needs to be followed.

Before starting the upgrade procedure, make sure:

- To check the Delivery Report before proceeding with this part of the document. The Delivery Report contains information about known problems, limitations and exceptions related to the system software that will be upgraded. It can contain complementary instructions and information, that may prevent system failure and damage.
- That the host system meets the latest prerequisites described in *Requirements on Virtualization and Cloud Infrastructure*, Reference [19].
- That the current 16.2 cluster is running on latest CP release.
- That the new Dynamic Activation 1 cluster has the private/internal IP addresses in the same subnet as the old Multi Activation 16.2 cluster.

15.2 General Upgrade Process

An upgrade from CEE based Multi Activation 16.2 to a CEE based Dynamic Activation 1 consists of one maintenance window.

During the upgrade, the old Multi Activation 16.2 cluster is left intact as it is, in case of rollback scenario, and a new Dynamic Activation 1 cluster is installed.

A new license must be ordered for the new Dynamic Activation 1 cluster.

The external VIP addresses are reused from the old Multi Activation 16.2 cluster.

Any modules or adaptations that have been manually added to this specific system before the upgrade will be removed. After the upgrade, such modules or adaptations need to be added again (manually).

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [18].

15.3 Upgrade Multi Activation 16.2 to Dynamic Activation 1

The following chart depicts the upgrade procedure from Multi Activation 16.2 to Dynamic Activation 1, see Figure 12.

Upgrade MA 16.2 to EDA 1

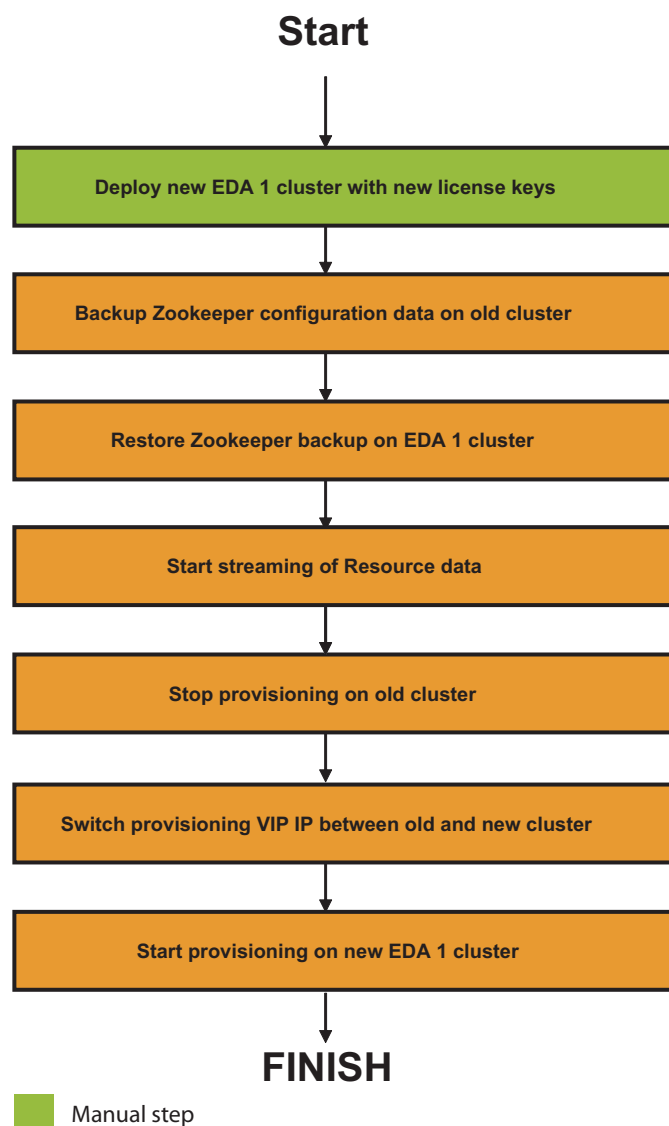


Figure 13 Upgrade Multi Activation 16.2 to Dynamic Activation 1



15.3.1 Data Migration

The following parts are migrated in the upgrade process:

- The Multi Activation configuration (application users, network elements, license counters).
- Customer adaptations that are stored in `/home/bootloader/CArepository` are copied to the new cluster. They are however not auto-deployed, which is something that has to be done as a post-upgrade task.

The following parts are not migrated in the upgrade process:

- Proclogs are stored on the external block storage and will be persisted in the upgrade process, and accessible on the old cluster for 30 days.

Note: This means, for example, that all crontab jobs are removed and recreated according to default setup for the latest target Dynamic Activation version.

15.3.2 Upgrade Process

1. Deploy the Dynamic Activation 1 according to instructions in section **Deploying Dynamic Activation in Cloud - ECEE** in *Software Installation for Virtual and Cloud Deployment*, Reference [16]
2. Add a provisioning client on the new system (Dynamic Activation 1). For instructions, refer to *User Guide for Resource Activation*, Reference [23].
3. On the new system (Dynamic Activation 1), from node-1, run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/

# ./virtUpgradeMigration.py migrate --old-cluster-ip <IP
for node-1 on old cluster>
```



Note: During the upgrade, the following is prompted:

```
Are you sure you want to continue connecting?
```

The password (for the old cluster) will need to be inserted several times depending on how many instances that are running on the old cluster.

After some time, when the following prompt appears, insert the provisioning client name created in Step 2.

```
Please enter provisioning client user name:
```

When the following prompt appears, insert the provisioning client user password.

```
INFO - *** Please enter your provisioning client
password.
Password:
```

If the old system was configured for Resource configuration the Cassandra database will also be migrated to the new cluster. This can be a very time-consuming process depending on how many devices that existed on the old cluster.

The old Multi Activation 16.2 cluster can continue to process new request during the migration. After the migration is finished, the data migration script needs to be run again, to migrate the delta from the first run.

4. Run CAI3G test traffic towards the new Dynamic Activation 1 provisioning VIP.

Note: As the provisioning VIP IP switch has not been done yet, the new Dynamic Activation cluster will at this point have a new VIP. This information can be found in the Stack overview in **Atlas**, under **Outputs** section with the name **VIP external address**.

Make sure that all specific system adaptations, modules, and customizations are added after the system upgrade. This to get the same functionality as before the upgrade.



Attention!

Traffic outage will occur during the delta migration and the `traffic-switch` script. This outage depends on how many new configurations that have been executed since the Resource Configuration data migration script was run in Step 3.

During the switch to the new cluster, traffic IP will be inaccessible for up to a minute. Since external IP will be switched during the delta migration and the `traffic-switch` script, it is advised to be logged in to node-1 on both old and new cluster through the SysOAM IPs, which are found in Stack overview for respective clusters.

5. If the GUI or test traffic is not working at this point, a re-deployment of the new cluster (Dynamic Activation 1) might be necessary depending on the problem.
6. On the new system (Dynamic Activation 1) from node-1, run the following commands to start the delta migration:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py migrate -t delta
--old-cluster-ip <IP for node-1 on old cluster>
```

Note: This delta migration will run much faster than the full migration. During this step the traffic is stopped on the old cluster.

7. If the delta migration fails a rollback can be performed.

To rollback at this point run the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py rollback -t delta
--old-cluster-ip <IP for node-1 on old cluster>
```

8. Perform a switch of the external traffic/O&M VIP between the old and the new cluster by executing the following commands:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/
# ./virtUpgradeMigration.py traffic-switch --old-cluster-ip <IP for node-1 on old cluster>
```



Note: Running the `./virtUpgradeMigration.py traffic-switch --old-cluster-ip` script will enable and start the Keepalived and HAProxy processes on node-1 and node-2 on both the old and the new cluster.

From this point, the old and new cluster have switched external VIP IPs with each other, so that the VIP used on the old cluster is re-used for Dynamic Activation cluster.

Note: It is only the external VIP IP that is switched. All SysOAM and internal IPs are not affected.

9. The new cluster should at this point be fully functional, and reachable through the external VIP that was previously associated with the old cluster. The old cluster is accessible through the external VIP, previously associated with the new cluster.
10. If GUI or traffic is not working properly on the new cluster, it is possible to rollback the IP setup by running the following commands from node-1 on the new cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>/  
  
# ./virtUpgradeMigration.py traffic-switch --old-cluster  
r-ip <IP for node-1 on old cluster>
```

11. To align the new IP setup for the two clusters, final changes need to be done in the Atlas GUI.

Note: This is only a visual alignment and will not affect the connectivity to the clusters in any way. Start with the old cluster.

- 1 Login into Atlas GUI as `admin` user.

Note: Start with the old cluster.

- 2 Navigate to the **System > Instances** page (left side menu).
- 3 In the **Name** column, find the name for node-1 (it could for example look like this `c135-1`), and click the link to reach the overview pages for these instances.
- 4 In the **Information** section, take note of the ID representing the instance.

Note: Save this UUID value for later steps.

- 5 Navigate to **System > Networks** and in the **Network Name** column click on the **vEma external network** link.
- 6 Scroll down to the **Ports** section, and in the **Name** column find the `<stack-name-old-cluster>-vip_external_port` link. Select it and click the **Edit Port** button that is located on the right side of the table.



A new window appears.

- 7 In the **Device ID** section, switch the `UUID` value with the `UUID` value saved in step 4 (Page 132)). Click **Save Changes**.
- 8 Perform the same changes for the new cluster. Start from Step 2 (Page 132).

15.3.3 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Multi Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users >Create Administrative User** in *System Administrators Guide for Virtual and Cloud Deployment*, Reference [11].





16 Configuration Data Migration

This section contains information on how to migrate configuration data:

- From Native:
 - Multi Activation 7.1 and 7.2 to Native, Virtual, or Cloud Dynamic Activation 1.
 - Multi Activation 15.0, 16.0, 16.1 or 16.2 to Virtual or Cloud Dynamic Activation 1.
 - Multi Activation 15.0 or 16.0 with SCXB2, NWI-E, and GEP3 blades, to Virtual or Cloud Dynamic Activation 1.
- From Virtual:

Note: Only migration of Resource Activation data is supported.

 - Multi Activation 7.2 to Virtual or Cloud Dynamic Activation 1.
 - Multi Activation 15.0 to Virtual or Cloud Dynamic Activation 1.
 - Multi Activation 16.0 to Virtual or Cloud Dynamic Activation 1.
 - Multi Activation 16.1 to Virtual or Cloud Dynamic Activation 1.
 - Multi Activation 16.2 to Virtual or Cloud Dynamic Activation 1.

16.1 Migrate Configuration

To migrate the configuration, perform the following on the old system:

1. If it does not already exist, create the `/var/log/installfiles/` directory on SC-1 (on Native), or node-1 (on Virtual and Cloud deployment):

```
# mkdir /var/log/installfiles/
```

2. Transfer the new software package (MA System Base SW) to the `/var/log/installfiles/` directory on SC1/node- 1 (on the old system).

3. Log in to the SC-1/node-1, and change directory:

```
# cd /var/log/installfiles/
```

4. Untar the software package (MA System Base SW):

```
# tar -zxf <Software_Package>.tar.gz
```



For the actual software packages, see the **Delivery Report**.

5. Change directory:

```
# cd <Prod_Number>-<Version>
```

6. Create backup of the mbean and the Multi Activation configurations:

```
# ./migratesystem.py backup -p /home
```

Move the tar file `mbeanbackup-*.tar.gz` to an external storage.

16.2 Restore Configuration

To restore the configuration, perform the following on the new system:

1. Go to the Dynamic Activation 1 GUI, navigate to the **Licenses** tab and click on the update symbol. Make sure that all Dynamic Activation 1 licenses are present.
2. Log in as user `root` to SC-1 (on Native), or node-1 (on Virtual or Cloud Dynamic Activation deployment), and change directory:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

3. Transfer the `mbeanbackup-*.tar.gz` tar file saved in Section 16.1 on page 135, to the `/home` directory.

4. Change directory:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

5. In the new Dynamic Activation 1 GUI, add a user with full Configuration Management Authorities in the **Access Control>User** tab. Then apply the changes.

6. Restore the mbean backup:

Note: Make sure to use absolute path to the backup file.

```
# ./migratesystem.py restore -p /home/mbeanbackup-<date ,time>.tar.gz -user <user created in the GUI>
```

7. When prompted, enter user name and password to a provisioning client with `Full authorities` to complete the restoration.
8. Due to function updates of various business logic, it is necessary to review any current existing customer Access Control settings. That is, some functions are moved and new ones have been added. For example, if a user had full HLR access and should still have full access after the upgrade, then there might exist new functionality that need to be added.





In the Dynamic Activation GUI, if necessary, navigate to the **Access Control > Users** tab, review the provisioning authorities for each user and update them accordingly for any new or moved function.

Note: New provisioning features need to be configured. For instructions, see *Configuration Manual for Resource Activation*, Reference [18].

16.3 CUDB Configuration

If the function updates of business logic involving new binary attributes in CUDB, it is necessary to update the Network Element configuration for CUDB on GUI.

To activate the new binary attributes, perform the following steps on all CUDB NEs:

1. Go to the Dynamic Activation 1 GUI, navigate to the **Network Elements > Network Elements** tab.
2. Click the change button  for the NE to modify. In **General** tab, click **Apply**.
3. Click the view button  for the NE to make sure that the new binary attributes are added to `Binary Attributes` field.





17 Generate Sentinel License Key Values

It is recommended to have the new license key in place before proceeding with the Dynamic Activation upgrade. This is to minimize traffic interruption when upgrading.

Note: The Sentinel license key values are hardware dependent.

Proceed with the following steps to extract the Sentinel license key values:

1. Download and unpack the [licensekey.zip](#) file.
2. Transfer the downloaded `licensekey` folder to the `/tmp` directory on SC-1/node-1.
3. Change directory on SC-1/node-1 to `/tmp/licensekey`:


```
# cd /tmp/licensekey
```
4. Change access permissions on the files in `/tmp/licensekey`:


```
# chmod 755 *
```
5. Obtain the license key values by running the `GenerateLicenseKeyValues.sh` script:


```
# ./GenerateLicenseKeyValues.sh
```

The following printout is an example:

Locking codes for 192.168.1.1:

```
Sentinel RMS Development Kit 8.5.1.1000 Host Locking Code Information Utility
Copyright (C) 2011 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1HK R594 Y25Y WEQY
Locking Code 1 (Old Style) : 2008-BA2FC
```

Locking codes for 192.168.1.2:

```
Sentinel RMS Development Kit 8.5.1.1000 Host Locking Code Information Utility
Copyright (C) 2011 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*166 VFS7 DN43 WURU
Locking Code 1 (Old Style) : 2008-B892A
```

Example 1 Printout License Information SC-1/node-1





Reference List

Ericsson Documents

- [1] *Glossary of Terms and Acronyms*, 0033-CSH 109 628 Uen
- [2] *Library Overview*, 18/1553-CSH 109 628 Uen
- [3] *Backup and Restore Guideline for Native Deployment*, 2/1553-CRH 109 1438 Uen
- [4] *Backup and Restore Guideline for Native Deployment*, 2/1553-1/CRH 109 1438 Uen
- [5] *Backup and Restore Guideline for Native Deployment*, 2/1553-2/CRH 109 1438 Uen
- [6] *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, 1/1531-CSH 109 628 Uen
- [7] *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, 3/1531-CSH 109 628 Uen
- [8] *Hardware Installation and IP Infrastructure Setup for Native Deployment on EBS*, 2/1531-CRH 109 1438 Uen
- [9] *Network Description and Configuration for Native Deployment* , 2/1551-CSH 109 628 Uen
- [10] *LOTC Management Guide*, User Guide, 1/1553-ANA 901 39/3 Uen
- [11] *System Administrators Guide for Virtual and Cloud Deployment*, 3/1543-CSH 109 628 Uen
- [12] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [13] *Migration Methods in ESA Upgrade Instruction*, 153 72-FAM 901 455 Uen
- [14] *DMX Software Management*, 6/1553-CNA 128 59/1 Uen
- [15] *BSP Jumpstart Instruction*, 2/1531-APP 111 01 Uen
- [16] *Software Installation for Virtual and Cloud Deployment*, 4/1531-CSH 109 628 Uen
- [17] *Software Installation for Native Deployment*, 1/1531-CSH 109 628 uen
- [18] *Configuration Manual for Resource Activation*, 2/1543-CSH 109 628 Uen



- [19] *Requirements on Virtualization and Cloud Infrastructure*, 2/2135-CSH 109 628 Uen
- [20] *System Administrators Guide for Native Deployment*, 1/1543-CRH 109 1438 Uen
- [21] *System Administrators Guide for Native Deployment*, 1/1543-1/CRH 109 1438 Uen
- [22] *System Administrators Guide for Native Deployment*, 1/1543-2/CRH 109 1438 Uen
- [23] *User Guide for Resource Activation*, 1/1553-CSH 109 628 Uen
- [24] *User Guide for Subscriber Activation*, 1/1553-CRH 109 1438 Uen
- [25] *User Guide for Subscriber Activation*, 1/1553-1/CRH 109 1438 Uen
- [26] *User Guide for Subscriber Activation*, 1/1553-2/CRH 109 1438 Uen