

Backup and Restore Guideline for Native Deployment

Ericsson Dynamic Activation 1

USER GUIDE

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 Groups	1
1.3	Typographic Conventions	1
1.4	Prerequisites	1
2	Backing Up and Restoring BSP Configuration	2
3	Dynamic Activation Backup and Restore	2
3.1	Scenario Mapping for Full System Backup	3
3.2	Scenario Mapping for Full System Restore	3
3.3	Backing Up and Restoring a Cluster LDEwS NFS	3
3.3.1	Backing Up a Cluster LDEwS NFS	3
3.3.2	Restoring a Cluster LDEwS NFS	4
3.4	Backing Up and Restoring Dynamic Activation NFS Specific Files	8
3.4.1	Backing Up NFS Specific Files	9
3.4.2	Restoring NFS Specific Files	10
3.5	Backing Up and Restoring Zookeeper	11
3.5.1	Backing Up Zookeeper	11
3.5.2	Restoring Zookeeper	12
3.6	Backing Up and Restoring Cassandra (OAuth Related Data)	12
3.6.1	Backing Up Cassandra	13
3.6.2	Restoring Cassandra	13
	Reference List	15





1 Introduction

This document provides high-level guidelines on how to back up and restore the Ericsson Dynamic Activation (EDA).

1.1 Purpose and Scope

The backup and restoration functionality in Dynamic Activation is not a complete solution with a separate backup media. Backup files created by the system must therefore be transferred to secondary storage.

1.2 Target Groups

The target groups for this document are as follows:

- System Administrator
- Network Administrator
- Network Supervision Administrator

1.3 Typographic Conventions

Typographic conventions are described in the document *Library Overview*, Reference [1].

1.4 Prerequisites

To use this document fully, users must meet the following prerequisites:

- Basic knowledge about the Dynamic Activation product.



2 Backing Up and Restoring BSP Configuration

To back up and restore the BSP configuration, refer to **Backup and Restore BSP Configuration**, Reference [5].

3 Dynamic Activation Backup and Restore

A backup can be performed on:

- A full system

A full system backup can be used for system restoration. For example, rollback of the system or recover the entire system after a crash. There is service downtime during the restoration.

Note: Export of Processing Log Data is not included in a full system backup.

- A subset of the system

This type of backup can be used for restoration of a part of the system. For example, replace one server in the system, or rollback provisioning logic configuration data. There is no service downtime during the restoration.

- Processing Log Data

The Processing Log Data is handled separately, see instructions in *System Administrators Guide for Native Deployment*, Reference [2].

After a severe system crash, it is necessary to review the system to determine which parts of the system that need to be restored.

Detailed instructions of backup and restore are described in the following subchapters.

Note: All backup and export files need to be stored on a safe remote server.



3.1 Scenario Mapping for Full System Backup

Different backups need to be used during a full system backup. Table 1 shows what backups need to be used in different scenarios.

Table 1 Scenario Mapping, Backup

Type of Backup	LDEwS NFS ⁽¹⁾	Zookeeper ⁽²⁾
Dynamic Activation full system backup	x	x

(1) See Section 3.3.1 on page 3

(2) See Section 3.5.1 on page 11

3.2 Scenario Mapping for Full System Restore

To perform a full system restore:

1. Perform a restore of Linux Distribution Extensions with SUSE (LDEwS) NFS, see Section 3.3.2 on page 4.
2. Perform a restore of Zookeeper, see Section 3.5.2 on page 12.

3.3 Backing Up and Restoring a Cluster LDEwS NFS

3.3.1 Backing Up a Cluster LDEwS NFS

Creating an NFS backup involves taking a copy of the shared replicated file system and store that data in an archive file on a remote server. The archive is of the format `.tar`, compressed with GZIP. The remote server must be accessible using SSH. The system can later be restored to the state it had when the backup was taken.

Time estimation to perform this section is about 5 minutes for 2+2 newly installed system in a test environment.

To create a backup and store it on a remote server:

Note: Files on local disk (not NFS-mounted disks) are not included in the LDEwS NFS backup.

1. Start the backup by issuing the following command:

Log in as user `root` on one of the SC nodes:

```
# lde-backup --create <user>@<server>:</path/file.tar.gz>
```

Where:

- `<user>` is a username available on the remote server.



- `<server>` is the hostname or IP address of the remote server.
 - `</path/file.tar.gz>` is the location and filename where the backup is stored on the remote server.
2. Enter the password for `<user>` on `<server>` when prompted.
 3. The system starts to create the backup. This can take a while depending on how much data is stored on the file system. If the backup completed successfully, the following text is displayed:

Backup completed

3.3.2 Restoring a Cluster LDEwS NFS

A restore of a cluster LDEwS NFS can only be performed when at least one SC node can be started in maintenance mode.

If no SC nodes can be started in maintenance mode, do the following:

1. Perform a maiden installation of LDEwS on an SC node.
2. Start the SC node up in maintenance mode.

Note: Files from local disk (not NFS-mounted disks) are not restored.

Verify that the current LDEwS installation on the SC node maps against the system that is about to be restored. If any deviations exist, perform a maiden installation on the SC node of the specific LDEwS release. If GEP3, BSP, and CMX configuration are used, follow the instructions in the document, *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [3]. If GEP5, BSP, and CMX are used, follow the instructions in *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [4].

When the maiden installation is completed, bring the SC node to maintenance mode and proceed with the following restore steps.

The following procedure applies to the Dynamic Activation GEP3 system and must be followed to restore a backup from a remote server. The instruction assumes that the system is operational in maintenance mode when the restore procedure starts. If not, contact Ericsson support personnel for further help.

Time estimation to perform this section is about 70 minutes.

1. Note the MAC address of `eth5` and IP address for SC-1, as these are used later. Both addresses can be found in `/cluster/etc/cluster.conf`.

If this file is not available, refer to *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [3], if using GEP3, or *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [4], if using GEP5, for information about how to retrieve the MAC address.



2. From a terminal window connected to the active DMXC, lock all SC and PL blades in the cluster:

```
> configure
```

```
(config)> ManagedElement=1,Equipment=1,Shelf=0,Slot=<slot position>,Blade=1,administrativeState=LOCKED
```

```
> commit -s
```

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

Repeat the command for every blade in the cluster.

3. Connect a serial console to the SC-1 blade:

```
# telnet <Console Server IP-address> <port number connected to SC-1>
```

Note: LDEwS uses 115200 as default communication speed.

4. From a terminal window connected to the active DMXC, unlock SC-1:

```
> configure
```

```
(config)> ManagedElement=1,Equipment=1,Shelf=0,Slot=<slot position>,Blade=1,administrativeState=UNLOCKED
```

```
> commit -s
```

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

Look for power-up information (BIOS boot) in the serial console. After about 30 seconds, the following output is displayed:

Press any key to continue.

Quickly use the up or down arrow keys to break the default operational boot, by selecting SUSE™ Linux™ Enterprise Server - Maintenance mode (Serial console).

5. When prompted for password, enter password `rootroot`.

```
Welcome to rescuGive root password for maintenance
# rootroot
```

6. Use the MAC address from Step 1 to find out which interface it is connected to:

```
# ifconfig -a | grep -i <MAC address>
```

For example:



```
# ifconfig -a | grep -i 00:1E:DF:7A:5B:12
```

eth3 **is used as an example in the following steps** and the following is printed:

```
eth3 Link encap:Ethernet HWaddr 00:1E:DF:7A:5B:12
```

7. Add a link between interface and VLAN ID:

```
# ip link add link eth3 name eth3.<PG_OM_SP1 VLAN ID>  
type vlan id <PG_OM_SP1 VLAN ID>
```

Note: Default setup value for VLAN ID is 184.

8. Connect the SC IP address to the added link between interface and VLAN ID:

```
# ip addr add <PG_OM_SP1_SC_1_IP>/28 dev eth3.<PG_OM_SP1  
VLAN ID>
```

9. Bring up eth3:

```
# ip link set dev eth3 up
```

10. Add default gateway:

```
# route add default gw <PG_OM_SP1_VRRP_IP>
```

11. Test the external communication with ping:

```
# ping <external address>
```

12. Restore the backup.

Enter `root` password when asked:

```
# cluster backup --restore <user>@<server>:</path/file.t  
ar.gz>
```

Where:

- `<user>` is a username available on the remote server.
- `<server>` is the IP address of the remote server.
- `</path/file.tar.gz>` is the location and filename of the backup to restore on the remote server.

13. Enter `root` password for a second time.

14. The system now starts to restore the backup. This can take a while depending on how much data is stored in the backup. If the restore completed successfully, the following output is displayed:



Restore completed

15. Perform a reboot on SC-1 which makes it start up in operational mode again:

```
# reboot
```

16. Connect a serial console to the SC2 blade:

```
# telnet <Console Server IP-address> <port number connected to SC-2>
```

Note: LDEwS uses 115200 as default communication speed.

17. From the terminal window connected to the active DMXC, unlock SC2:

```
> configure
```

```
(config)> ManagedElement=1,Equipment=1,Shelf=0,Slot=3,Blade=1,administrativeState=UNLOCKED
```

```
> commit -s
```

18. In the terminal window connected to SC2, during the BIOS startup sequence wait for the console printout **Press F3 for GEP PopUp** and then press **F3**. Select **00** as device to boot from, which is the blade 2, SC2, backplane interface. This means that SC2 does a PXE boot from SC-1.

Note: If Putty is used as terminal, the keyboard must be set to **Xterm R6** to get **F<x>** buttons to work to enter GEP IPMI.

If the serial console does not show the BIOS startup, immediately lock the blade again (within 30 seconds) and fix the serial connection communication. It is vital not to let SC-2 boot normally from the previous disk content. Because it can start synchronizing with SC-1 and possibly corrupt the SC-1 state. There is a great **NEED** to succeed in pressing **F3** in the serial console to get a list of boot options.

19. The software installation now starts and the following text is shown:

```
Installing, please wait...
```

The time it takes to install the software depends on which hardware is used. It is completed once the following text is shown:

```
Installation completed successfully
```

If anything went wrong during the installation, the following message is shown instead:

```
Installation failed (see /root/install.log)
```



20. Wait for DRBD sync. Run the following command to view the progress.

```
# drbd-overview
```

Note: No SC redundancy is available before DRBD sync is completed.

It is not recommended to start the PL blades before a 100% sync is completed.

21. From a terminal window connected to the active DMXC, unlock all PL nodes:

```
> configure
```

```
(config)> ManagedElement=1,Equipment=1,Shelf=0,Slot=<slot position>,Blade=1,administrativeState=UNLOCKED
```

```
> commit -s
```

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

Repeat the command for all PL nodes.

22. Log on to SC-1 and enter the following command to restart the application:

```
# bootloader.py node activate --host all
```

3.4 Backing Up and Restoring Dynamic Activation NFS Specific Files

Everything in the following directories is backed up:

- /home/bootloader
- /home/dveinstaller
- /home/actadm
- /home/dvecli
- /home/casadm
- /opt/ericsson/activation/bootloader

Backup

Perform the backup procedure whenever:

- A major change of data is conducted (in this area).
- According to site-specific requirements.

Examples of scenarios when this type of backup needs to be performed are:



- Local site backup strategy.
- Manual changes.
- Installations of emergency packages (EPs), or intermediate correction packages (ICPs).
- Updates of software.

It is a feature backup procedure where the backup-set has different areas of use:

- Specific file and directory restored from a subset.
- Specific node restored from a subset.
- All files restored from a subset.

The main use of this subset is to avoid an NFS restore, which can cause a severe downtime to the system. If a specific NFS file, directory or similar is lost, it must be possible to retrieve it by use of this backup. The backup-set is based on damage control. That is, it is end-user controlled, and based on the situation to determine when and which file or files that need to be restored.

Restore

Performed the restore procedure at any major loss of data in specific NFS areas. For example:

- Corrupted data or files.
- Missing data or files.
- Restore of specific file from a subset.
- Restore of specific directory.
- Restore of specific node directories and files.
- Restore of an entire subset.

If necessary, a specific file can be retrieved from above mentioned backup-set to restore a missing or corrupt file. The files reside in the specified directories of the backup.

3.4.1 Backing Up NFS Specific Files

This section describes how to perform a backup of the Dynamic Activation NFS-specific files. The backup script is installed as `/opt/dve/bin/pgSoftwareBackup.sh`.

To back up NFS-specific files:



1. Log on as user `root` on one of the SC nodes in the cluster.
2. Run the following command to back up the Dynamic Activation NFS-specific files:

```
# /opt/dve/bin/pgSoftwareBackup.sh backup <backup_dir_path> <identifier_for_filename>
```

For example:

```
# /opt/dve/bin/pgSoftwareBackup.sh backup /home/ config
```

3. When the backup is done, the following printout is shown:

```
Backup stored as /home/dveinstaller/config-BootloaderBackup-20141114_124650.tar.gz
```

3.4.2 Restoring NFS Specific Files

This section contains information on how to restore NFS-specific configuration files. Both a total system restore, and restore of a specific file from a subset.

3.4.2.1 Total Restore

This section describes how to perform a total restore of Dynamic Activation NFS-specific files.

1. Log in as user `root` on one of the SC nodes in the cluster.
2. Make sure that the backup `tar.gz` file is stored on the SC node.
3. Run the following command to restore the Dynamic Activation NFS-specific files:

```
# /opt/dve/bin/pgSoftwareBackup.sh restore <full_path_and_backup_tar.gz_file_name>
```

When prompted, enter `yes`, and press **Enter**

3.4.2.2 Subset Restore

This section describes how to restore a specific file from a subset.

On a suitable disk, create a `temp` directory with a sufficient size, to extract the backup.

Note: The following step-list is an example of restoring a license file.

1. Create a `restore_temp` directory:

```
$ mkdir /var/log/restore_temp
```
2. Extract the backup in the newly created `restore_temp` directory:



```
$ sudo -u actadm tar zxvf <path_to_backup_tar_file> -C
/var/log/restore_temp
```

3. Restore the specific file from the `restore_temp` directory to its original directory:

For example:

```
$ sudo -u actadm cp -r /var/log/restore_temp/home/actadm/licenses/lserverc /home/actadm/licenses/lserverc
```

4. Restart the sentinel server on the SC nodes to reread the license file, see start/stop instructions in *System Administrators Guide for Native Deployment*, Reference [2].

Note: This is only an example. Depending on which file or directory that is to be restored, it needs a specific action. For the license example above, a reread by the Application Server is needed. If a Dynamic Activation application configuration file is to be restored, the action is to run the bootloader command `bootloader.py node activate --host <hostname>`. The `<hostname>` is the hostname of the node that is to be restored.

5. When the restore is finished, remove the `restore_temp` directory that was used for extraction of the backup file:

```
$ sudo -u actadm rm -rf /var/log/restore_temp
```

3.5 Backing Up and Restoring Zookeeper

This chapter describes how to back up and restore the Zookeeper in Dynamic Activation. This involves, for example, network element and user configuration.

Note: Backing up and restoring Zookeeper-data is a software version-dependent procedure. The Zookeeper-data backed up from a specific system must only be restored on the same specific software release. This to ensure full functionality of the restored data.

3.5.1 Backing Up Zookeeper

To perform a backup of Zookeeper:

1. Log in as an administrator on one of the SC nodes in the cluster.
2. Start the backup process by executing the script, as follows:

```
$ sudo zookeeperBackup.sh backup <backup_dir_path>
<identifier_for_filename>
```

For example:

```
$ sudo zookeeperBackup.sh backup /tmp/ config
```



3. When the backup process is done, the following printout is displayed:

```
Backup stored as /tmp/config-zookeeperBackup-20141114_154150.tar.gz
```

3.5.2 Restoring Zookeeper

- Note:** This involves stopping and starting the Dynamic Activation application on all nodes, which results in traffic downtime.

When the configuration data has been restored, alarms that are no longer valid can still persist in the system. Use the `fmsendmessage` command to delete the alarms manually. For more information, refer to *System Administrators Guide for Native Deployment*, Reference [2].

1. Log in as an administrator on one of the SC nodes in the cluster and run the following command:

```
$ sudo zookeeperBackup.sh restore <full_path_and_backup_tar.gz_file_name>
```

Caution!

This causes traffic downtime on the Dynamic Activation Application.

For example:

```
$ sudo zookeeperBackup.sh restore /tmp/config-zookeeperBackup-20141114_154150.tar.gz
```

When prompted, enter **yes**, and press **Enter**

The restore command is finished when the following printout is displayed:

```
Restore finished: /tmp/config-zookeeperBackup-20141114_154150.tar.gz
```

2. Go to the Dynamic Activation GUI and check the user and network element configurations.

3.6 Backing Up and Restoring Cassandra (OAuth Related Data)

This section describes how to back up and restore the Cassandra database tables. The OAuth related data is to be backed up.



3.6.1 Backing Up Cassandra

To perform a backup of Cassandra:

1. Log in as an administrator on the first SC node (SC-1).
2. Start the backup process by executing the following script:

```
$ sudo -u actadm cassandra_backup.py backup oauth
```

3. Enter the full path where the backup is to be stored:

Enter full path to backup folder: /<path>

For example:

Enter full path to backup folder: /home/actadm/backup/

4. When the backup process is done, one backup file per node is stored in the backup folder.

For example, in a four nodes cluster the following files are to be stored in the backup folder:

```
CL15-SC-1:~ # ls -l
total 1008
-rw-r--r--. 1 root root 111949 Jun 22 14:30 CL15-SC-1_20150622_1
-rw-r--r--. 1 root root 298944 Jun 22 14:30 CL15-SC-2_20150622_1
-rw-r--r--. 1 root root 291973 Jun 22 14:30 CL15-PL-3_20150622_1
-rw-r--r--. 1 root root 293897 Jun 22 14:30 CL15-PL-4_20150622_1
```

3.6.2 Restoring Cassandra

Note: Restoring Cassandra requires stopping and starting the Dynamic Activation application on all nodes. This results in traffic downtime. Restoring also means that all data in the Cassandra database tables (OAuth related data) are to be replaced with data from the backup.

1. Log in as an administrator on SC-1, and disable the Dynamic Activation application processes by executing the following command:

Caution!

The following command causes traffic downtime on the Dynamic Activation application.

```
$ bootloader.py node stop --host all
```



2. Run the following command to start the Cassandra restore process:

Caution!

The following command causes all old OAuth related data to be replaced in the Cassandra database.

```
$ sudo -u actadm cassandra_backup.py restore
```

3. Enter the full path where the backup is stored:

Enter full path to backup folder: /<path>

For example:

Enter full path to backup folder: /home/actadm/backup/

4. Log in as an administrator on SC-1, and enable the Dynamic Activation application processes again by executing the following command:

```
$ bootloader.py node start --host all
```



Reference List

Ericsson Documents

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [3] *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, 2/1531-CSH 109 628 Uen
- [4] *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, 3/1531-CSH 109 628 Uen
- [5] *Backup and Restore BSP Configuration*, 25/1543-APR 901 0549/1 Uen

Other Documents

- [6] *ExtremeXOS Command Reference Guide for Release 15.6*,
http://documentation.extremenetworks.com/exos_commands/downloads/EXOS_Command_Reference_15_6.pdf