Oracle® Communications Network Charging and Control

Upgrade Operations Guide

Release 15.2

January 2026

Copyright

Contents

Appendix A

About This Document

Audience

This guide is for system administrators who upgrade the NCC platform.

Scope

This document includes all the information required to upgrade the Oracle Communications Network Charging and Control (NCC) platform.

Prerequisites

Before upgrading NCC, you should have a solid understanding of UNIX, Oracle Linux, and a familiarity with IN concepts as well as an understanding of Oracle databases, Oracle Real Application Clusters (Oracle RAC), SQL, and PL/SQL. Attempting to upgrade the NCC system without the appropriate background skills could damage the system, including causing temporary or permanent incorrect operation, loss of service, or rendering your system beyond recovery.

This guide describes system tasks that should be carried out only by suitably trained operators.

Related Documents

See the following documents for information about installing and managing NCC:

- *Installation Guide*
- *System Administrator's Guide*
- *Configuration User's Guide*
- *Service Management System User's Guide*

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Network Charging and Control (NCC) documentation.

Formatting Convention	Type of Information
Special Bold	Items you must select, such as names of tabs. Names of database tables and fields.
Italics	Name of a document, chapter, topic or other publication. Emphasis within text.
Button	The name of a button to click or a key to press. **Example:** To close the window, either click **Close**, or press **Esc**.
Key+Key	Key combinations for which the user must press and hold down one key and then press another. Example: **Ctrl+P** or **Alt+F4**.
`Monospace`	Examples of code or standard output.
`Monospace Bold`	Text that you must enter.
variable	Used to indicate variables or text that should be replaced with an actual value.
menu option > menu option >	Used to indicate the cascading menu option to be selected. Example: **Operator Functions > Report Functions**
hypertext link	Used to indicate a hypertext link.

Chapter 1

Introduction to Upgrading

Overview

Introduction

This chapter describes the Oracle Communications Network Charging and Control (NCC) components that are upgraded and makes general recommendations.

In this chapter

This chapter contains the following topics.

About the Upgrade

Releases upgraded

Upgrading to NCC release 15.2 upgrades the NCC platform from NCC 15.1.

NCC node upgrade order

You upgrade each node on the NCC platform independently and sequentially in three phases:

1. Upgrade each Voucher and Wallet Server (VWS) pair in this order: secondary node, then primary node.
2. Upgrade all Service Logic Controller (SLC) nodes, one by one.
3. Upgrade the Service Management System (SMS).

Note:

- Service-critical functions remain available through redundant peer nodes during the upgrade process.
- You need to install openSSL version 1.1.1* for Linux.
- Java 21.0.9 must be installed in SMS, SLC, and VWS nodes for 15.2.
- Solaris is not supported from 15.1 release.

NCC database and application upgrade table

The following table lists the name of the base packages for the nodes on which you install each database and application patch, and the prerequisite patch numbers.

Upgrade process will involve two steps. One needs to apply database patch followed by application patch. Ex: 15.1 Database patch (P36748610) is pre-requisite for applying 15.2 Database patch. On the same lines 15.1 Application patch (P36748631) is pre-requisite for applying 15.2 Application patch.

If the database and application are hosted on the same node, then both patches are installed on that node. If the database is remote, only the database patch is installed on the database node, and only the application patch is installed on the application node.

Before you install a patch on a node, check that the prerequisite patch is already installed. For example, the P37848963SMS patch is the prerequisite for the P37848975SMS patch on the SMS node.

For more information about the contents of the patch, see *Patch contents* (on page 10). For information about where to install patches, see *Where to install patches* (on page 10).

Note: The prerequisite patch numbers are not applicable if the previous release was a fresh install using the Oracle Universal Installer (the installer).

Node Type	Upgrade Patch Number	Pre-requisite
SMS database	P37848963SMS	15.1.0.0.0 package Or P36748610SMS
SMS application	P37848975SMS	P36748631SMS
SLC database	P37848963SCP	15.1.0.0.0 package Or P36748610SCP
SLC application	P37848975SCP	P36748631SCP
VWS database	P37848963BE	15.1.0.0.0 package Or P36748610BE
VWS application	P37848975BE	P36748631BE

About backward compatibility

The NCC application and upgrade patches are backward compatible. For example, backwards compatibility is maintained between:

- SLC and VWS nodes
- Primary and secondary VWS nodes

General recommendations

Upgrading an environment of NCC is a complex process.

You should:

- Carefully study this upgrade guide, the updated NCC 15.2 user documentation, and the patch readme text file. See *NCC Release Notes* for a list of the updated documentation.
- Prepare a detailed step-by-step upgrade plan specific to the target environment being upgraded.
- Validate and rehearse the upgrade on a test environment that replicates your production system.
- Ensure a validated backup and restore process is in place for the production environment prior to proceeding with the upgrade.

Chapter 2

About the Upgrade Process

Overview

Introduction

This chapter describes the stages of a complete Oracle Communications Network Charging and Control (NCC) end-to-end upgrade process and the general tasks you perform at each stage.

In this chapter

This chapter contains the following topics.

Upgrade Process Overview

About upgrade stages

There are two main stages to upgrading NCC: preparation and upgrade. Each stage includes a series of tasks you perform.

Preparation stage

You perform the following tasks to prepare the system for upgrade:

- Back up the NCC databases and ensure database integrity.

  You can use the backup files to roll back the upgrade if necessary. You ensure database integrity by making sure triggers and constraints are enabled. This ensures that any operations that could corrupt the database are aborted.
- Back up configuration files and create new configuration files for the upgrade.
- Download and unpack the upgrade patch files on the target system.
- Update the replication configuration for changes to the tables replicated.

For instruction on the preparation tasks, see *Preparing for the Upgrade* (on page 7).

Upgrade stage

When you upgrade NCC, you upgrade the Service Management System (SMS), Voucher and Wallet Server (VWS), and Service Logic Controller (SLC) nodes independently. The overall steps to upgrading a node include stopping processes on the node, installing upgrade patches, adding upgrade configuration files, and restarting processes on the node. Upgrading VWS and SLC nodes include additional steps specific to those types of nodes. The upgrade patches update the database schema and data and the NCC software.

Note: Service-critical functions remain available through redundant peer nodes during the upgrade process.

You upgrade the nodes on the NCC platform in three phases:

1. **1** Upgrade each VWS node pair.

   Sequentially upgrade each VWS pair. Upgrade one VWS pair at a time. Within a VWS pair, upgrade the secondary and then the primary VWS separately. This allows for continuous service with minimal interruption because at least one VWS is always available.
2. **2** Upgrade SLC nodes.

   Upgrading SLC nodes is very similar to upgrading VWS nodes: while the peer SLC nodes are handling all production traffic, you can upgrade another SLC.
3. **3** Upgrade the SMS.

For instructions on upgrading the NCC nodes, see *Upgrading NCC* (on page 13).

Making sure VWS and SLC nodes are stable during the upgrade

You can minimize interruptions to service by ensuring that each node is stable before upgrading the next node. For example, when upgrading a VWS pair, you can follow this process:

- Upgrade the secondary VWS node.
- Wait while traffic is moved to the secondary VWS node.
- Monitor the secondary VWS node to make sure it is working correctly.
- Upgrade the primary VWS node and repeat the process.

You follow a similar process when upgrading SLC nodes.

If you have more than one pair of VWS nodes, you can upgrade a VWS pair and then wait for a period of time, such as one or two days, before upgrading the next pair. This can help you to manage interruptions to services; for example, when different VWS node pairs provide different services.

About Configuring Replication

Ways to configure replication

You configure replication when you upgrade the SMS nodes. You can configure replication in two ways:

- By using the SMS UI. This results in all replication processes (`updateLoader`, `smsStatsDaemon`, `smsAlarmDaemon`, `replicationIF`) reconnecting at the same time, and therefore can be difficult to monitor.
- By using a command line interface to manually create a new **replication.config** file and then manually stopping and restarting the processes one by one. This provides more control and easier monitoring, and no SMS UI access is required.

Instructions on how to configure replication by using the SMS UI are provided in *Upgrading the SMS* (on page 29). For more detailed information about configuring replication by using the SMS UI, see *NCC Service Management System User's Guide*. For instructions on manually configuring replication from a command line, see *Manually Configuring Replication* (on page 15).

About Service Interruption

About minimizing the impact of service interruption

During the upgrade, system availability will be impacted. The upgrade process is designed to retain end user service to a maximum degree during the upgrade. This is particularly important when upgrading the VWS and SLC nodes because these are the key elements providing end user service.

Note: At various times when individual nodes are being upgraded, capacity is reduced. Depending on how redundancy has been configured, the failover for SLC nodes is reduced or does not exist.

Service interruption on SMS

During the upgrade, you stop the NCC application processes. This means that all services and functions running from the SMS node will be interrupted until the processes are restarted.

Services interruption on the SMS occurs only while you upgrade the SMS node. The services and functions interrupted depend on the environment specific configuration. This list gives typical services and functions that will be interrupted:

- SMS UI access
- Provisioning Interface (PI) access
- Downstream replication to VWS and SLC nodes
- VWS call detail record (CDR) processing
- Update requests from VWS and SLC nodes: this includes Subscriber Self Management, which is executed from SLC control plans.

Note: Update requests will be queued during the upgrade and processed after the interruption.

Minimizing service interruption on VWS

During the upgrade, service interruption on the VWS is minimized by the following two features:

- Backward compatibility between NCC 15.2 VWS nodes and NCC 15.1 SLC nodes for the releases upgraded. See *Releases upgraded* (on page 1). This means you can upgrade all VWS nodes while the SLC nodes remain operational.
- Backward compatibility between the NCC 15.2 and NCC 15.1 VWS synchronization processes. This means you can upgrade one node of a VWS pair while the other node continues to process traffic. When the first node is upgraded, the VWS node pair resynchronizes. You can then upgrade the second node while the first node processes traffic.

Minimizing service interruption on SLC

The following attributes of the SLC allow you to perform a phased upgrade of all SLC nodes with no or minimal service interruption:

- Independence: SLC nodes do not interact with each other.
- Redundancy: where each network function is supported on multiple redundant SLC nodes in an N+1 or better configuration.

Note: The specific redundancy configuration deployed will determine the number of SLC nodes that can be taken out of service and upgraded simultaneously.

Upgrade Utility Tool

You can use the upgrade utility tool to perform direct upgrade from 12.0.2.0.0 to 15.2.0.0.0 in one go.

You can download the patch 38831642 to get this utility.

Patch contains the following two files:

- Upgrade_Script.sh
- NCC_RELEASE_LIST.txt.

Upgrade_Script.sh takes target release, path to the folder that contains required patches and Node name. It also creates a log file in '/IN/service_packages/PATCH' path with the following file name format: NCC_UPGRADE_<timestamp>.txt

Example:
./Upgrade_Script.sh "15.2.0.0.0" "/tmp/patches" SCP

Patch folder contains the following files:

- p29198348_120300_Linux-x86-64.zip
- p32877328_120400_Linux-x86-64.zip
- p33568261_120400_Linux-x86-64.zip
- p34150550_120600_Linux-x86-64.zip
- p34602145_120700_Linux-x86-64.zip
- p35996355_150100_Linux-x86-64.zip
- p36748610_151000_Linux-x86-64.zip
- p37460578_120500_Linux-x86-64.zip
- p37848963_152000_Linux-x86-64.zip

Compatibility Matrix

The below table lists the supported upgrade paths.

Product Version	15.1.0.0.0	15.2.0.0.0	OS
12.0.2.0.0 through 15.0.0.0.0	No	No	Solaris 11.4
12.0.2.0.0 through 15.0.0.0.0	Yes	Yes	OEL 8.X

Note:

This script is tested on OEL 8.X version. Operating system can be later upgraded to OEL 9.X.

This script does not support remote database upgrades.

Prerequisites

1) You need to upgrade OS and DB of all the nodes before starting upgrade.
2) Ensure that operating system is Solaris 11.4 or Oracle Enterprise Linux 8.x.
3) Ensure that Oracle Database is upgraded to 19c.
4) Create a soflink libclntshcore.so.12.1 > libclntshcore.so.19.1
5) Install compatssl10 on Linux environment and openssl 1.0.0 on Solaris.

Backup Steps

For backup steps, refer to the following sections in Chapter 3:

- Backing Up Database Tables and Ensuring Their Integrity
- Preparing Upgrade Configuration Files

Rollback Failover Handling

If any error occurs during upgrade, then script will uninstall all the patches it has installed so far. But if any error occurs while uninstalling the patches, you need to perform the uninstallation of the remaining patches manually. For more information, refer Chapter 5 Rolling Back the Upgrade.

Chapter 3

Preparing for the Upgrade

Overview

Introduction

This chapter explains the tasks that you must perform before upgrading Oracle Communications Network Charging and Control (NCC).

In this chapter

This chapter contains the following topics.

Backing Up Database Tables and Ensuring Their Integrity

Introduction

Before you upgrade, you must ensure that data is backed up by performing a full database backup. You should use the mechanism normally used when performing system maintenance to back up the NCC database. The backup should be scheduled to run immediately before commencing this patch upgrade.

You should also ensure that the integrity of the database is maintained during the upgrade.

Ensuring database integrity

You must verify that application triggers and constraints are enabled on all Service Management System (SMS), Voucher and Wallet Server (VWS) and Service Logic Controller (SLC) nodes to ensure:

- The integrity of the database is maintained during the upgrade
- No problems occur during the upgrade due to triggers and constraints having become accidentally disabled

Repeat these steps on each node to verify that application triggers and constraints are enabled.

Step	Action
1	Log in to the database node as the oracle user.

2	Enter the following commands to verify that triggers and constraints are enabled:
	`sqlplus '/ as sysdba'`
	`select table_name, constraint_name,status from dba_constraints where status != 'ENABLED' and owner != 'SYSTEM' and owner != 'SYS';`
	`select table_name, trigger_name,status from dba_triggers where status != 'ENABLED' and owner != 'SYSTEM' and owner != 'SYS';`
	Result: If no rows are returned, all triggers and constraints are enabled. If any triggers or constraints are returned, contact your database administrator for assistance.

Preparing Upgrade Configuration Files

Introduction

The NCC 15.2 release notes include information about new and updated configuration. Review the release notes for any configuration file changes or additions. You will prepare updated configuration files that include all the configuration changes relevant to you, and you will copy these files into place during the upgrade.

To prepare updated configuration files, perform the following tasks:

1. Back up the existing configuration files on all nodes. See *Backing up configuration files* (on page 8).
2. Copy the existing configuration files to a new location and update the configuration files in the new location with the configuration changes. See *Preparing new configuration files* (on page 9).

Note: Some patches automatically update the configuration files with configuration changes. After installing the upgrade patches on a node, you must review the existing configuration files for additional configuration updates and apply these updates to the configuration files in the new location.

Backing up configuration files

Follow these steps on all SMS, VWS, and SLC nodes in turn to back up the old configuration files.

Step	Action
1	Create a backup directory on the node: `mkdir -p /IN/service_packages/NCC152UP/config/old/`
2	Copy the existing configuration files to the backup directory by entering the following command for each file: `cp /IN/service_packages/config_file_name /IN/service_packages/NCC152UP/config/old/backup_config_file_name` where: • *config_file_name* is the name of the configuration file • *backup_config_file_name* is the name you give the configuration file Back up the following configuration files on the specified nodes: • **eserv.config** on all nodes • **SLEE.cfg** on VWS and SLC nodes • **acs.conf** on SLC nodes Give the backup files meaningful names. For example, **eserv.config_pre_NCC152**.

3	Copy the existing **.html** and **.jnlp** files to the backup directory on the SMS node by entering the following command:
	`cp /IN/html/file_name /IN/service_packages/NCC152UP/config/old/backup_file_name`
	where:
	• *file_name* is the name of the **.html** or **.jnlp** file
	• *backup_file_name* is the name you give the **.html** or **.jnlp** file
	Back up the following files on the SMS node:
	• **acs.jnlp, ccp.jnlp, sms.jnlp,** and **vpn.jnlp**
	Back up the following files on the SMS node to **/IN/service_packages/NCC152UP/Guiconfig/old/** (if present):
	smsGui.bat, smsGui.sh, acsGui.sh, acsGui.bat, ccpGui.sh, ccpGui.bat, vpnGui.sh, and vpnGui.bat.
	`cp /IN/html/file_name /IN/service_packages/NCC152UP/Guiconfig/old/ backup_file_name`

Preparing new configuration files

Follow these steps on all nodes to create new versions of the configuration files that have changes or additions.

Step	Action
1	Make a new directory for the configuration files that you will be updating: **`mkdir -p /IN/service_packages/NCC152UP/config/new/`**
2	Go to the new directory.
3	Copy the existing configuration files to the new directory by entering the following command for each file: **`cp /IN/service_packages/`***`config_file_name`* where *config_file_name* is the configuration file name.
4	Use a text editor such as vi to update the configuration files in the new directory.

Upgrade and downgrade in a remote database setup

To determine whether the database and application are hosted on the same node or on separate nodes, perform the following steps before performing an upgrade or downgrade:

Step	Action
1	Identify the node on which the database is installed.
2	Identify the node on which the application is installed.
3	If the database and application are hosted on the same node, install both the database patch and the application patch on that node.
4	If the database is hosted on a remote node: a. Install the database patch on the database node only. b. Install the application patch on the application node only.
5	Verify that the patches are installed on the appropriate nodes before proceeding with the upgrade or downgrade.

Prerequisites

To verify database connectivity in a remote database setup, perform the following steps:

Step	Action
1	Attempt to connect to the database using a connect string. For example: `sqlplus /@SMF`
2	If the connection fails on the remote database server, create an Oracle wallet before proceeding with the upgrade or downgrade patch installation. To create an Oracle wallet, see “Creating the Oracle Wallet on the Remote Database Server” in *Oracle Communications Network Charging and Control Installation Guide*.
3	Ensure that the Oracle wallet is created before installing any upgrade or downgrade patches.

Unpacking the Patches

Patch contents

A single distribution upgrade .zip file exists containing the following:

Item	Description
README.txt	The top level README file detailing the content of the zip file.
SMS/NCC_15_2_0_0_0-PATCH37848963_<OS>.zip	The database patch that needs to be installed on the node with the database installed.
SMS/NCC_15_2_0_0_0-PATCH37848975_<OS>.zip	The application patch that needs to be installed on the node running the application.

The database and application .zip file contained within has all the distributions for all nodes:

- P37848963SMS
- P37848963SCP
- P37848963BE
- Patch37848963_v1_0_README.txt

- P37848975SMS
- P37848975SCP
- P37848975BE
- Patch37848975_v1_0_README.txt

Notes:

- Always carefully study the readme text file for the SMS patch prior to proceeding with the upgrade. This file contains additional information about the release.
- For information on how to unpack the patch **.zip** file, see *Unpacking the patch file* (on page 11).

Where to install patches

The following table lists the type of node on which to install the different patches for each component. The type of node is indicated by the letters at the end of the patch filename.

Example

P37848963SMS should be installed on the SMS node.

If the Patch Filename Ends In	Install on This Type of Node
SMS	SMS
SCP	SLC
BE	VWS

PATCH37848963: The database patch, install this patch on any node which has the database server install and hosts the SMS, SCP or E2BE database instances using the rules in the table above.

PATCH37848975: The application patch, install this patch on any node which runs the NCC application using the rules in the table above.

Notes: The database host may be on separate node to the NCC application and may not have the same user policy. A database patch requires access to the Oracle system user and an account with sysdba privileges.

Unpacking the patch file

You unpack the patches for NCC release 15.2 on all SMS, VWS, and SLC nodes. Before unpacking the patch files, ensure you have the following disk space available on each node:

- 3 GB of disk space for unpacking the patches. You can unpack the patches in any location. However, this document assumes the patches will be unpacked in the **/var/spool/pkg/NCC152** directory:
- 2 GB of disk space to install the patches on each node in the **/IN** directory.

Follow these steps to unpack the patches.

Step	Action
1	Download the NCC 15.2 patches contained within the patch **.zip** file to the **/var/spool/pkg/PATCH** directory. The patch files are available from the Oracle Support website, located at **https://support.oracle.com**. **Note:** The application patch number and database patch number for NCC 15.2 is 37848975 and 37848963 respectively.
2	Go to the patch directory and as the root user, enter the following command to unzip the patch: **`unzip`** *`filename`***`.zip`** where *`filename`* is the name of the patch **.zip** file. **Result:** Creates a directory containing the ZIP file. **Example:** **SMS/NCC_15_2_0_0_0-PATCH37848963_svr4_v1_0.zip** **SMS/NCC_15_2_0_0_0-PATCH37848975_svr4_v1_0.zip**
3	Extract the patch from the **.zip** file: **`./extract_patches.sh`** **Result:** The patches are extracted. **Example:** **PATCH37848963** The patch contains the following files: • Patch37848963_v1_0_README.txt • P37848963BE • P37848963SCP • P37848963SMS **PATCH37848975** The patch contains the following files: • Patch37848975_v1_0_README.txt • P37848975BE • P37848975SCP • P37848975SMS
4	Ensure that the prerequisites are satisfied. For information about the prerequisite packages and prerequisite patch numbers, see NCC components upgrade table.

Chapter 4

Upgrading NCC

Overview

Introduction

This chapter explains how to install the Oracle Communications Network Charging and Control (NCC) upgrade patches and then upgrade the Service Management System (SMS), Service Logic Controller (SLC), and Voucher and Wallet Server (VWS).

In this chapter

This chapter contains the following topics.

About Upgrading

Upgrade order

Installing the upgrade requires each node of the NCC platform to be upgraded independently and sequentially in the following order:

1. Upgrade each VWS pair in this order: secondary node, then primary node.
2. Upgrade all SLC nodes, one by one.
3. Upgrade the SMS nodes.

Upgrading an individual node

Upgrading an individual node typically consists of the following high level steps:

1. Shut down the NCC application processes.
2. Install the NCC upgrade patch on the node, as per the NCC components upgrade table.
3. Restart the NCC application processes on the node.

Note: Service-critical functions remain available through redundant peer nodes during the upgrade process.

About upgrading the NCC remote database

If you are using a remote database for NCC, you perform the database upgrade on the remote database machine, not the application machine. There is a separate patch for database changes. See page 9 (upgrade patch table) for details.

Before you upgrade to NCC release 15.2, check whether the Oracle sys user can log in to the database as sysdba on the database machine. Enter the following command as the smf_oper user:

```
sqlplus "sys/password as sysdba"
```

where *password* is the password for the sys user. If the SQL prompt appears, the sys user can log in as sysdba and no configuration is necessary.

Installing database patches in a remote database setup

If all databases (SMS, SLC, and VWS/VWS2) are hosted on the same remote database server, perform the following steps before installing the database patches:

1. On the database node, locate the `Release:` field in the `/IN/bin/ocncc` file.
2. Make a note of, or back up, the value of the `Release:` field before installing the VWS database patch.
3. Install the VWS database patch.
   After the VWS database patch is installed, the `Release:` value in the `/IN/bin/ocncc` file is updated.
4. Before installing the SLC and SMS database patches, restore the `Release` value in the `/IN/bin/ocncc` file to the value you backed up before installing the VWS database patch.
5. During the upgrade on the database node, ensure that the `ORACLE_SID` environment variable is set to the database instance that is being upgraded.

   Example

   If you are upgrading from release 15.1.0.0.0 to 15.2.0.0.0.0, update the `/IN/bin/ocncc` file to set:

   ```
   Release: 15.1.0.0.0
   ```
6. Then install the SMS and SLC database patches.

Installing application patches in a remote database setup

To update the release version before installing an application patch on an application node, perform the following steps:

1. On the application node, open the `/IN/bin/ocncc` file.
2. Update the `Release:` value to the release number of the application patch.

   Example:

   If you are upgrading from release 15.1.0.0.0 to 15.2.0.0.0.0, update the `/IN/bin/ocncc` file to set:

   ```
   Release: 15.2.0.0.0
   ```
3. Install the application patches.

Using GNU Screen

About using GNU Screen

Use GNU Screen or a similar tool to perform every upgrade-related action on any NCC node. After installing GNU Screen, start a new screen session each time you perform an upgrade action. For example, start a screen session before installing a package on a node and running its configuration script.

Using GNU Screen ensures that shell sessions do not hang if there are any network connection issues between the session client and the telnet or ssh server on the node being upgraded. Using GNU Screen ensures that you can recover the shell session if the network connection is lost, and that any processes you were running in that shell session will not be stopped or left hanging.

Using GNU Screen for a shell session

Follow these steps to start a GNU Screen session to perform upgrade-related actions on a node of NCC.

Note: You must have already installed GNU Screen on the system.

Step	Action
1	Log in as the root user.
2	Enter **`screen`** at the command line. **Tips:** • To see all screen sessions, enter: **`screen –ls`** • If the connection is lost, re-attach to the screen session by entering: **`screen -DR`** *id* where *id* is the session ID.
3	When the upgrade action completes, exit the screen session by using the standard exit command. **Note:** For more information about GNU Screen, see the GNU Screen user documentation.

Manually Configuring Replication

About replication configuration

You configure replication at specific points during the upgrade process.

You can configure replication automatically by using the SMS UI or manually configure replication from a command line. This section describes how to configure replication from a command line.

For more information, see *About Configuring Replication* (on page 4).

Instructions on how to configure replication by using the SMS UI are included in the *Service Management System User's Guide*. If you choose to configure replication manually, perform the following tasks instead of using the SMS UI when you upgrade the SMS nodes.
To manually configure replication and stop and restart the replication process, you perform the following tasks.

Step	Action
1	Verify that the replication processes are running. See *Verifying that replication is running* (on page 16).
2	Configure replication. See *Configuring replication from the command line* (on page 16).
3	Stop and restart the replication processes. See *Stopping and starting replication processes* (on page 17).
4	Verify that the replication processes are running.

Verifying that replication is running

You verify replication is running to ensure it is working before you modify the replication configuration. Then, if any problems occur when you restart replication, you will know that the problems have been caused by the modifications, and not as a result of a pre-existing problem.

Follow these steps on all SMS nodes to verify replication is running.

Step	Action

1	From the command line on the SMS node, enter the following commands to verify that there are no synchronization processes running:
	`tail -f /IN/service_packages/SMS/tmp/smsMaster.log`
	`tail -f`
	`/IN/service_packages/SMS/tmp/resyncServer[SLCNODEID|VWSNODEID].log`
	`ps -ef | grep -i sync`
	Result: No resyncs should be ongoing.

2	Log in to the SMS node as the smf_oper user and enter:
	`sqlplus /`
	`select * from rep_pending_queue;`
	`select count(*) from rep_ora_renumbered;`
	`select unique table_name from rep_ora_renumbered;`
	Result: The ROE_EVENTID value for all replication nodes in the REP_PENDING_QUEUE table should be approximately the same, and should gradually but slowly increase. This means that updates are being replicated to the nodes.
	If replication is not running, you should determine the reason and resolve any problems. See *NCC Service Management System User's Guide* for more information.

Configuring replication from the command line

When configuring replication from the command line, you use the following two NCC utilities:

- `repConfigWrite` to manually create the **replication.config** file. `repConfigWrite` obtains the replication configuration from the database and writes it to the **replication.config** file in the location specified by the `output` parameter.
- `copyCnf` to copy the new **replication.config** file to the VWS and SLC nodes.

Follow these steps to configure replication from the command line.

Step	Action
1	Log in to the SMS as the smf_oper user.

2	Back up the **replication.config** file on the SMS node by entering the following commands:
	`cd /IN/service_packages/SMS/bin`
	`cp ../etc/replication.config ../etc/replication.bak`

Step **Action**

3 As the smf_oper user, make a backup of the **replication.config** file on each VWS or SLC node by entering the following commands:

> **Note**: Passwordless ssh between SMS-SLC and SMS-VWS must be configured. If not, change the script accordingly.

```
bash
cd /IN/service_packages/SMS/bin
for NODE in hostname_list
do
  ssh $NODE cp /IN/service_packages/SMS/etc/replication.config \
    /IN/service_packages/SMS/etc/replication.bak
done
```

where *hostname_list* is a space-separated list of host names for the VWS or SLC nodes, reachable from the SMS.

4 Create a new **replication.config** file by entering the following commands:

```
repConfigWrite -user smf_user/smf_password -output
../etc/replication.config
ls -lart ../etc
```

where:

- *smf_user* is the smf user on the local database
- *smf_password* is the password for the smf user

> **Note:** The new **replication.config** file replaces the existing **replication.config** file in the **/IN/service_packages/SMS/etc** directory.

5 Copy the new **replication.config** file created in step 4 to each VWS or SLC node by entering the following commands:

```
for NODE in hostname_list
do
  copyCnf /IN/service_packages/SMS/etc/replication.config $NODE
done
```

where *hostname_list* is a space-separated list of host names for the VWS or SLC nodes, reachable from the SMS.

> **Note:** If you are running the NCC applications in a clustered environment, you must also copy the new **replication.config** file to the other SMS nodes in the cluster.

Stopping and starting replication processes

After configuring replication, you stop and restart the replication processes.

Follow these steps to stop and restart replication processes from the command line.

Step **Action**

1 Open terminal sessions to all nodes.

> **Warning:** The next step will interrupt the replication subsystem. You should go through this procedure as quickly as possible to minimize the length of the interruption. Replication updates are normally queued and therefore will be processed when the replication subsystem is brought back up again.

Step	Action
2	Do the following to stop all `updateLoader` processes on the VWS and SLC nodes: • On Linux: For VWS: **`systemctl stop updateLoaderWrapper.service`** For SLC: **`systemctl stop updateLoader.service`**
3	Verify that the `updateLoader` processes have stopped by checking for connection errors in the **smsMaster.log** file in **/IN/service_packages/SMS/tmp** on the SMS nodes. **Result:** You should see TCP connection errors which indicate that the `updateLoader` processes have disconnected. **smsMaster.log example** `Feb  6 10:28:34 smsMaster(4919) ERROR: TCP connection to 192.168.45.38.33007 was lost`
4	When all `updateLoader` processes have been stopped, restart the `smsMaster` processes on the SMS. If you are running the NCC applications in a clustered environment, you will need to do this at the same time for all cluster nodes running `smsMaster`. Log in to the SMS as the smf_oper user and enter the following commands: **`ps -ef | grep smsMaster`** **`kill`** *`PID1 PID2`* where: *PID1* and *PID2* are the PIDs for the two `smsMaster` processes. **Note:** Update requesters (`replicationIf`, `StatsDaemons`, and so on) are not stopped and should reconnect immediately.
5	Do the following to restart the `updateLoader` processes on the VWS and SLC nodes: • On Linux: For VWS: **`systemctl restart updateLoaderWrapper.service`** For SLC: **`systemctl restart updateLoader.service`**

Step	Action

6	Enter the following command to check for FULL resyncs on the SMS node:
	`tail -f /IN/service_packages/SMS/tmp/smsMaster.log`
	When a FULL resync has started, then:
	a) Log in as the smf_oper user on the SMS node.
	b) Enter these commands:
	`ps –aef | grep [Rr]esyncServer`
	`kill -9` *PID1 PID2*
	where *PID1* and *PID2* are the PIDs of the `resyncServer` and `smsCompareResyncServer` processes on the node that is doing a full resync
	c) As the root user on the SLC or VWS replication node where the full `resync` is ongoing, enter:
	`pkill –USR2 updateLoader`
	Result: This causes the `updateLoader` process to read its queued orders file. It should report:
	`"Node back in sync"`
	Note: At this point, the interruption to the replication subsystem has ended.
	d) You can double check for hanging resynchronization processes by entering the following commands as the root user:
	`for NODE in` *hostname_list*
	`do`
	`  ssh $NODE ls /IN/service_packages/SMS/tmp/???-queuedOrders.dat`
	`done`
	where *hostname_list* is a space-separated list of hostnames for VWS or SLC nodes, reachable from the SMS
	Result: No **queuedOrders** files should exist.

7	On the SMS, verify that replication is running. For details, see *Verifying that replication is running* (on page 16).

Upgrading the VWS

About upgrading the VWS

To upgrade VWS nodes to NCC release 15.2, complete these procedures in the order listed, on each primary and secondary VWS pair. For each pair of nodes, upgrade the secondary VWS node first, and then the primary VWS node.

Step	Action
1	Update the timeout configuration for the `beCDRMover`. See *Updating beCDRMover timeout configuration* (on page 20).
2	Disable the `beGroveller` process on the VWS. See *Disabling grovelling on the VWS* (on page 20). **Note:** You should disable the `beGroveller` for the period required to upgrade both the primary and the secondary VWS.
3	Stop the SLEE on the VWS. See *Stopping the SLEE* (on page 21).
4	Verify that the system is running. See *Verifying the system is running* (on page 21).
5	Stop the NCC processes and cronjobs on the VWS. See *Stopping NCC processes and cronjobs* (on page 22).

Step	Action
6	Install the upgrade patches on the VWS. See *Installing patches on the VWS* (on page 22).
7	Install the updated configuration files on the VWS. See *Installing the updated configuration files* (on page 23).
8	Restart the NCC processes and cronjobs on the VWS. See *Restarting NCC processes and cronjobs* (on page 23).
9	Restart the SLEE on the VWS. See *Restarting the SLEE* (on page 23).
10	Re-enable the `beGroveller` process on the VWS only after you have upgraded both the primary and the secondary VWS nodes. See *Re-enabling grovelling on the VWS* (on page 24).
11	Verify that `BeClient` processes are running correctly on the VWS. See *Verifying BeClient processes on the VWS* (on page 24).

Updating beCDRMover timeout configuration

Before you upgrade the VWS nodes, update the configuration for the `beCDRMover` process to set the `timeout` parameter to a low value, such as 4 seconds. By setting a low `timeout` value, you ensure that the upgrade process is not slowed down by the `beCDRMover` process.

Note: When the `timeout` parameter is set to a high value, the upgrade process will take longer. For example, if the `timeout` parameter is set to 600 seconds, the `beCDRMover` can take up to 10 minutes to respond to a SIGTERM, which in turn will make the patch upgrade process very slow.

Follow these steps to set the `beCDRMover` `timeout` parameter.

Step	Action

1	Set the `timeout` parameter in the beCDRMover section of the **eserv.config** file on the VWS to a low value, by using the following syntax:
	`beCDRMover = {`
	`    timeout = int`
	`}`
	where *int* is the number of seconds before `beCDRMover` times out. You should set the `timeout` parameter to the recommended value of 4 or less.

2	Reload the configuration by sending a SIGHUP to `beCDRMover`. For more information about the `beCDRMover` process and `beCDRMover` configuration, see *NCC Voucher and Wallet Server Technical Guide*.

Disabling grovelling on the VWS

Disable grovelling while you upgrade the primary and secondary VWS nodes to ensure that wallet transactions are not duplicated by the `beGroveller` process during the upgrade.

You disable `beGroveller` by setting the `noProcessingTimes` parameter in the beGroveller section of the **eserv.config** file on the VWS. For example, the following configuration disables the `beGroveller` process for six hours starting at 06:00 AM.

```
beGroveller = {
    noProcessingTimes = [
        { startsAt = "06:00", endsAt = "12:00" }
    ]
}
```

Follow these steps to disable grovelling for a specified period.

Step	Action
1	Make a note of the current configuration for the `noProcessingTimes` parameter. After completing the upgrade on the VWS node, you must reset the configuration for the `noProcessingTimes` parameter to its original value.
2	Set the `noProcessingTimes` parameter for the period of time required to upgrade the primary and secondary VWS nodes.
3	Reload the configuration by sending a SIGHUP to `beGroveller`.

Stopping the SLEE

To stop the SLEE on the VWS, as the ebe_oper user, enter the following command:

```
slee-ctrl stop
```

Note:

- While the SLEE is stopped, all traffic should fail over to the peer VWS.
- If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1 or 15.1, log in as smf_oper user to stop the SLEE.

Verifying the system is running

Follow these steps to verify that the system is running correctly before proceeding with the upgrade.

Step	Action
1	On the SMS, verify that CCS CDRs are being received from the peer VWS by entering the following commands: **`cd /IN/service_packages/CCS/logs/`***`CDR-store`***`/`** **`ls -l	grep`** *`VWS_peer`* where: • *CDR-store* is the directory used to store CDRs • *VWS_peer* is the name of the peer VWS node **Note:** The folder used for storing CDRs will depend on the `ccsCDRLoader` configuration and the custom CDR archiving scripts.
2	On the SLC, verify that `BeClient` can still connect to the BE pair by checking the `syslog` for messages such as: `"Can contact either BE from BE Pair…"`
3	Go to the **/IN/service_packages/E2BE/sync/** directory on the peer VWS, and verify that the sync files are being queued in this directory by entering the command: **`while true; do du  -h; sleep 10; done`**.

Stopping NCC processes and cronjobs

Follow these steps to stop NCC processes and cronjobs on the VWS node.

Step	Action
1	Log in to the VWS node you are upgrading as the ccs_oper user. **Note**: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, or 15.0.1, log in as smf_oper user to change the cron jobs.
2	Stop all cronjobs that use NCC application binaries or scripts or that lock NCC database tables, or both, by commenting out all the jobs in `ccs_oper` crontab.
3	As the root user, stop the NCC applications that are not started from the SLEE. Do the following to stop the **inittab** processes: • On Linux: Run the following command: **`/IN/bin/OUI_systemctl.sh stop`**

Installing patches on the VWS

Install all patches that have a suffix of BE on the VWS node you are upgrading. Patches should be installed in the order listed in the NCC upgrade table.

Note: On the database host if you use Oracle Database 12.1, before installing the patches, login to the database machine as sysdba and run the following command to grant execute on SYS.ora12c_strong_verify_function to public:

```
SQL> grant execute on SYS.ora12c_strong_verify_function to public;

Grant succeeded.
```

Follow these steps to install a patch.

Step	Action
1	As the root user, log in to the VWS node on which you want to install the patch and go to the patch directory. **Note**: If the node is just running as a db host only install the database patch. If the node is running both the db and the application, install the database patch first followed by the application patch.
2	Do the following to install the patch: • On Linux: **`rpm -i --nodeps P`***`Patch_numberSuffix`* where: • *Patch_number* is the number of the patch you are adding. • *Suffix* is BE
3	Enter the following command to run the patch package configuration script: **`/IN/service_packages/PATCH/Patch`***`Patch_numberSuffix`***`/bin/configure.sh`** where: • *Patch_number* is the number of the patch you are adding. • *Suffix* is BE

Installing the updated configuration files

Follow these steps to install updated configuration files required on the VWS node you are upgrading.

Note: These are the configuration files that you prepared earlier in the upgrade process. See *Preparing Upgrade Configuration Files* (on page 8) for details.

Step	Action
1	Compare the current configuration files with the old configuration files to check for any automatic updates applied during patch installation by entering the following command for each configuration file on the VWS: `diff backup_config_file current_config_file` where: • *backup_config_file* is the backed up copy of the configuration file. See *Backing up configuration files* (on page 8) • *current_config_file* is the current configuration file after the upgrade patches have been installed
2	Note any reported differences.
3	Go to the directory where you created the updated configuration files for the VWS node you are currently upgrading, for example **/IN/service_packages/NCC152UP/config/new**.
4	If any differences were reported in step 1, edit `current_config_file` to include these changes.

5	Copy `current_config_file` to the directory where they will be used.
	See New configuration files for a list of the directories in which to install the updated configuration files.
	Example
	`cd /IN/service_packages/NCC151UP/config/new`
	`cp eserv.config /IN/service_packages`
	`cp SLEE.cfg /IN/service_packages/SLEE/etc`

Restarting NCC processes and cronjobs

Do the following to restart the NCC processes and cronjobs on the VWS node.

- On Linux:

Step	Action
1	Uncomment the previously commented cron jobs. Enter the following command to restart all services: `/IN/bin/OUI_systemctl.sh restart`

Restarting the SLEE

To restart the SLEE on the VWS, as the ebe_oper user, enter the command:

```
slee-ctrl start
```

Note: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1 or 15.1, log in as smf_oper user to restart the SLEE.

Log off the session where the upgrade was performed and create a new login session. This new session is required so that environment changes made by the patch upgrade on the VWS are reflected in the ebe_oper session that restarts the SLEE.

Re-enabling grovelling on the VWS

Re-enable the `beGroveller` process on the VWS node only after you have upgraded both the primary and the secondary VWS nodes.

To re-enable the `beGroveller` process, restore the configuration that was specified for the `noProcessingTimes` parameter before you disabled the `beGroveller` process. Then reload the configuration by sending a SIGHUP to `beGroveller`.

You configure the `noProcessingTimes` parameter in the beGroveller section of the **eserv.config** file on the VWS.

Verifying BeClient processes on the VWS

Follow these steps to verify `BeClient` processes are running on the VWS node.

Step	Action

1	Enter the following command to verify the VWS is starting up correctly and synchronizing with the peer VWS:
	- On Linux:
	`tail -f /var/log/messages`
	Result: Successful startup messages are logged for the VWS processes (`beServer`, `beVWARS`, and so on).
	Result: After a couple of minutes, `sync` starts and the following messages are logged:
	`beSync(18712) NOTICE: BE Synchronisation process is running 28035 seconds`
	`behind target (28040s total delay)`
	You may see multiple occurrences of `beWriter` messages. You can ignore these messages. For example:
	`Apr 26 23:26:31 beid beWriter: [ID 953149 user.warning] beWriter(29194)`
	`WARNING:`
	`remote syncBuffer [seqNo 8316183..8316184] 1 items in (4294 .. 4295):`
	`output timed out message 8316184 Apr 26 23:26:31 beid beWriter: [ID`
	`848595 user.crit] beWriter(29194) CRITICAL:`
	`syncBuffer remote: Incoming message has seqNo 8316107, before last sent`
	`seqNo 8316185, either a subsequent message timed out of this is a`
	`duplicate.`

2	Skip this step if you are upgrading the secondary VWS node. If you are upgrading the primary VWS node, after `sync` has completed, enter the following commands to verify that CDRs are being generated on the SMS: **`cd /IN/service_packages/CCS/logs/`**`*CDR-store*`**`/`** **`ls –l | grep`** `*VWS_name*` where: - *CDR-store* is the directory used to store CDRs - *VWS_name* is the name of the VWS you are upgrading. **Result:** You should see newly generated CDRs coming from the primary VWS node. **Note:** The directory used for storing CDRs is dependent on the `ccsCDRLoader` configuration and the custom CDR archiving scripts.

Step	Action
3	Verify `BeClient` processes on the SLC nodes: **`tail -f /IN/service_packages/CCS/tmp/BeClient.log`** **Result:** All `BeClient` processes should have reconnected to the primary VWS node which should have taken over traffic again.

Upgrading the SLC

About upgrading the SLC

To upgrade SLC nodes to NCC release 15.2, complete these procedures in the order listed on each SLC.

Step	Action
1	Monitor calls and redirect traffic to the peer SLC. See *Monitoring calls and redirecting traffic* (on page 25).
2	Stop the SLEE on the SLC. See *Stopping the SLEE* (on page 25).
3	Stop the NCC applications on the SLC. See *Stopping the NCC cronjobs and applications* (on page 26).
4	Install the upgrade patches on the SLC. See *Installing patches on the SLC* (on page 26).
5	Install the updated configuration files on the SLC. See *Installing the updated configuration files* (on page 27).
6	Restart the NCC application processes on the SLC. See *Restarting processes and cronjobs on the SLC* (on page 28).
7	Restart the SLEE on the SLC. See *Restarting the SLEE* (on page 28).
8	Verify the system startup. See *Verifying the SLC startup* (on page 29).

Monitoring calls and redirecting traffic

Follow these steps to monitor for outstanding calls and to direct traffic away from this SLC.

Step	Action
1	Log in as the acs_oper user. **Note**: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1 or 15.1, log in as smf_oper user to check the outstanding calls.
2	Go to the **/IN/service_packages/SLEE/bin/** directory.
3	Redirect traffic away from this SLC, using the `check` command to monitor for any outstanding calls: **`./check -b 10`**

Stopping the SLEE

To stop the SLEE, log in to the SLC as the acs_oper user and enter the command:

```
slee-ctrl stop
```

Note:

- While the SLEE is stopped, all traffic should fail over to the peer nodes.

- If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1 or 15.1 install, log in as smf_oper user to stop the SLEE.

Stopping the NCC cronjobs and applications

Follow these steps to stop NCC cronjobs on the SLC node, and all NCC applications that are not started from the SLEE.

Step	Action
1	Log in to the SLC as the acs_oper user. **Note**: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1 or 15.1, log in as smf_oper user to stop and change the cron jobs in SLC.
2	Edit the crontab by entering the following command: `crontab -e` **Note:** • The crontab for the acs_oper user is located in the following directory by default: **/var/spool/cron/crontabs/acs_oper.** • If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1 or 15.1, log in as smf_oper user to verify the crontab.
3	Stop the `rca_get_read_count` cronjob by commenting out the line in the crontab that runs **rca_get_read_count.sh.**
4	As the root user, stop the NCC applications that are not started from the SLEE. Do the following to stop NCC processes: • On Linux: Run the following command: **`/IN/bin/OUI_systemctl.sh stop`**

Installing patches on the SLC

Install all patches that have a suffix of SCP on the SLC node you are upgrading. Patches should be installed in the order listed in the NCC upgrade table.

Note: On the database host if you use Oracle Database 12.1, before installing the patches, login to the database machine as sysdba and run the following command to grant execute on SYS.ora12c_strong_verify_function to public:

```
SQL> grant execute on SYS.ora12c_strong_verify_function to public;

Grant succeeded.
```

Follow these steps to install a patch.

Step	Action
1	As the root user, log in to the SLC node on which you want to install the patch and go to the patch directory. **Note**: If the node is just running as a db host only install the database patch. If the node is running both the db and the application, install the database patch first followed by the application patch.

Step	Action
2	Do the following to install the patch: - On Linux: `rpm -i --nodeps PPatch_numberSuffix` where: - *Patch_number* is the number of the patch you are adding - *Suffix* is SCP
3	Enter the following command to run the patch package configuration script: `/IN/service_packages/PATCH/PatchPatch_numberSuffix/bin/configure.sh` where: - *Patch_number* is the number of the patch you are adding - *Suffix* is SCP

Installing the updated configuration files

Follow these steps to add new configuration files on the SLC node you are upgrading.

Note: These are the configuration files that you prepared earlier on in the upgrade process. See *Preparing Upgrade Configuration Files* (on page 8) for details.

Step	Action
1	Compare the current configuration files with the old configuration files to check for any automatic updates applied during patch installation by entering this command for each configuration file on the SLC: `diff backup_config_file current_config_file` where: - *backup_config_file* is the backup copy of the configuration file. See *Backing up configuration files* (on page 8) - *current_config_file* is the current configuration file after the upgrade patches have been installed
2	Note any reported differences.
3	Go to the directory where you created the updated configuration files for the SLC node you are currently upgrading, for example **/IN/service_packages/NCC152UP/config/new**.
4	If any differences were reported in step 1, edit the updated configuration files to include these changes.

5	Copy the updated configuration files to the directory where they will be used.
	See New configuration files on the SLC for a list of the directories in which to install the updated configuration files.
	Example
	`cd /IN/service_packages/NCC152UP/config/new`
	`cp eserv.config /IN/service_packages`
	`cp SLEE.cfg /IN/service_packages/SLEE/etc`
	`cp acs.conf /IN/service_packages/ACS/etc`

Configuration file changes on SLC

The following table lists the location for new configuration files on the SLC node.

Configuration File	Location
eserv.config	**/IN/service_packages**
SLEE.cfg	**/IN/service_packages/SLEE/etc**
acs.conf	**/IN/service_packages/ACS/etc**

A new ACS chassis plugin has been added as part of Sabre release. This needs to be listed in acs.conf, in order to load the same during SLEE start-up.

Add the following entry in 'acs.conf' along with the list of existing chassis plugins:

```
ChassisPlugin libccsChassisActions.so
```

Updating SLEE.cfg file for SMINAPCA

To enable the SMINAP feature, set the following configuration in the **SLEE.cfg** file, available in path: **/IN/service_packages/SLEE/etc folder.**

Define the necessary entries in **SLEE.cfg** as smf_oper user, to redirect the desired network SKs to smInapCA.

```
SERVICE=CCS_SMINAPCA 1 slee_acs CCS
SERVICEKEY=INTEGER 99 CCS_SMINAPCA
SERVICEKEY=INTEGER 350 smInapCa #350
```

Add the below line to start the smInapCA instance from the slee process, in the **SLEE.cfg** file.

```
INTERFACE=smInapCA smInapCA.sh /IN/service_packages/SMINAPCA/bin/ EVENT
```

Restarting processes and cronjobs on the SLC

Follow these steps to restart the NCC processes and cronjobs on the SLC.

Step	Action
1	Restart the NCC processes by entering the following command: • On Linux: **`/IN/bin/OUI_systemctl.sh restart`**
2	As the acs_oper user, restart the `rca_get_read_count` cronjob by editing the crontab. **Note**: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to edit the crontab.
3	Uncomment the line in the crontab that runs **rca_get_read_count.sh** by removing the "#" from the beginning of the line.

Restarting the SLEE

To restart the SLEE on the SLC, as the acs_oper user, enter the command:

```
slee-ctrl start
```

Note: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, or 15.0.1 install, then log in as smf_oper user for restarting the SLEE.

Verifying the SLC startup

Enter the following command to verify that the SLC starts up correctly and that traffic is being processed:

- On Linux:

```
tail -f /var/log/messages
```

Upgrading the SMS

About upgrading the SMS

To upgrade the SMS nodes to NCC release 15.2, complete these procedures in the order listed on each SMS.

Step	Action
1	Stop the NCC cronjobs on the SMS. See *Stopping NCC cronjobs* (on page 29).
2	Stop the NCC applications on the SMS. See *Stopping NCC applications* (on page 30).
3	Install the upgrade patches on the SMS. See *Installing patches on the SMS* (on page 30).
4	Install the updated configuration files on the SMS. See *Installing the updated configuration files* (on page 31).
5	Restart the NCC services on the SMS. See *Restarting the SMS* (on page 32).

Stopping NCC cronjobs

Follow these steps to stop NCC cronjobs on the SMS.

Important:

- This will stop all cronjobs that use NCC application binaries or scripts, or that lock NCC database tables, or both.
- SMS services will be interrupted following this procedure.

Step	Action
1	Log in to the SMS.
2	Comment out the following jobs in the `acs_oper` crontab: • `acsDbCleanup.sh` **Note:** If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the crontab.

Step	Action
3	Comment out the following jobs in the `ccs_oper` crontab: - `ccsWalletExpiry` - `ccsPeriodicCCRecharge` - `ccsCDRTrimFilesStartup.sh` - `ccsExpiryMessageLoader` - `ccsPeriodicCharge` - `ccsbt_deactivate_cleanup.sh` - `ccsbt_execute.sh` (there can be more than one) **Note:** If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the crontab.
4	Comment out the following jobs in the `smf_oper` crontab: - `smsDbCleanup.sh` - `smsCdrProcess.sh` - `smsReportsCleanerStartup.sh`
5	Comment out the following jobs in the `uis_oper` crontab: - `cdrLoaderCron.sh` **Note:** If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the crontab.

Stopping NCC applications

To stop the application processes on a single non-clustered SMS node:

Step	Action
On Linux:	
1	Run the following command: **`/IN/bin/OUI_systemctl.sh stop`**

To stop the application processes on a clustered SMS, shut down each resource group on the SMS node that you are upgrading by performing the following steps:

Step	Action
1	Determine the resource groups for all running processes by using the `scstat` command; for example: **`scstat -g | egrep -i 'group: sms|group: acs|group: ccs|group: mmx|group: rims' |grep -i Online |awk '{print $2}' |sort -u`**
2	Shut down each resource group with the `scswitch` command; for example: **`scswitch -F -g`** *`resource-1`*`,` *`resource-2`*`,` *`resource-3`*

Installing patches on the SMS

Install all patches that have a suffix of SMS on the SMS node. Patches should be installed in the order listed in the NCC upgrade table.

Note: On the database host if you use Oracle Database 12.1, before installing the patches, login to the database machine as sysdba and run the following command to grant execute on SYS.ora12c_strong_verify_function to public:

```
SQL> grant execute on SYS.ora12c_strong_verify_function to public;
Grant succeeded.
```

Follow these steps to install a patch.

Step	Action
1	Log in to the SMS node on which you want to install the patch as the root user and go to the patch directory. **Note**: If the node is just running as a db host only install the database patch. If the node is running both the db and the application, install the database patch first followed by the application patch
2	Do the following to install the patch: • On Linux: **`rpm -i --nodeps P`***`Patch_numberSuffix`* where: • *Patch_number* is the number of the patch you are adding • *Suffix* is SMS
3	Enter the following command to run the patch component configuration script: `/IN/service_packages/PATCH/`**`Patch`***`Patch_numberSuffix`*`/bin/configure.sh` where • *Patch_number* is the number of the patch you are adding • *Suffix* is SMS

Installing the updated configuration files

Follow these steps to install the updated configuration files required on the SMS node you are upgrading.

Note: These are the configuration files that you prepared earlier on in the upgrade process. See *Preparing Upgrade Configuration Files* (on page 8) for details.

Step	Action
1	Compare the current configuration files with the old configuration files to check for any automatic updates applied during patch installation by entering this command for each configuration file on the SMS: **`diff`** *`backup_config_file current_config_file`* where: • *backup_config_file* is the backup copy of the configuration file. See *Backing up configuration files* (on page 8) • *current_config_file* is the current configuration file after the upgrade patches have been installed
2	Note any reported differences.
3	Go to the directory where you created the updated configuration files for the SMS node you are currently upgrading; for example: **IN/service_packages/NCC152UP/config/new**.
4	If any differences were reported in step 1, edit the updated configuration files to include these changes.

Step	Action

5	Copy the updated configuration files to the directory where they will be used.
	See New configuration files on the SMS for a list of the directories in which to install the updated configuration files.
	Example
	`cd /IN/service_packages/NCC152UP/config/new`
	`cp eserv.config /IN/service_packages`

Restarting the SMS

Follow these steps to restart services on the SMS.

Step	Action
1	Restart the previously stopped services. Do one of the following: • If NCC is installed on a single non-clustered SMS: On Linux: a) Run the following command: **`/IN/bin/OUI_systemctl.sh restart`** • If NCC is installed on a clustered SMS, use the **`scswitch`** command on the upgraded SMS cluster node to restart each resource group that you shut down previously; for example: **`scswitch -Z -g`** *`resource-1`*, *`resource-2`*, *`resource-3`*

2	Check that the SMS processes are running by entering the following commands:
	`tail -f /IN/service_packages/SMS/tmp/smsNamingServer.log`
	`tail -f /IN/service_packages/SMS/tmp/smsTaskAgent.log`
	`tail -f /IN/service_packages/SMS/tmp/smsMaster.log`
	`tail -f /IN/service_packages/CCS/tmp/ccsBeOrb.log`
	Restart any processes that are not running.

3	Continuously monitor the **syslog** file using the following command: • On Linux: **`tail -f /var/log/messages`**
4	Uncomment the cronjobs you previously commented out.
5	Clear the temporary Internet files from the Java cache.
6	Restart the SMS UI.

Accessing SMS UI

To access the SMS user interface (UI), do the following:

- Ensure the Java SE Runtime Environment version 21 is installed on your machine.
- If required, obtain, and install the trusted certificate for the database connection into your keystore.
- Obtain the application zip file containing jars and other files (smsGui.bat or smsGui.sh) from **/IN/html** path of SMS node.
- In Windows, run **smsGui.bat** to start the application.

- In other machines:
  - Change the permission of **smsGui.sh** using `chmod 755 smsGui.sh` command.

- Run the application using `bash smsGui.sh` command.

Note: As part of the upgrade, sample **smsGUI.sh** and **smsGui.bat** files (*.example) are placed in **/IN/html** on the SMS host machine. After the upgrade, the parameters, especially the CLASSPATH and the variables, need to be changed based on the original .sh/.bat files.

Sample files are included at the end of this document.

Chapter 5

Rolling Back the Upgrade

Overview

Introduction

This chapter explains how to roll back the Oracle Communications Network Charging and Control (NCC) upgrade on the Service Management System (SMS), Service Logic Controller (SLC), and Voucher and Wallet Server (VWS).

In this chapter

This chapter contains the following topics.

About Rolling Back the Upgrade

Introduction to rolling back the upgrade

You may need to roll back the NCC release 15.2 upgrade, for example, if the upgrade is unsuccessful and the post-upgraded software is not functioning as expected.

Rollback order

Rolling back the upgrade requires each node on the NCC platform to be rolled back independently and sequentially in the following order:

1. Roll back the SMS nodes.
2. Roll back all SLC nodes, one by one.
3. Roll back each VWS pair in reverse order: primary node, then secondary node.

Rolling back an individual node

Rolling back an individual node includes two steps. 15.2 Application patch must be rolled back before rolling back 15.2 database patch. In general, roll back of patches should be done in reverse order of applying patches.

Rolling back an individual node consists of the following high-level steps:

1. Shut down the NCC application processes.
2. Remove the NCC upgrade patches on the node, one by one.
3. Restart the NCC application processes on the node.

Rollback considerations for remote database and application setup

This section describes additional steps to consider when uninstalling application and database patches during a rollback.

Uninstalling application patches

If the `Release:` field in the `/IN/bin/ocncc` file was manually updated during the installation of an application patch, you must manually update this value again after the downgrade, following the steps below:

1. Continue with the application patch removal steps for the node.
2. On the application node, open the `/IN/bin/ocncc` file.
3. Update the `Release:` value to the appropriate release version after the downgrade.

Note: Ensure that the `Release:` value reflects the correct version before proceeding with post-rollback activities.

Uninstalling database patches

Follow the steps below to ensure that the environment is set for the correct database during a downgrade on the database node:

1. On the database node, set the `ORACLE_SID` environment variable to the database instance that is being downgraded.
2. Verify that the environment is correctly set.
3. Proceed with the database patch removal.

Launching SMS GUI

After completing the rollback, you can access the SMS user interface.

For instructions, see “Launching the SMS GUI” in the *Oracle Communications Network Charging and Control Installation Guide*.

Rolling Back the SMS Upgrade

About rolling back the SMS upgrade

To roll back the upgrade on the SMS, complete these procedures, in the order listed, on all the SMS nodes that have been upgraded to NCC release 15.2.

Step	Action
1	Stop the NCC cronjobs on the SMS. See *Stopping NCC cronjobs* (on page 37).
2	Stop the NCC applications on the SMS. See *Stopping NCC applications during rollback* (on page 37).
3	Remove NCC release 15.2 patches from the SMS. See *Removing patches on the SMS* (on page 38).
4	Configure the replication.config file. See *Configuring replication file* (on page 38).
5	Restore backed up configuration files. See *Restoring backed up configuration files* (on page 39).
6	Restart the SMS. See *Restarting the SMS* (on page 40).

Stopping NCC cronjobs

Follow these steps to stop NCC cronjobs on the SMS.

Important:

- This will stop all cronjobs that use NCC application binaries or scripts or that lock NCC database tables, or both.
- SMS services will be interrupted following this procedure.

Step	Action
1	Log in to the SMS.
2	Comment out the following jobs in the `acs_oper` crontab: • `acsDbCleanup.sh` **Note**: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the crontab.
3	Comment out the following jobs in the `ccs_oper` crontab: • `ccsWalletExpiry` • `ccsPeriodicCCRecharge` • `ccsCDRTrimFilesStartup.sh` • `ccsExpiryMessageLoader` • `ccsPeriodicCharge` • `ccsbt_deactivate_cleanup.sh` • `ccsbt_execute.sh` (there can be more than one) **Note**: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the crontab.
4	Comment out the following jobs in the `smf_oper` crontab: • `smsDbCleanup.sh` • `smsCdrProcess.sh` • `smsReportsCleanerStartup.sh`
5	Comment out the following jobs in the `uis_oper` crontab: • `cdrLoaderCron.sh` **Note**: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the crontab.

Stopping NCC applications during rollback

To stop the application processes on a single non-clustered SMS node:

Step	Action
On Linux:	
1	Run the following command: **`/IN/bin/OUI_systemctl.sh stop`**

To stop the application processes on a clustered SMS, shut down each resource group on the SMS node that you are rolling back by performing the following steps:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Determine the resource groups for all running processes by using the `scstat` command; for example:
scstat -g | egrep -i 'group: sms|group: acs|group: ccs|group: mmx|group: rims' |grep -i Online |awk '{print $2}' |sort -u</td></tr>
<tr><td>2</td><td>Shut down each resource group with the **scswitch** command; for example:
scswitch -F -g *resource-1*, *resource-2*, *resource-3*</td></tr>
</table>

Removing patches on the SMS

Remove all patches that have a suffix of SMS from the upgraded SMS nodes. You must remove patches in the reverse order to the order used for installation, listed in the NCC components upgrade table.

Follow these steps to remove a patch.

Step	Action
1	As the root user, log in to the SMS node on which you want to remove a patch. **Note**: If the node is just running as a db host only remove the database patch. If the node is running both the db and the application, remove the application patch first followed by the database patch. This is the reverse of the install.
2	Run the patch unconfiguration script by entering the following command: **Note:** On a cluster model, run the patch unconfiguration script only on the primary node. **/IN/service_packages/PATCH/Patch***Patch_numberSuffix***/bin/unconfigure.sh** where: • *Patch_number* is the number of the patch you are removing • *Suffix* is SMS
3	Do the following to remove the patch: • On Linux: **rpm -e P***Patch_numberSuffix* where: • *Patch_number* is the number of the patch you are removing • *Suffix* is SMS

Configuring replication file

After you remove the patches, create the replication config file and copy it to all nodes.

When configuring replication from the command line, you use the following two NCC utilities:

- `repConfigWrite` to manually create the **replication.config** file. `repConfigWrite` obtains the replication configuration from the database and writes it to the **replication.config** file in the location specified by the `output` parameter.
- `copyCnf` to copy the new **replication.config** file to the VWS and SLC nodes.

Follow these steps to configure replication from the command line.

Step	Action
1	Log in to the SMS as the smf_oper user.

2	Create a new **replication.config** file by entering the following commands:
	`cd /IN/service_packages/SMS/bin`
	`repConfigWrite -user smf_user/smf_password -output ../etc/replication.config`
	`ls -lart ../etc`
	where:
	• *smf_user* is the smf user on the local database
	• *smf_password* is the password for the smf user
	Note: The new **replication.config** file replaces the existing **replication.config** file in the **/IN/service_packages/SMS/etc** directory.

3	Copy the new **replication.config** file created in step 2 to each VWS or SLC node by entering the following commands:
	`for NODE in hostname_list`
	`do`
	`  copyCnf /IN/service_packages/SMS/etc/replication.config $NODE`
	`done`
	where *hostname_list* is a space-separated list of host names for the VWS or SLC nodes, reachable from the SMS.
	Note: If you are running the NCC applications in a clustered environment, you must also copy the new **replication.config** file to the other SMS nodes in the cluster.

Restoring backed up configuration files

Follow these steps to restore the old configuration files on the SMS node on which you are rolling back the upgrade.

Note: These are the configuration files that you backed up earlier in the upgrade process. See *Preparing Upgrade Configuration Files* (on page 8).

Step	Action
1	Go to the configuration files backup directory for the SMS node you are rolling back: `cd /IN/service_packages/NCC152UP/config/old`

2	Copy the backed up configuration files to their original directories.
	See *Restored configuration files on the SMS* (on page 39) for a list of the directories in which to restore configuration files on the SMS node.
	Example
	`cd /IN/service_packages/NCC152UP/config/old`
	`cp eserv.config_pre_NCC152/IN/service_packages/eserv.config`

Restored configuration files on the SMS

The following table lists the backup configuration files and the location in which to restore them on the SMS node.

Backup Configuration File	Restore to
eserv.config_pre_NCC152	**/IN/service_packages/eserv.config**

Restarting the SMS

Follow these steps to restart services on the SMS.

Step	Action
1	Restart the previously stopped services. Do one of the following: • If NCC is installed on a single non-clustered SMS: On Linux: a) Run the following command: **`/IN/bin/OUI_systemctl.sh restart`** • If NCC is installed on a clustered SMS, use the **`scswitch`** command to restart each resource group that you shut down previously, for example: **`scswitch -Z -g`** *`resource-1, resource-2, resource-3`*
2	Uncomment the cronjobs previously commented out.
3	Clear the temporary internet files in the Java cache.
4	Restore the previously backed-up files (smsGui.bat, smsGui.sh, acsGui.sh, acsGui.bat, ccpGui.sh, ccpGui.bat, vpnGui.sh, and vpnGui.bat) from **/IN/service_packages/CCC152UP/Guiconfig/old/** to the **/IN/html** folder.
5	Restart the SMS UI.

Accessing SMS UI

To access the SMS user interface (UI), do the following:

- Ensure the Java SE Runtime Environment version 21 is installed on your machine.
- If required, obtain, and install the trusted certificate for the database connection into your keystore.
- Obtain the application zip file containing jars and other files (**smsGui.bat** or **smsGui.sh**) from **/IN/html** path of SMS node.

Rolling Back the SLC Upgrade

About rolling back the SLC upgrade

To roll back the upgrade on SLC nodes, complete these procedures in the order listed, on all the SLC nodes that have been upgraded to NCC release 15.2.

Step	Action
1	Stop the NCC applications on the SLC. See *Stopping the NCC cronjobs and applications* (on page 41).
2	Stop the SLEE on the SLC. See *Stopping the SLEE* (on page 41).
3	Remove the upgrade patches from the SLC. See *Removing patches from the SLC* (on page 41).
4	Restore the backed up configuration files on the SLC. See *Restoring backed up configuration files* (on page 42).
5	Restart the NCC application processes on the SLC. See *Restarting processes and cronjobs on the SLC* (on page 43).
6	Restart the SLEE on the SLC. See *Restarting the SLEE* (on page 43).
7	Verify the system startup. See *Verifying the SLC startup* (on page 43).

Stopping the NCC cronjobs and applications

Follow these steps to stop NCC cronjobs on the SLC node, and all NCC applications that are not started from the SLEE.

Step	Action
1	Log in to the SLC as the acs_oper user. **Note**: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the cronjobs.
2	Edit the crontab by entering the following command: `crontab -e` **Note:** • The crontab for the acs_oper user is located in the following directory by default: **/var/spool/cron/crontabs/acs_oper.** • If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to verify the crontab.
3	Stop the `rca_get_read_count` cronjob by commenting out the line in the crontab that runs **rca_get_read_count.sh.**
4	As the root user, do the following to stop NCC applications that are not started from the SLEE: • On Linux, run the following command: **`/IN/bin/OUI_systemctl.sh stop`**

Stopping the SLEE

To stop the SLEE, log in to the SLC as the acs_oper user and enter the command:

```
slee-ctrl stop
```

Note:

- While the SLEE is stopped, all traffic should fail over to the peer nodes.
- If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to stop the SLEE.

Removing patches from the SLC

Remove all patches that have a component for the SLC node from the upgraded SLC node. You must remove component patches in the reverse order to the order used for installation, listed in the NCC components upgrade table.

Follow these steps to remove a patch.

Step	Action
1	As the root user, log in to the SLC node on which you want to remove a patch. **Note**: If the node is just running as a db host only remove the database patch. If the node is running both the db and the application, remove the application patch first followed by the database patch. This is the reverse of the install.

Step	Action
2	Enter the following command to run the patch unconfiguration script: **/IN/service_packages/PATCH/Patch***Patch_numberSuffix***/bin/unconfigure.sh** where: • *Patch_number* is the number of the patch you are removing • *Suffix* is SCP
3	Do the following to remove the patch: • On Linux: **rpm -e P***Patch_numberSuffix* where: • *Patch_number* is the number of the patch you are removing • *Suffix* is SCP

Restoring backed up configuration files

Follow these steps to restore the old configuration files on the SLC node on which you are rolling back the upgrade.

Note: These are the configuration files that you backed up earlier in the upgrade process. See *Preparing Upgrade Configuration Files* (on page 8).

Step	Action
1	Go to the configuration files backup directory for the SLC node you are rolling back; for example, **/IN/service_packages/NCC152UP/config/old**.
2	Copy the backed up configuration files to their original directories. See *Restored configuration files* (on page 42) for a list of the directories in which to restore configuration files on SLC nodes. **Example:** **cd /IN/service_packages/NCC152UP/config/old** **cp eserv.config_pre_NCC152 /IN/service_packages/eserv.config** **cp SLEE.cfg_pre_NCC152 /IN/service_packages/SLEE/etc/SLEE.cfg** **cp acs.conf_pre_NCC152 /IN/service_packages/ACS/etc/acs.conf**

Restored configuration files

The following table lists the backup configuration files and the location in which to restore them on the SLC node.

Backup Configuration File	Restore to
eserv.config_pre_NCC152	/IN/service_packages/eserv.config
SLEE.cfg_pre_NCC152	/IN/service_packages/SLEE/etc/SLEE.cfg
acs.conf_pre_NCC152	/IN/service_packages/ACS/etc/acs.conf

Restarting processes and cronjobs on the SLC

Follow these steps to restart the NCC processes and cronjobs on the SLC.

Step	Action
1	Restart the NCC processes by entering the following command: • On Linux: `/IN/bin/OUI_systemctl.sh restart`
2	As the acs_oper user, restart the `rca_get_read_count` cronjob by editing the crontab. **Note**: If you are upgrading from 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to edit the crontab.
3	Uncomment the line in the crontab that runs **rca_get_read_count.sh** by removing the "#" from the beginning of the line.

Restarting the SLEE

To restart the SLEE on the SLC as the acs_oper user, enter the command:

```
slee-ctrl start
```

Note: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to restart the SLEE.

Verifying the SLC startup

Enter the following command to verify that the SLC starts up correctly and that traffic is being processed:

- On Linux:

```
tail -f /var/log/messages
```

Rolling Back the VWS Upgrade

About rolling back the VWS upgrade

To roll back the upgrade on the VWS, complete these procedures, in the order listed, on all the VWS nodes that have been upgraded to NCC release 15.2. Roll back VWS pairs in reverse order of installation.

Step	Action
1	Disable `beGroveller` on the VWS. See *Disabling grovelling during the rollback* (on page 44).
2	Stop the SLEE on the VWS. See *Stopping the SLEE* (on page 44).
3	Set up system monitoring. See *Setting up system monitoring* (on page 44).
4	Stop the NCC processes and cronjobs on the VWS. See *Stopping NCC processes and cronjobs* (on page 45).
5	Remove the upgrade patches from the VWS. See *Removing patches on the VWS* (on page 45).
6	Restore the backed up configuration files on the VWS. See *Restoring backed up configuration files* (on page 46).

Step	Action
7	Restart the NCC processes and cronjobs on the VWS. See *Restarting NCC processes and cronjobs* (on page 47).
8	Restart the SLEE on the VWS. See *Restarting the SLEE* (on page 47).
9	Re-enable `beGroveller` process on the VWS. See *Re-enabling grovelling on the VWS* (on page 47).
10	Verify `BeClient` processes on the VWS are working. See *Verifying BeClient processes on the VWS* (on page 47).

Disabling grovelling during the rollback

Disable grovelling while you roll back the upgrade to the primary and secondary VWS nodes to ensure that wallet transactions are not duplicated by the `beGroveller` process during the roll back process.

To disable grovelling for a specified period, set the `noProcessingTimes` parameter in the beGroveller section of the **eserv.config** file on the VWS, and then reload the configuration by sending a SIGHUP to `beGroveller`.

For example, the following configuration disables the `beGroveller` process for six hours starting at 06:00 AM.

```
beGroveller = {
    noProcessingTimes = [
        { startsAt = "06:00", endsAt = "12:00" }
    ]
}
```

Note: Before you update the **eserv.config** configuration file, make a note of the current configuration for the `noProcessingTimes` parameter. After you complete rolling back the upgrade on the VWS node, you must reset the configuration for the `noProcessingTimes` parameter to its original value.

Stopping the SLEE

To stop the SLEE on the VWS, as the ebe_oper user, enter the following command:
```
slee-ctrl stop
```

Note:

- While the SLEE is stopped, all traffic should fail over to the peer VWS.
- If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to stop the SLEE.

Setting up system monitoring

Follow these steps to monitor the system prior to rolling back the upgrade on the VWS node.

Step	Action
1	Enter the following command to monitor the `syslog` on the peer VWS node: • On Linux: **`tail -f /var/log/messages`**

Step	Action
2	Enter the following command to monitor `syslog` on the SMS and SLC nodes for errors on Linux: • On Linux: **`tail -f /var/log/messages`** **Result:** Only the connection loss to the upgraded VWS node is reported; the system continues using the peer VWS node.
3	On the SMS, verify that Charging Control Services (CCS) CDRs are being received from the peer VWS node by entering these commands: **cd /IN/service_packages/CCS/logs/***CDR-store***/** **ls –l | grep** *VWS_peer* where: • *CDR-store* is the directory used to store CDRs • *VWS_peer* is the name of the peer VWS node **Note:** The folder used for storing CDRs will depend on the `ccsCDRLoader` configuration and the custom CDR archiving scripts.

Stopping NCC processes and cronjobs

Follow these steps to stop NCC processes and cronjobs on the VWS node.

Step	Action
1	Log in to the VWS node as ccs_oper user. **Note**: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to change the cronjobs.
2	Stop all cronjobs that use NCC application binaries or scripts or that lock NCC database tables, or both, by commenting out all the jobs in `ccs_oper` crontab. **Note**: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, comment out all the jobs in `smf_oper` crontab.
3	As the root user, do the following to stop NCC applications that are not started from the SLEE: • On Linux, run the following command: **`/IN/bin/OUI_systemctl.sh stop`**

Removing patches on the VWS

Remove all patches that have a suffix of BE from the upgraded VWS node. You must remove patches in the reverse order to the order used for installation, listed in the NCC upgrade table.

Follow these steps to remove a patch.

Step	Action
1	As the root user, log in to the VWS node on which you want to remove a patch. **Note**: If the node is just running as a db host only remove the database patch. If the node is running both the db and the application, remove the application patch first followed by the database patch. This is the reverse of the install.
2	Enter the following command to run the patch unconfiguration script: **`/IN/service_packages/PATCH/Patch`***`Patch_numberSuffix`***`/bin/unconfigure.sh`** where: • *Patch_number* is the number of the patch you are removing • *Suffix* is BE
3	Do the following to remove the patch: • On Linux: **`rpm -e P`***`Patch_numberSuffix`* where: • *Patch_number* is the number of the patch you are removing • *Suffix* is BE

Restoring backed up configuration files

Follow these steps to restore the old configuration files on the VWS node on which you are rolling back the upgrade.

Note: These are the configuration files that you backed up earlier in the upgrade process. See *Preparing Upgrade Configuration Files* (on page 8).

Step	Action
1	Go to the configuration files backup directory for the VWS node you are rolling back; for example, **/IN/service_packages/NCC152UP/config/old**.

2	Copy the backed up configuration files to their original directories.
	See *Restored configuration files* (on page 46) for a list of the directories in which to restore configuration files on the VWS node.
	Example
	`cd /IN/service_packages/NCC152UP/config/old`
	`cp eserv.config_pre_NCC152 /IN/service_packages/eserv.config`
	`cp SLEE.cfg_pre_NCC152 /IN/service_packages/SLEE/etc/SLEE.cfg`

Restored configuration files

The following table lists the backup configuration files and the location in which to restore them on the VWS node.

Backup Configuration File	Restore to
eserv.config_pre_NCC152	**/IN/service_packages/eserv.config**
SLEE.cfg_pre_NCC152	**/IN/service_packages/SLEE/etc/SLEE.cfg**

Restarting NCC processes and cronjobs

Follow these steps to restart the NCC processes and cronjobs on the VWS node.

- On Linux:

Step	Action
1	Uncomment the previously commented cron jobs.
2	Enter the following command to restart all services: **`/IN/bin/OUI_systemctl.sh restart`**

Restarting the SLEE

To restart the SLEE on the VWS, as the ebe_oper user, enter the command:

```
slee-ctrl start
```

Note: If the system is running 12.0.2, 12.0.3, 12.0.4, 12.0.5, 12.0.6, 15.0.0, 15.0.1, or 15.1, log in as smf_oper user to restart the SLEE.

Re-enabling grovelling on the VWS

Re-enable the `beGroveller` process on the VWS node only after you have rolled back both the primary and the secondary VWS nodes.

To re-enable the `beGroveller` process, restore the configuration that was specified for the `noProcessingTimes` parameter before you disabled the beGroveller process. Then reload the configuration by sending a SIGHUP to `beGroveller`.

You configure the `noProcessingTimes` parameter in the `beGroveller` section of the **eserv.config** file on the VWS.

Verifying BeClient processes on the VWS

Follow these steps to verify `BeClient` processes are running on the VWS node.

Step	Action
1	Enter the following command to verify the VWS is starting up correctly and synchronizing with the peer VWS: • On Linux: **`tail -f /var/log/messages`** **Result:** Successful startup messages are logged for the VWS processes (`beServer`, `beVWARS`, and so on).

2	After the startup completes, monitor the progress of `sync` by keeping the tail open and by entering these commands on the peer VWS:
	`cd /IN/service_packages/E2BE/sync`
	`while true`
	`do`
	`find . -type f | wc -l`
	`sleep 10`
	`done`

Step **Action**

Result: After a couple of minutes, `sync` starts and the following messages are logged:

```
beSync(18712) NOTICE: BE Synchronisation process is running 28035 seconds
behind target (28040s total delay)
```

You may see multiple occurrences of `beWriter` messages. You can ignore these messages. For example:

```
Apr 26 23:26:31 beid beWriter: [ID 953149 user.warning] beWriter(29194)
WARNING:
remote syncBuffer [seqNo 8316183..8316184] 1 items in (4294 .. 4295):
output timed out message 8316184 Apr 26 23:26:31 beid beWriter: [ID
848595 user.crit] beWriter(29194) CRITICAL:
syncBuffer remote: Incoming message has seqNo 8316107, before last sent
seqNo 8316185, either a subsequent message timed out of this is a
duplicate.
```

3 Skip this step if you are rolling back the secondary VWS node.

If you are rolling back the primary VWS node, after `sync` has completed, enter the following commands to verify that CDRs are being generated on the SMS:

```
cd IN/service_packages/CCS/logs/CDR-store/
ls –l | grep VWS_name
```

where:

- *CDR-store* is the directory used to store CDRs
- *VWS_name* is the name of the VWS you are upgrading.

Result: You should see newly generated CDRs coming from the primary VWS node.

Note: The directory used for storing CDRs will depend on the `ccsCDRLoader` configuration and the custom CDR archiving scripts.

4 Verify `BeClient` processes on the SLC nodes:

```
tail –f /IN/service_packages/CCS/tmp/BeClient.log
```

Result: All `BeClient` processes should have reconnected to the primary VWS node which should have taken over traffic again.

Appendix A

Examples of smsGui.bat and smsGui.sh files

The following are examples of **smsGui.bat** and **smsGui.sh** files:

smsGui.bat

```
@echo off


REM Copyright (c) 2025 Oracle. All rights reserved.
REM
REM This material is the confidential property of Oracle Corporation or its
REM licensors and may be used, reproduced, stored or transmitted only in
REM accordance with a valid Oracle license or sublicense agreement.
REM
REM
REM smsGui.bat: runs the SMS application
REM Run: execute smsGui.bat


REM Set JAR_PATH to the current directory
set JAR_PATH=%~dp0


REM Enable delayed expansion
setlocal enabledelayedexpansion


REM Set classpath
set
CLASSPATH=%JAR_PATH%;%JAR_PATH%sms.jar.sig;%JAR_PATH%common.jar.sig;%JAR_PATH%ojdbc11.jar.sig;%J
AR_PATH%oraclepki.jar.sig;%JAR_PATH%acs.jar.sig;%JAR_PATH%osd.jar.sig;%JAR_PATH%PIsecurity.jar.s
ig;%JAR_PATH%pi.jar.sig;%JAR_PATH%dap.jar.sig;%JAR_PATH%jaxb-runtime-
4.0.5.jar.sig;%JAR_PATH%jaxb-core-4.0.5.jar.sig;%JAR_PATH%istack-commons-runtime-
4.1.2.jar.sig;%JAR_PATH%jakarta.xml.bind-api-
4.0.4.jar.sig;%JAR_PATH%http_client.jar.sig;%JAR_PATH%orawsdl.jar.sig;%JAR_PATH%ccs.jar.sig;%JAR
_PATH%UIS_GW.jar.sig;%JAR_PATH%UPC.jar.sig;%JAR_PATH%upcMacros.jar.sig;%JAR_PATH%rims.jar.sig;%J
AR_PATH%xms.jar.sig;%JAR_PATH%smcb.jar.sig;%JAR_PATH%np.jar.sig;%JAR_PATH%lcp.jar.sig;%JAR_PATH%
enum.jar.sig;%JAR_PATH%ses.jar.sig;%JAR_PATH%vpn.jar.sig;%JAR_PATH%rca.jar.sig;%JAR_PATH%asm-
9.7.1.jar.sig;%JAR_PATH%asm-analysis-9.7.1.jar.sig;%JAR_PATH%asm-tree-
9.7.1.jar.sig;%JAR_PATH%asm-util-9.7.1.jar.sig;%JAR_PATH%glassfish-corba-csiv2-idl-
5.0.0.jar.sig;%JAR_PATH%glassfish-corba-internal-api-5.0.0.jar.sig;%JAR_PATH%glassfish-corba-
omgapi-5.0.0.jar.sig;%JAR_PATH%glassfish-corba-orb-5.0.0.jar.sig;%JAR_PATH%gmbal-api-only-
4.0.3.jar.sig;%JAR_PATH%osgi.core-8.0.0.jar.sig;%JAR_PATH%pfl-basic-5.1.0.jar.sig;%JAR_PATH%pfl-
dynamic-5.1.0.jar.sig;%JAR_PATH%pfl-tf-5.1.0.jar.sig;%JAR_PATH%management-api-
3.2.3.jar.sig;%JAR_PATH%ohj.jar.sig;%JAR_PATH%help-
share.jar.sig;%JAR_PATH%oracle_ice.jar.sig;%JAR_PATH%jewt.jar.sig;%JAR_PATH%share.jar.sig


IF "%NCC_SERVICE_DBHOST%"=="localhost" (
    SET "DATABASE_HOST_PROPERTY=-Djnlp.sms.databaseHost=NCC_DBHOST:LPORT:OUI_ORACLE_SID"
) ELSE (
    SET "DATABASE_HOST_PROPERTY=-Djnlp.sms.databaseHost=NCC_DBHOST:LPORT/NCC_SERVICE_DBHOST"
)


REM Starting GUI....
java ^
     -Djava.util.Arrays.useLegacyMergeSort=true ^
     -Djnlp.sms.TZ=GMT ^
     -Djnlp.sms.host=OUI_HOSTNAME ^
     -Djnlp.sms.OhcHelp=true ^
     -Djnlp.sms.OhcNccHelpLinks=OHCFLAG ^
     -Djnlp.sms.logo=SMS/images/oracle.gif ^
     -Djnlp.sms.databaseID=LPORT:OUI_ORACLE_SID ^
      %DATABASE_HOST_PROPERTY% ^
     -Djnlp.sms.EncryptedSSLConnection=false ^
     -Djnlp.sms.sslCipherSuites="(TLS_RSA_WITH_AES_128_CBC_SHA)" ^
     -Djnlp.sms.secureConnectionDatabaseHost="(DESCRIPTION= (ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCPS)(HOST=NCC_DBHOST)(PORT=SECPORT))) (CONNECT_DATA=
(SERVICE_NAME=OUI_ORACLE_SID)))" ^
     -Djnlp.sms.piUsersPasswordPolicyMessage="The new password must be at least 9 characters
long and have at least 2 uppercase characters, 2 lowercase characters, 2 digits and 2 special
characters, and must be 4 characters or more different from the previous password if there was
one." ^
     -Djnlp.sms.showEFM=1 ^
     -Djnlp.sms.OverWriteSwingFont=false ^
     -Djnlp.sms.OverWriteSwingFontValue="MV Boli" ^
     -Djnlp.acs.SuppressTagID=TRUE ^
     -Djnlp.acs.maximiseAcsScreens=false ^
     -Djnlp.ECEExtensions=true ^
     -Djnlp.acs.Profile8="Account Reference Profile" ^
     -Djnlp.acs.Profile9="Product Type Profile" ^
     -Djnlp.acs.Profile10="Control Plan Profile (App 3)" ^
     -Djnlp.acs.Profile12="CCS Global Profile" ^
     -Djnlp.acs.Profile13="CCS Temporary Profile (App 6)" ^
     -Djnlp.acs.Profile14="CCS Temporary Profile (App 7)" ^
     -Djnlp.acs.Profile15="CCS Temporary Profile (App 8)" ^
     -Djnlp.acs.ssfs="vssp,sca" ^
     -Djnlp.acs.scfs=scf ^
     -Djnlp.vpn.INProtocol=IN_PROTOCOL ^
     -Djnlp.osd.WSDLDirectory="/IN/html/wsdls" ^
     -Djnlp.osd.WSDLURL="http://SHORTHOSTNAME/wsdls" ^
     -Djnlp.ccs.UseAnnouncements=YES ^
     -Djnlp.ccs.BeORBTimeoutms=5000 ^
     -Djnlp.ccs.VRRedeemMinVoucherLength=9 ^
     -Djnlp.ccs.VRRedeemMaxVoucherLength=15 ^
     -Djnlp.ccs.defaultEDRSearchAge=2 ^
     -Djnlp.ccs.allowTTC=true ^
     -Djnlp.ORB_HOST=SHORTHOSTNAME ^
     -Djnlp.sms.ldapDbUser="LdapDbUserName" ^
     -Djnlp.sms.ldapProviderURL="ldaps://LdapHostAddress" ^
     -Djnlp.sms.ldapAuthType=simple ^
     -Djnlp.sms.ldapSecurityPrincipal="uid=#username#,ou=OU,dc=Domain,dc=com" ^
     -Djnlp.sms.ldapSecurityProtocol=ssl ^
     -Djnlp.sms.ldapTemplateAttribute=LdapTemplateAttributeName ^
     -cp "%CLASSPATH%" ^
UserScreens.Application

REM End delayed expansion
endlocal
```

smsGui.sh

```
#!/bin/bash

################################################################################
#
# Copyright (c) 2025  Oracle. All rights reserved.
#
# This material is the confidential property of Oracle Corporation or its
# licensors and may be used, reproduced, stored or transmitted only in
# accordance with a valid Oracle license or sublicense agreement.
#
#
# smsGui.sh : runs the SMS application
# Run: bash smsGui.sh
#
################################################################################

JAR_PATH=$(pwd)

JAXB_VERSION=4.0.5
GMBAL_VERSION=4.0.3
PFL_VERSION=5.1.0
ISTACK_VERSION=4.1.2
GLASSFISH_VERSION=5.0.0
ASM_VERSION=9.7.1
ASM_COMMON_VERSION=7.3.1
JAKARTA_XML_BIND=4.0.4
OSGI_VERSION=8.0.0
MANAGEMENT_API_VERSION=3.2.3

CLASSPATH=$JAR_PATH/:\
$JAR_PATH/sms.jar.sig:\
$JAR_PATH/common.jar.sig:\
$JAR_PATH/ojdbc11.jar.sig:\
$JAR_PATH/oraclepki.jar.sig:\
$JAR_PATH/acs.jar.sig:\
$JAR_PATH/osd.jar.sig:\
$JAR_PATH/PIsecurity.jar.sig:\
$JAR_PATH/pi.jar.sig:\
$JAR_PATH/dap.jar.sig:\
$JAR_PATH/http_client.jar.sig:\
$JAR_PATH/orawsdl.jar.sig:\
$JAR_PATH/ccs.jar.sig:\
$JAR_PATH/UIS_GW.jar.sig:\
$JAR_PATH/UPC.jar.sig:\
$JAR_PATH/upcMacros.jar.sig:\
$JAR_PATH/rims.jar.sig:\
$JAR_PATH/xms.jar.sig:\
$JAR_PATH/smcb.jar.sig:\
$JAR_PATH/np.jar.sig:\
$JAR_PATH/lcp.jar.sig:\
$JAR_PATH/enum.jar.sig:\
$JAR_PATH/ses.jar.sig:\
$JAR_PATH/vpn.jar.sig:\
$JAR_PATH/rca.jar.sig:\
$JAR_PATH/ohj.jar.sig:\
$JAR_PATH/help-share.jar.sig:\
$JAR_PATH/oracle_ice.jar.sig:\
$JAR_PATH/jewt.jar.sig:\
$JAR_PATH/share.jar.sig:\
$JAR_PATH/jaxb-runtime-$JAXB_VERSION.jar.sig:\
$JAR_PATH/jaxb-core-$JAXB_VERSION.jar.sig:\
$JAR_PATH/istack-commons-runtime-$ISTACK_VERSION.jar.sig:\
$JAR_PATH/jakarta.xml.bind-api-$JAKARTA_XML_BIND.jar.sig:\
$JAR_PATH/asm-$ASM_VERSION.jar.sig:\
$JAR_PATH/asm-analysis-$ASM_VERSION.jar.sig:\
$JAR_PATH/asm-tree-$ASM_VERSION.jar.sig:\
$JAR_PATH/asm-util-$ASM_VERSION.jar.sig:\
$JAR_PATH/glassfish-corba-csiv2-idl-$GLASSFISH_VERSION.jar.sig:\
$JAR_PATH/glassfish-corba-internal-api-$GLASSFISH_VERSION.jar.sig:\
$JAR_PATH/glassfish-corba-omgapi-$GLASSFISH_VERSION.jar.sig:\
$JAR_PATH/glassfish-corba-orb-$GLASSFISH_VERSION.jar.sig:\
$JAR_PATH/gmbal-api-only-$GMBAL_VERSION.jar.sig:\
$JAR_PATH/osgi.core-$OSGI_VERSION.jar.sig:\
$JAR_PATH/pfl-basic-$PFL_VERSION.jar.sig:\
$JAR_PATH/pfl-dynamic-$PFL_VERSION.jar.sig:\
$JAR_PATH/pfl-tf-$PFL_VERSION.jar.sig:\
$JAR_PATH/management-api-$MANAGEMENT_API_VERSION.jar.sig:

if [ "NCC_SERVICE_DBHOST" = "localhost" ]; then
    DATABASE_HOST_PROPERTY="-Djnlp.sms.databaseHost=NCC_DBHOST:LPORT:OUI_ORACLE_SID"
else
    DATABASE_HOST_PROPERTY="-Djnlp.sms.databaseHost=NCC_DBHOST:LPORT/NCC_SERVICE_DBHOST"
fi

echo "Starting GUI...."
exec ${JAVA_HOME}/bin/java \
     -Djava.util.Arrays.useLegacyMergeSort=true \
     -Djnlp.sms.TZ=GMT \
     -Djnlp.sms.host=OUI_HOSTNAME \
     -Djnlp.sms.OhcHelp=true \
     -Djnlp.sms.OhcNccHelpLinks=OHCFLAG \
     -Djnlp.sms.logo=SMS/images/oracle.gif \
     -Djnlp.sms.databaseID=LPORT:OUI_ORACLE_SID \
      $DATABASE_HOST_PROPERTY \
     -Djnlp.sms.EncryptedSSLConnection=false \
     -Djnlp.sms.sslCipherSuites="(TLS_RSA_WITH_AES_128_CBC_SHA)" \
     -Djnlp.sms.secureConnectionDatabaseHost="(DESCRIPTION= (ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCPS)(HOST=NCC_DBHOST)(PORT=SECPORT))) (CONNECT_DATA=
(SERVICE_NAME=OUI_ORACLE_SID)))" \
     -Djnlp.sms.piUsersPasswordPolicyMessage="The new password must be at least 9 characters
long and have at least 2 uppercase characters, 2 lowercase characters, 2 digits and 2 special
characters, and must be 4 characters or more different from the previous password if there was
one." \
     -Djnlp.sms.showEFM=1 \
     -Djnlp.sms.OverWriteSwingFont=false \
     -Djnlp.sms.OverWriteSwingFontValue="MV Boli" \
     -Djnlp.acs.SuppressTagID=TRUE \
     -Djnlp.acs.maximiseAcsScreens=false \
     -Djnlp.ECEExtensions=true \
     -Djnlp.acs.Profile8="Account Reference Profile" \
     -Djnlp.acs.Profile9="Product Type Profile" \
     -Djnlp.acs.Profile10="Control Plan Profile (App 3)" \
     -Djnlp.acs.Profile12="CCS Global Profile" \
     -Djnlp.acs.Profile13="CCS Temporary Profile (App 6)" \
     -Djnlp.acs.Profile14="CCS Temporary Profile (App 7)" \
     -Djnlp.acs.Profile15="CCS Temporary Profile (App 8)" \
     -Djnlp.acs.ssfs="vssp,sca" \
     -Djnlp.acs.scfs=scf \
     -Djnlp.vpn.INProtocol=IN_PROTOCOL \
     -Djnlp.osd.WSDLDirectory="/IN/html/wsdls" \
     -Djnlp.osd.WSDLURL="http://SHORTHOSTNAME/wsdls" \
     -Djnlp.ccs.UseAnnouncements=YES \
     -Djnlp.ccs.BeORBTimeoutms=5000 \
     -Djnlp.ccs.VRRedeemMinVoucherLength=9 \
     -Djnlp.ccs.VRRedeemMaxVoucherLength=15 \
     -Djnlp.ccs.defaultEDRSearchAge=2 \
     -Djnlp.ccs.allowTTC=true \
     -Djnlp.ORB_HOST=SHORTHOSTNAME \
     -Djnlp.sms.ldapDbUser="LdapDbUserName" \
     -Djnlp.sms.ldapProviderURL="ldaps://LdapHostAddress" \
     -Djnlp.sms.ldapAuthType=simple \
     -Djnlp.sms.ldapSecurityPrincipal="uid=#username#,ou=OU,dc=Domain,dc=com" \
     -Djnlp.sms.ldapSecurityProtocol=ssl \
     -Djnlp.sms.ldapTemplateAttribute=LdapTemplateAttributeName \
     -cp "$CLASSPATH" \
UserScreens.Application
```