

Backup and Restore

Ericsson Service-Aware Policy Controller

USER GUIDE

Copyright

© Ericsson España, S.A. 2016. 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.

Abstract

The purpose of this document is to provide a guide to perform **backup and restore** in the SAPC .



Contents

1	Introduction	1
1.1	Document Purpose and Scope	1
1.2	Revision Information	1
2	Preconditions	3
3	Backup and Restore Overview	5
4	Backup and Restore Procedures	7
4.1	Create Backup	7
4.2	Restore Backup	8
5	Restrictions	11
	Glossary	13





1 Introduction

1.1 Document Purpose and Scope

The purpose of this document is to provide a guide to perform **backup and restore** in the SAPC.

1.2 Revision Information

Rev. A	This is the first release of this document.
---------------	---





2 Preconditions

The following conditions must be fulfilled:

- CBA components are installed.
- The SAPC product software has been installed and configured





3 Backup and Restore Overview

A backup consists of a snapshot of the system in the moment this operation is performed, called System Data backup.

For more information about backup and restore, refer to [System Backup and Restore](#).





4 Backup and Restore Procedures

System Data backup is used to do a system data fallback to recover to a former version of the whole system with consistency.

After restoring a System Data backup, the SAPC reestablishes the following information:

- Software installed.
- Node configuration.
- Static Subscriber profile and provisioning information stored in the SAPC database.
- Dynamic Subscriber information (that is, usage accumulators) stored in the SAPC database.

And the SAPC loses the following data:

- IP-CAN sessions.
- Time Trigger events.

System Data backup consists of the following files:

Table 1 System Data Backup Paths and Files.

Path / File	Description
/cluster/brf/backup/<backup-name>/	<ul style="list-style-type: none"> • Software installed • Node configuration • Static Subscriber information • Dynamic Subscriber information

4.1 Create Backup

Caution!

To guarantee the content of the backup, do not execute any configuration or provisioning operation during the backup procedure.

To perform the SAPC System Data backup, execute the following steps:

1. Verify that there is enough space in /cluster, following the procedure Check Disk Space described in Preventive Maintenance.



2. Access to the SAPC, using ECLI, according to [System Administrator Guide](#).
3. Verify that the SAPC status is correct following the procedure described in [Preventive Maintenance](#).
4. Follow the procedure explained in [Create Backup](#), using **BrmBackupManager=SYSTEM_DATA**.
5. Check IMM Persistent Back End, following the procedure described in [Preventive Maintenance](#).

Once the backup is completed, the operation has finished and the backup is ready. Check the operation result, following the procedure described in [View Progress Report](#).

4.2 Restore Backup

Caution!

Restoring a System Data backup implies downtime in configuration, provisioning, and traffic, as the SAPC is restarted after the restore.

Do!

Do not execute any configuration or provisioning operation during the restore procedure.

To perform the SAPC System Data restore, execute the following steps:

1. Access to the SAPC, using ECLI, according to [System Administrator Guide](#).
2. Verify that the SAPC status is correct following the procedure described in [Preventive Maintenance](#).
3. In Geographical Redundancy, stop the data replication between zones, following the procedure explained in [Temporarily Disable Geographical Redundancy](#).
4. Follow the procedure explained in [Restore Backup](#), using **BrmBackupManager=SYSTEM_DATA**.
5. At this step, the SAPC is restarted automatically.



6. Wait until the system is operational again. Check the restore operation result, following the procedure described in [View Progress Report](#), and check the SAPC Status following the procedure described in [Preventive Maintenance](#).
7. Check IMM Persistent Back End, following the procedure described in [Preventive Maintenance](#).

At this stage, the SAPC is ready to process traffic, and configuration and provisioning operations can be executed.

Caution!

Do not cancel an ongoing system data restore, as the System Data may become inconsistent.

The only way to fix this problem is to perform a complete restore again.





5 Restrictions

The default disk capacity in Systems Controllers (SC) for VNF deployments permits to store up to five backups files in the local persistent storage media (this maximum depends on the specific provisioned data).

Extra capacity for backups storage can be configured, before the deployment, during the OVA creation. See the dimensioning guidelines to determine the needed size and the [OVFgen Tool](#) to configure it. Otherwise, to store more backup files, the recommended option is to use [Export Backup](#) operation to export backup files to an external storage system.

For PNF deployments, the maximum number of stored backups depends on the disk capacity of the system and the provisioning of the node. See the dimensioning guidelines to determine the backups storage capacity. To store more backup files, follow the previous recommendation of exporting them to an external storage system





Glossary

BRF
Backup and Restore Framework

CLI
Command-Line Interface

PNF
Physical Node Function

SC
System Controller

VNF
Virtualized Network Function