Oracle® Communications Network Charging and Control

Installation Guide

Release 15.2

January 2026

Copyright

Copyright © 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Appendix B

Maintaining a Remote Database 157

About This Document

Audience

This guide is for system administrators who install or uninstall Oracle Communications Network Charging and Control (NCC).

Prerequisites

Before installing or uninstalling NCC, you should have an understanding of UNIX and a familiarity with IN concepts as well as an understanding of Oracle databases, SQL, and PL/SQL.

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

Related Documents

See the following documents for related information about NCC:

- *Concepts*
- *System Administrator's Guide*
- *Configuration User's Guide*
- *Security 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

NCC Installation Overview

Overview

Introduction

This chapter describes the Oracle Communications Network Charging and Control (NCC) installed components and provides an overview of the NCC installation procedure.

In this chapter

This chapter contains the following topics.

NCC Installed Components Overview

About NCC Installed Components

During the NCC installation process, you install and configure the following components:

- Oracle Database
- NCC software packages

NCC Software

The following table describes the NCC software sub-components installed.

Component	Provides
SMS	Service Management System (SMS) support for all other components. For example: • Data replication. • Statistics and alarm collection. • Security (users and permissions). • Report generation.
SLEE	The Service Logic Execution Environment (SLEE) for the Voucher and Wallet Server (VWS) and Service Logic Controller (SLC) nodes.
ACS	Base call handling and processing capabilities, and the Control Plan Editor.
CCS	Rating, charging, subscriber and voucher capabilities.
SMCB	SMS rating and charging capabilities.
BE	Real-time charging, voucher redemption, and session control capabilities.
DSY	Diameter Sy Interface
MM	All messaging capabilities.

Component	Provides
MM Navigator	Routing information lookup capabilities for messaging services.
RAP	CAMEL roaming capabilities.
UIS and UPC	USSD capabilities.
DAP	Outbound XML capabilities.
OSD	Inbound XML capabilities.
LCP	Location based capabilities.
SCA	SIP capabilities.
VSSP	ISUP capabilities.
SIGTRAN	M3UA and SUA capabilities.
PI	Provisioning capabilities.
CAP3_GW	CAP3 capabilities.
DCA	Inbound Diameter capabilities.
DCD	Outbound Diameter capabilities.
ECA	Inbound EDR/CDR processing capabilities.
ENUM	ENUM capabilities.
IS41	Inbound IS41 (CDMA) capabilities.
LCA	Inbound LDAP capabilities.
MFW	MAP Firewall capabilities.
MOB_ROAM	Additional roaming capabilities.
NGW	Notification Gateway capabilities.
NP_SERVICE_PACK	Number portability capabilities.
RCA	RADIUS capabilities.
SES	Subscriber event capabilities.
SEI	SMS to email capabilities.
SMINAP	CAPv1 capabilities.
TFR	TCAP relay capabilities.
VPN	Virtual private networking capabilities.

Certification

This release has been certified on:

- Oracle Database 19.25, Oracle Database and Client 26ai for Engineered Systems
- Oracle OCI VM with OEL 8.10 (Build time) and Oracle OCI VM with OEL 9.6 (Runtime)
- OpenSSL 1.1.1

Note: Solaris is not supported from 15.1 release.

NCC Installation Procedure Overview

Overview of the Installation Procedure

You install NCC on each Service Management System (SMS), Voucher and Wallet Server (VWS), and Service Logic Controller (SLC) node. The installation procedure follows these steps:

Step	Action
1	Plan your installation. When planning your installation, you will need to: • Determine the scale of your implementation, for example, whether it is a small test system or a large production system. • Determine how many physical machines you need. • Plan the system topology, for example, which SMS, VWS, or SLC nodes will run on which machines.
2	Review the following system requirements: • Hardware requirements, such as disk space and memory size • Software requirements, such as operating system version, file system layout, and file sizes • Information requirements, such as IP addresses and host names
3	Perform pre-installation tasks: • Perform system preparation tasks such as disabling services and configuring the location of log files. • Install and configure the Oracle database on local or remote server. • Install and configure additional third-party software.
4	Install the NCC product software on all nodes and optionally install service templates. **Note:** If the database is on a remote server, ensure the required table spaces are added. See *Advanced Storage and Memory Sizing* (on page 23) for more details.
5	Perform mandatory post-installation configuration tasks.
6	Verify the installation.

Installation Options

You install NCC by using the NCC Oracle Universal Installer (the installer). Using the installer, you can perform either a GUI installation or a silent installation using response files, similar to Oracle database installation.

Service Templates

About Service Templates

You can install the following service templates when you install NCC using the NCC Installation Manager:

- Prepaid Charging Service Template (PCST)

Installing a service template automatically performs initial configuration and setup for the service. You will need to perform additional post installation configuration tasks to complete the service setup.

Prepaid Charging Service Template

The Prepaid Charging Service Template (PCST) includes example control plans and tariffing configuration. It provides a list of prepaid services that can be used to differentiate the operator from competitors in the market.

For more information on prepaid services and their configuration, see *Configuration User's Guide*.

Supporting Multi-Byte UTF-8 Character Sets

NCC uses the AL32UTF8 database character set that supports multi-byte UTF-8 and traditional character sets. The NCC Installation Manager automatically sets the character set to AL32UTF8 when you install NCC.

Ensuring a Successful Installation

Introduction

The NCC installation should be performed only by qualified personnel. You must be familiar with the Linux operating systems and Oracle Database software. You should be experienced with installing Linux packages. It is recommended that the installation and configuration of the Oracle database be performed by an experienced database administrator.

Installation Guidelines

Follow these guidelines:

- As you install each component (for example, Oracle Database), verify that the component is installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing the software, make sure your system has the required base software. In addition, make sure that you know all of the required configuration values, such as host names and port numbers.
- As you create new configuration values, write them down. In some cases, you might need to re-enter configuration values later in the procedure.

Chapter 2

Planning Your NCC Installation

Overview

Introduction

This chapter explains how to plan an Oracle Communications Network Charging and Control (NCC) installation.

In this chapter

This chapter contains the following topics.

About Planning Your NCC Installation

Planning Your NCC Installation

When planning your NCC installation, you will need to decide:

- How many Service Management System (SMS), Voucher and Wallet Server (VWS), and Service Logic Controller (SLC) nodes to install
- Which node to install on which server
- If external storage is used, how to connect each server to the external storage
- If databases will be co-located at nodes or located remotely
- How to connect NCC servers together in your network
- How to connect NCC servers with the rest of your network
- How to integrate the NCC solution into the telco infrastructure

Before installing NCC, you should create an implementation plan that includes the following elements:

- A logical and physical overview of the solution, listing all nodes used in the solution and how they interact (for example: protocols used, and so on). If the solution is deployed geographically across multiple sites, then this should be reflected here.
- Hardware details for each node, including connected hardware such as external storage
- Rack mounting and cabling details
- Storage and database details
- IP network details
- Telco network integration details

For an overview of the NCC architecture, see the discussion about the NCC system architecture in *NCC Concepts*.

About Cohosting NCC Nodes

Cohosting multiple NCC nodes on a single physical server was certified in combination with virtualization technologies, such as the following:

- Oracle OCI VM with OEL
- Hardware partitioning such as dynamic domains

Each node should have its own operating system, database instance, and storage layout. You could also use an existing database available on a remote server. See *Installing the Oracle Database Software* (on page 51) for details.

Detailed Planning

Storage Planning

Document the storage configuration. For each SMS, VWS, and SLC node, include the following information:

- How the internal disks will be organized
- Whether disks will be managed by a volume manager or a RAID controller or both
- What data will be stored on each disk or disk group
- How the external storage will be organized; for example, what are the Logical Unit Numbers (LUN), RAID groups, and so on
- How the servers will be connected to the storage and how you will make this access redundant
- Details of any specific parameters that will be set in the external storage, volume manager, and file systems.

Database Planning

Document all database parameters for each SMS, VWS, and SLC node, including the following:

- Where the different database elements (such as data files, redo logs, archive logs, and so on) will be stored.
- The values defined for the oracle environment variables (such as ORACLE_SID, ORACLE_BASE, ORACLE_HOME, MULTITENANT_DB (required for 26ai), CDB_NAME (required for 26ai), and so on)
- The System Global Area (SGA) parameters
- Any other specific instance parameters you will use.

Network Planning

To plan the network implementation:

- Document the different internal and external IP networks that will be used and create a schematic overview of these networks. Use this overview to describe which nodes have access to which networks.
- Document the physical configuration of the network. For example, document which Network Interface Card (NIC) ports will be used for which networks.
- Document how redundancy will be achieved; for example, through IP network multipathing (IPMP).
- Document Network Time Protocol (NTP) configuration. Either list existing NTP servers or define which nodes will be configured as NTP servers.
- Create a host register containing details of all IP addresses and netmasks for all nodes and networks.

Integration Planning

Plan for integration with the telco environment by documenting at least the following items:

- How the SLC nodes will be integrated into the telco environment. Create a schematic overview and use this overview to describe the interaction between the SLC nodes and the telco infrastructure (for example: MSC Signaling Gateways, IPs, and so on).
- Which transport and application protocols will be used in which scenarios (for example: M3UA, SUA, INAP, Camel, MAP, and so on).
- How traffic will be routed to and from the SLC nodes. For example, record details of SCCP/SUA routing, including SCCP addressing parameters, global title addresses, subsystems, and so on.
- How traffic will be load-balanced across the SLC nodes.
- Any protocol specific details for each application protocol. For example, for INAP or Camel, record which subsystem numbers and service keys will be used and which type of service will be invoked for each protocol.
- A detailed call-flow for each call scenario, showing the signaling units and signaling unit parameters being received and returned by the SLC nodes.

OSD Configuration Planning

You configure Open Services Development (OSD) to enable SLC nodes to receive HTTP/SOAP requests. The requests trigger control plans on the SLC. When configuring OSD, you should determine:

- How many OSD interfaces will run on each SLC
- The IP address and TCP port that each interface will use to listen for incoming connections

The SMS and VWS nodes also send HTTP/SOAP requests to the SLC nodes in order to submit SMS notifications. This means that at a minimum, you must configure OSD interfaces as targets for the SMS and VWS nodes.

Tip: You should use an:

- Internal LAN (if available) for the HTTP/SOAP traffic sent from the VWS and SMS nodes to the SLC nodes.
- External LAN for the HTTP/SOAP traffic coming from external systems

You should document the OSD configuration in a table and keep this information available for reference during the installation and configuration process.

OSD Configuration Example

The following table lists example OSD configuration for SMS notification requests.

SLC nodes	OSD interface	Sample IP:port values	Source nodes	Scenario
SLC1	osdInterface	10.1.0.10:2222	SMS, VWS1, VWS2	SMS Notification request
SLC2	osdInterface	10.1.0.20:2222	SMS, VWS1, VWS2	SMS Notification request

Replication Planning

You should document all replication elements, node IDs, and IP addresses in a table. This information will be needed when you configure replication following the installation.

Replication Reference Table Example

The **Replication** column in the following table shows the typical values for a fully configured system.

Node		**Replication**		**UpdateRequester ID**			
Name	Type	Node ID	Internal IP Address	Alarms	AVD	Stats	Rep IF
test_SMS	SMS	1	10.0.0.10	-	-	-	-
test_SLC1	SLC	301	10.0.0.11	601	-	701	901
test_SLC2	SLC	302	10.0.0.12	602	-	702	902
test_VWS1	VWS	351	10.0.0.21	651	611	751	951
test_VWS2	VWS	352	10.0.0.22	652	612	752	952

The table headings map to the following configuration fields:

- *Name* is the **Description**
- *Node ID* is the **Node Number** - this must be unique across the system
- *UpdateRequester ID* - this must be unique across the system
- *Internal IP Address* is the **Primary Node IP Address**

See the chapter on replication in *Service Management System Technical Guide* for information on replication and node numbering standards.

Chapter 3

NCC System Requirements

Overview

Introduction

This chapter describes the hardware and software requirements for Oracle Communications Network Charging and Control (NCC).

In this chapter

This chapter contains the following topics.

Network Requirements

Introduction

All NCC nodes require IP network connectivity to communicate with each other, as well as with other network elements such as management clients, provisioning systems, or telephony signaling transfer points. A typical NCC implementation comprises the following logical networks:

- Management
- Billing
- Internal communication
- Signaling

IP Networks

The following table describes the logical IP networks and their NCC implementation.

Network	Type	Purpose
Management	External	Provides external component access to the NCC nodes; for example, to UIs for performing operations, to provisioning systems for creating subscriber accounts and recharging accounts, to a data warehouse for collecting event detail record (EDRs), and so on. It also allows the nodes to transmit data to peripheral systems, such as network management systems (as SNMP traps).
Billing	Internal	Use an internal network for billing communication between the NCC nodes, such as call reservation requests or wallet information requests. The billing network should not be accessible by external systems.

Network	Type	Purpose
Internal communication	Internal	Use for all internal communications between the NCC nodes, including data replication but excluding billing communication. The Internal network should not be accessible by external systems.
Signaling	External	Use two signaling networks for redundant signaling connectivity between the SLC nodes and the telephony network. For integration into: • A GSM or CDMA network, set up a multi-homed SCTP association between Signaling Gateways and the SLC nodes to carry M3UA or SUA (SIGTRAN) traffic. • An NGN network, use the signaling networks to set up two separate TCP/IP connections between the Media Gateway Controller (MGC or softswitch) and each SLC node. The connections between the SLC nodes and the Signaling Gateways or MGCs can be switched (systems on the same IP subnet) or routed (for systems on different IP subnets).

Connecting Networks

When setting up the NCC network connections, you should:

- Connect management, billing, and internal networks to all nodes.
- Connect signaling networks to SLC nodes only.
- Use a single physical network for each logical network to ensure optimal performance and stability in production implementations. However, logical networks can share a single or multiple physical networks, if required.
- Ensure full redundancy for each network by using two or more network ports connected to an independent ethernet network.
- Use IP network multipathing (IPMP) to implement IP address and network interface failover capabilities on the NCC nodes.

Logical Network Settings

The following table lists the settings you should use for bandwidth, latency, security, redundancy, and external routing for each type of logical network.

Logical Network	Bandwidth	Latency	Security	Redundancy	External Routing
Management	High	Medium	Yes	Yes	Yes
Billing	High	Low	No	Yes	No
Internal	High	Medium	No	Yes	No
Signaling	High	Low	No	Yes	Yes

Note: If you do not require routing for connectivity to peer signaling nodes, then you will not need external routing for the signaling network.

Logical Network Settings Table

This table explains the bandwidth, latency, security, redundancy, and external routing settings listed in *Logical Network Settings* (on page 10).

Setting	Description
Bandwidth	An indicator of the required bandwidth for this connection. Typical model IP connections have low bandwidth requirements, allowing them to be satisfied with shared infrastructure. Medium bandwidth requirements may require some quality of service. High bandwidth requirements may require a dedicated link, for example, over an E1/T1 bearer.
Latency	Latency requirements are relevant to performance and volume testing. The level of latency reflects how time critical the response is.
Security	The level of security required depends on whether or not the information being passed is sensitive or is financial information such as vouchers. You may need a dedicated connection for high levels of security.
Redundancy	Redundancy enables failover protection if a connection is lost.
External Routing	External routing is needed if the subnet will require routing beyond the NCC solution.

Memory Requirements

About Memory Requirements

You will require at least eight gigabytes of RAM per node to completely install NCC. You may require additional memory depending on the size and complexity of the deployment.

The exact amount of memory required on each SMS, VWS, and SLC node depends on memory requirements of:

- The operating system
- The NCC application processes running on the node
- The Oracle Database instance processes and System Global Area (SGA) settings

Note: For information about advanced memory sizing, see *Advanced Storage and Memory Sizing* (on page 23).

Database Memory

For more information on memory requirements for the NCC applications, including example settings for small, medium, and large production systems, see *Advanced Storage and Memory Sizing* (on page 23).

The following table lists the minimum NCC Oracle database SGA settings for each NCC node in your environment. You should review all settings for your specific deployment.

SGA Element	Recommended minimum setting (MB)		
	SMS	VWS	SLC
log_buffer	16	10	16
java_pool_size	160	0	160
shared_pool_size	512	512	512
pga_aggregate_target	256	64	256

SGA Element	Recommended minimum setting (MB)		
large_pool_size	160	32	160
db_cache_size	48	128	48
db_keep_cache_size	32	32	32
db_recycle_cache_size	32	32	32
db_32k_cache_size	128	0	128

Storage Requirements

Introduction

Each node in a NCC installation will consist of a number of logical sets of data. On some nodes, additional sets of data may be required, such as Oracle Archive logs, or data files may be divided to help optimize performance. For example, redo logs and data files could be separated in the Oracle Database Instance set.

You should follow these recommendations if possible:

- Dedicate the boot disk to OS and do not use it to store any other logical data groups.
- Maintain a mirror of the boot disk for redundancy.

General Storage Requirements

Each NCC node will consist of at least the minimum logical sets of data listed in the following table.

Data Set	Mount Point
Operating system with **/var** file system and swap space	Boot disk
NCC applications (binaries, libraries, log files, temporary files)	**/IN** (mandatory)
Oracle Database Server (binaries, $ORACLE_BASE, $ORACLE_HOME)	**/u01** (recommended)
Oracle Database instance (for example, data files, log files)	/oracle/datafiles (Recommended for 19c) **/u01/app/oracle/oradata** (Recommended for 26ai)
Oracle redo log files	**/oracle/redologs** (Recommended for 19c) **/u01/app/oracle/oradata** (Recommended for 26ai)

Swap sizing should be based on the following guidelines for each node.

For Oracle Enterprise Database 19*c*:

System RAM Size	Recommended Swap Size
1GB to 2GB	= 1.5x System RAM
>2GB to <16GB	= System RAM
>16GB	= 16GB

SMS Storage Requirements

The following table details the mount points and minimum storage requirements for the SMS node.

Data Set	Mount Point	Minimum Size
NCC applications	**/IN**	20 GB
Oracle Database server 19.25.0 and 26ai Enterprise Edition	**/u01**	20GB for 19c 30GB for 26ai
Oracle Database instance	**/oracle/datafiles**	80 GB

VWS Storage Requirements

The following table details the mount points and minimum storage requirements for the VWS node.

Data Set	Mount Point	Minimum Size
NCC applications	**/IN**	20 GB
Oracle Database server	**/u01**	20GB for 19c 30GB for 26ai
Oracle Database instance	**/oracle/datafiles**	45 GB

SLC Storage Requirements

The following table details the mount points and minimum storage requirements for the SLC node.

Data Set	Mount Point	Minimum Size
NCC applications	**/IN**	20 GB
Oracle Database server	**/u01**	20GB for 19c 30GB for 26ai
Oracle Database instance	**/oracle/datafiles**	25 GB

SMS Tablespace Requirements

The following table lists the minimum tablespace sizing required for an installation on the SMS node.

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
ACS	ACS_DATA	200	2	400
	ACS_INDEX	200	1	200
	ACS_SUBURB_DATA1	200	4	800
	ACS_SUBURB_INDEX 1	200	4	800
CCS	CCS_CDR	2001	1	2001
	CCS_CDR_I	2001	1	2001
	CCS_DATA	2001	1	2001
	CCS_EVENT	2001	1	2001

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
	CCS_EVENT_I	2001	1	2001
	CCS_INDEX	2001	1	2001
	CCS_SUBS	2001	1	2001
	CCS_SUBS_I	2001	1	2001
	CCS_VOUCHERS	2001	1	2001
	CCS_VOUCHERS_I	2001	1	2001
	CCS_XDB	2001	1	2001
ENUM	EN_DATA	200	1	200
	EN_INDEX	200	1	200
	EN_SUBS	200	1	200
	EN_SUBS_I	200	1	200
LCP	LCP_DATA	200	1	200
	LCP_INDEX	200	1	200
MM	MMX_DATA	200	1	200
	MMX_INDEX	200	1	200
NP_SERVICE_PACK	NP_DATA	200	1	200
	NP_INDEX	200	1	200
	NP_SUBS	200	1	200
	NP_SUBS_I	200	2	400
OSD	OSD_DATA	200	1	200
	OSD_INDEX	200	1	200
PI	PI_DATA	200	1	200
	PI_INDEX	200	1	200
RCA	RCA_DATA	200	1	200
	RCA_INDEX	200	1	200
SES	SES_DATA	200	1	200
	SES_INDEX	200	1	200
SMS	REP_DATA	2001	1	2001
	SMF_ALARMS	2001	1	2001
	SMF_ALARMS_I	2001	1	2001
	SMF_AUD	2001	2	4002
	SMF_AUD_I	2001	1	2001
	SMF_DATA	200	2	400
	SMF_INDEX	200	1	200

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
	SMF_STATS	2001	1	2001
	SMF_STATS_I	2001	1	2001
	SYSAUX	2001	1	2001
	SYSTEM	512	1	512
	TOOLS	2001	1	2001
	UNDOTBS2	2001	5	10005
	USERS	2001	1	2001
UIS	UIS_CDR	200	1	200
	UIS_CDR_I	200	1	200
	UIS_DATA	200	1	200
	UIS_INDEX	200	1	200
UPC	UPC_DATA	200	1	200
	UPC_INDEX	200	1	200
VPN	VPN_DATA	200	1	200
	VPN_INDEX	200	1	200

VWS Tablespace Requirements

The following table lists the minimum tablespace sizing required on the VWS node.

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
ACS	ACS_DATA	200	2	400
	ACS_INDEX	200	1	200
BE	BE_DATA	200	1	200
	BE_EVENT	2001	1	2001
	BE_EVENT_I	2001	1	2001
	BE_SUBS	2001	1	2001
	BE_SUBS_I	2001	1	2001
	BE_VOUCHERS	2001	1	2001
	BE_VOUCHERS_I	2001	1	2001
	SYSAUX	500	1	500
	SYSTEM	450	1	450
	TEMP	2001	5	10005
	REDO	101	16	1616

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
	TOOLS	200	1	200
	UNDO	2001	5	10005
	USERS	200	1	200
CCS	CCS_DATA	200	1	200
	CCS_INDEX	200	1	200
	CCS_SUBS	2001	1	2001
	CCS_SUBS_I	2001	1	2001
	CCS_VOUCHERS	2001	1	2001
	CCS_VOUCHERS_I	2001	1	2001
SMS	SMF_DATA	100	1	100
	SMF_INDEX	100	1	100

SLC Tablespace Requirements

The following table lists the minimum tablespace sizing required on the SLC node.

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
ACS	ACS_DATA	200	2	400
	ACS_INDEX	200	1	200
	ACS_SUBURB_DATA1	200	4	800
	ACS_SUBURB_INDEX 1	200	4	800
CCS	CCS_SCP_DATA	200	1	200
	CCS_SCP_INDEX	200	1	200
	CCS_SUBS	2001	1	2001
	CCS_SUBS_I	2001	1	2001
ENUM	EN_DATA	200	1	200
	EN_INDEX	200	1	200
	EN_SUBS	200	1	200
	EN_SUBS_I	200	1	200
LCP	LCP_DATA	200	1	200
	LCP_INDEX	200	1	200
MM	MMX_DATA	200	1	200
	MMX_INDEX	200	1	200
NP_SERVICE_PACK	NP_DATA	200	1	200
	NP_INDEX	200	1	200

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size
	NP_SUBS	200	1	200
	NP_SUBS_I	200	1	20
OSD	OSD_DATA	200	1	200
	OSD_INDEX	200	1	200
RCA	RCA_DATA	200	1	200
	RCA_INDEX	200	1	200
SES	SES_DATA	200	1	200
	SES_INDEX	200	1	200
SMS	SMF_DATA	100	1	100
	SMF_INDEX	100	1	100
	SYSAUX	2001	1	2001
	SYSTEM	2001	1	2001
	TOOLS	2001	1	2001
	UNDOTBS1	2001	2	4002
	USERS	2001	1	2001
UIP	UIS_CDR	200	1	200
	UIS_CDR_INDEX	200	1	200
	UIS_DATA	200	1	200
	UIS_INDEX	200	1	200
UPC	UPC_DATA	200	1	200
	UPC_INDEX	200	1	200
VPN	VPN_DATA	200	1	200
	VPN_INDEX	200	1	200

Software and Hardware Requirements

Introduction

This section details the hardware platforms and prerequisite software required to install NCC.

For details on installing the required system software, see the installation and setup documentation supplied with the software.

Hardware Platforms

The following table lists the minimum recommended and mandatory hardware platforms for the NCC applications.

Hardware	Mandatory / Recommended	Required for
Linux x86	Mandatory	All nodes
Storage Array (RAID)	Recommended	SMS only
A PC with a screen resolution of 1024x768 pixels	Recommended	Installer and Clients

Prerequisite Software

For the list of additional Oracle and third-party software that you should install prior to installing NCC, see *Network Charging and Control Compatibility Matrix*.

Preparing the System

Introduction

Check the kernel parameters on the system to ensure the system is optimally configured.

Kernel Parameters

For Oracle 19*c* database the minimum values are the same except for project.max-shm-memory, which depends on the amount of physical RAM in the system. If RAM is in the range 1 GB to 16 GB, you should set the minimum value for project.max-shm-memory to half the size of the physical memory. If RAM is greater than 16 GB, you should set project.max-shm-memory to a value of at least 8 GB.

For Linux:

1. Determine the sum of process parameters for all database instances on the system, the overhead for Oracle background processes, the system and other application requirements.
2. Set semmns (total semaphores system-wide) to the larger of the value in 1 or 32000.
3. Set semmsl (semaphores per set) to 250.
4. Set semmni (total semaphore sets) to semmns/semmsl rounded up to the nearest multiple of 1024.
5. For Linux and Oracle 19*c*, set the maximum number of asynchronous I/O requests allowed in /etc/sysctl.conf as follows:

```
fs.aio-max-nr = 3145728
```

After changing the /etc/sysctl.conf, run the following command as root to set the values in the system:

```
# /sbin/sysctl -p /etc/sysctl.conf
```

Modifying Resource Control Values

For Linux, set the values by editing /etc/sysctl.conf and then using the following /sbin/sysctl command:

```
# /sbin/syctl -p /etc/sysctl.conf
```

Setting the Semaphore Parameters for Linux

To set the semaphore parameters:

Step	Action
1	Log in as the root user.
2	Open the **/etc/sysctl.conf** file in a text editor.
3	Set values to the appropriate semaphore requirements. For example: **kernel.sem = 2048 65536 128 2048** **fs.file-max = 6815744** **kernel.sem = 2048 65536 128 2048** **kernel.shmmni = 4096** **kernel.shmall = 1073741824** **kernel.shmmax = 4398046511104** **kernel.panic_on_oops = 1** **net.ipv4.conf.all.rp_filter is 2** **net.ipv4.conf.all.rp_filter = 2** **net.ipv4.conf.default.rp_filter is 2** **net.ipv4.conf.default.rp_filter = 2** **fs.aio-max-nr = 1048576** **net.ipv4.ip_local_port_range = 9000 65500** **kernel.core_pattern = /var/crash/core-%h-%p-%e** **net.ipv4.tcp_rmem = 16777216 16777216 16777216** **net.ipv4.tcp_wmem = 16777216 16777216 16777216** **net.ipv4.tcp_mem = 16777216 16777216 16777216** **net.core.optmem_max = 16777216** **net.core.rmem_max = 2096304** **net.core.wmem_max = 16777216** **net.core.rmem_default = 16777216** **net.core.wmem_default = 16777216**
4	Save and close the file.
5	Activate the new semaphore settings by entering the following command: **/sbin/sysctl -p**

Tuning the System's ZFS Performance

Set the following parameters in your **/etc/system** file.

To tune the NCC system's performance:

Note: The following settings are recommended for a machine with 16 GB of memory.

Step	Action
1	Disable ZFS from forcing a flush of the disk array write cache: `set zfs:zfs_nocacheflush=1`
2	Set the ZFS file system's maximum cache size. For example, to set the maximum cache size to 5 GB: `set zfs:zfs_arc_max=0x140000000`
3	Set the ZFS file system's minimum cache size. For example, to set the minimum cache size to 5 GB: `set zfs:zfs_arc_min=0x140000000`

4	If your file system cache is small, disable prefetching:
	`set zfs:zfs_prefetch_disable=1`
	`set zfs:zfs_immediate_write_sz=8000`

Setting the Time Zone

Introduction

The same time zone must be used for all machines on which the NCC applications are installed. GMT is the recommended time zone for all machines; however, the local time zone may be configured for hosts on which the NCC GUI client runs.

Setting Time Zones to GMT

The NCC applications use the default time zone unless it is overridden in the user's profile.

Locale and time zone are configured through SMF service properties.

Note: Ensure all accounts default to the GMT time zone. If you set or change the default time zone, set it on each node, and then restart each node.

To set the time zone to GMT in Linux:

Step	Action
1	Log in as the root user.
2	Run the following command: **`timedatectl set-timezone GMT`**
3	If the application is configured to read RTC time in local timezone, run the following command to set RTC in UTC: **`timedatectl set-local-rtc 0`**
4	Edit **`/etc/profile`** and alter the TZ line to: **`export TZ=GMT`**

5	Run the following command to check the time zone:
	`-bash-4.2$ timedatectl`
	The result would appear as:
	`Warning: ignoring the TZ variable, reading the system's timezone setting only.`
	
	`Local time: Thu 2017-03-16 04:10:02 GMT`
	`Universal time: Thu 2017-03-16 04:10:02 UTC`
	`Timezone: GMT (GMT, +0000)`
	`NTP enabled: no`
	`NTP synchronized: yes`
	`RTC in local TZ: no`
	`DST active: n/a`

You should synchronize the date and time for all nodes through Network Time Protocol (NTP). If no NTP server is available, then you should use the SMS nodes as NTP servers.

Important: It is critical that the date and time are synchronized across all NCC nodes.

Checking the Time Zone

Follow these steps to verify that a UNIX system has time zones configured correctly for GUI operations and time zone dependent discounts.

Step	Action
1	Log on to the machine for which you want to check the time zone.

2 Run the following command:

```
env | grep TZ
```

Result:

```
TZ = GMT
```

This indicates that the time zone directory is set to GMT.

Follow these steps to verify time zone on Linux machine.

Step	Action
1	Log in as a root user to the machine for which you want to check the time zone.
2	Run the following command to check the time zone: **-bash-4.2$ timedatectl** **Result:** Warning: ignoring the TZ variable, reading the system's timezone setting only. Local time: Thu 2017-03-16 04:10:02 GMT Universal time: Thu 2017-03-16 04:10:02 UTC Timezone: GMT (GMT, +0000) NTP enabled: no NTP synchronized: yes RTC in local TZ: no DST active: n/a This indicates that the time zone is set to GMT.

Chapter 4

Advanced Storage and Memory Sizing

Overview

Introduction

Precise storage and memory requirements depend on too many factors to be predicted accurately. This chapter provides estimate requirements for a number of example deployment scenarios of Oracle Communications Network Charging and Control (NCC).

In this chapter

This chapter contains the following topics.

Types of Implementations

Introduction

This section provides estimated storage and memory requirements for a number of example deployment scenarios.

Example Size Scenarios

The following table describes the different scenarios for which sizing information is provided.

Scenario	Description
Test system	This is the basic system installed as a minimum using the NCC Installer. It comprises: • One SMS node • One VWS pair (two nodes) • One SLC node This system corresponds to the minimum storage requirements detailed in *Storage Requirements* (on page 12). **Note**: For 26ai remote database setup, additional node is required.

Scenario	Description
Small production system	A production system covering: • Less than 1 million subscribers • Less than 24 million vouchers • Less than 1 million EDRs per day with 4 weeks retention Comprising: • One SMS node • One VWS pair (two nodes) • Two SLC nodes For details, see *Small Production System Example* (on page 24). **Note**: For 26ai remote database setup, additional node is required.
Medium production system	A production system covering: • Less than 1 million subscribers • Less than 120 million vouchers • Less than 10 million EDRs per day with 12 weeks retention Comprising: • One SMS node • Two VWS pairs (four nodes) • Four SLC nodes For details, see *Medium Production System Example* (on page 30). **Note**: For 26ai remote database setup, additional node is required.
Large production system	A production system covering: • Less than 10 million subscribers • Less than 240 million vouchers • Less than 20 million EDRs per day with 24 weeks retention Comprising: • One SMS node • Four VWS pairs (eight nodes) • Eight SLC nodes For details, see *Large Production System Example* (on page 34). **Note**: For 26ai remote database setup, additional node is required.

Small Production System Example

Introduction

This section provides examples of the estimated minimum storage and memory sizing requirements for deploying the NCC applications in a small production environment.

Disk Storage on the SMS

The following table describes the estimated minimum disk storage required on the SMS to deploy the NCC applications in a small production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17411	2%	17759	109
	NCC application data files	67732	2%	69087	
	CCS BE EDRs stored in the database	24012	2%	24492	
/oracle/redologs	Oracle redo logs	1616	2%	1648	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/oracle/archivelogs	Oracle archive logs	102400	2%	104448	102
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/IN	NA	23896	2%	24376	24
Grand Total	NA	NA		257238	253

Disk Storage on the VWS

The following table describes the estimated minimum disk storage required on the VWS to deploy the NCC applications in a small production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	40
	NCC application data files	22610	2%	23062	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/oracle/archivelogs	Oracle archive logs	20480	2%	20890	21
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/IN	NA	20480	2%	20890	21

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	40
	NCC application data files	22610	2%	23062	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
Grand Total	NA	NA	NA	99657	100

Disk Storage on the SLC

The following table describes the estimated minimum disk storage required on the SLC to deploy the NCC applications in a small production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	26
	NCC application data files	7702	2%	7856	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/IN	NA	20480	2%	20890	21
Grand Total	NA	NA	NA	63561	65

Oracle Datafiles on the SMS

Oracle redo logs should be sufficiently sized to ensure that, under production load, a log switch occurs every 15 to 20 minutes. If redo logs are sized too small, then they fill up more quickly necessitating a redo log switch, which is a relatively expensive operation. The redo log switch interval can be determined by looking at the timestamps of the log switch messages that appear in the Oracle alert log. After installation, redo log sizes can be changed if desired by following the instructions in the Oracle Database documentation.

The following table provides details of the Oracle data files on the SMS for which sizing should be reviewed for a small production system.

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
SYSAUX	SYSAUX	SMF	500	1	500
SYSTEM	SYSTEM	SMF	2001	1	2001
TEMP	TEMP	SMF	2001	5	10005
TOOLS	TOOLS	SMF	2001	1	2001

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
UNDOTBS1	UNDOTBS1	SMF	2001	5	10005
SMS	USERS	SMF	2001	1	2001
ACS	CONTROL FILES	SMF	300	3	900
SMS	REDO LOGS	SMF	100	16	1600
ACS	ACS_DATA	SMF	200	1	200
	ACS_INDEX	SMF	200	1	200
CCS	CCS_DATA	SMF	2001	1	2001
	CCS_EVENT	SMF	2001	1	2001
	CCS_EVENT_I	SMF	2001	1	2001
	CCS_INDEX	SMF	2001	1	2001
	CCS_SUBS	SMF	2001	2	4002
	CCS_SUBS_I	SMF	2001	1	2001
	CCS_VOUCHERS	SMF	2001	2	4002
	CCS_VOUCHERS_I	SMF	2001	2	4002
	CCS_XDB	SMF	2001	1	2001
LCP	LCP_DATA	SMF	200	1	200
	LCP_INDEX	SMF	200	1	200
MM	MMX_DATA	SMF	300	1	300
	MMX_INDEX	SMF	300	1	300
OSD	OSD_DATA	SMF	300	1	300
	OSD_INDEX	SMF	200	1	200
PI	PI_DATA	SMF	200	1	200
	PI_INDEX	SMF	200	1	200
SMS	REP_DATA	SMF	2001	1	2001
	SMF_ALARMS	SMF	2001	3	6003
	SMF_ALARMS_I	SMF	2001	2	4002
	SMF_AUD	SMF	2001	7	14007
	SMF_AUD_I	SMF	2001	1	2001
	SMF_DATA	SMF	2001	1	2001
	SMF_INDEX	SMF	200	2	400
	SMF_STATS	SMF	2001	1	2001
	SMF_STATS_I	SMF	2001	2	4002

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
UIP	UIS_CDR	SMF	2001	1	2001
	UIS_CDR_I	SMF	2001	1	2001
	UIS_DATA	SMF	200	1	200
	UIS_INDEX	SMF	200	1	200
UPC	UPC_DATA	SMF	200	1	200
	UPC_INDEX	SMF	200	1	200

Partitioned Files on the SMS

The following table provides the estimated storage (in MB) for the partitioned tablespaces on the SMS in a small production environment.

Partitioned Tablespace Name	File Size	Weekly Storage	Data Files Per Week	Weekly Partitions Allocated	Total Tablespace Size (MB)
CCS_CDR_Yyyyy_Www	2001	3800	2	5	24012

Oracle Datafiles on the VWS

The following table provides details of the Oracle data files on the VWS for which sizing should be reviewed.

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
SYSAUX	SYSAUX	SCP	500	1	500
SYSTEM	SYSTEM	SCP	2001	1	2001
TEMP	TEMP	SCP	2001	5	10005
TOOLS	TOOLS	SCP	2001	1	2001
UNDO	UNDO	SCP	2001	5	10005
SMS	USERS	SCP	2001	1	2001
ACS	CONTROL FILES	SCP	300	3	900
SMS	REDO LOGS	SCP	100	16	1600
ACS	ACS_DATA	SCP	200	1	200
	ACS_INDEX	SCP	200	1	200
BE	BE_DATA	SCP	200	1	200
	BE_SUBS	SCP	2001	2	4002
	BE_SUBS_I	SCP	2001	1	2001
	BE_VOUCHERS	SCP	2001	1	2001
	BE_VOUCHERS_I	SCP	2001	1	2001

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
CCS	CCS_DATA	SCP	200	7	1400
	CCS_INDEX	SCP	200	2	400
	CCS_SUBS	SCP	2001	1	2001
	CCS_SUBS_I	SCP	2001	1	2001
	CCS_VOUCHERS	SCP	2001	2	4002
	CCS_VOUCHERS_I	SCP	2001	1	2001
SMS	SMF_DATA	SCP	100	1	100
	SMF_INDEX	SCP	100	1	100
UIP	UIS_DATA	SCP	200	1	200
	UIS_INDEX	SCP	200	1	200

Oracle Datafiles on the SLC

The following table provides details of the Oracle data files on the SLC for which sizing values should be reviewed.

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
SYSAUX	SYSAUX	E2BE	500	1	500
SYSTEM	SYSTEM	E2BE	2001	1	2001
TEMP	TEMP	E2BE	2001	5	10005
TOOLS	TOOLS	E2BE	2001	1	2001
UNDOTBS1	UNDOTBS1	E2BE	2001	5	10005
SMS	USERS	E2BE	2001	1	2001
ACS	CONTROL FILES	E2BE	300	3	900
SMS	REDO LOGS	E2BE	100	16	1600
ACS	ACS_DATA	E2BE	200	1	200
	ACS_INDEX	E2BE	200	1	200
CCS	CCS_SCP_DATA	E2BE	200	2	400
	CCS_SCP_INDEX	E2BE	200	2	400
	CCS_SCP_SUBS	E2BE	2001	1	2001
	CCS_SCP_SUBS_I	E2BE	2001	1	2001
LCP	LCP_DATA	E2BE	200	1	200
	LCP_INDEX	E2BE	200	1	200
MM	MMX_DATA	E2BE	300	1	300
	MMX_INDEX	E2BE	300	1	300

Component	Tablespace Name	Database Instance	Data File Size (MB)	Number of Files	Total Size (MB)
OSD	OSD_DATA	E2BE	300	1	300
	OSD_INDEX	E2BE	200	1	200
SMS	SMF_DATA	E2BE	100	1	100
	SMF_DATA	E2BE	100	1	100
UIS	UIS_CDR	E2BE	2001	0	0
	UIS_CDR_INDEX	E2BE	2001	0	0
	UIS_DATA	E2BE	200	1	200
	UIS_INDEX	E2BE	200	1	200
UPC	UPC_DATA	E2BE	200	1	200
	UPC_INDEX	E2BE	200	1	200

Note: Consider the disk space specified above for SMS, SLC, and VWS for 26ai remote database as well.

Memory Sizing for a Small Production System

The following table provides the estimated minimum memory requirements (in MB) for the NCC applications deployed on a small production system.

SGA Element	SMS	VWS	SLC
log_buffer	16	16	16
java_pool_size	150	0	0
shared_pool_size	512	128	128
pga_aggregate_target	512	128	128
large_pool_size	256	32	0
db_cache_size	256	128	32
db_keep_cache_size	4096	5012	2048
db_recycle_cache_size	2048	2048	0
db_32k_cache_size	2048	0	0
NCC applications	4096	4096	4096

Medium Production System Example

Introduction

This section provides examples of the minimum storage and memory sizing requirements for deploying the NCC applications in a medium sized production environment.

Disk Storage on the SMS

The following table describes the estimated minimum disk storage required on the SMS to deploy the NCC applications in a medium sized production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	37418	2%	38166	677
	NCC application data files	109753	2%	111948	
	CCS BE EDRs stored in database	532266	2%	542911	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	30015	2%	30615	30
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/oracle/archivelogs	Oracle archive logs	102400	2%	104448	102
/IN	NCC application	20480	2%	20890	55
	Incoming & processed EDR flat files	34180	2%	34863	
Grand Total	NA	NA	NA	890696	872

Disk Storage on the VWS

The following table describes the estimated minimum disk storage required on the VWS to deploy the NCC applications in a medium sized production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	56
	NCC application data files	38218	2%	38982	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/oracle/archivelogs	Oracle archive logs	20480	2%	20890	21
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	56
	NCC application data files	38218	2%	38982	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/IN	NA	20480	2%	20890	21
Grand Total	NA	NA	NA	115577	116

Disk Storage on the SLC

The following table describes the estimated minimum disk storage required on the SLC to deploy the NCC applications in a medium sized production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	31
	NCC application data files	13705	2%	13979	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/IN	NA	20480	2%	20890	21
Grand Total	NA	NA	NA	69684	70

Additional Oracle Datafiles on the SMS

The following table provides details of the additional Oracle data files that will be used on the SMS. These data files are in addition to the minimum created automatically by the installation process for a test system.

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
TEMP	TEMP	2001	15	30015
UNDOTBS	UNDOTBS1	2001	15	30015
	UNDOTBS2	2001	15	30015
CCS	CCS_EVENT	2001	3	6003
	CCS_EVENT_I	2001	1	2001
	CCS_SUBS	2001	6	12006

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
	CCS_SUBS_I	2001	2	4002
	CCS_VOUCHERS	2001	10	20010
	CCS_VOUCHERS_I	2001	8	16008
SMS	SMF_ALARMS	2001	3	6003
	SMF_ALARMS_I	2001	2	4002
	SMF_AUD	2001	7	14007
	SMF_AUD_I	2001	1	2001
	SMF_STATS	2001	1	2001
	SMF_STATS_I	2001	2	4002

Partitioned Files on the SMS

The following table provides the estimated storage (in MB) for the partitioned tablespaces on the SMS in a medium sized production environment.

Partitioned Tablespace Name	File Size	Weekly Storage	Data Files Per Week	Weekly Partitions Allocated	Total Tablespace Size (MB)
CCS_CDR_Yyyyy_Www	2001	37700	19	13	532266

Additional Oracle Datafiles on the VWS

The following table provides details of the additional Oracle data files that will be used on the VWS. These data files are in addition to the minimum created automatically by the installation process for a test system.

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
BE	BE_SUBS	2001	3	6003
	BE_SUBS_I	2001	2	4002
	BE_VOUCHERS	2001	1	2001
	BE_VOUCHERS_I	2001	1	2001
CCS	CCS_DATA	200	5	1000
	CCS_INDEX	200	2	400
	CCS_SUBS	2001	4	8004
	CCS_SUBS_I	2001	1	2001
	CCS_VOUCHERS	2001	4	8004
	CCS_VOUCHERS_I	2001	2	4002

Additional Oracle Datafiles on the SLC

The following table provides details of the additional Oracle data files that will be used on the SLC in a medium production environment. These data files are in addition to the minimum created automatically by the installation process for test system.

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
CCS	CCS_SCP_DATA	200	2	400
	CCS_SCP_INDEX	200	2	400
	CCS_SUBS	2001	4	8004
	CCS_SUBS_I	2001	1	2001

Note: Consider the disk space specified above for SMS, SLC, and VWS for 26ai remote database as well.

Memory Sizing for a Medium Production System

The following table provides the estimated minimum memory requirements (in MB) for the NCC applications deployed in a medium sized production environment.

SGA Element	SMS	VWS	SLC
log_buffer	16	16	16
java_pool_size	150	0	0
shared_pool_size	512	128	128
pga_aggregate_target	512	128	128
large_pool_size	512	32	0
db_cache_size	512	128	32
db_keep_cache_size	8192	12960	6464
db_recycle_cache_size	8192	2048	0
db_32k_cache_size	8192	0	0
NCC applications	8192	8192	8192

Large Production System Example

Introduction

This section provides examples of the minimum storage and memory sizing requirements for deploying the NCC applications in a large production environment.

Disk Storage on the SMS

The following table describes the estimated minimum disk storage required on the SMS to deploy the NCC applications in a large production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
Data files (shared / global)					
ASM +DATA Diskgroup	Core Oracle database	107453	2%	109602	2240
	NCC application data files	163780	2%	167056	
	CCS BE EDRs stored in database	1976988	2%	2016528	
ASM +REDO Diskgroup	Oracle redo logs	1600	2%	1632	2
ASM +TEMP Diskgroup	Oracle TEMP tablespace	50025	2%	51026	50
Other (shared / global)					
ASM +CRS Diskgroup	Oracle OCR	512	2%	522	1
ASM +CRS Diskgroup	Oracle voting	512	2%	522	1
/global/oracle	Oracle shared	10240	2%	10445	11
/global/IN	IN application logs	51200	2%	52224	51
/global/CCS	Processed EDR flat files	68359	2%	69727	69
/global/CDR	Incoming EDR flat files for CDRLoader1	17090	2%	17432	18
Other (private / local)					
/IN	NCC applications	20480	2%	20890	21
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
ASM +ARCH1 Diskgroup	Oracle archive logs	102400	2%	104448	102
ASM +ARCH2 Diskgroup	Oracle archive logs	102400	2%	104448	102
Total					
Shared/Global	NA	NA	NA	2549009	2495
Private/Local	NA	NA	NA	261120	258
Grand Total	NA	NA	NA	2810129	2753

Disk Storage on the VWS

The following table describes the estimated minimum disk storage required on the VWS to deploy the NCC applications in a large production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	59
	NCC application data files	41820	2%	42656	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/oracle/archivelogs	Oracle archive logs	20480	2%	20890	21
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/IN	NA	20480	2%	20890	21
Grand Total	NA	NA	NA	119251	119

Disk Storage on the SLC

The following table describes the estimated minimum disk storage required on the SLC to deploy the NCC applications in a large production environment.

Mount Point	Contents	Required Space (MB)	Block Overhead	Allocated Space (MB)	Total Mount Point Space (GB)
/oracle/datafiles	Core Oracle database	17408	2%	17756	37
	NCC application data files	19708	2%	20102	
/oracle/redologs	Oracle redo logs	1600	2%	1632	2
/oracle/tempfiles	Oracle TEMP tablespace	10005	2%	10205	10
/u01	Oracle software	20000 for 19c 30000+ minimum for 26ai	2%	5222	6
/IN	NA	20480	2%	20890	21
Grand Total	NA	NA	NA	75807	76

Additional Oracle Datafiles on the SMS

The following table provides details of the additional Oracle data files that will be used on the SMS in a large production environment. These data files are in addition to the minimum created automatically by the installation process for a test system.

Component	Tablespace Name	Datafile Size (MB)	Number of Files	Total Size (MB)
TEMP	TEMP	2001	25	50025
UNDOTBS	UNDOTBS1	2001	25	50025
	UNDOTBS2	2001	25	50025
CCS	CCS_EVENT	2001	6	12006
	CCS_EVENT_I	2001	1	2001
	CCS_SUBS	2001	12	24012
	CCS_SUBS_I	2001	3	6003
	CCS_VOUCHERS	2001	19	38019
	CCS_VOUCHERS_I	2001	16	32016
SMS	SMF_ALARMS	2001	3	6003
	SMF_ALARMS_I	2001	2	4002
	SMF_AUD	2001	7	14007
	SMF_AUD_I	2001	1	2001
	SMF_STATS	2001	1	2001
	SMF_STATS_I	2001	2	4002

Partitioned Files on the SMS

The following table provides the estimated storage (in MB) for the partitioned tablespaces on the SMS in a large production environment.

Partitioned Tablespace Name	File Size	Weekly Storage	Data Files Per Week	Weekly Partitions Allocated	Total Tablespace Size (MB)
CCS_CDR_Yyyyy_Www	2001	75350	38	25	1976988

Additional Oracle Datafiles on the VWS

The following table provides details of the additional Oracle data files that will be used on the VWS in a large production environment. These data files are in addition to the minimum created automatically by the installation process for a test system.

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
BE	BE_SUBS	2001	3	6003
	BE_SUBS_I	2001	2	4002

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
	BE_VOUCHERS	2001	1	2001
	BE_VOUCHERS_I	2001	1	2001
CCS	CCS_DATA	200	4	800
	CCS_INDEX	200	1	200
	CCS_SUBS	2001	6	12006
	CCS_SUBS_I	2001	1	2001
	CCS_VOUCHERS	2001	4	8004
	CCS_VOUCHERS_I	2001	2	4002

Additional Oracle Datafiles on the SLC

The following table provides details of the additional Oracle data files that will be used on the SLC in a large production environment. These data files are in addition to the minimum created automatically by the installation process for a test system.

Component	Tablespace Name	Data File Size (MB)	Number of Files	Total Size (MB)
CCS	CCS_SCP_DATA	200	2	400
	CCS_SCP_INDEX	200	2	400
	CCS_SUBS	2001	6	12006
	CCS_SUBS_I	2001	2	4002

Note: Consider the disk space specified above for SMS, SLC, and VWS for 26ai remote database as well.

Memory Sizing for a Large Production System

The following table provides the estimated minimum memory requirements (in MB) for the NCC applications deployed in a large production environment.

SGA Element	SMS	VWS	SLC
log_buffer	16	16	16
java_pool_size	150	0	0
shared_pool_size	512	128	128
pga_aggregate_target	512	128	128
large_pool_size	512	32	0
db_cache_size	512	128	32
db_keep_cache_size	16384	17696	12368
db_recycle_cache_size	8192	2048	0
db_32k_cache_size	16384	0	0
NCC applications	8192	8192	8192

Node-Specific Users

This section provides information on the node-specific users and the privileges they should have.

Users on SMS Database Instance

Ensure the SMS database instance contains a user called SMF with the following privileges:

GRANTEE	PRIVILEGE	ADMIN OPTION
SMF	ALTER ANY INDEX	YES
SMF	ALTER ANY PROCEDURE	YES
SMF	ALTER ANY ROLE	YES
SMF	ALTER ANY SEQUENCE	YES
SMF	ALTER ANY TABLE	YES
SMF	ALTER ANY TRIGGER	YES
SMF	ALTER TABLESPACE	NO
SMF	ALTER USER	NO
SMF	CREATE ANY DIRECTORY	NO
SMF	CREATE ANY PROCEDURE	NO
SMF	CREATE ANY SEQUENCE	NO
SMF	CREATE ANY SYNONYM	NO
SMF	CREATE ANY TABLE	NO
SMF	CREATE ANY TRIGGER	NO
SMF	CREATE ANY VIEW	NO
SMF	CREATE DATABASE LINK	NO
SMF	CREATE MATERIALIZED VIEW	NO
SMF	CREATE PROCEDURE	NO
SMF	CREATE PUBLIC SYNONYM	NO
SMF	CREATE ROLE	NO
SMF	CREATE SEQUENCE	NO
SMF	CREATE SESSION	YES
SMF	CREATE TABLE	NO
SMF	CREATE TABLESPACE	NO
SMF	CREATE TRIGGER	NO
SMF	CREATE TYPE	NO
SMF	CREATE USER	NO
SMF	CREATE VIEW	NO
SMF	DELETE ANY TABLE	YES
SMF	DROP ANY DIRECTORY	NO
SMF	DROP ANY INDEX	NO
SMF	DROP ANY PROCEDURE	NO
SMF	DROP ANY ROLE	NO
SMF	DROP ANY SEQUENCE	NO

GRANTEE	PRIVILEGE	ADMIN OPTION
SMF	DROP ANY TABLE	NO
SMF	DROP ANY VIEW	NO
SMF	DROP PUBLIC DATABASE LINK	NO
SMF	DROP PUBLIC SYNONYM	NO
SMF	DROP TABLESPACE	NO
SMF	DROP USER	NO
SMF	EXECUTE ANY PROCEDURE	NO
SMF	GRANT ANY PRIVILEGE	NO
SMF	GRANT ANY ROLE	NO
SMF	INSERT ANY TABLE	YES
SMF	SELECT ANY TABLE	YES
SMF	UNLIMITED TABLESPACE	NO
SMF	UPDATE ANY TABLE	YES

Users on SLC Database Instance

Ensure the SLC database instance contains a user called SCP with the following privileges:

GRANTEE	PRIVILEGE	ADMIN OPTION
SCP	ALTER ANY INDEX	YES
SCP	ALTER ANY PROCEDURE	YES
SCP	ALTER ANY ROLE	YES
SCP	ALTER ANY SEQUENCE	YES
SCP	ALTER ANY TABLE	YES
SCP	ALTER ANY TRIGGER	YES
SCP	ALTER TABLESPACE	NO
SCP	ALTER USER	NO
SCP	CREATE ANY DIRECTORY	NO
SCP	CREATE ANY PROCEDURE	NO
SCP	CREATE ANY SEQUENCE	NO
SCP	CREATE ANY SYNONYM	NO
SCP	CREATE ANY TABLE	NO
SCP	CREATE ANY TRIGGER	NO
SCP	CREATE ANY VIEW	NO
SCP	CREATE DATABASE LINK	NO
SCP	CREATE MATERIALIZED VIEW	NO
SCP	CREATE PROCEDURE	NO
SCP	CREATE PUBLIC SYNONYM	NO
SCP	CREATE ROLE	NO
SCP	CREATE SEQUENCE	NO
SCP	CREATE SESSION	YES
SCP	CREATE TABLE	NO

GRANTEE	PRIVILEGE	ADMIN OPTION
SCP	CREATE TABLESPACE	NO
SCP	CREATE TRIGGER	NO
SCP	CREATE USER	NO
SCP	CREATE VIEW	NO
SCP	DELETE ANY TABLE	YES
SCP	DROP ANY INDEX	NO
SCP	DROP ANY PROCEDURE	NO
SCP	DROP ANY ROLE	NO
SCP	DROP ANY SEQUENCE	NO
SCP	DROP ANY TABLE	NO
SCP	DROP PUBLIC DATABASE LINK	NO
SCP	DROP PUBLIC SYNONYM	NO
SCP	DROP TABLESPACE	NO
SCP	DROP USER	NO
SCP	EXECUTE ANY PROCEDURE	NO
SCP	GRANT ANY PRIVILEGE	NO
SCP	GRANT ANY ROLE	NO
SCP	INSERT ANY TABLE	YES
SCP	SELECT ANY TABLE	YES
SCP	UNLIMITED TABLESPACE	NO
SCP	UPDATE ANY TABLE	YES

Users on VWS Database Instance

Ensure the VWS database instance contains a user called E2BE_ADMIN with the following privileges:

GRANTEE	PRIVILEGE	ADMIN OPTION
E2BE_ADMIN	ALTER SESSION	YES
E2BE_ADMIN	CREATE ANY CONTEXT	NO
E2BE_ADMIN	CREATE ANY DIRECTORY	NO
E2BE_ADMIN	CREATE ANY TRIGGER	NO
E2BE_ADMIN	CREATE MATERIALIZED VIEW	NO
E2BE_ADMIN	CREATE PROCEDURE	NO
E2BE_ADMIN	CREATE PUBLIC SYNONYM	NO
E2BE_ADMIN	CREATE ROLE	NO
E2BE_ADMIN	CREATE SEQUENCE	NO
E2BE_ADMIN	CREATE SESSION	YES
E2BE_ADMIN	CREATE TABLE	NO
E2BE_ADMIN	CREATE TRIGGER	NO
E2BE_ADMIN	CREATE USER	NO
E2BE_ADMIN	CREATE VIEW	NO
E2BE_ADMIN	DROP ANY CONTEXT	NO

GRANTEE	PRIVILEGE	ADMIN OPTION
E2BE_ADMIN	DROP PUBLIC SYNONYM	NO
E2BE_ADMIN	DROP USER	NO
E2BE_ADMIN	GRANT ANY PRIVILEGE	NO
E2BE_ADMIN	GRANT ANY ROLE	NO
E2BE_ADMIN	UNLIMITED TABLESPACE	NO

Chapter 5

NCC Pre-Installation Tasks

Overview

Introduction

This chapter explains the tasks you should perform before installing Oracle Communications Network Charging and Control (NCC).

In this chapter

This chapter contains the following topics.

Preparing the System for Installation

About Preparing the System

To prepare the system before you install NCC, you log in to each node in turn as the root user, and perform the following tasks:

- (Optional) Disable automount for the top directory of the mount point for all entries in the **auto_home** map file. See *Disabling automount for the Home Directory* (on page 44).
- Configure the log notice alarms. See *Configuring Where to Log Notice Alarms* (on page 44).
- Configure the directory to use for reporting core dumps and storing core files. See *Configuring Core Dump Reporting* (on page 44).
- Disable any unnecessary system services. See *Disabling System Services* (on page 45).
- Open ports to NCC in your Linux firewall. See *Opening Ports in Your Linux Firewall* (on page 46).
- Enable the SSH root login. See *Enabling SSH Root Login* (on page 47).
- Ensure Java 21.0.6 is installed. See the Oracle Java documentation.
- Create the **/IN** Directory. See *Creating the /IN Directory* (on page 48).
- Ensure bzip2 utility is installed.

NCC Installation Options

You can install NCC in the GUI mode (using Oracle Universal Installer) or in silent mode.

- **GUI mode:** Use the GUI mode when you want to interact with the Installer during installation. See *Installation Types*.
- **Silent mode:** Use the silent mode when you are installing NCC using the same configuration repeatedly. The silent mode does not use the GUI and it runs in the background. See *Installing NCC in Silent Mode* for more information.

Disabling automount for the Home Directory

(Optional) Disable `automount` for each node's *home* top directory, where *home* is the highest level directory used for installation. Disabling automount for this location allows you to create an Oracle user for the database administrator in the *home* directory.

Follow these steps to disable `automount` for the *home* directory.

Step	Action
1	Open the following file in a text editor: For Linux: **`/etc/auto.master`**
2	Comment out the line containing `auto_home` by inserting **#** at the beginning of the line. For example: **#** `/home  auto_home -nobrowse`
3	Save and close the file.
4	Restart autofs to remount the file system by running the command: For Linux: systemctl restart autofs.service
5	Create a symbolic link **/export/home** to **/home** by running the command: **`ln -s /home /export/home`** **Result:** This allows you to write to both the **/export/home** and the **/home** directories. Note: If **/export** does not exist, create one before linking **/home** by running: **`mkdir /export`**

Configuring Where to Log Notice Alarms

Configure where to log notice alarms, which contain informational messages that are generated during the installation process.

Follow these steps to log notice level alarms.

Step	Action
1	Open the following file in a text editor: For Linux: **/etc/rsyslog.conf**
2	Add the following line: For Linux: **`*.=notice;kern.=debug;daemon.=notice;mail.=crit`** *logfile* where *logfile* is the log file name including the absolute path; for example, **/var/log/messages**.
3	Save and close the file.
4	For Linux only, restart logging by running the command: systemctl restart rsyslog.service

Configuring Core Dump Reporting

On Linux

1. In /etc/profile, if there is a **`ulimit -S -c 0`** command, change it to or add the following command:

```
ulimit -S -c unlimited > /dev/null 2>&1
```
This will set the soft limit for core files to be unlimited.

2. In /etc/security/limits.conf, set:

   * soft core unlimited

3. In /etc/sysctl.conf, define the path of the core dump and the file name format for core files:

```
kernel.core_pattern = /var/crash/core-%h-%p-%e
where the format specifiers are
%h - system hostname
%p - PID of dumped process
%e - executable file name
```

4. In /etc/sysctl.conf, set **`fs.suid_dumpable`** to 2 to make core dumps readable by root only:

```
fs.suid_dumpable = 2
```
Load the changed sysctl settings:

```
# sysctl -p
```

5. In /etc/abrt/abrt-action-save-package-data.conf, set the following:

   `OpenGPGCheck = no` (to collect core dumps from unsigned packages)

   `ProcessUnpackaged = yes` (to collect core dumps from unpackaged software)

6. Restart the abrtd daemon.

   For Oracle Linux:

```
/bin/systemctl restart abrtd.service
/bin/systemctl restart abrt-ccpp.service
```

Important: You should use a dedicated volume for storing core files to ensure that other system, or application directories, are not affected if this directory becomes full.

Disabling System Services

You can disable the following system services, if they are not needed:

- FTP
- Telnet
- Rlogin
- Sendmail

For Linux, use the **`systemct1`** command to disable the system services.

Example commands:

systemctl stop ftp.service

systemctl stop telnet.service

systemctl stop rlogin.service

systemctl stop sendmail.service

systemctl disable -now ftp.service

Opening Ports in Your Linux Firewall

Follow these steps to open ports in your Linux firewall.

Step	Action
1	Log in as the root user.
2	Run the following command to configure the tables provided by the Linux kernel firewall: **`yum install iptables-services`**
3	Run the following command to view your firewall's current configuration: **`iptables -L`**
4	Run the following command for each NCC port through which the firewall should accept incoming traffic: **`iptables -A INPUT -p tcp --dport`** *`portNumber`* **`-j ACCEPT`** where *portNumber* is the NCC port through which the firewall accepts incoming traffic. For more information on ports, see *List of Ports Used by NCC* (on page 46). The new configuration rule is added to your firewall rules table.
5	Run the following command to save the configuration in the firewall rules table: **`/sbin/service iptables save`**
6	Run the following command to reinitialize the iptables service: **`service iptables restart`** The configuration changes take effect after you reinitialize the iptables service.
7	Run the following command to backup your firewall rules table to an external file: **`iptables-save >`** *`filename`* where *filename* is the path and name of the file in which to save your firewall rules table. You can use this file to distribute the firewall rules table to other nodes or to restore your firewall rules table after a system reboot.

Important: Your changes to the firewall rules table are lost after a system reboot. After a system reboot, you must re-open the ports in your Linux firewall by running the following command:

`iptables-restore <` *`filename`*

where *filename* is the path and name of the file you saved in step 7.

List of Ports Used by NCC

The following table lists the ports used by NCC.

Port Number	Description
25	Email client port
53	ENCA port
80	acsStatisticsDBInserter, acsStatsMaster, and acsStatsLocal port
161	smsAlarmRelay port
1490	Used by ACS
1495	ccsSSMMaster port
1500	ccsMFileCompiler and beServer port
1521	SQL*Net port
1812	radiusControlAgent core port
1813	radiusControlAgent accounting port
2003	SEI EMI report port

Port Number	Description
2027	ccsVWARSExpiry and ccsExpiryMessageGenerator port CCS GPG key import screens, cmnPushFiles/cmnReceiveFiles for CCS EDRs
2028	cmnPushFiles/cmnReceiveFiles for ACS EDRs
2031	cmnPushFiles/cmnReceiveFiles for UIS EDRs
2484	Oracle database secure listening port
2500	Email server port
2999	piClientIF port
3033	SMPP remote port
3072	smsTrigDaemon and xmlTcapInterface port
3615	SCA remote communication port
3799	radiusControlAgent dynamic authorization port
3868	diameterControlAgent and diameterBeClient listening port
4099	dapIF listening port
5060	SCA TCP and UDP port
5096	XMS TCP and UDP port
5556	ccsBeOrb naming server port
7654	sigtran_monitor_daemon listening port
7669	smsCompareResyncServer
8888	smsInterface port
9999	xmlInterface port
12343	smsMaster and updateLoader port
12344	smsCompareResyncClient port
12696	VWS node port
14875	m3uaCdmaGateway test interface port
14876	m3uaCdmaGateway soak test interface port

Enabling SSH Root Login

Follow these steps to enable SSH root login.

Step	Action
1	In the **/etc/ssh/sshd_config** file, set the `PermitRootLogin` parameter value to **`yes`**.
2	Save and close the file.
3	Run the following command: For Linux: `$ systemctl restart ssh.service`

Installing HTTPD

Follow these steps to install HTTPD.

Step	Action
1	Login as root user.

Step	Action
2	For Linux, do the following: a) Set SELinux to Permissive. b) Run the following commands: **# yum install httpd** **# service httpd start**

Creating Users

The following sections explain the procedures to create users and groups in each NCC node.

The NCC application requires a single user of any given name to operate. A default username of 'smf_oper' is provided but can be changed at install time. The NCC_runtime_user can invoke the NCC installation, but this is not mandatory. If you select to use a different user, then it is mandatory to first create the NCC_runtime_user.

User profiles

If you plan to run the NCC application as a different NCC_runtime_user to the default, it is required to either set:

1 The home directory of the NCC_runtime_user to '/IN/service_packages/SMS'

2 Add the following line entry to the .profile of the NCC_runtime_user so the correct environment is configured automatically at login following the installation.

```
if [ -f /IN/service_packages/SMS/.profile-??* ]; then
. /IN/service_packages/SMS/.profile-??*;
fi
```

Creating esg group for Each Node

Follow these steps to create esg group for each NCC Node:

Step	Action
1	Login as root user.
2	Run the following command to create the esg group: **/usr/sbin/groupadd -g** *gid* **esg** where *gid* is a unique group id for the operating system

Creating the /IN Directory

Follow these steps to create the **/IN** directory. The directory must be accessed through the primary user account installing NCC.

Step	Action
1	Log in as the root user.
2	Run the following command: $ **mkdir /IN**
3	Run the following command to set the permissions for the **/IN** directory: **chmod 775 /IN** **chown** *NCC_installation_user*:**esg /IN**

About Checking Prerequisite Requirements

Verify that your system meets prerequisite requirements before you install NCC. The installer includes a prerequisite check mode that performs the following tests:

- The system meets minimum software and hardware requirements
- The esg group exists
- The Oracle user, NCC_runtime_user and NCC_installation_user exists and belongs to the esg group and the group that owns the Oracle database (for example 'dba').
- The **/IN** directory exists and has readable, writable, and executable (775) file permissions
- JAVA_HOME and JAVA_HOME/bin should be set in PATH variable, so that java executable can be accessed from any location

Perform a prerequisite check by running the following command on each NCC node:

touch *oraInvFile*

java -jar ./nccInstaller_*platform*.**jar -invPtrLoc** *oraInvFile* **-prereqchecker -silent -entryPoint** *nodeType*

where:

- *platform* is **Linux**.
- *oraInvFile* is the name and location of the Oracle Inventory file (**/IN/oraInst.loc**). You can point to the default file created by the Oracle Database installer. If the NCC installation user account cannot read the default file, create an **oraInst.loc** file in a writeable location.
- *nodeType* is the type of test to perform. Valid values are shown in the following table:

nodeType Value	Tests Performed
minimum	• Checks that all users and groups have been created. • Checks that the **/IN** directory exists.
sms	• Checks that all users and groups required by the SMS have been created. • Checks that the **/IN** directory exists.
slc	• Checks that all users and groups required by the SLC have been created. • Checks that the **/IN** directory exists. • Check SLC software dependencies.
vws	• Checks that the users and groups required by the VWS have been created. • Checks that the **/IN** directory exists. • Check VWS software dependencies.

During the prerequisite check process, the installer informs you whether your system passes each test by using one of the following settings:

Setting	Description
Passed	Your node passed the specified test.
Failed	Your node did not pass the specified test. This setting is for informational purposes only. It does not prevent you from installing NCC.
Not executed	The installer could not perform the specified test. This output includes additional information about how to perform the test manually.

The following shows sample output from the **nccInstaller**_*platform*.**jar** script when *nodeType* is set to **slc**:

```
Preparing to launch the Oracle Universal Installer from /tmp/OraInstall2025-10-
14_11-20-27AM\
Oracle Prerequisite Checker Version 13.9.4.0.0 Production\
Copyright (C) 1999, 2022, Oracle. All rights reserved.\
\
Starting execution of prerequisite checks\
Total No of checks: 9\
\
Performing check for CheckEsgGroupExists\
Checking OS group esg exists.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for CheckUserBelongsToEsgGroup\
Checking you belong to the OS esg group.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for CheckOracleBelongsToEsgGroup\
Checking oracle user belongs to the OS esg group.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for checkUserBelongsToDbaGroup\
Checking you belong to the OS database group.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for CheckDirectoryExists\
Checking /IN directory exists and has 775 permisions.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for CheckXinetdExists\
Checking xinetd (linux) or inetd (solaris) are installed.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for CheckHttpd\
Checking httpd (linux) or apache2 (solaris) are installed.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
Performing check for CheckMemory\
Checking system memory:must be greater than or equal to 8GB.\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
============================================================\
```

```
Performing check for CheckDbConnectivity\
Checking Oracle DB connectivity (sqlplus '/ as sysdba').\
Check complete. The overall result of this check is: Passed\
\
\
Check complete: Passed\
=====================================================\
PrereqChecks complete\
\
\
The log(s) can be found here: /tmp/OraInstall2025-10-14_11-20-27AM.
```

Installing a Browser

Browser and Java for NCC UI

To enable you to access the NCC UI, ensure that the required Java version and the browser listed in the following table are installed on your client system.

Note: NCC supports client systems that use Windows XP or higher.

Browser/Java	Description
Java	Java 21.0.9
Browser	Any browser supporting the required Java version, such as Microsoft Edge 144 or Chrome 124.0

Installing and Configuring Oracle Database

About Installing and Configuring Oracle Database

You need to install Oracle Database Server on all nodes:

- Enterprise Edition for SMS or Standard Edition for non-partitioned deployments
- Standard Edition for all other nodes (SLC, VWS1, VWS2)

Installing the Oracle Database Software

You can install Oracle database for NCC in the following ways:

- Install Oracle database on remote host.
- Install Oracle database on local host.

Install Oracle Enterprise Database Server 19c (or) 26ai.

Oracle Database Software Installation Guidelines

Follow these guidelines when installing Oracle Enterprise Database software.

Installation Entity	Guideline Value
Oracle Software Owner User	Username: **oracle** Home directory: **/home/oracle**
OSDBA Group	**dba**

Installation Entity	Guideline Value
Oracle Base Directory (ORACLE_BASE)	**/u01/app/oracle**
Oracle Home Directory (ORACLE_HOME)	**/u01/app/oracle/product/19.0.0** for 19c **/u01/app/oracle/product/23.0.0** for 26ai
Oracle database datafile directory	**/oracle/datafiles** for 19c **/u01/app/oracle/oradata** for 26ai

Oracle user **.profile** (**/home/oracle/.profile**)	Configure the **oracle** user's **.profile** file with the following variables consistent with your environment.
	
	`# Set up terminal, non-interactive, default vt100`
	`TERM=vt100`
	`export TERM`
	
	`if [ -t 0 ] ; then`
	`  # Set some options`
	`  set -o vi`
	`  stty erase "^H" kill "^U" intr "^C" eof "^D"`
	`  stty hupcl ixon ixoff`
	`  set -o vi`
	`fi`
	
	`umask 022`
	
	`MAIL=/usr/mail/${LOGNAME:?}`
	`export MAIL`
	
	`ORACLE_BASE=/u01/app/oracle`
	`export ORACLE_BASE`
	
	`ORACLE_HOME=$ORACLE_BASE/product/`*`release_version`*
	`export ORACLE_HOME`
	
	`LD_LIBRARY_PATH_64=$ORACLE_HOME/lib`
	`export LD_LIBRARY_PATH_64`
	
	`LD_LIBRARY_PATH=$ORACLE_HOME/lib`
	`export LD_LIBRARY_PATH`
	
	`PATH=$PATH:$ORACLE_HOME/bin:/usr/bin:/etc:/usr/ccs/bin:/usr/openwin/bin:/usr/local/bin:/usr/sbin`
	`EDITOR=vi`
	`export EDITOR`
	
	`ORACLE_SID=[SMF|SCP|E2BE]`
	
	where *`release_version`* is 19.0.0 (for 19c)/23.0.0 (for 26ai) as per the Oracle database version used.
	
	Note: ORACLE_SID must be set to one of:
	• **SMF** for SMS node
	• **SCP** for SLC nodes
	• **E2BE** for VWS nodes
	
	`export ORACLE_SID`
	`ulimit -n 4096`
	`export PATH`

Installation Entity	Guideline Value

Global profile
(**/etc/profile**)
	Configure your system's global profile as required for your environment. For example,
	`PS1='${LOGNAME}@$(/usr/bin/hostname):$([[ "${LOGNAME}" == "root" ]] && printf "%s" "${PWD}# " ||`
	`printf "%s" "${PWD}$ ")'`
	`ORACLE_BASE=/u01/app/oracle`
	`export ORACLE_BASE`
	`ORACLE_HOME=$ORACLE_BASE/product/`*`release_version`*
	`export ORACLE_HOME`
	`ORACLE_CLIENT_HOME=$ORACLE_HOME`
	`export ORACLE_CLIENT_HOME`
	`LD_LIBRARY_PATH=$ORACLE_CLIENT_HOME/lib:$LD_LIBRARY_PATH`
	`export LD_LIBRARY_PATH`
	`PATH=$PATH:$ORACLE_HOME/bin`
	`export PATH`
	`ORACLE_SID=[SMF|SCP|E2BE]`
	Where *release_version* is 19.0.0 (for 19c)/23.0.0 (for 26ai) as per the Oracle database version used.
	Note: ORACLE_SID must be set to one of:
	• **SMF** for SMS node
	• **SCP** for SLC nodes
	• **E2BE** for VWS nodes
	`export ORACLE_SID`

System resources for Oracle (Linux only)	**1** Determine the sum of process parameters for all database instances on the system, the overhead for Oracle background processes, the system and other application requirements.
	2 Set semmns (total semaphores system-wide) to the larger of the value in 1 or 32000.
	3 Set semmsl (semaphores per set) to 250.
	4 Set semmni (total semaphore sets) to semmns/semmsl rounded up to the nearest multiple of 1024.
	5 For Linux and Oracle 19*c*, set the maximum number of asynchronous I/O requests allowed in /etc/sysctl.conf as follows:
	`fs.aio-max-nr = 3145728`
	After changing the /etc/sysctl.conf, run the following command as root to set the values in the system:
	`# /sbin/sysctl -p /etc/sysctl.conf`

Oracle Server Installation Guidelines

Follow these guidelines when using Oracle Universal Installer to install Oracle 19*c* on all nodes.

Installation Option	Guideline Values
Installation Method	Basic
Installation Type	Enterprise edition for partitioned SMS nodes Standard editions for VWS, SLC, and non-partitioned SMS nodes
Create Starter Database	No
Configuration Option	Install database software only

Oracle 19*c*/26ai Client Installation Guidelines

Follow these guidelines when using Oracle Universal Installer to install the Oracle 19*c* client.

Installation Option	Guideline Values
Installation Type	Custom
Download Software	Skip software updates
Available Product Components	Oracle Database Utilities, Oracle Net Listener
Oracle Net Configuration Assistant	Oracle Net configuration is not needed. When prompted by the Oracle Net Configuration Assistant, cancel the assistant by clicking **Cancel** and confirming you want to cancel the assistant.

Configuring the Oracle Database to Start Automatically

You should implement startup scripts to automatically start the local database instance on system startup.

You can use the **/etc/init.d/oracleDB.sh** example Oracle startup and shutdown scripts to configure the system to start the Oracle database automatically on startup (and shut down automatically on system shutdown).

You should configure automatic startup for the Oracle database at system run level 2 instead of the default run level 3. Automatic shutdown can be configured for run levels 0 and 1 as well. You create symbolic links in the appropriate run level directories to the example startup and shutdown scripts.

To configure automatic startup and shutdown for using the example scripts, log in as the root user, and run the following commands:

For Linux:

```
chmod 700 /etc/init.d/dbora.sh
ln -s /etc/init.d/dbora.sh /etc/rc0.d/K10oracle
ln -s /etc/init.d/dbora.sh /etc/rc1.d/K10oracle
rm -f /etc/rc2.d/K10oracle
ln -s /etc/init.d/dbora.sh /etc/rc2.d/S99oracle
rm -f /etc/rc3.d/S99oracle
```

Note: After entering these commands, the symbolic link between **/etc/init.d/oracleDB.sh** and **K10oracle** in the **/etc/rc0.d** and the **/etc/rc1.d** directories mean that the Oracle instance will be stopped when the system is set to an init level below 2.

Oracle Database Instances

You can opt to automatically create Oracle database instances during the installation of the NCC software packages. A single database instance is created on each NCC node.

The following table shows the mapping between each node type and the named database instance on the node.

Node Type	Database Instance
SMS	SMF
VWS	E2BE
SLC	SCP

Setting Database Parameters for SMS Databases

Oracle recommends setting the following database parameters in the underlying databases used by Service Management System (SMS) nodes.

Database Parameter	Guideline Value
JOB_QUEUE_PROCESSES	**20**

To set the database parameters for SMS databases:

Step	Action
1	Ensure that you have SYSDBA privileges.
2	Go to the computer on which the Oracle database is installed.
3	Start SQL*Plus: `-bash-5.1$ sqlplus /NOLOG`
4	Connect to the database as SYSDBA: `SQL> CONNECT / AS SYSDBA`
5	Set the **JOB_QUEUE_PROCESSES** initialization parameter to: `ALTER SYSTEM SET JOB_QUEUE_PROCESSES=20 SCOPE=BOTH`
6	Shut down Oracle database: `SQL> SHUTDOWN`
7	Restart Oracle database: `SQL> STARTUP`
8	Exit SQL*Plus: `SQL> EXIT`

Chapter 6

Installing NCC

Overview

Introduction

This chapter describes how to install Oracle Communications Network Charging and Control (NCC). Before you install NCC, read the following chapters:

- NCC Installation Overview
- Planning Your NCC Installation
- NCC System Requirements
- Advanced Storage and Memory Sizing
- NCC Pre-Installation Tasks

In this chapter

This chapter contains the following topics.

NCC Installation Types

When installing NCC in the GUI mode, you can select the type of installation:

SMS Node: Service Management System (SMS) installs the NCC SMS application and the SMS database. See *Installing NCC on the SMS Node Using the GUI* (on page 59).

SLC Node: Service Logic Controller (SLC) installs the NCC SLC application and the SLC database. See *Installing NCC on the SLC Node Using the GUI* (on page 63).

SLC With Test Tools: Service Logic Controller (SLC) installs the NCC SLC application, the SLC Test Tools, and the SLC database. See *Installing NCC on the SLC with Testing Tools Node Using the GUI* (on page 66).

VWS Node: Voucher and Wallet Server (VWS) installs the NCC application, the VWS database, and the VWS application. See *Installing NCC on the VWS Node Using the GUI* (on page 69).

Prerequisites for Network Charging and Control Installation on 26ai

Installation of Remote Database (Using Application, Database and Schema Installation)

- DB and schema installation on 26ai requires a CDB container. Download and run the script provided in Patch 38882230. The installation details are included in the README file within the downloaded patch.
- Create a directory for SMF/SCP/E2BE as follows:

```
mkdir -p /u01/app/oracle/oradata/<directory_name>/pdbseed
cd /u01/app/oracle/
chmod -R 775 oradata
```

- Ensure the OraInventory directory in the path **/scratch/u01/app/oracle/** has 775 permissions. If not, run the following command:

```
chmod -R 775 /scratch/u01/app/oracle/OraInventory
```

- Add ncc_install_user to the dba and esg groups (as root) if not already added.

```
usermod -G dba,esg <ncc_install_user>
```

Add or update the following environment variables in **/etc/profile**:

```
export MULTITENANT_DB=TRUE
export CDB_NAME= <CDB name used while running the
create_MultiTenantDB_structure.sh script>
export ORACLE_SID=<SMF|SCP|E2BE>
```

(set based on installation type)

- Copy the Oracle Central Inventory location file from /etc/oraInst.loc to /IN as ncc_install_user, then set its permissions to 775.
- For installing the SMS DB and schema on a remote database running 26ai, update /etc/profile with ORACLE_SID for SMF.

```
export ORACLE_SID=SMF
```

- Run the OUI installer as specified in the section *Installing NCC on the SMS Node Using the GUI*.
- Repeat the steps above to install the SCP database and schema. Update /etc/profile with export ORACLE_SID=SCP, open a new session, launch the OUI installer, and proceed as described in the section *Installing NCC on the SLC Node Using the GUI*.
- Before installing VWS for the E2BE database and schema, modify the existing init<CDB_NAME>.ora file on the remote database at /u01/app/oracle/product/23.0.0/dbs/ (file: /u01/app/oracle/product/23.0.0/dbs/init<CDB_NAME>.ora).
- In the Cache and I/O section of init<CDB_NAME>.ora, add the following line at the end: db_2k_cache_size=52428800
- Shut down and start the Oracle instance, then open all pluggable databases.

```
su - oracle
export ORACLE_SID=<CDB name used while running the
create_MultiTenantDB_structure.sh script>
sqlplus / as sysdba
SQL> shutdown immediate;
SQL> exit
```

```
export ORACLE_SID=<CDB name used while running the
create_MultiTenantDB_structure.sh script>
sqlplus / as sysdba
SQL>startup
SQL> ALTER PLUGGABLE DATABASE ALL OPEN;
```

Note: To open a specific PDB, run:

```
SQL> ALTER PLUGGABLE DATABASE <PDB_NAME> OPEN;
```

- Update /etc/profile to include export ORACLE_SID=E2BE, open a new session, and launch the OUI installer as ncc_install_user to install the E2BE database and schema. Proceed as described in the section *Installing NCC on the VWS Node Using the GUI*.

Installing Application Only on Application Nodes (SMS, SLC, and VWS)

Download and install the Oracle 26ai Client (Enterprise) for engineered systems on the application nodes to enable remote database connections.

Ensure the OraInventory directory at /scratch/u01/app/oracle/OraInventory has 775 permissions. If not, run: `chmod -R 775 /scratch/u01/app/oracle/OraInventory`

Add the following environment variables to /etc/profile in addition to ORACLE_SID:

```
export MULTITENANT_DB=TRUE
```

```
export CDB_NAME= <CDB name used while running the
create_MultiTenantDB_structure.sh script>
```

`export ORACLE_SID=<SMF|SCP|E2BE>` (set based on installation type)

Copy the Oracle Central Inventory location file (oraInst.loc) from /etc/ to /IN as ncc_install_user, then set permissions to 775:

```
chmod 775 /IN/oraInst.loc
```

Refer to the section *Installing NCC (Application Only) on the SMS/SLC/VWS Node Using the GUI (26ai)* to install the application only with the 26ai client.

Installing NCC on the SMS Node Using the GUI

Install NCC on an Oracle Linux 9.6 server.

Note: Solaris is not supported from 15.1 release.

To install NCC on an SMS node:

Step	Action
1	Log in as the root user.
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **cd /var/spool/pkg** **mkdir NCC** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.

Step	Action
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_*platform*.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_*platform*.zip** file: **unzip NCC_v15_2_0_0_0_*platform*.zip**
5	Log in as the user (non-root) installing NCC. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **export DISPLAY=***IP_address*:0 **export JAVA_HOME=***Java_home* where: • *IP_address* is the IP address of the computer on which you run the SMS GUI. • *Java_home* is the directory in which JDK 21.0.9 is installed.
7	Ensure that the SMS node meets all prerequisites by running the following commands: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_***platform***.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint sms**
8	Do one of the following: • To start the Installer: **java -jar ./nccInstaller_***platform***.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_***platform***.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The installer screen appears.
9	Click **Next**. The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **SMS**.

Step	Action
13	Click **Next**. The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the username with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Server Paths screen appears.
15	Confirm one of the following: **The database, schema, and application will be installed.** Select this option to install all items on the same node. (Must be selected for the database node in a remote database installation also.) **The database already exists and both the schema and application will be installed.** Select this option if you have already created the database including datafiles on this or a remote node but not the database schema or application. **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	If you are installing all items on the same node: In the **Base directory** field, retain the default, **/u01/app/oracle.** In the **Oracle home directory** field, enter **/u01/app/oracle/product/19.0.0** for 19*c* database. In the **Oracle home directory** field, enter **/u01/app/oracle/product/23.0.0** for 26ai database. In the **Datafile directory** field, enter the path to the **datafiles** directory in which to create NCC database instance data files. In the **Redolog directory** field, enter the path to the **redolog** directory in which to create NCC database redo log files. Example: For 26ai, set **datafiles** and **redolog** directory to **/u01/app/oracle/oradata.** Click **Next**.

Step	Action
17	Select the database type. If items already exist on the same or remote node: Select one of the below options: a. If you select **Standard Database** option, configure the following: In the **Oracle database password** field, enter the password for the Oracle database administrative accounts. In the **Confirm password** field, enter the password again to confirm. **Note**: If the password is less than 8 characters, a warning appears. You can click **OK** to proceed. b. If you select **RAC/Multi-tenant Database** option (required for 26ai installation), configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/19.0.0** for 19*c* client. In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0** for 26ai. In the **Oracle SID** field, enter **SMF**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password for the Oracle database administrative accounts on associated with the **Database hostname**. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: For 26ai, set the **Service database hostname** field as **smf.**<*remote database host shortname*>.
18	In the **Screen superuser password** field, enter the password for the SMS GUI administrator account.
19	In the **Confirm password** field, enter the password again to confirm.
20	Click **Next**. The PI Admin screen appears.
21	In the **PI admin password** field, enter the password for the PI administrator user account.
22	In the **Confirm password** field, enter the password again to confirm.
23	Click **Next.** The SMS EDR Paths screen appears.
24	In the **CDR Loader Input directory** field, retain the default path to the directory of a single system to store CDR input files.
25	In the **CDR Loader Output directory** field, retain the default path to the directory of a single system to store CDR output files.
26	Click **Next**. The Default Template Screen appears. If you want the default templates to be installed, check the Install PCST checkbox, else uncheck the Install PCST checkbox.
27	Click **Next**. The System Currency Details screen appears.

Step	Action
28	Set the following fields: Base Value - default is 100 Big Symbol - default is $ Little Symbol - default is c Separator - default is .
29	Click **Next**. Prerequisite check screen appears.
30	Based on the OS, few prerequisite checks are performed on clicking **Next**. The Installation Summary screen appears.
31	Review the selections you have made in the preceding screens and click **Install.** The Installation Progress screen appears.
32	Click **Next**. The Installation Complete screen appears.
33	Click **Finish**. (For 26ai on a remote database server setup) After installing SMS on the remote server, rename the IN directory to IN_SMS.
34	(Not required to run on the database node in a remote database installation) Log onto the SMS as the root user. **`cd /IN/bin`** **`./postinstallRoot.sh [-n]`** where -n is an optional flag. It is used to indicate if NCC will be installed without a VWS node. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.
35	(Not required to run on the database node in a remote database installation) Log onto the SMS as the NCC_runtime user (the user that was given in step 15 for application owner field). **`cd /IN/bin`** **`./postinstallUser.sh`** The script will prompt for information to be used as part of the runtime configuration. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC on the SLC Node Using the GUI

Install NCC on an Oracle Linux 9.6 server.

Note:

- Ensure that SMS is installed before installing SLC.
- Solaris is not supported from 15.1 release.

To install NCC on the SLC node:

Step	Action
1	Log in as the root user.
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **cd /var/spool/pkg** **mkdir NCC** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_*platform*.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_*platform*.zip** file: **unzip NCC_v15_2_0_0_0_*platform*.zip**
5	Log in as the user (non-root) installing NCC, and go to the **/var/spool/pkg/NCC** directory. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **export DISPLAY=***IP_address***:0** **export JAVA_HOME=***Java_home* where: • *IP_address* is the IP address of the computer on which the NCC GUI installer appears. • *Java_home* is the directory in which JDK 21.0.9 is installed.
7	Ensure that the SLC node meets all prerequisites by running the following command: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint slc**
8	Do one of the following: • To access the Installer: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The Installer screen appears.
9	Click **Next.** The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.

Step	Action
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **SLC**.
13	Click **Next.** The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the user name with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Server Paths screen appears.
15	Confirm one of the following: **The database, schema, and application will be installed**. Select this option to install all items on the same node. (Must be selected for the database node in a remote database installation also.) **The database already exists and both the schema and application will be installed.** Select this option if you have already created the database including datafiles on this or a remote node but not the database schema or application. **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	If you are installing all items on the same node: In the **Base directory** field, retain the default, **/u01/app/oracle**. In the **Oracle home directory** field, enter **/u01/app/oracle/product/19.0.0** for 19*c* database. In the **Oracle home directory** field, enter **/u01/app/oracle/product/23.0.0** for 26ai database. In the **Datafile directory** field, enter the path to the **datafiles** directory in which to create NCC database instance data files. In the **Redolog directory** field, enter the path to the **redolog** directory in which to create NCC database redo log files. Example: For 26ai, set **datafiles** and **redolog** directory to **/u01/app/oracle/oradata.** Click **Next**. Select the database type.

Step	Action
17	If items already exist on the same or remote node: Select one of the below options: a. If you select **Standard Database** option, configure the following: In the **Oracle database password** field, enter the password for the Oracle database administrative accounts. In the **Confirm password** field, enter the password again to confirm. **Note**: If the password is less than 8 characters, a warning appears. You can click **OK** to proceed. b. If you select **RAC/Multi-tenant Database** option (required for 26ai installation), configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/19.0.0** for 19*c* client. In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0** for 26ai. In the **Oracle SID** field, enter **SCP**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password for the Oracle database administrative accounts on associated with the **Database hostname**. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: For 26ai, set the **Service database hostname** field as **scp**.*<remote database host shortname>*.
18	In the **SMS Host name** field, enter the qualified hostname for the SMS server used to configure the clients that will connect to the SMS server.
19	Click **Next.** The Installation Summary screen appears.
20	Review the selections you have made in the preceding screens, and click **Install.** The Installation Progress screen appears.
21	Click **Next**. The Installation Complete screen appears.
22	Click **Finish**. (For 26ai on a remote database server setup) After installing SLC on the remote server, rename the IN directory to IN_SLC.

23	(Not required to run on the database node in a remote database installation) Log onto the SLC as the root user.
	`cd /IN/bin`
	`./postinstallRoot.sh`
	Note: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC on the SLC with Testing Tools Node Using the GUI

Install NCC on an Oracle Linux 9.6 server.

Note:

- Ensure that SMS is installed before installing SLC with Test Tools.

- Solaris is not supported from 15.1 release.

To install NCC on the SLC with Testing Tools node:

Step	Action
1	Log in as the root user.
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **cd /var/spool/pkg** **mkdir NCC** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_*platform*.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_*platform*.zip** file: **unzip NCC_v15_2_0_0_0_*platform*.zip**
5	Log in as the user (non-root) installing NCC and go to the **/var/spool/pkg/NCC** directory. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **export DISPLAY=***IP_address***:0** **export JAVA_HOME=***Java_home* where: • *IP_address* is the IP address of the computer on which the NCC GUI Installer appears. • *Java_home* is the directory in which JDK 21.0.9 is installed.
7	Ensure that the SLC node meets all prerequisites by running the following command: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint slc**
8	Do one of the following: • To access the Installer: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The Installer screen appears.

Step	Action
9	Click **Next**. The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **SLC With Test Tools** to install the SLC application, the SLC with Testing Tools, and the SLC database.
13	Click **Next**. The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the user name with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Server Paths screen appears.
15	Confirm one of the following: **The database, schema, and application will be installed.** Select this option to install all items on the same node. (Must be selected for the database node in a remote database installation also.) **The database already exists and both the schema and application will be installed.** Select this option if you have already created the database including datafiles on this or a remote node but not the database schema or application. **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	If you are installing all items on the same node: In the **Base directory** field, retain the default, **/u01/app/oracle**. In the **Oracle home directory** field, enter **/u01/app/oracle/product/19.0.0** for 19*c* database. In the **Oracle home directory** field, enter **/u01/app/oracle/product/23.0.0** for 26ai database. In the **Datafile directory** field, enter the path to the **datafiles** directory in which to create NCC database instance data files. In the **Redolog directory** field, enter the path to the **redolog** directory in which to create NCC database redo log files. For 26ai, set **datafiles** and **redolog** directory to **/u01/app/oracle/oradata.** Click **Next**. Select the database type.

Step	Action
17	If items already exist on the same or remote node: Select one of the below options: a. If you select **Standard Database** option, configure the following: In the **Oracle database password** field, enter the password for the Oracle database administrative accounts. In the **Confirm password** field, enter the password again to confirm. **Note**: If the password is less than 8 characters, a warning appears. You can click **OK** to proceed. b. If you select **RAC/Multi-tenant Database** option (required for 26ai installation), configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/19.0.0** for 19*c* client. In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0** for 26ai. In the **Oracle SID** field, enter **SCP**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password for the Oracle database administrative accounts on associated with the **Database hostname**. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: For 26ai, set the **Service database hostname** field as **scp**.*<remote database host shortname>*.
18	In the **SMS Host name** field, enter the qualified hostname for the SMS server used to configure the clients that will connect to the SMS server.
19	Click **Next.** The Installation Summary screen appears.
20	Review the selections you have made in the preceding screens and click **Install.** The Installation Progress screen appears.
21	Click **Next**. The Installation Complete screen appears.
22	Click **Finish**. (For 26ai on a remote database server setup) After installing SLC on the remote server, rename the IN directory to IN_SLC.

23	(Not required to run on the database node in a remote database installation) Log onto the SLC as the root user.
	`cd /IN/bin`
	`./postinstallRoot.sh`
	Note: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC on the VWS Node Using the GUI

Install NCC on an Oracle Linux 9.6 server.

Note:

- Ensure that SMS is installed before installing VWS.

- Solaris is not supported from 15.1 release.

To install NCC on a VWS node:

Step	Action
1	Log in as the root user.
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **cd /var/spool/pkg** **mkdir NCC** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_***platform***.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_***platform***.zip** file: **unzip NCC_v15_2_0_0_0_***platform***.zip**
5	Log in as the user (non-root) installing NCC and go to the **/var/spool/pkg/NCC** directory. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **export DISPLAY=***IP_address***:0** **export JAVA_HOME=***Java_home* where: • *IP_address* is the IP address of the computer on which the NCC GUI appears. • *Java_home* is the directory in which JDK 21.0.9 is installed.
7	Ensure that the VWS node meets all prerequisites by running the following command: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_***platform***.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint vws**
8	Do one of the following: • To access the Installer: **java -jar ./nccInstaller_***platform***.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_***platform***.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The Installer screen appears.

Step	Action
9	Click **Next**. The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **VWS**.
13	Click **Next.** The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the username with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Server Paths screen appears.
15	Confirm one of the following: **The database, schema, and application will be installed**. Select this option to install all items on the same node. (Must be selected for the database node in a remote database installation also.) **The database already exists and both the schema and application will be installed**. Select this option if you have already created the database including datafiles on this or a remote node but not the database schema or application. **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	If you are installing all items on the same node: In the **Base directory** field, retain the default, **/u01/app/oracle**. In the **Oracle home directory** field, enter **/u01/app/oracle/product/19.0.0** for 19*c* database. In the **Oracle home directory** field, enter **/u01/app/oracle/product/23.0.0** for 26ai database. In the **Datafile directory** field, enter the path to the **datafiles** directory in which to create NCC database instance data files. In the **Redolog directory** field, enter the path to the **redolog** directory in which to create NCC database redo log files. For 26ai, set **datafiles** and **redolog** directory to **/u01/app/oracle/oradata.** Click **Next**. Select the database type.

Step	Action
17	If items already exist on the same or remote node: Select one of the below options: a. If you select **Standard Database** option, configure the following: In the **Oracle database password** field, enter the password for the Oracle database administrative accounts. In the **Confirm password** field, enter the password again to confirm. **Note**: If the password is less than 8 characters, a warning appears. You can click **OK** to proceed. b. If you select **RAC/Multi-tenant Database** option (required for 26ai installation), configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/19.0.0** for 19*c* client. In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0** for 26ai. In the **Oracle SID** field, enter **E2BE**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password for the Oracle database administrative accounts on associated with the **Database hostname**. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: For 26ai, set the **Service database hostname** field as **e2be**.*<remote database host shortname>*.
18	In the **SMS Host name** field, enter the qualified hostname for the SMS server used to configure the clients that will connect to the SMS server.
19	Click **Next.** The VWS Config screen appears.
20	Enter the information for VWS configuration.
21	In the **SMS EDR Input directory** field, enter the full name and path to the directory to store SMS EDR input files.
22	Select the **Primary VWS node** check box to install the primary node of a VWS pair.
23	Click **Next.** The Installation Summary screen appears.
24	Review the selections you have made in the preceding screens and click **Install**. The Installation Progress screen appears.
25	Click **Next**. The Installation Complete screen appears.
26	Click **Finish**. (For 26ai on a remote database server setup) After installing VWS on the remote server, rename the IN directory to IN_VWS and rename the IN_SMS directory to IN (or create soflink as "ln -s IN_SMS IN").
27	(Not required to run on the database node in a remote database installation) Log onto the VWS as the root user. **`cd /IN/bin`** **`./postinstallRoot.sh`** **Note:** You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Step	Action
28	(Not required to run on the database node in a remote database installation) Log onto the VWS as the NCC_runtime user. **cd /IN/bin** **./postinstallUser.sh** The script will prompt for information to be used as part of the runtime configuration. **Not:** You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC in Silent Mode

Use silent install mode when you are installing NCC using the same configuration repeatedly. Silent install mode does not use the GUI, and it runs in the background.

About the Response File

A response file contains answers to installation questions that you would otherwise provide in an interactive installation session. Each answer is stored as a value for a variable identified in the response file.

You can generate a response file that contains the parameters and values during the NCC GUI installation.

To generate a complete response file, run the following command to launch the Installer in the GUI mode:

java -jar ./nccInstaller_*platform***.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record** *-destinationFilePath*

where *destinationFilePath* is the response file location.

Note: The generated response file does not have a user password for security reasons. You must add the following parameters manually to the response file:

ORACLE_DATABASE_*PASSWORD*
ORACLE_DATABASE_*PASSWORD_CONFIRM*

NCC_SCREENS_SU_*PASSWORD*
NCC_SCREENS_SU_*PASSWORD_CONFIRM*

PI_ADMIN_*PASSWORD*
PI_ADMIN_*PASSWORD_CONFIRM*

where:

- *password* is the password for the Oracle database, NCC screens, and PI Admin.
- *password_confirm* is the same password entered for the Oracle database, NCC screens, and PI Admin.

Installing NCC in Silent Mode

To install NCC in silent mode:

Step	Action
1	Create a copy of the *response* file that was generated during the GUI installation and open it in a text editor.
2	Enter the values in the parameters to reflect the NCC installation requirements. **Note:** In silent install mode, the NCC installer treats incorrect context, format, or type values within a response file as if no value were specified.
3	Save and close the file.
4	Go to the **/IN** directory and run the following command: **`java -jar ./nccInstaller_`***`Platform`***`.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -silent -responseFile`** *`path`* where *`path`* is the NCC response file name and location. For example: `${JAVA_HOME}/bin/java -jar./nccInstaller_Linux.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -silent -responseFile /tmp/smsinstallresponse.rsp` The installation runs silently in the background.

Following install on the SMS

Note: You do not need to run the following steps on the database node in a remote database installation.

Step	Action
1	Log onto the SMS as the root user. **`cd /IN/bin`** **`./postinstallRoot.sh [-n]`** where -n is an optional flag. It is used to indicate if NCC will be installed without a VWS node. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.
2	Log onto the SMS as the NCC_runtime user. **`cd /IN/bin`** **`./postinstallUser.sh`** The script will prompt for information to be used as part of the runtime configuration. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Following install on the SLC

Note: You do not need to run the following steps on the database node in a remote database installation.

Step	Action
1	Log onto the SLC as the root user. **cd /IN/bin** **./postinstallRoot.sh** **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Following install on the VWS

Note: You do not need to run the following steps on the database node in a remote database installation.

Step	Action
1	Log onto the VWS as the root user. **cd /IN/bin** **./postinstallRoot.sh** **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.
2	Log onto the VWS as the NCC_runtime user. **cd /IN/bin** **./postinstallUser.sh** The script will prompt for information to be used as part of the runtime configuration. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC (Application Only) on the SMS Node Using the GUI (For 26ai)

Install NCC on an Oracle Linux 9.6 server.

Note: Solaris is not supported from 15.1 release.

To install NCC on an SMS node:

Step	Action
1	Log in as the root user.
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **cd /var/spool/pkg** **mkdir NCC** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.

Step	Action
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_*platform*.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_*platform*.zip** file: **unzip NCC_v15_2_0_0_0_*platform*.zip**
5	Log in as the user (non-root) installing NCC. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **export DISPLAY=***IP_address*:0 **export JAVA_HOME=***Java_home* where: • *IP_address* is the IP address of the computer on which you run the SMS GUI. • *Java_home* is the directory in which JDK 21.0.9 is installed.
7	Ensure that the SMS node meets all prerequisites by running the following commands: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint sms**
8	Do one of the following: • To start the Installer: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The installer screen appears.
9	Click **Next**. The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **SMS**.

Step	Action
13	Click **Next**. The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the username with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Location screen appears.
15	Select the following: **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	Click **Next**. Select the **RAC/Multi-tenant Databas**e option. Click **Next**.
17	Configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0**. In the **Oracle SID** field, enter **SMF**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password as entered in the remote database server for smf database user. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: In the **Service database hostname** field, enter **smf.**<*remote database host shortname*>.
18	In the **Screen superuser password** field, enter the password for the SMS GUI administrator account.
19	In the **Confirm password** field, enter the password again to confirm.
20	Click **Next**. The PI Admin screen appears.
21	In the **PI admin password** field, enter the password for the PI administrator user account.
22	In the **Confirm password** field, enter the password again to confirm.
23	Click **Next.** The SMS EDR Paths screen appears.
24	In the **CDR Loader Input directory** field, retain the default path to the directory of a single system to store CDR input files.
25	In the **CDR Loader Output directory** field, retain the default path to the directory of a single system to store CDR output files.
26	Click **Next**. The Default Template Screen appears. If you want the default templates to be installed, check the Install PCST checkbox, else uncheck the Install PCST checkbox.

Step	Action
27	Click **Next**. The System Currency Details screen appears.
28	Set the following fields: Base Value - default is 100 Big Symbol - default is $ Little Symbol - default is c Separator - default is .
29	Click **Next**. Prerequisite check screen appears.
30	Based on the OS, few prerequisite checks are performed on clicking **Next**. The Installation Summary screen appears.
31	Review the selections you have made in the preceding screens, and click **Install.** The Installation Progress screen appears.
32	Click **Next**. The Installation Complete screen appears.
33	Click **Finish**.
34	Log onto the SMS as the root user. **cd /IN/bin** **./postinstallRoot.sh [-n]** where -n is an optional flag. It is used to indicate if NCC will be installed without a VWS node. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.
35	Log onto the SMS application node as NCC_runtime user (the user that was given in step 15 for application owner field). **cd /IN/bin** **./postinstallUser.sh** The script will prompt for information to be used as part of the runtime configuration. **Note**: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC (Application Only) on the SLC Node Using the GUI (For 26ai)

Install NCC on an Oracle Linux 9.6 server.

Note:

- Ensure that SMS is installed before installing SLC.
- Solaris is not supported from 15.1 release.

To install NCC on the SLC node:

Step	Action
1	Log in as the root user.

Step	Action
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **cd /var/spool/pkg** **mkdir NCC** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_*platform*.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_*platform*.zip** file: **unzip NCC_v15_2_0_0_0_*platform*.zip**
5	Log in as the user (non-root) installing NCC, and go to the **/var/spool/pkg/NCC** directory. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **export DISPLAY=***IP_address***:0** **export JAVA_HOME=***Java_home* where: • *IP_address* is the IP address of the computer on which the NCC GUI installer appears. • *Java_home* is the directory in which JDK 21.0.9 is installed.
7	Ensure that the SLC node meets all prerequisites by running the following command: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint slc**
8	Do one of the following: • To access the Installer: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The Installer screen appears.
9	Click **Next.** The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.

Step	Action
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **SLC** or **SLC with Test Tools**.
13	Click **Next.** The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the user name with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Server Paths screen appears.
15	Select the following: **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	Click **Next**. Select the **RAC/Multi-tenant Databas**e option. Click **Next**.
17	Configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0**. In the **Oracle SID** field, enter **SCP**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password for the Oracle database administrative accounts on associated with the **Database hostname**. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: In the **Service database hostname** field, enter **scp**.*<remote database host shortname>*.
18	In the **SMS Host name** field, enter the fully qualified hostname of the SMS application server used to configure the clients that will connect to the SMS server.
19	Click **Next.** The Installation Summary screen appears.
20	Review the selections you have made in the preceding screens, and click **Install.** The Installation Progress screen appears.
21	Click **Next**. The Installation Complete screen appears.
22	Click **Finish**.

Step	Action
23	Log onto the SLC application node as the root user. **`cd /IN/bin`** **`./postinstallRoot.sh`** **Note:** You can reuse the script at any time to complete or retry failures occurring on previous invocations.

Installing NCC (Application Only) on the VWS Node Using the GUI (For 26ai)

Install NCC on an Oracle Linux 9.6 server.

Note:

- Ensure that SMS is installed before installing VWS.
- Solaris is not supported from 15.1 release.

To install NCC on a VWS node:

Step	Action
1	Log in as the root user.
2	Create a **NCC** sub-directory in the **/var/spool/pkg** directory: **`cd /var/spool/pkg`** **`mkdir NCC`** **Note:** The amount of space available in this directory must be at least three times the size of the archive. For example, if the archive is 500 MB, the temporary directory should be at least 1500 MB.
3	Go to the Oracle software delivery Web site: http://edelivery.oracle.com/ and download the **NCC_v15_2_0_0_0_*platform*.zip** software pack to the **/var/spool/pkg/NCC** directory, where *platform* is **Linux**.
4	Go to the **/var/spool/pkg/NCC** directory and unzip the **NCC_v15_2_0_0_0_*platform*.zip** file: **`unzip NCC_v15_2_0_0_0_`***`platform`***`.zip`**
5	Log in as the user (non-root) installing NCC, and navigate to the **/var/spool/pkg/NCC** directory. **Note:** Ensure that the non-root user installing NCC has access to the esg and Oracle database group (for example, dba).
6	Run the following commands: **`export DISPLAY=`***`IP_address`***`:0`** **`export JAVA_HOME=`***`Java_home`*** where: • *IP_address* is the IP address of the computer on which the NCC GUI appears. • *Java_home* is the directory in which JDK 21.0.6 is installed.

Step	Action
7	Ensure that the VWS node meets all prerequisites by running the following command: **touch /IN/oraInst.loc** **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -prereqchecker -silent -entryPoint vws**
8	Do one of the following: • To access the Installer: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc** • To start the Installer and create a silent installer response file during the installation: **java -jar ./nccInstaller_*platform*.jar -invPtrLoc /IN/oraInst.loc -logLevel finest -record -destinationFile** *path* where *path* is the response file location. The Installer screen appears.
9	Click **Next**. The Installation Inventory screen appears. In the **Inventory Directory** field, enter the path to the OraInventory directory, or click **Browse** to select the directory. In the **Operating System Group** field, select group (esg) from the drop-down list. Click **Next**. The Installation Location screen appears.
10	In the **Name** field, enter **/IN**.
11	Click **Next**. The Installation Type screen appears. **Note:** The NCC installer creates an **oraInventory** directory if it does not detect any installed Oracle products on the system. The **oraInventory** directory contains information about all Oracle products installed on your system. You can find the default location of the **oraInventory** directory by opening the **/etc/oraInst.loc** (Linux) file.
12	Select **VWS**.
13	Click **Next.** The Oracle User screen appears.
14	In the **Oracle DB Owner** field, retain the default **oracle**, which is the username with permissions to create the Oracle database instance. Verify the **Oracle DB Group** field. Specify the NCC runtime user in the **Application Owner** field. Click **Next**. The Database Server Paths screen appears.
15	Select the following: **The database and schema already exists and only the application will be installed**. Select this option if the database and schema already exists on this or a remote node and you want to only install the application.
16	Click **Next**. Select the **RAC/Multi-tenant Database** option. Click **Next**.

Step	Action
17	Configure the following: In the **Oracle client home** directory field, enter **/u01/app/oracle/product/23.0.0**. In the **Oracle SID** field, enter **E2BE**. In the **Database hostname** field, enter the host where the database is located. In the **Oracle database password** field, enter the password for the Oracle database administrative accounts on associated with the **Database hostname**. In the **Database Port** field, enter the port that is required to connect to the database host. In the **Service database hostname** field, enter the fully qualified service DB hostname. **Note**: In the **Service database hostname** field, enter **e2be**.*<remote database host shortname>*.
18	In the **SMS Host name** field, enter the fully qualified hostname for the SMS application server used to configure the clients that will connect to the SMS server.
19	Click **Next.** The VWS Config screen appears.
20	Enter the information for VWS configuration.
21	In the **SMS EDR Input directory** field, enter the full name and path to the directory to store SMS EDR input files.
22	Select the **Primary VWS node** check box to install the primary node of a VWS pair.
23	Click **Next.** The Installation Summary screen appears.
24	Review the selections you have made in the preceding screens, and click **Install**. The Installation Progress screen appears.
25	Click **Next**. The Installation Complete screen appears.
26	Click **Finish**.

27	Log onto the VWS as the root user.
	`cd /IN/bin`
	`./postinstallRoot.sh`
	Note: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

28	Log onto the VWS application node as NCC_runtime user.
	`cd /IN/bin`
	`./postinstallUser.sh`
	The script will prompt for information to be used as part of the runtime configuration.
	Not: You can reuse the script at any time to complete or retry failures occurring on previous invocations.

About Installation Logs

You can check the log files in the **oraInventory/logs** directory. The default location of the **oraInventory** directory is in the **/IN/oraInst.loc** file.

Use the following log files to monitor installation and post-installations:

- **installAction***TimeStamp***.log**
- **oraInstall***TimeStamp***.err**
- **oraInstall***TimeStamp***.out**
- **silentInstall***TimeStamp***.log** (for the silent mode installation)

where *TimeStamp* is the date and time the log file was created.

The database schema installation log files for NCC are available in /IN/logs directory.

Removing Files After a Failed Installation

If **nccInstaller***_platform***.jar** fails during the installation process, some NCC files may remain on your system.

Follow these steps to remove any NCC files that remain on your system after a failed installation.

Step	Action
1	**Note**: For the 26ai setup, do not run the **`removeDatabase.sh`** script on the remote database server or the application server. As root user, remove any remaining NCC files by running the following command: Go to the /IN/bin directory. **`./removeDatabase.sh`** **`./removeApplication.sh`** Remove the **inventory.lock** file from the **/u01/app/oraInventory/locks** directory.

Additional Notes (for 26ai)

To remove any remaining NCC files after a failed installation on the remote database node:

Change to the IN directory for the specific application (SMS, SLC, or VWS); for example, SLC.

As `<ncc_install_user>` user, rename the folder (example: IN_SLC) back to IN.

```
cd /IN/bin
```

Run `sudo ./removeApplication.sh` to remove only the application.

Do not use **removeDatabase.sh** to remove databases in 26ai. To remove a specific database after a failed installation (for example, SCP database of SLC) or to prepare for reinstallation, follow the steps below:

```
#su – oracle
export ORACLE_SID=<CDB name used while running the
create_MultiTenantDB_structure.sh script>
sqlplus / as sysdba

SQL>Alter pluggable database SCP close immediate;
SQL>Drop pluggable database SCP including datafiles;
```

Launch the OUI installer as specified in the section *Installing NCC on the SLC Node Using the GUI* to install SLC with the SCP database and schema.

To remove any remaining NCC files after a failed installation on application nodes (SMS, SLC, or VWS):

```
cd /IN/bin

sudo ./removeApplication.sh
```

Do not run **removeDatabase.sh** on application nodes; they only use the 26ai client to connect to a remote database.

Post-installation on the Application Node (26ai Client) and the Remote Database Node (26ai Database Server)

- Create the softlinks (if not already present) on the application nodes (SMS, SLC, and VWS) running the 26ai client before running the post-installation steps.

```
cd /scratch/u01/app/oracle/product/23.0.0/lib

ln -s libclntsh.so libclntsh.so.19.1
ln -s libclntshcore.so libclntshcore.so.19.1

cd /usr/lib/oracle/21/client64/lib/ (If the path exists)

ln -s libclntsh.so libclntsh.so.19.1
ln -s libclntshcore.so libclntshcore.so.19.1
```

- If the IN_SMS folder was renamed to IN (or a softlink from IN to IN_SMS was created), update the ownership of the SMS files under /IN/service_packages to run maintenance scripts on the remote database server. Perform the following steps on the remote database server in the directories listed below.
  - SMS – All files and folder present inside this folder should have smf_oper:esg owner and group
  - CCSVCHRPART – All files and folder present inside this folder should have oracle:esg owner and group
  - CCSPART – This folder and all files and folder present inside this folder should have oracle:esg owner and group
  - CCS – All files and folder present inside this folder should have smf_oper:esg owner and group

- The following maintenance cron jobs must be set up for the oracle user on the remote database server. If they are not present, configure them as follows:
  - Switch to the oracle user on the remote database server.

```
su - oracle

crontab -e


# CDRs Partitions

30 * * * * ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSPART/bin/CCSPART_capacity_monitor.sh ) >
/IN/service_packages/CCSPART/tmp/CCSPART_capacity_monitor.sh.log 2>&1

30 7 * * * ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSPART/bin/CCSPART_log_cleaner.sh ) >
/IN/service_packages/CCSPART/tmp/CCSPART_log_cleaner.sh.log 2>&1

32 1 * * * ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSPART/bin/CCSPART_maintenance.sh ) >
/IN/service_packages/CCSPART/tmp/CCSPART_maintenance.sh.log 2>&1

0 2 * * *  ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSPART/bin/CCSPART_statistics.sh ) >
/IN/service_packages/CCSPART/tmp/CCSPART_statistics.sh.log 2>&1


# Voucher Partitions
```

```
40 * * * * ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSVCHRPART/bin/CCSVCHRPART_capacity_monitor.sh )
>
/IN/service_packages/CCSVCHRPART/tmp/CCSVCHRPART_capacity_monitor.sh.l
og 2>&1

20 7 * * * ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSVCHRPART/bin/CCSVCHRPART_log_cleaner.sh ) >
/IN/service_packages/CCSVCHRPART/tmp/CCSVCHRPART_log_cleaner.sh.log
2>&1

30 2 * * * ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSVCHRPART/bin/CCSVCHRPART_maintenance.sh ) >
/IN/service_packages/CCSVCHRPART/tmp/CCSVCHRPART_maintenance.sh.log
2>&1

0 3 * * *  ( . /IN/service_packages/CCS/.profile ;
/IN/service_packages/CCSVCHRPART/bin/CCSVCHRPART_statistics.sh ) >
/IN/service_packages/CCSVCHRPART/tmp/CCSVCHRPART_statistics.sh.log
2>&1
```

Chapter 7

Post-Installation Tasks

Overview

Introduction

This chapter describes the post-installation tasks you must perform after installing Oracle Communications Network Charging and Control (NCC).

In this chapter

This chapter contains the following topics.

About Post-Installation Tasks

Post Installation Initial Configuration Tasks

The post-installation configuration tasks set the initial configuration for each NCC node. You should perform these tasks after completing the NCC installation on all nodes.

See *Post-Installation Initial Configuration* (on page 88) for more information.

About CDR Storage Configuration Tasks

The call data records (CDRs) generated by the system will be stored in the database. On production deployments, you should configure table partitioning for the CCS_BE_CDR table to define the following:

- The number of files needed each week to store CDR data
- The number of weeks to hold CDR data before it is purged from the database
- The location for the CDR data files

For details on CDR table partitioning configuration, see *Setting Up CDR Storage* (on page 93).

Note: For more information on CDR and EDR records, and how they are generated, see *Event Detail Record Reference Guide*.

About SSL Configuration Tasks

NCC supports secure network logins through Secure Socket Layer (SSL) connections from the NCC UI to the database. You specify whether SSL connections to the database are enabled on your system by setting the `jnlp.sms.EncryptedSSLConnection` in the script (**.bat** or **.sh**). At installation, this property is set to true, and SSL connections to the database are enabled by default. To disable SSL connections to the database, set `jnlp.sms.EncryptedSSLConnection` to false. See *Disabling SSL Connections to the SMS Database* (on page 88) for more information.

If you plan to use SSL connections to the database, you must perform a number of additional configuration tasks. See *Enabling SSL Connections to the Database* (on page 94) for more information.

Disabling SSL Connections to the SMS Database

Follow these steps to disable SSL connections to the database.

Step	Action
1	Open the **smsGui.bat/smsGui.sh**, **acsGui.sh/acsGui.bat**, **vpnGui.sh/vpnGui.bat**, and **ccpGui.sh/ccpGui.bat** files on the SMS node. The **smsGui.bat/smsGui.sh**, **acsGui.sh/acsGui.bat**, and **vpnGui.sh/vpnGui.bat** files are located in the **/IN/html** directory. The **ccpGui.sh/ccpGui.bat** files is located in the **/IN/html/ccp** directory.
2	Set the `jnlp.sms.EncryptedSSLConnection` property to false by adding the following entry: **`-Djnlp.sms.EncryptedSSLConnection="false"`**
3	Save and close the file.

To test without configuring secure login, turn off the security checking in the script.

For example, set the following in the **smsGui.bat/smsGui.sh** file:

`-Djnlp.sms.EncryptedSSLConnection="false"`

Configuring Variables in Scripts

You must set the value for GPG and GPG_HOME variables in the following scripts:

- /IN/service_packages/CCS/.profile-sms
- ccsAccountWithPrivacy.sh
- ccsVoucherStartup.sh

Example:

export GPG="/bin/gpg"

export GPG_HOME="/IN/service_packages/SMS/.gnupg"

Post-Installation Initial Configuration

About Initial Configuration Tasks

Perform the following initial configuration tasks after completing the NCC installation on all nodes:

- Set up IP addresses and hostnames to servers. See *Setting IP Addresses and Hostnames* (on page 89).
- Update the tablespace storage allocation on each node in accordance with system implementation type. For example, a large production system will require greater storage allocation than a small production system. See *Update Oracle Tablespace Storage* (on page 89).
- Update Oracle SGA parameters on each node. See *Update Oracle SGA Parameters* (on page 90).
- Update the Oracle **`cpu_count`** parameter. See *Update Oracle cpu_count Parameter* (on page 90).
- Update the Oracle Database default profile password for life time. See *Update Oracle Database Default Profile Password Life Time* (on page 90).
- Set shared memory limits for the NCC system. See *Setting Shared Memory Limits* (on page 90).
- Set the number of database connections. See *Setting the Number of Connections to the Database* (on page 91).

- If you want to use Internet Protocol version 6 (IPv6) addresses, update the **eserv.config** file with the configuration for CORBA services. See *About CORBA Services Configuration for IPv6* (on page 92).

Setting IP Addresses and Hostnames

Ensure that the **/etc/hosts** file on all nodes includes entries for all hosts and their aliases. Some host aliases are automatically defined when you install NCC. Therefore, you should include at least the following predefined host entries in the **/etc/hosts** file.

- *sms_host* sms usms usms.CdrPush
- *be_host_1* be1
- *scp_host* scp uas1 acsStatsMaster uas.ccsSSMMaster
- *be_host_2* be2

where:

- *sms_host* is the IP address for the SMS node
- *be_host_1* is the IP address for the primary VWS node
- *scp_host* is the IP address for the SLC node
- *be_host_2* is the IP address for the secondary VWS node

Perform these steps on each node to set up IP addresses and hostnames for the servers.

Step	Action
1	Log in to the node.

2	Configure all network interfaces in the **/etc/hosts** file. Refer to your network plan for configuration values. See *Network Planning* (on page 6) for more information.
	Example /etc/hosts file
	`localhost`
	`127.0.0.1 localhost`
	`192.68.44.136 be1`
	`192.68.44.130 sms usms usms.CdrPush`
	`192.68.44.133 scp uas1 acsStatsMaster uas.ccsSSMMaster`
	`192.68.44.139 be2`

3	For platforms that are built on a zone server, modify the loop-back interface (lo0) and localhost entries to remove any association with the server hostname.
	For example, change the following entry from:
	`::1 pte69-zone1 localhost`
	`127.0.0.1 pte69-zone1 localhost loghost`
	to this:
	`::1 localhost`
	`127.0.0.1 localhost loghost`

4	On the SMS node, restart the smsMaster process.

Update Oracle Tablespace Storage

On each node in turn, update the tablespace storage allocation on the database instance on the node, to suit your deployment. Add or resize data files as required. See your Oracle Database administrator for information on resizing your tablespaces.

Update Oracle SGA Parameters

On each node in turn, update the Oracle SGA parameters for the database instance on the node to suit your deployment.

Update Oracle cpu_count Parameter
cpu_count specifies the number of CPUs available for Oracle Database to use. This parameter greatly affects the size of **Startup Overhead In Shared Pool** and is therefore set to **4** in the default **init.ora** files installed by NCC.

The **cpu_count** parameter may either be unset allowing Oracle Database to use all CPUs be tuned for a specific target system. Because this may increase the size of **Startup Overhead In Shared Pool**, the **shared_pool_size** parameter must be updated accordingly. The recommended initial value for **shared_pool_size** is **Startup Overhead In Shared Pool** + 256M.

The current size of the **Startup Overhead In Shared Pool** can be retrieved with the following SQL query:

```
select * from v$sgainfo where name = 'Startup overhead in Shared Pool';
```

See the chapter on configuring memory manually in *Oracle Database Administrator's Guide* for more information about specifying the shared pool size for your database.

Review Oracle lock_sga Parameter

On some hardware and operating system combinations, the lock_sga parameter may be set to TRUE to prevent System Global Area (SGA) memory swapping and paging, and so improving database performance.

Note:

- If setting lock_sga to TRUE is not supported by the hardware and operating system combination, the database may fail to start if lock_sga is TRUE. Therefore lock_sga is set to FALSE in the default init.ora files installed by NCC.
- If lock_sga is set to TRUE on systems with insufficient memory, other processes may reduce in performance due to non-SGA memory swapping.

See the chapter on tuning the System Global Area in Oracle Database Administrator's Guide for more information on the lock_sga parameter.

Update Oracle Database Default Profile Password Life Time

An Oracle database user is created for each NCC user based on the default user profile in the database. The default profile includes a password expiration duration of 180 DAYS for Oracle 19*c* databases.

When using Oracle 19*c* databases, set the default profile **PASSWORD_LIFE_TIME** parameter to **UNLIMITED** before creating NCC users to avoid login errors due to expired passwords. If your security policy requires user password changes at regular intervals you must implement a procedure allowing users to change their passwords before expiration to prevent access failure. See *Oracle Database Security Guide* for the version of Oracle database you are using for a detailed description of how to use password management and protection.

Setting Shared Memory Limits

On Linux, follow these steps on each node to set shared memory limits for the NCC system.

1. Determine the sum of process parameters for all database instances on the system, the overhead for Oracle background processes, the system and other application requirements.
2. Set semmns (total semaphores system-wide) to the larger of the value in 1 or 32000.
3. Set semmsl (semaphores per set) to 250.

4 Set semmni (total semaphore sets) to semmns/semmsl rounded up to the nearest multiple of 1024.
5 For Linux and Oracle 19c/26ai, set the maximum number of asynchronous I/O requests allowed in /etc/sysctl.conf as follows:

```
fs.aio-max-nr = 3145728
```

After changing the /etc/sysctl.conf, run the following command as root to set the values in the system:

```
# /sbin/sysctl -p /etc/sysctl.conf
```

Setting the Number of Connections to the Database

Oracle database static parameters are defined in the **initSMF.ora** file located in the **$ORACLE_HOME/dbs** directory.

The **processes** parameter in the Static Parameters section of **initSMF.ora** defines the maximum number of connections allowed to the Oracle database. For a NCC installation, set this parameter to 400 or a higher.

Example configuration in initSMF.ora

```
# Static Parameters
####################
....
processes = 400
...
```

Setting the beServiceTrigger User and Password

If you configured the `beServiceTrigger` as part of the SMS postInstallUser.sh script, then you can skip this section.

`beServiceTrigger` sends BPL requests to the NCC Open Services Development (OSD) application for event processing. The `beServiceTrigger` user allows `beServiceTrigger` to access external systems, such as a client ASP that is accessed through OSD during event processing. `beServiceTrigger` retrieves the user credentials (username and password) from a secure credentials vault on the SMS node. The credentials vault is used for storing user names and passwords securely and for authorizing users. For more information about `beServiceTrigger`, see *Voucher and Wallet Server Technical Guide*.

If you want to use `beServiceTrigger` for sending real time wallet notifications to OSD, set the `beServiceTrigger` user credentials by using the `beServiceTriggerUser` utility. To enable `beServiceTrigger` to connect to the OSD interface on the SLC, set the user and password for `beServiceTrigger` and the OSD client ASP to be the same.

Follow these steps to set the `beServiceTrigger` username and password.

Step	Action
1	Log in to the SMS as `smf_oper` user.
2	Go to the following directory, where the `beServiceTriggerUser` utility is located: `/IN/service_packages/E2BE/bin`
3	Run the following command to set the username and password for `beServiceTrigger`: `beServiceTriggerUser -d/@SMF`
4	Restart the SLEE on the VWS by running the following command as `smf_oper` user: `/IN/service_packages/SLEE/bin/slee-ctrl restart`

About CORBA Services Configuration for IPv6

The **/IN/service_packages/eserv.config** file on the SMS defines configuration for NCC.

/IN/service_packages/eserv.config

If you are using IP version 6 addresses, you must include the CorbaServices section in the **eserv.config** file. If you are using only IP version 4 addresses, the procedure in this section is optional.

The CorbaServices section in the **eserv.config** configuration file on the SMS node defines common connection parameters for CORBA services. The CorbaServices configuration overrides the default and command-line values specified for CORBA listen ports and addresses. You configure the CorbaServices section of the **eserv.config** file on the SMS by using the following syntax:

```
CorbaServices = {
    AddressInIOR = "hostname"
    smsTaskAgentOrbListenPort = port
    smsReportDaemonOrbListenPort = port
    smsTrigDaemonOrbListenPort = port
    ccsBeOrbListenPort = port
    OrbListenAddresses = [
        "ip_address1",
        "ip_address2",
]
}
```

where:

- *hostname* is the hostname or IP address to place in the IOR (Interoperable Object Reference) for the CORBA service.
- *port* is the number of the port on which the CORBA service will listen.
- *ip_address1,ip_address2* list the IP addresses on which CORBA services listen for incoming requests. The list of IP addresses in the `OrbListenAddresses` parameter can include both IP version 6 and IP version 4 addresses.

  If the `OrbListenAddresses` parameter is not set, or you do not specify any IP addresses, the CORBA service listens on all the IP addresses available on the host. Loopback IP addresses and special IP addresses, as defined in RFC 5156, are excluded.

For more information about configuring CORBA services, see *NCC Service Management System Technical Guide*.

Example CORBA Services Configuration on the SMS

The following example shows the CorbaServices configuration section in the **eserv.config** file for CORBA services on the SMS node.

```
CorbaServices = {
    AddressInIOR = "sms_machine.oracle.com"
    OrbListenAddresses = [
        "2001:db8:0:1050:0005:ffff:ffff:326b"
        "192.0.2.0"
    smsTaskAgentOrbListenPort = 6332
    smsReportDaemonListenPort = 6333
    smsTrigDaemonOrbListenPort = 6334
    ccsBeOrbListenPort = 6335
}
```

Setting Up CDR Storage

About CDR Storage Configuration

If you installed NCC in a production environment, configure CDR table (CCS_BE_CDR) partitioning to define how CDRs will be stored.

Note: We cannot partition CDR table if the SMS node is on remote database because partitioning requires DBA privilege.

Setting Up CDR Table Partitioning

Follow these steps to set up CDR table partitioning for CDR storage.

Step	Action
1	As the root user on the SMS node, edit the **/IN/service_packages/CCSPART/etc/ccspart.cfg** file.
2	Specify appropriate values for these parameters: • **WEEKLY_DATAFILE_COUNT**: Specify the number of 200 MB data files required per week to hold CDR data. Note: CDR data files may contain multiple CDR records, potentially of different types. • **WEEKS_TO_KEEP_PARTITION**: Specify the number of weeks CDR data should remain available on the SMS node before being purged from the database. • **DATAFILE_PATH**: Specify the location on the disk where CDR data files will be created. • **WEEKS_TO_KEEP_ONLINE:** Specify the number of weeks to keep partitions online from current week before moving them to READ ONLY.

Setting Up Voucher Storage

About Voucher Storage Configuration

If you installed NCC in a production environment, configure voucher table (CCS_VOUCHER_REFERENCE) partitioning to define how vouchers will be stored.

Note: You cannot partition voucher table if the SMS node is on remote database because partitioning requires DBA privilege.

Setting Up Voucher Table Partitioning

Follow these steps to set up voucher table partitioning for voucher storage.

Step	Action
1	As the root user on the SMS node, edit the **/IN/service_packages/CCSVCHRPART/etc/ccs_voucher_reference_part.cfg** file.

Step	Action
2	Specify appropriate values for these parameters: • **WEEKLY_DATAFILE_COUNT**: Specify the number of 200 MB data files required per week to hold voucher data. Note: Voucher data files may contain multiple voucher records, potentially of different types. • **WEEKS_TO_KEEP_PARTITION**: Specify the number of weeks voucher data should remain available on the SMS node before being purged from the database. • **DATAFILE_PATH**: Specify the location on the disk where voucher data files will be created.

Enabling SSL Connections to the Database

About SSL Connections to the Database

NCC supports secure network logins through Secure Socket Layer (SSL) connections from the NCC UI to the database.

To configure SSL connections to the database, perform the following steps on the SMS node:

Step	Action
1	Create the Oracle wallet that identifies the database server. See About Creating the Oracle Wallet.
2	Update the **listener.ora** file to define the location of the Oracle wallet and the listen port for SSL connections to the database. See *Updating the listener.ora file* (on page 97).
3	Update the **sqlnet.ora** file to define the location of the Oracle wallet. See *Updating the sqlnet.ora file* (on page 99).
4	The NCC installation automatically sets the Java application properties to enable SSL connections to the database. Check the configuration in your .sh/,bat files to ensure that configuration has been set correctly. See *About Java Applet Configuration* (on page 102).
5	Clear the temporary Internet files from the Java cache.

Setting Up the Oracle Wallet to Use Self-Signed Certificates

Follow these steps to set up the Oracle server wallet to use self-signed certificates by using **setupOracleWallet.sh**.

Step	Action
1	Log in to the SMS as oracle user.
2	Run the following command: **`/IN/service_packages/SMS/bin/setupOracleWallet.sh`**
3	Answer *y* to the following prompt: `Do you wish to proceed with the configuration (y/n):`

Step	Action
4	When requested, enter the following information: • The base directory for the Oracle wallet • The two-letter international country (ISO) code for your country • The wallet password to use for the root CA wallet and the server wallet. You will be prompted for the password each time the wallet is accessed. **Note:** Wallet passwords have length and content validity checks applied to them. Generally, passwords should have a minimum length of eight characters and contain alphabetic characters combined with numbers and special characters.
5	Answer *y* to the following prompt: `Would you like to use a self-signed root certificate to sign the SMS server certificate?` When processing completes, the self-signed root certificate is exported to the following file: **./root/b64certificate.txt** **./root** is a sub-directory of the base directory for the Oracle wallet. You must import this certificate into the Java **lib\security\cacerts** file on each client PC.

Adding Trusted Certificates to the Keystore on Client PCs

If you are using self-signed certificates, update the keystore on client PCs to trust certificates from the SMS server that have been signed by the root CA.

Note: Certificates signed by a commercial CA are already trusted by definition, therefore update the keystore on client PCs only if you are using self-signed certificates.

Follow these steps to add a trusted certificate for the SMS server to the Java keystore on a client PC.

Step	Action
1	Copy the root CA certificate **./root/b64certificate.txt** to the client PC.
2	As an Administrator user on the client PC, open the command tool window and run the following command: **keytool -importcert -keystore "***cacerts_path***\java\lib\security\cacerts" -alias SMS -file "***path***\\b64certificate.txt"** where *cacerts_path* is the path to the **java\lib\security\cacerts** file and *path* is the location of the certificate file on the client PC.
3	When prompted, enter the password for the keystore. **Note:** The Java installation sets the keystore password to **changeit** by default.
4	Answer yes to the following prompt: `Trust this certificate? [no]:` Oracle keytool updates the keystore on the client PC to trust certificates from the SMS server that have been signed with the root CA.

Setting Up the Oracle Wallet to Use CA-Signed Certificates

Note: This procedure assumes that the commercial CA's own root certificate is available in the following file:

./root/b64certificate.txt

./root is a sub-directory of the base directory for the Oracle wallet.

Follow these steps to set up the Oracle server wallet to use certificates signed by a commercial CA by using **setupOracleWallet.sh**.

Step	Action
1	Log in to SMS as the oracle user.
2	Run the following command: **/IN/service_packages/SMS/bin/setupOracleWallet.sh**
3	Answer `y` to the following prompt: `Do you wish to proceed with the configuration (y/n):`
4	When requested, enter the following information: • The base directory for the Oracle wallet • The two-letter international country (ISO) code for your country • The password to use for the server wallet. You will be prompted for the password each time the wallet is accessed. **Note:** Wallet passwords have length and content validity checks applied to them. Generally, passwords should have a minimum length of eight characters and contain alphabetic characters combined with numbers and special characters.
5	Answer `n` to the following prompt: `Would you like to use a self-signed root certificate to sign the SMS server certificate?` The script creates the server auto login wallet and exports the certificate-signing request to the following file: **./server/creq.txt** **./server** is a sub-directory of the base directory for the Oracle wallet.
6	Send the certificate-signing request to the commercial CA for signing.
7	When the commercial CA returns the signed certificate, place the signed certificate in the following file: **./server/cert.txt**
8	Place the root certificate from the commercial CA in the following file: **./root/b64certificate.txt**
9	Log in as the oracle user on the SMS and run the following command: **/IN/service_packages/SMS/bin/setupOracleWallet.sh** `-s` **./server/cert.txt** `-t` **./root/b64certificate.txt** `-w` *wallet_base_directory* • **./server/cert.txt** specifies the location of the signed server certificate • **./root/b64certificate.txt** specifies the location of the root certificate from the commercial CA • *wallet_base_directory* specifies the Oracle wallet base directory The **setupOracleWallet.sh** script completes by adding the trusted CA certificate and the CA-signed certificate to the server wallet.

Updating the listener.ora file

Follow these steps to configure the Oracle listener.

Step	Action
1	Log in to SMS as the `oracle` user, or run the following command from a root login to become the user `oracle`: `su - oracle` **Note:** Logging in as the `oracle` user ensures that the path to all of the Oracle binaries is correct and that file ownership for Oracle files is preserved.
2	Go to the directory containing the **listener.ora** file. The location of the **listener.ora** file depends on the version of Oracle Database installed and the options selected at installation. It is located in one of the following directories by default: *ORACLE_HOME*`/network/admin` `/var/opt/oracle/` where *ORACLE_HOME* is the directory in which your Oracle Database is installed.
3	Edit the **listener.ora** file by using a text editor such as vi; for example: `vi listener.ora`

4	Add a new description to the listener description list that specifies the protocol and port to use for secure SSL connections to the database. You must set `PROTOCOL` to **TCPS** and `PORT` to **2484** for secure SSL connections.
	Use the following syntax:
	`LISTENER=`
	`  (DESCRIPTION_LIST =`
	`  (DESCRIPTION=(ADDRESS_LIST=`
	`  (ADDRESS=`
	`  (PROTOCOL=TCPS)`
	`  (HOST=`*hostname*`)`
	`  (PORT=2484)`
	`  )))`
	`)`
	where *hostname* is the hostname of the SMS node.
	Note: The standard Oracle listener TCP port is 1521. However, SSL connections use the standard port for the TCPS protocol, port 2484, instead. The TCPS protocol entry in the **listener.ora** file must appear *after* the TCP protocol entry.
	Note: If there is a firewall between screen clients and the SMS, you must open port 2484 in the firewall.

Step	Action

Example:

The following example shows DESCRIPTION_LIST configuration for an SMS node called “hostSMP”:

```
LISTENER=
  (DESCRIPTION_LIST =
  (DESCRIPTION=(ADDRESS_LIST=
     (ADDRESS=
         (PROTOCOL=IPC)
         (KEY=SMF)
        )))
  (DESCRIPTION=(ADDRESS_LIST=
     (ADDRESS=
         (PROTOCOL=TCP)
         (HOST=hostSMP)
         (PORT=1521)
        )))
  (DESCRIPTION=(ADDRESS_LIST=
     (ADDRESS=
         (PROTOCOL=TCPS)
         (HOST=hostSMP)
         (PORT=2484)
        )))
     )
)
```

Note: For the SMF database, ORACLE_SID has been set to SMF. The listener can be made aware of this by adding an ADDRESS entry to ADDRESS_LIST.

5 Add a new `WALLET_LOCATION` entry that specifies the directory that contains the server wallet that was created by **setupOracleWallet.sh**.

Use the following syntax:

```
WALLET_LOCATION =
     (SOURCE =
         (METHOD = FILE)
         (METHOD_DATA = (DIRECTORY = directory_name))
)
```

where *directory_name* is the Oracle server directory.

Example

The following example shows a `WALLET_LOCATION` configuration for the Oracle server wallet created in the directory named **/u01/app/wallets/oracle/server**

```
WALLET_LOCATION =
     (SOURCE =
         (METHOD = FILE)
         (METHOD_DATA = (DIRECTORY =/u01/app/wallets/oracle/server))
)
```

Step	Action

6	Add the following entries:
	`SSL_CLIENT_AUTHENTICATION=FALSE`
	`SSL_CIPHER_SUITES=(TLS_RSA_WITH_AES_128_CBC_SHA)`
	Notes: You must also:
	• Configure the same entries for `WALLET_LOCATION`, `SSL_CLIENT_AUTHENTICATION`, and `SSL_CIPHER_SUITES` in the **sqlnet.ora** file.
	• Set the `jnlp.sms.sslCipherSuites` in the script and the `SSL_CIPHER_SUITES` parameter to the same value.

7	Save and close the file.

8	Stop and restart the listener using the updated configuration by running the following commands:
	`lsnrctl stop`
	`lsnrctl start`

Updating the sqlnet.ora file

Follow these steps to configure the Oracle **sqlnet.ora** file for SSL connections to the database.

Note: You must configure new entries for WALLET_LOCATION, SSL_CLIENT_AUTHENTICATION, and SSL_CIPHER_SUITES in the **sqlnet.ora** file that are the same as those configured in the **listener.ora** file.

Step	Action
1	Log in to the SMS as the `oracle` user, or run the following command from a root login to become the `oracle` user: `su - oracle` **Note:** Logging in as the `oracle` user ensures that the path to all Oracle binaries is correct and that file ownership for Oracle files is preserved.
2	Go to the directory containing the **sqlnet.ora** file. The location of the **sqlnet.ora** file depends on the version of Oracle database installed and the options selected at installation. It is located in one of the following directories by default: *ORACLE_HOME*/**network/admin** **/var/opt/oracle/** where *ORACLE_HOME* is the directory in which the Oracle database is installed.
3	Edit the **sqlnet.ora** file by using a text editor such as vi; for example: `vi sqlnet.ora`

4	Add a new WALLET_LOCATION entry that specifies the directory of the server wallet that was created by **setupOracleWallet.sh**.
	Use the following syntax:
	`WALLET_LOCATION =`
	`(SOURCE =`
	`(METHOD = FILE)`
	`(METHOD_DATA = (DIRECTORY = directory_name))`
	`)`
	where *directory_name* is the Oracle server directory.

Step	Action

	Example
	The following example shows a WALLET_LOCATION configuration for the Oracle server wallet created in the directory named **/u01/app/wallets/oracle/server**
	`WALLET_LOCATION =`
	`(SOURCE =`
	`(METHOD = FILE)`
	`(METHOD_DATA = (DIRECTORY =/u01/app/wallets/oracle/server))`
	`)`

5	Add the following new entries:
	`SSL_CLIENT_AUTHENTICATION=FALSE`
	`SSL_CIPHER_SUITES=(TLS_RSA_WITH_AES_128_CBC_SHA)`

6	Save and close the file.

Updating the eserv.config file

The default /IN/service_packages/eserv.config file on the VWS contains placeholder variables that need to be changed to actual values before the application can startup.

Parameter	Usage
${OUI_BE_SERVER_ID}	The VWS billing engine domain number this node belongs to. **Note**: Creating a domain is a manual activity following the NCC installation.
${OUI_SLC_HOST}	The SLC hostname of the node running OSD services. This enables notifications to be generated from the VWS to be sent by the SLC to the external network.

Note: All affected parameters can be auto populated by the /IN/bin/postiInstallUser.sh script on the VWS. If you select to use this procedure, then you are required to have

- A fully installed SMS node.
- Each VWS node is already defined in the replication configuration on the SMS.
- The VWS billing engine domain is defined in the CCS configuration on the SMS.

Configure SEI in the SLC Node

(Optional) Configure SEI in the SLC node. See the discussion about SEI configuration in *SMS Email Interface Technical Guide.*

Configuring Replication and Table Nodes

One way to configure replication is through the SMS screens.

To configure replication nodes and tables, see the discussion about replication nodes in *Service Management System User Guide*.

Note: Replicate the smf_normalization, smf_denormalization, and smf_seed tables on the SLC and VWS nodes for the slee processes to load Credential Vault data.

The NCC installer also provides a command line utility script to create a replication node on a fully operational SMS node. This avoids using the SMS screens. Run the script as the NCC_runtime_user:

/IN/bin/addReplicationNode.sh -n <node_number> -h <host_name> [-p <primary ip address>] [-s <secondary ip address>] [-d <description>]

-n <node_number>	Mandatory	Unique replication node id of the slave. Must be between 301 and 399. 301 - 349 defines SLC node. 350 - 399 defines VWS node.
-h <host_name>	Mandatory	Unqualified hostname of the replication slave.
-p <primary ip address>	Optional	Either IP address or hostname of the slave node. If not supplied, will use the -h parameter.
-s <secondary ip address>	Optional	Secondary IP address or hostname of slave node. No default value. This can be null.
-d <description>	Optional	Node description.

Note:

- The script does not validate either the hostname or ip address.
- When configuring SLC nodes an attempt to initiate a full replication resync will occur. The resync will fail if the SLC node is not installed or the updateLoader is not running on the SLC. The configuration will persist and a resync can be attempted at a later date by the user.
- If you require spaces in the description then use quotes round the entire string.

A replication node can be removed using a further utility script. Run the script as the NCC_runtime_user.

/IN/bin/removeReplicationNode.sh -n <node_number>

-n <node_number> mandatory. Node number.

Creating an ACS Customer

To create an ACS customer, see the discussion about creating an ACS customer in *Advanced Control Services User Guide*.

Creating a Domain

One way to configure the domain is through the SMS screens.

To create a domain, see the discussion about domain in *Charging Control Services User Guide.* After creating a new domain, restart the SMS screen and create **`replication.config`** file. To create **`replication.config`** file, see the discussion about Table Replication in *Charging and Control Service Management System User's Guide*.

The NCC installer also provides a command line utility script to create a domain on a fully operational SMS node. This avoids using the SMS screens. Run the script as the NCC_runtime_user:

/IN/bin/addUbeDomain.sh -n <name> -m <max_accounts> [-c] [-v] [-t] [-a]

-n <name> mandatory. Domain name.

-m <max_accounts> mandatory. Maximum number of accounts allowed.

-c optional. Defines a charging domain.

-v optional. Defines a voucher domain.

-t optional. Defines a tracking domain.

-a optional. Sets all the -c -v -t parameters.

Note: The domain is not fully created at this point.

Each VWS node configured is required to be assigned to the billing domain. Run the script as the NCC_runtime_user:

```
/IN/bin/addUbeDomainNode.sh -d <domain_name> -m <node_name> -n <node_number>
[-a <address>] [-r <remote_db>] [-s <oracle_sid>] [-c <client_port>] [-i
<internal_port>]
```

-d <domain_name> mandatory. Domain name.

-m <node_name> mandatory. Node name.

-n <node_number> mandatory. The replication node id. Must be between 350 and 399.

-a <address> optional. The hostname or ip address of the node, derived from the node number if not supplied.

-r <remote_db> optional. Hostname of the remote database, only supply if database node is not on target node.

-s <oracle_sid> optional. Oracle SID on remote database, default E2BE.

-c <client_port> optional. Client port, default 1500.

-i <internal_port> optional. Internal port, default 1600.

Note: The domain is not fully created at the point.

To finalize the domain configuration and establish replication to each node in the domain, run the script as the NCC_runtime_user:

```
IN/bin/addUbeDomainReplication.sh -d <domain_name> -p <primary_node_id> [-s
<secondary_node_id>]
```

-d <domain_name> mandatory. Domain name.

-p <primary_node_id> mandatory. Primary node replication id.

-s <secondary_node_id> optional. Secondary node replication id.

Note: The script will attempt to initiate a full replication resync. The resync will fail if the VWS node is not installed or the updateLoader is not running. The configuration will persist and a resync can be attempted at a later date by the user.

Changes by the addUbeDomainReplication.sh script can be undone. Run the script as the NCC_runtime_user:

```
/IN/bin/removeUbeDomainReplication.sh -d <domain_name>
```

<domain_name> mandatory. Domain name.

Creating a MFILE

To create the MFILE, see the discussion about MFILE generation in *Charging Control Services User Guide*.

About Java Applet Configuration

To enable secure SSL connections to the database, the following Java application configuration must be set in the **acsGui.sh/acsGui.bat**, **ccpGui.sh/ccpGui.bat**, **smsGui.sh/smsGui.bat**, and **vpnGui.sh/vpnGui.bat** files.

Follow these steps to configure the Java applet parameters for the secure SSL connections to the database if they have not been configured by the installation.

Step	Action
1	Log in as the root user.
2	Edit the **acsGui.sh/acsGui.bat**, **ccpGui.sh/ccpGui.bat**, **smsGui.sh/smsGui.bat**, and **vpnGui.sh/vpnGui.bat** files by using a text editor such as vi; for example: **`vi /IN/html/smsGui.sh`** **or** **`vi /IN/html/smsGui.bat`** The **acsGui.sh/acsGui.bat**, **smsGui.sh/smsGui.bat**, and **vpnGui.sh/vpnGui.bat** files are located in the **/IN/html/** directory. The **ccpGui.sh/ccpGui.bat** file is located in the **/IN/html/ccp** directory.
3	Configure the `secureConnectionDatabaseHost` Java property value in the resources section of the **.sh** or **.bat** file. Set PROTOCOL to **TCPS** and set PORT to **2484**. The property values must be all on one line in the **.sh** or **.bat** file: **`-Djnlp.sms.secureConnectionDatabaseHost="(DESCRIPTION= (ADDRESS_LIST= (ADDRESS=(PROTOCOL=TCPS) (HOST=`*`host_ip_addr`*`)(PORT=2484))) (CONNECT_DATA= (SERVICE_NAME=`*`db_sid`*` )))"`** where: • *`host_ip_addr`* is the host name or IP address of the SMS node • *`db_sid`* is the database SID
4	Set the `EncryptedSSLConnection` property in the resources section of the **.sh** or **.bat** file to *true*: **`-Djnlp.sms.EncryptedSSLConnection="true"`**
5	Set the `sslCipherSuites` property in the script file to TLS_RSA_WITH_AES_128_CBC_SHA: **`-Djnlp.sms.sslCipherSuites="(TLS_RSA_WITH_AES_128_CBC_SHA)"`**
6	Save and close the file.

Chapter 8

NCC Post Template Installation Tasks

Overview

Introduction

This chapter provides information about service templates. It describes the additional tasks you must perform before the template configuration will be fully operational.

Note: If you did not select a template service configuration in the Installation Manager then you should perform the *Post-Installation Tasks* (on page 87) only.

For information about configuring the system, see *Configuration User's Guide*.

In this chapter

This chapter contains the following topics.

About Post Installation Tasks

Service Template Post Installation Tasks

This table lists the post installation tasks that you perform after installing the Prepaid Charging Service Template (PCST) configuration

Note: "Yes" in a column indicates that you should perform this task for this service template configuration. "No" in a column indicates that you should not perform this task for this service template configuration.

Post Install Task to Perform	NCC and PCST
SMS Node Configuration (on page 106)	Yes
OSD Configuration (on page 118)	Yes
Configuration Files on the SMS (on page 122)	Yes

Post Install Task to Perform	NCC and PCST
VWS Node Configuration (on page 124)	Yes
MFile Generation (on page 127)	Yes
Starting the SLEE on the VWS (on page 130)	Yes
SLC Node Configuration (on page 130)	Yes
Messaging Manager Configuration (on page 130)	Yes
Messaging Manager Scheme Configuration (on page 132)	Yes
M*M SMSCs Configuration and Node Mapping* (on page 137)	Yes
SCTP Configuration (on page 141)	Yes
Sigtran Configuration (on page 141)	Yes
eserv.config *Configuration on the SLC* (on page 143)	Yes
Configuring and Starting the SLEE (on page 145)	Yes

SMS Node Configuration

About SMS Node Configuration

This section describes the minimum configuration tasks you should perform on the SMS node. You perform these tasks in the Service Management System UI:

- Configure the node details for all NCC nodes.
- Configure the nodes that will be used by the replication processes.
- Configure the resource limits and global business prefix for the service provider.
- Configure the VWS domains. In a standard configuration, a pair of VWS (primary and secondary) servers is used.
- Add VWS pair details to the VWS domains.
- Configure the replication tables used in replicating data to nodes.

Launching SMS Using Java

Follow these steps to launch Service Management System using Java:

- Ensure the Java SE Runtime Environment version 21 is installed on your computer.
- 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) in **/IN/html** directory of SMS node.
- In Windows, run **smsGui.bat** to run the application.
- On other machines:
  - Change the permission of **smsGui.sh** using `chmod 755 smsGui.sh` command.
  - Run the application using `bash smsGui.sh` command.
- The SMS Login window will appear.

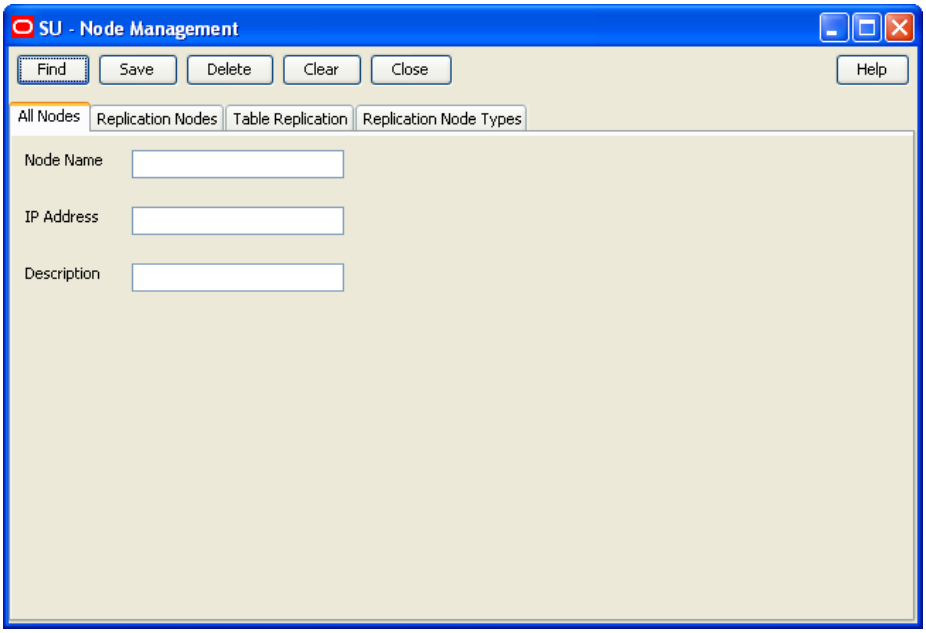
Logging On To SMS

Follow these steps to log on to the SMS from the SMS Login screen.

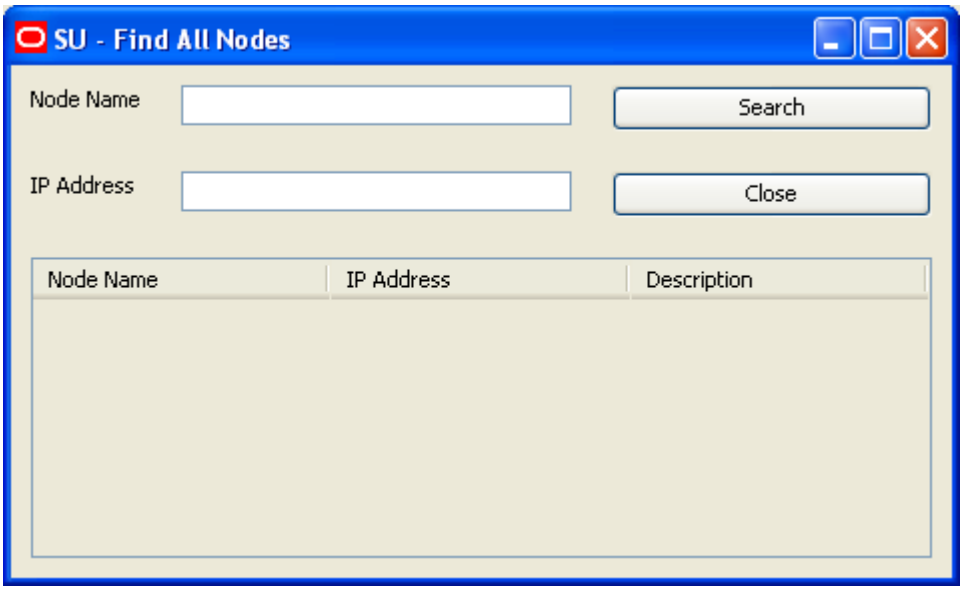
Step	Action
1	In the **User Name** field, enter **su**.
2	In the **Password** field, enter the password for the SU user. Passwords are case sensitive. **Note:** This will be the password that you specified for the SU users on the **Environment** tab in the Installation Manager window.
3	Click **OK**. **Result:** A security warning will pop up.
4	Click **Run**.

Configuring Node Details

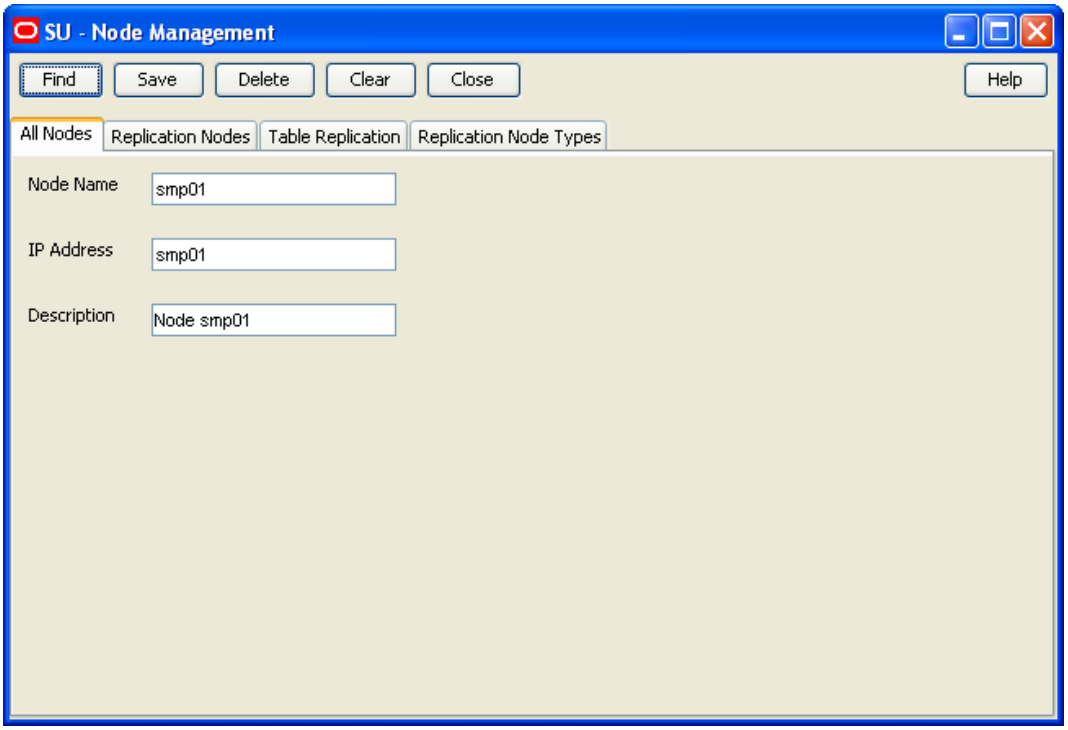
Follow these steps to configure the details for all nodes.

Step	Action
1	In the Service Management System UI, select **Operator Functions > Node Management**. **Result:** You see the **All Nodes** tab in the Node Management screen.  **Note**: For remote database installation, the SMS application host details are not available on the Node Management screen. Add the SMS application host details: • **Node Name**: Short name of the SMS application host • **IP Address**: IP address of the SMS application host • **Description**:<Any relevant Text> Click **Save** to add the SMS application host details.

Step	Action
2	Click **Find**. **Result:** You see the Find All Nodes screen.



3	Click **Search**. **Result:** You should see an entry for the SMS node in the node table.
4	Select the node on the table and click **Close**. **Result:** You see the node details on the **All Nodes** tab.



5	Verify the node details and make any necessary changes.

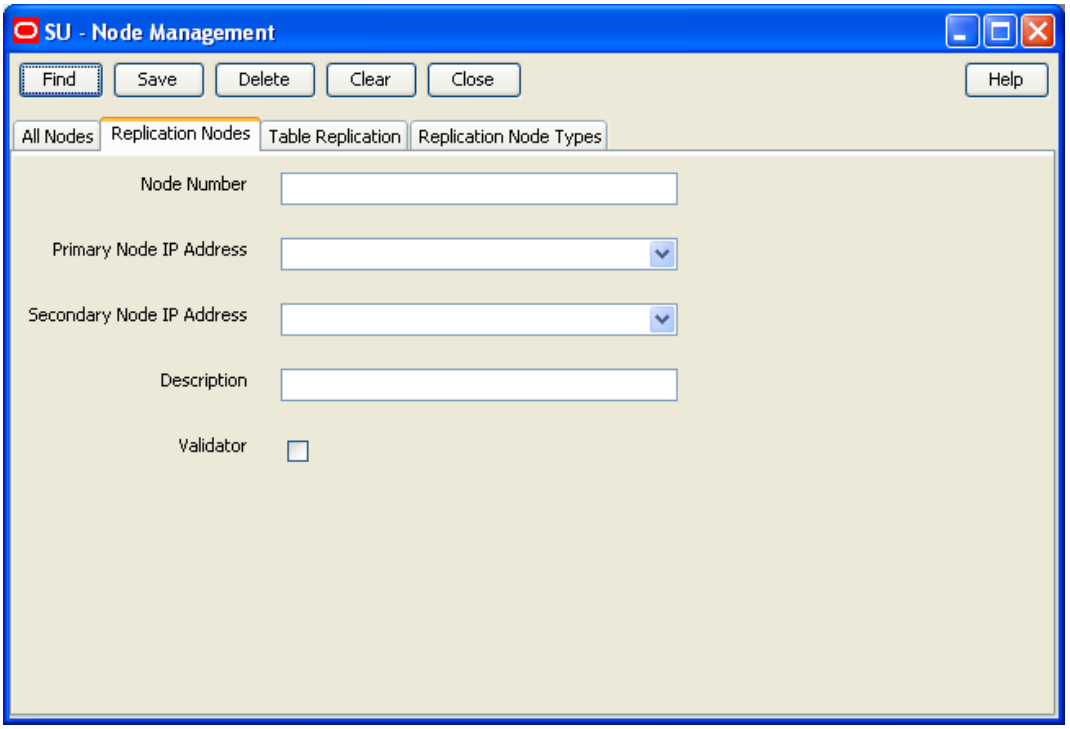
Note: You should use the Internal IP Address for the node or hostname. If you use the hostname, then this must resolve to the correct internal IP address for the node.

Step	Action
6	Click **Save**.
	Note: If you are unable to save the node details after making changes to the **IP Address** field, then you will need to delete the existing record and create a new one.
7	Repeat steps 2 through 6 for all other nodes. To clear field values before adding another node, click **Clear**.

Configuring Replication Nodes

Follow these steps to configure the nodes used in replication.

Step	Action
1	Select the **Replication Nodes** tab in the Node Management screen.



2	Enter the replication node information, referring to the table you created during *Replication Planning* (on page 7). In the **Node Number** field, enter the replication node ID. For example, for the primary SMS node you are configuring, enter **1**.
3	Select the corresponding internal IP address from the **Primary IP** drop down list.
4	Enter the node description in the **Description** field.
5	If you are configuring the SMS node, select the **Validator** check box. For all other nodes this box should not be selected.
6	Click **Save**.

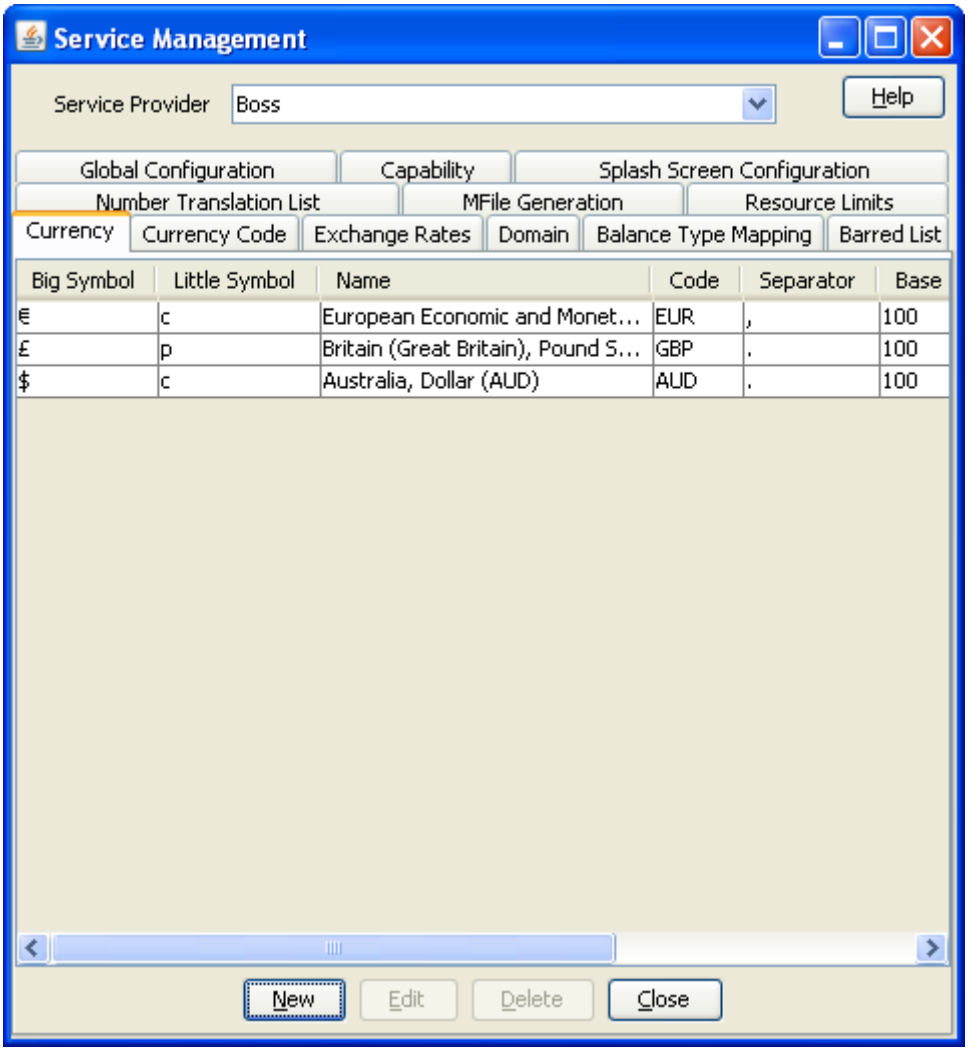
Step	Action
7	Repeat steps 2 to 6 for all the other nodes, skipping step 5 for SLC and VWS nodes. **Tip:** Use the Find screen for replication nodes to review replication node configuration. For further information on replication configuration, refer to the *Service Management System User's Guide*. **Note**: For a remote database setup, do the following: Click **Find** on the **Replication Nodes** tab. Enter **1** in **Node Number** field. Click **Search**. Select the Node Number 1 entry from the results. Select Close Change the **Primary Node IP Address** to the SMS application host IP address configured earlier. Click **Save**.

Configuring Resource Limits

Follow these steps to configure resource limits. You must set resource limits for your service provider before you create VWS domains.

Step	Action
1	From the **Services** menu in the Service Management System UI, select **Prepaid Charging > Service Management.** **Result:** You see the Service Management screen.

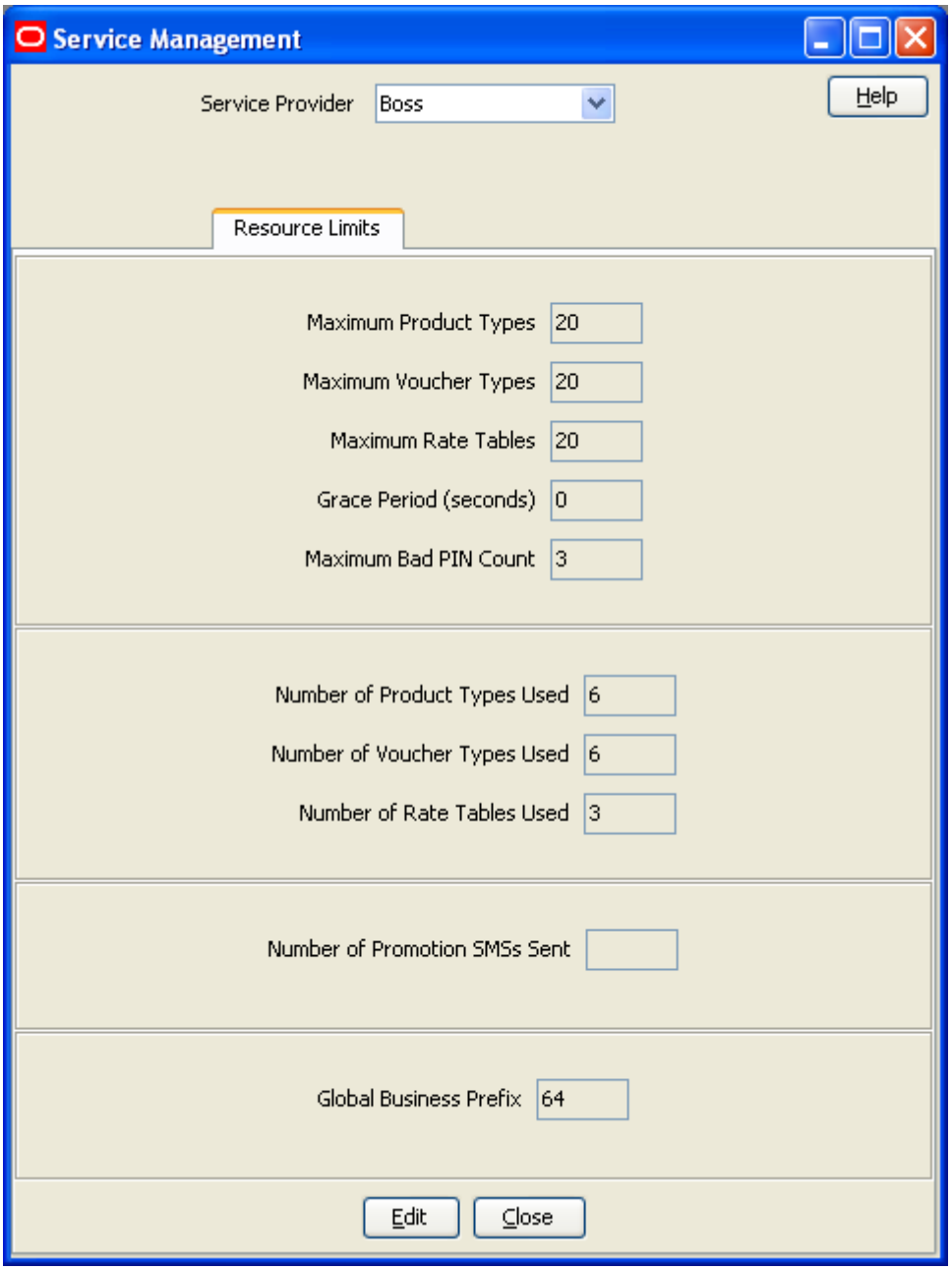
Step	Action



2 Select the **Resource Limits** tab.

Result: You see the **Resource Limits** tab on the Service Management screen.

Step	Action



3 Select the service provider for whom you want to set resource limits.

Note: The default service provider for the PCST is `OCNCCtemplate`.

4 Click **Edit**.

5 Select the **Limits** option and specify the service provider's limits for the following:

- Maximum Product Types
- Maximum Voucher Types
- Maximum Rate Tables
- Grace Period (period of time in seconds before a call begins to be charged)
- Maximum Bad Pin Count

Step	Action
6	Select the **Business Prefix** option, and specify the **Global Business Prefix** for the service provider.
7	Click **Save**.
	Note: This defines the minimum configuration for service provider limits.

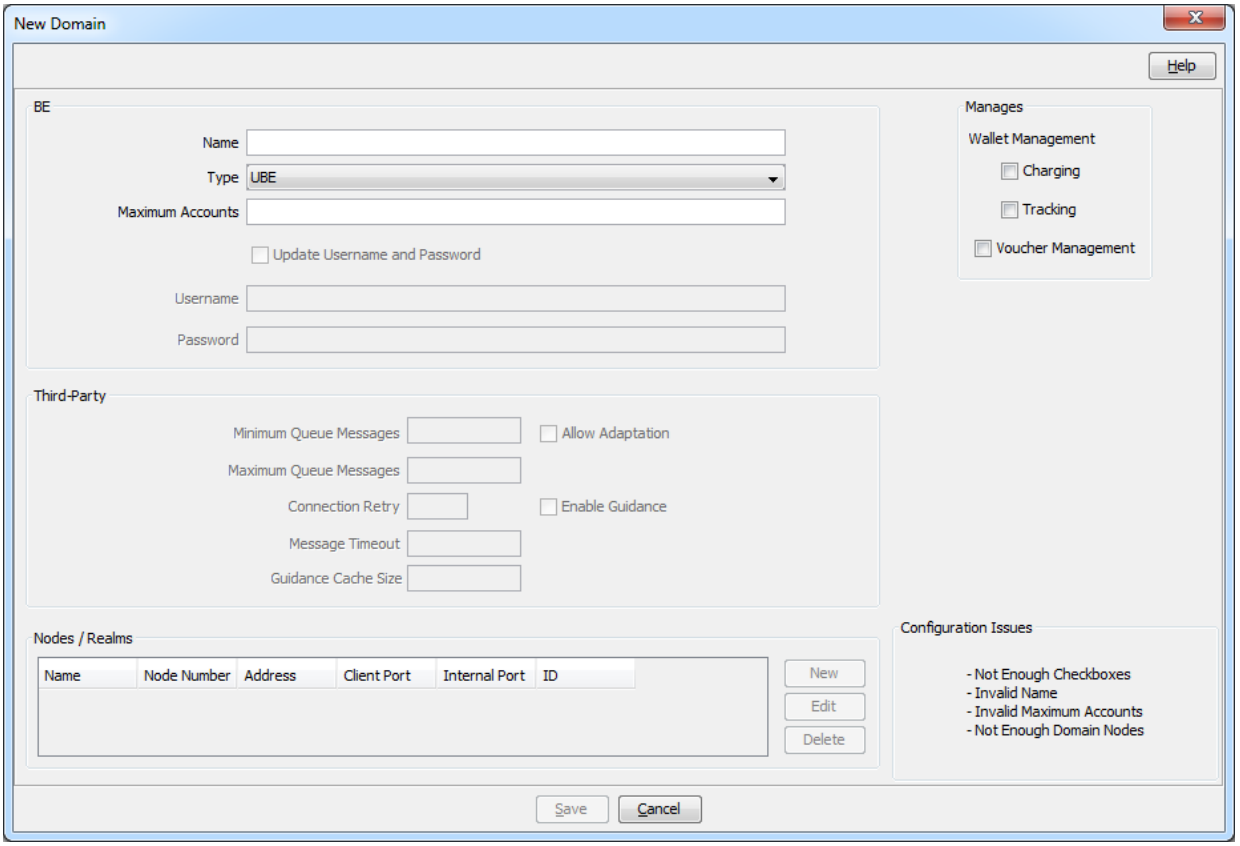
Configuring VWS Domains

Follow these steps to configure the VWS domains. For each domain you will need to define a pair of servers (a primary VWS and a secondary VWS).

Step	Action
1	From the **Services** menu in the Service Management System UI, select **Prepaid Charging > Service Management.**
2	Select the service provider for whom you want to configure the VWS domain.
	Note: The default service provider for the PCST is `OCNCCtemplate`.
3	Select the **Domain** tab, and click **New**. **Result:** The *New Domain screen* (See example on page 114) appears.
4	Enter the domain name in the **Name** field. For example, enter **`VWS Domain 1`**.
5	From the **Type** drop down list, select `UBE`.
6	Specify the maximum number of accounts this domain will be able to handle in the **Maximum Accounts** field. For example, enter **`1000000`**.
7	In the **Manages** section, select **Charging**, **Tracking** and **Voucher Management**.
8	In the **Nodes** section, add the primary and secondary nodes. See *Adding node details* (on page 114) for details.
9	Click **Save**.
10	Repeat steps 3 through 9 for each VWS domain. For more information on domains, refer to *Service Management* in *Charging Control Services User's Guide*.

Example New Domain Screen

Here is an example New Domain screen.

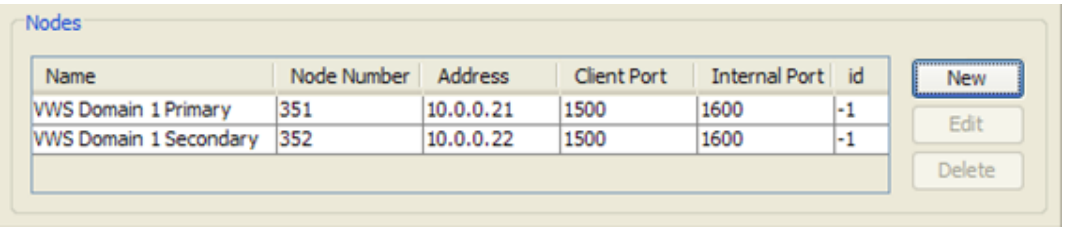


Adding Node Details

Follow these steps to add primary and secondary nodes to a VWS domain.

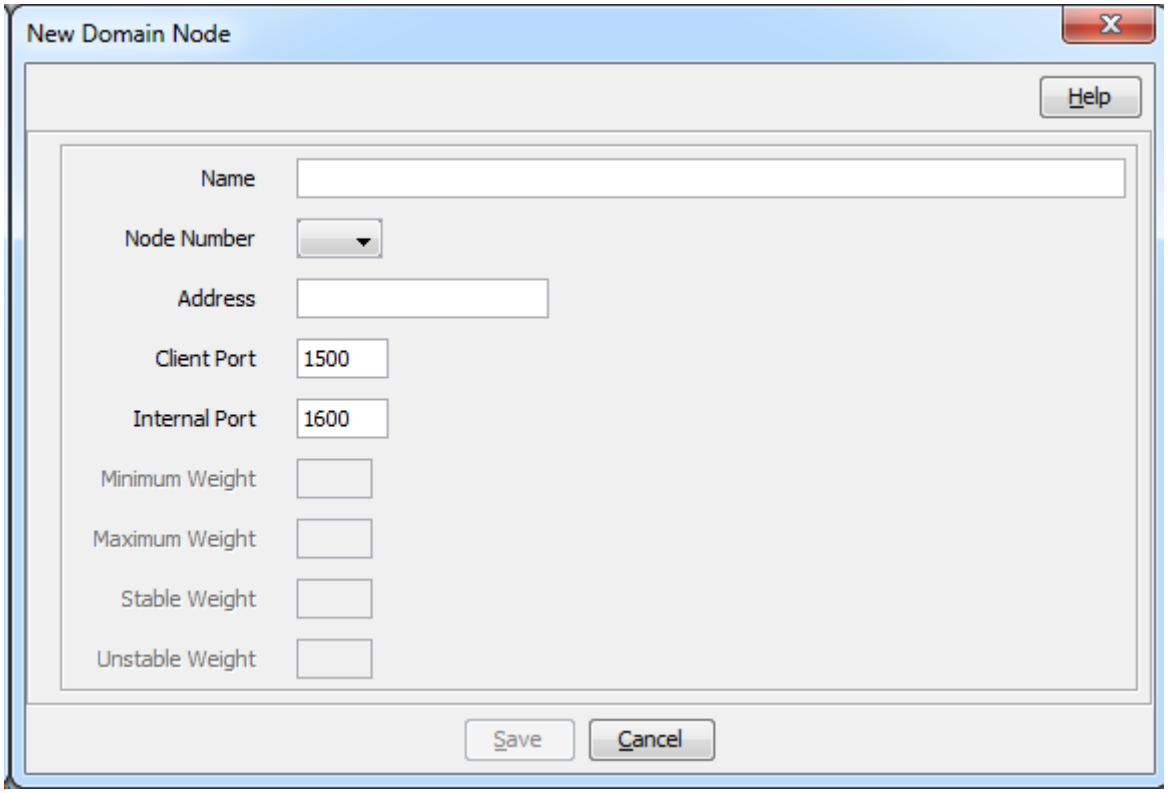
Step	Action
1	From the Nodes section of the New Domain screen, click **New**. **Result:** The *New Domain Node screen* (See example on page 115) appears.
2	Enter the node name in the **Name** field, for example, **`VWS Domain Primary`**. You must enter a unique name.
3	Select the **Node Number** from the drop down list. This will be the corresponding replication node ID for this VWS node. **Note:** Where there is more than one node for a domain, the lower numbered node is the primary node.
4	The node's IP address is automatically populated in the **Address** field. If you have a dedicated billing network, change this to the dedicated billing IP address for this node.
5	The **Client Port** field is automatically set to `1500`. You may change this if required.
6	The **Internal Port** field is automatically set to `1600`. You may change this if required.
7	Click **Save**.

Step	Action
8	Repeat steps 1 through 7 to add the secondary node for this domain. **Result:** The new nodes are listed in the Nodes section of the screen.



Example New Domain Node Screen

Here is an example New Domain Node screen.



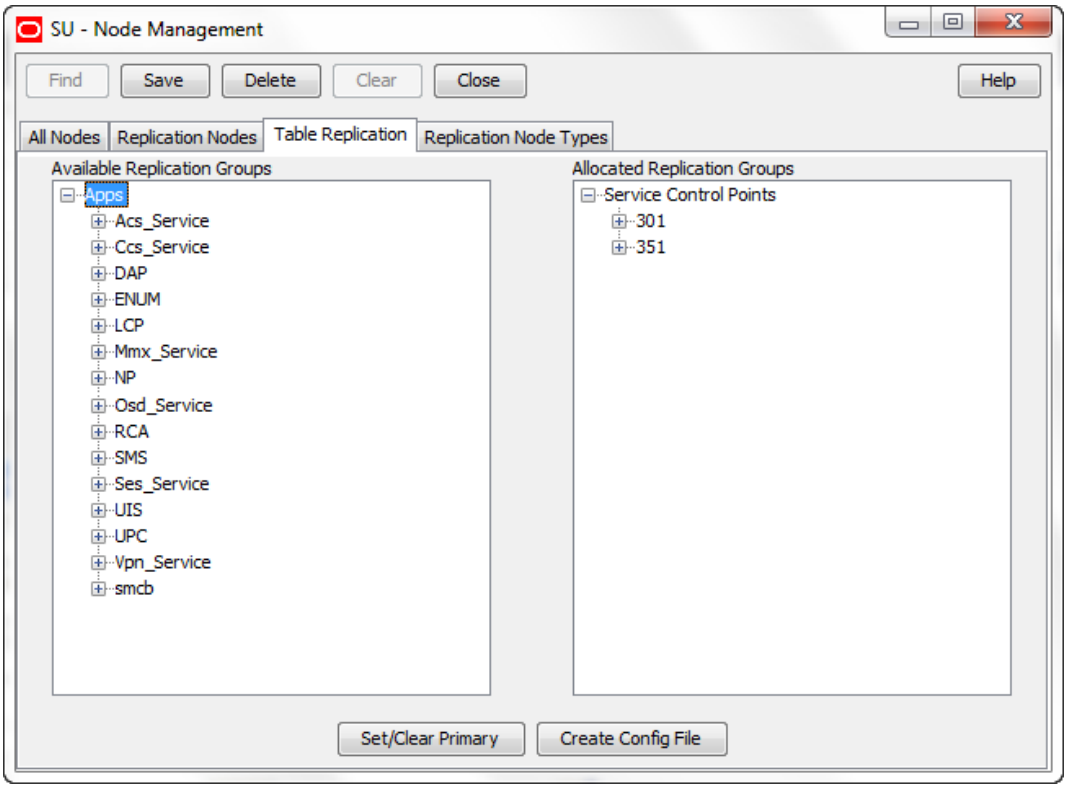
Configuring Replication Tables

Follow these steps to configure table replication for each node.

Note: You must add all tables to be replicated to each node. For VWS nodes, some replication tables will be configured automatically during the VWS domain creation.

Step	Action
1	In the Service Management System UI, select **Operator Functions > Node Management**, then select the **Table Replication** tab.

Step	Action



2 Add all the required tables to be replicated to each node (the node can be identified by replication ID).

To add a table, drag and drop the table from the **Available Groups** section on the left to the relevant node number in the **Allocated Replication Groups** section on the right.

3 The required tables for the SLC and VWS have been pre-configured. To immediately add all the required tables select `Apps` in the **Available Replication Groups** list.

4 Keeping the mouse button depressed, drag the icon across to the **Allocated Replication Groups** list. Drop on the required node name by releasing the mouse button.

Result: The **Node Type Filter Selection** dialog appears.

5 Select the **Node Type** from the drop-down list. Select:

- `scp` for SLC
- `be` for VWS

Note: Some replication groups are added automatically when you create a domain.

6 Click **OK**.

Result: The replication group will be allocated to the selected node.

7 When replication tables have been configured for all the nodes, click **Save**.

Result: You see the **Save Complete** message and the details are saved.

Note: Do not click **Create Config File** as you do not need to create the replication configuration file at this stage. This will be created as part of VWS node configuration.

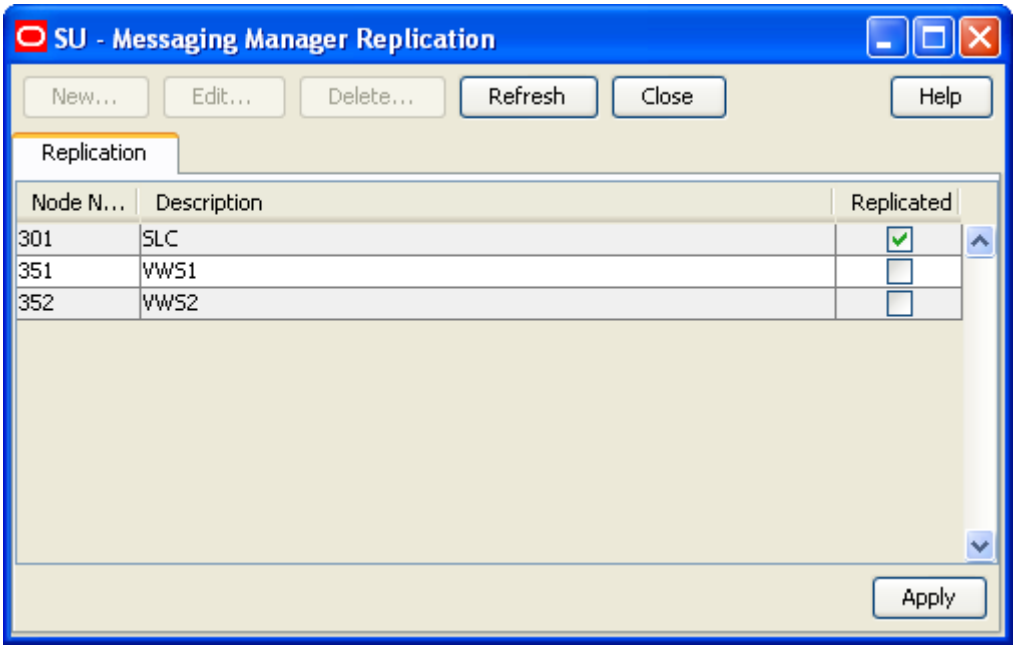
8 Click **Close**.

Result: The Node Management screen will be closed.

9 From the **File** menu on the Service Management System screen, select **Logout & Exit**.

Result: All your updates will be saved to the database, including any updates that have been cached.

Step	Action
10	Re-open the SMS main screen. See Accessing SMS for more information.
11	Select **Services > Messaging Manager > Replication**. **Result:** You see the **Replication** tab in the Messaging Manager Replication screen.



12	Select only the check box for all SLC nodes. **Important:** You should ensure that check boxes for all VWS nodes are not selected.
13	Click **Apply**, and then click **Close**.

Configuring VSSP

To complete VSSP configuration, add the lines in the following files:

- **acs.conf**:
  ```
  ssf (vssp,NOA=4,Address=32495123452,interface=vssp)
  ssf (sca,NOA=4,Address=32495123452,interface=sca)
  ```
  See *acs.conf configuration file* (on page 123) for details.
- **smsGui.bat/smsGui.sh:**
  ```
  -Djnlp.acs.ssfs="sca"
  ```
  This file is located at **/IN/html/**.

Setting Default Currency

You must set a default currency for your country. The system currency is set when you install the SMS software using the OUI. You configure the system currency in the Global Configuration screen and the Currency tab in the SMS GUI.

If you have installed a service template, the default currency is automatically set to the first country in the list that has the selected default currency. To correctly set the default currency for your country:

1. Create a new currency with the correct country.
2. Delete the old one.

See the discussion of currency configuration and global configuration in *Charging Control Services User's Guide* for more information.

OSD Configuration

About OSD Configuration

Open Services Development (OSD) enables third parties to submit html (WSDL) files that invoke control plans. You should perform the following configuration in the Open Services Development screen for OSD:

- On the **Service Providers** tab configure the OSD ports for all OSD interfaces on all SLC nodes.
- On the **Client ASPs** tab configure the clients that will be using OSD. For SMS notifications, this will be all the SMS and VWS nodes.

Note: Use the information you prepared in *OSD configuration planning* (on page 7) to configure details of the OSD interfaces, IP addresses and TCP port numbers.

If you will be using `beServiceTrigger` to send real time wallet notifications to OSD, then you must ensure that the `beServiceTrigger` user has been set up. See *Setting the beServiceTrigger User and Password* (on page 91). To enable `beServiceTrigger` to connect to the client ASP, you must set the user and password for `beServiceTrigger` and for the client ASP to be the same.

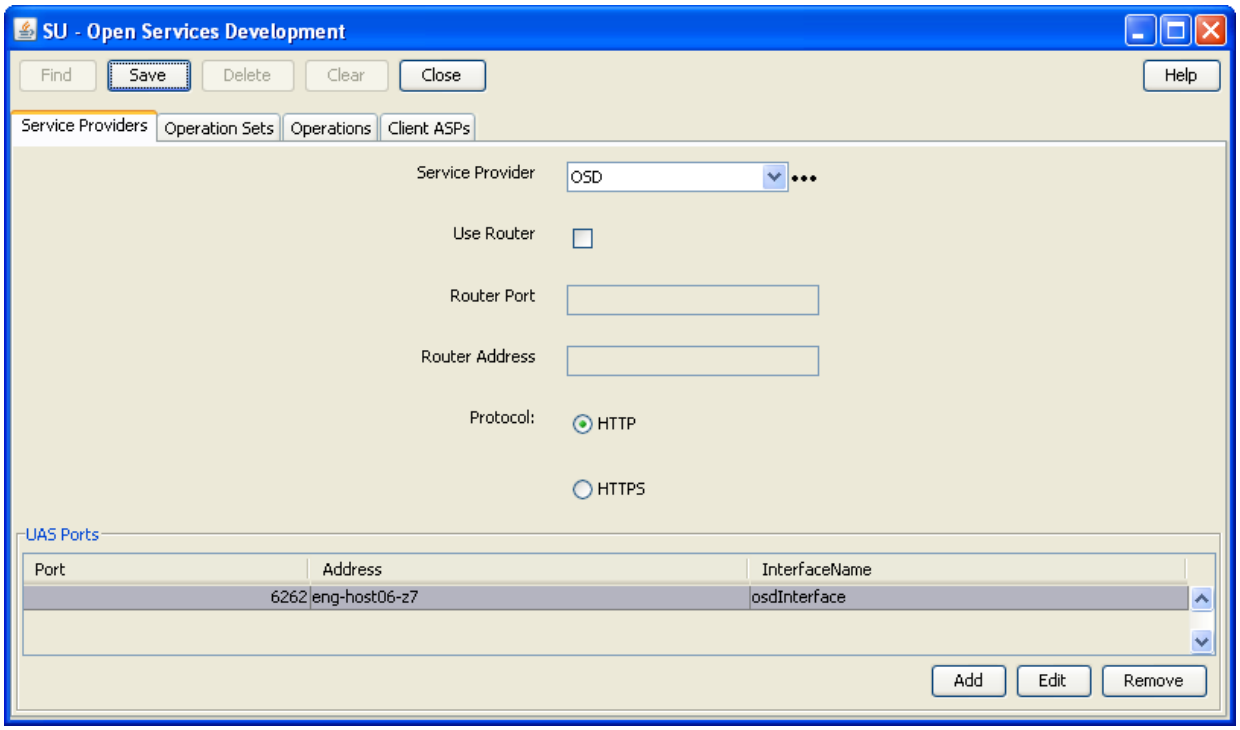
Accessing OSD

Follow these steps to open the Open Services Development (OSD) screen.

Step	Action
1	Launch the Service Management System UI. See *Launching SMS Using Java* (on page 106) for details.
2	From the **Services** menu, select **Open Services Development**. **Result:** You see the **Service Providers** tab in the Open Service Development window.

Service Providers Tab

Here is an example **Service Providers** tab in the Open Services Development screen.



Configuring OSD Ports

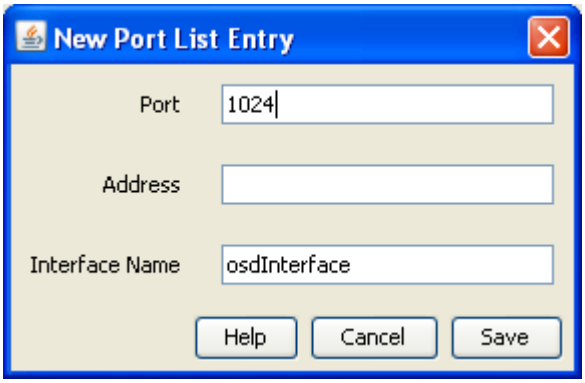
Configure OSD ports by defining the IP address, port, and interface name for all OSD interfaces on all SLC nodes. Follow these guidelines:

- If the OSD port will be used for internal communication between the SLC nodes, and the SMS or VWS nodes, then configure the SLC port and IP address to match the **eserv.config** file triggering section address and port information for the SMS or VWS nodes.
- Configure the interface name for the OSD port to match the configured OSD interface running on the SLC SLEE.

Follow these steps to configure OSD ports for the `OCNCCtemplate` service provider.

Step	Action
1	Click the **Service Providers** tab in the Open Service Development screen. **Result:** You see the **Service Providers** tab in the Open Services Development screen. For an example screen, see Service Providers tab.
2	Select `OCNCCtemplate` from the **Service Provider** drop down list.

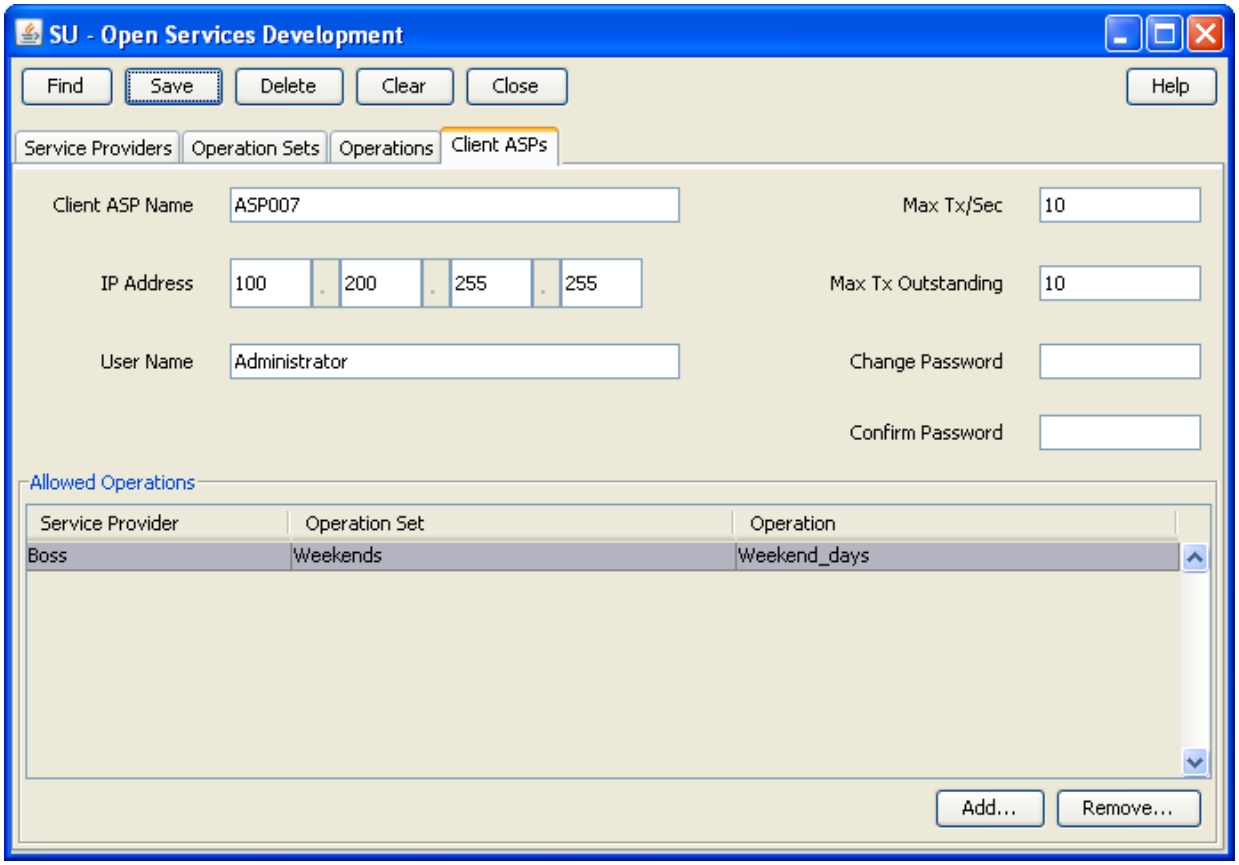
Step	Action
3	Click **Add**. **Result:** You see the New Port List Entry screen.



4	Add the IP **Address**, **Port** and **Interface Name** for all OSD interfaces on all SLC nodes using the information prepared in *OSD configuration planning* (on page 7).
5	After adding each entry, click **Save**.

Client ASPs Tab

Here is an example **Client ASPs** tab.



Configuring Client ASPs

Use the information you prepared in *OSD configuration planning* (on page 7) to configure the client ASPs that will be using OSD. You should add clients for:

- SMS notifications, for all the SMS and VWS nodes.

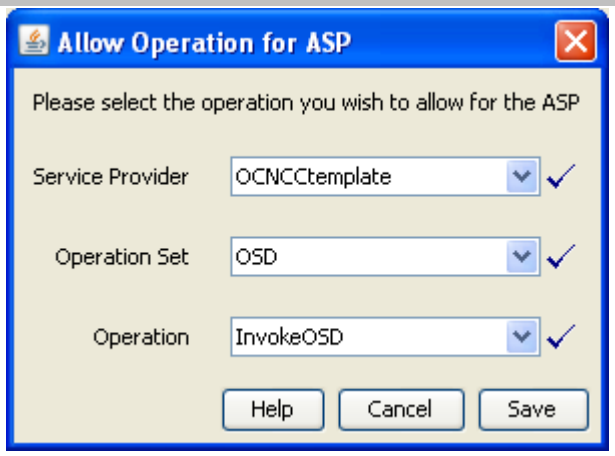
Follow these steps to configure the client ASPs.

Step	Action
1	Select the **Client ASPs** tab in the Open Services Development screen. **Result:** You see the **Client ASPs** tab. For an example screen, see Client ASPs tab.
2	Enter the name of the node in the **Client ASP Name** field. This will be one of the following: • The name of the SMS or VWS node for which you are configuring the ASP.
3	In the **IP Address** field, enter the IP address from which the client ASP node will connect to the SLC node.
4	In the **User Name** field, enter the username that the client ASP will use to authenticate itself on the SLC. **Important:** To enable `beServiceTrigger` to connect to the client ASP, you must specify the username for `beServiceTrigger` for VWS and SMS client ASPs.
5	Set **Max Tx/Sec** to `10`.
6	Set **Max Tx Outstanding** to `10`.
7	Set the password for the SOAP HTML header in the **Change Password** and **Confirm Password** fields. **Important:** To enable `beServiceTrigger` to connect to the client ASP, you must set password to the password for `beServiceTrigger` for VWS and SMS client ASPs.
8	Click **Save**. **Result:** The **Add** button becomes available.
9	Click **Add** to add allowed operations for this ASP. To add allowed operations for VWS or SMS clients, see Adding allowed operations for VWS and SMS clients.
10	Repeat these steps until all the clients have been configured.

Adding Allowed Operations for VWS and SMS Clients

Follow these steps to add the `InvokeOSD` operation to the list of allowed operations for a VWS or SMS client ASP.

Step	Action
1	On the **Client ASPs** tab, click **Add**. **Result:** The **Allow Operation for ASP** screen appears, with the following default field values: • **Service Provider** is the currently selected provider in other tabs. • **Operation Set** is the first in the list for the provider. • **Operation** is the first in the list for the operation set.

Step	Action
	
2	Select the `OCNCCtemplate` **Service Provider** from the drop down list.
	Note: The selected provider will be updated in the other OSD tabs and you will be prompted to save any unsaved changes.
3	Select the `OSD` **Operation Set** from the drop down list.
4	Select the `InvokeOSD` **Operation** from the drop down list.
5	Click **Save**.

Configuration Files on the SMS

About SMS Configuration Files

Some configuration for the NCC software components is set in the following configuration files on the SMS node:

- **eserv.config**
- **acs.conf**

You should review the configuration in these files. For details, see *Checking* **eserv.config** *File Parameters* (on page 143).

eserv.config Configuration File

The **eserv.config** file is a shared configuration file, from which most NCC applications read their configuration. Each NCC node (SMS, VWS, and SLC) has its own version of the configuration file, containing configuration relevant to that machine. The configuration file contains many different parts or sections, each application reads the parts of the **eserv.config** file that contains data relevant to it. It is located in the **/IN/service_packages/** directory.

The **eserv.config** file format allows hierarchical groupings, and most applications make use of this to divide up the options into logical groupings.

Example eserv.config Parameter Section

This example shows CCS wallet handler configuration in **eserv.config**.

```
CCS = {
    reservationHandler = {
        reservationLengthTolerance = 60 # in milliseconds
        summariseWalletTolerance = 60000
```

```
    }
}
```

To identify a particular configuration item in the file, use notation such as this:

```
CCS.reservationHandler.summariseWalletTolerance
```

acs.conf Configuration File

The **acs.conf** configuration file contains configuration specific to the ACS application. It is located in the **/IN/service_packages/ACS/etc/** directory.

Checking Configuration File Parameters

This table lists the configuration parameters that you should review in **eserv.config** and **acs.conf**.

To make changes, log in as the user root and edit the relevant configuration file.

Parameter	Description	File name
`CCS.ccsProfileDaemon.triggering.osd_scps`	Set to a comma separated list of the IP:port combinations for all OSD interfaces on the SLC nodes that will be used for sending notification SMS messages. (Use the source IP address). **Example** `osd_scps=["10.1.0.10:2222","10.1.0.20.2222"]`	**eserv.config**
`CCS.ccsCDRLoader.AcctHistPlugin.acsCustomerIdData.acsCustomerId`	Change the parameter value to the ID of the 'OCNCCtemplate' ACS Customer. To determine the ACS Customer ID enter the following SQL command: **`select id from acs_customer where name = 'OCNCCtemplate';`**	**eserv.config**
`triggering.scps`	Defined in the triggering section for the smsTrigDaemon process. This sets the SLC that will receive BPL execution requests from the SMS. Set to a comma separated list of the IP:port combinations for the SLCs. Set port to **`3072`**, and use the internal IP address, if configured. **Example** `scps=["10.1.0.10:3072","10.1.0.20.3072"]`	**eserv.config**
`acsStatisticsDBInserter.MasterServerLocation`	Set to an IP address or hostname for the SLC running the acsStatsMaster. Normally set to the first SLC node. You should use the default setting: "acsStatsMaster". The hostname must resolve to the correct SLC IP address using the **/etc/hosts** file. See *Setting IP Addresses and Hostnames* (on page 89). **Example** `MasterServerLocation acsStatsMaster`	**acs.conf**

VWS Node Configuration

Introduction

The configuration tasks in this section define the minimum configuration for the VWS node. They are:

- Replicate data to the VWS domains. See *Replicating Data to the VWS* (on page 124).
- Check configuration in **eserv.config**. See *Checking* **eserv.config** (on page 126).
- Reread configuration for the inittab processes. See *Rereading Configuration for inittab Processes* (on page 127).

You should perform the tasks in this section if you installed:

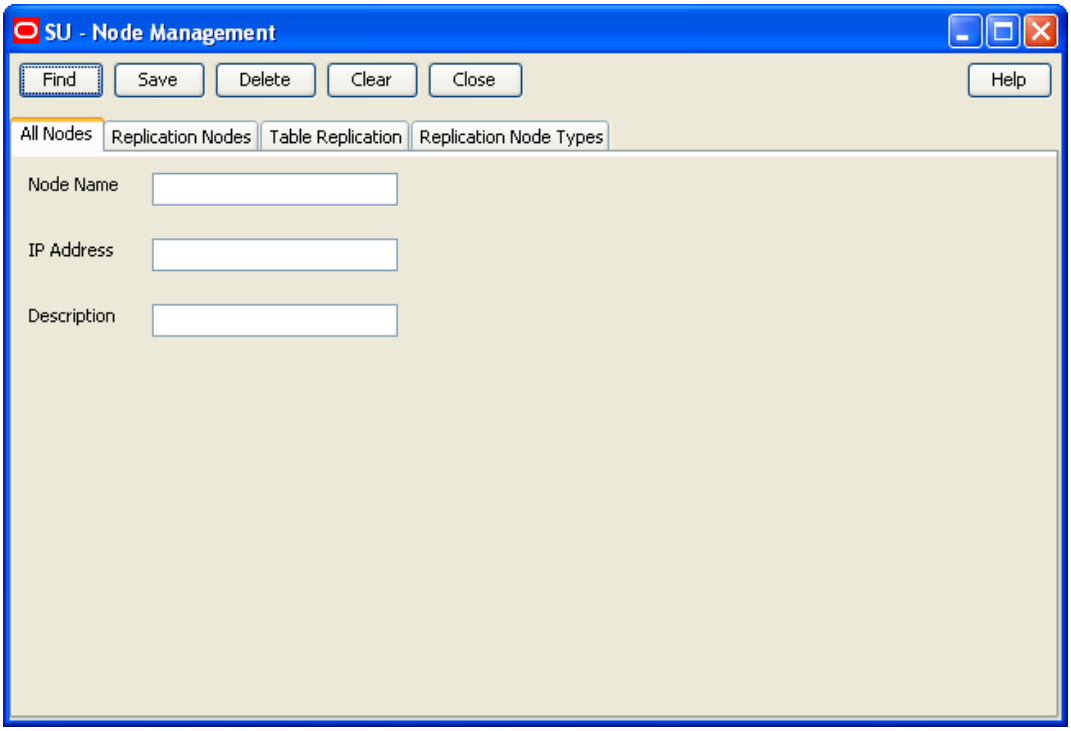
- NCC software and Prepaid Charging Service Template (PCST)

After completing these configuration tasks you must:

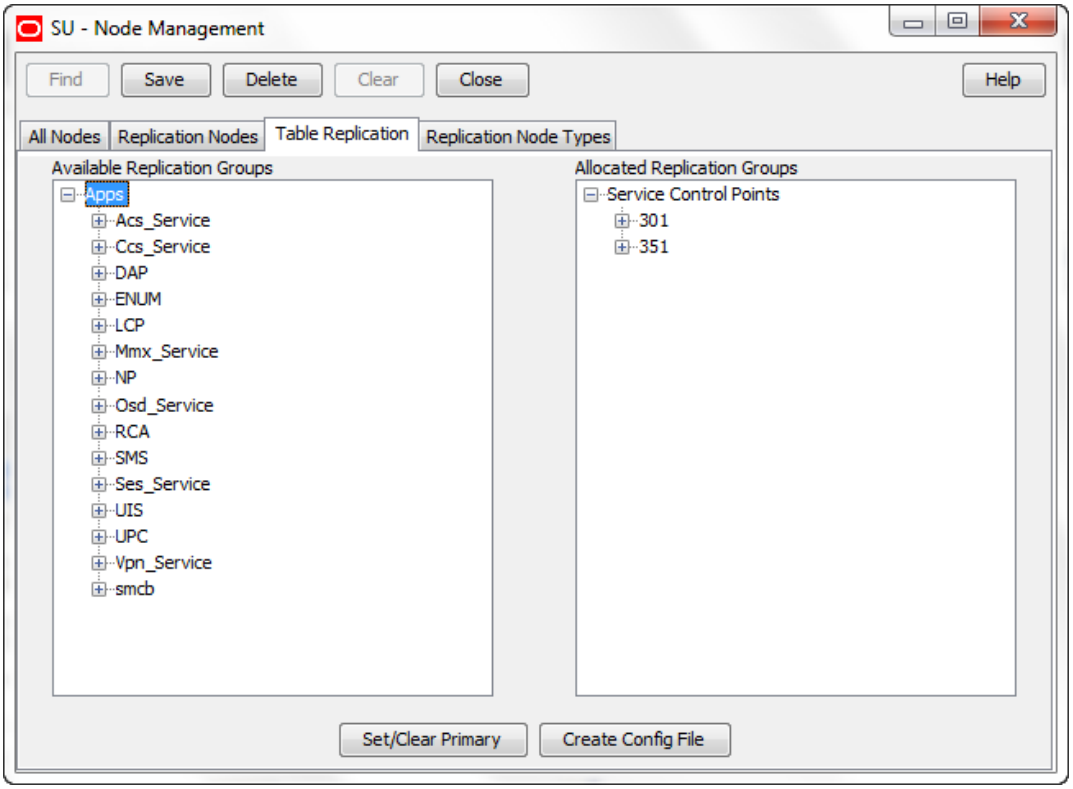
- Generate MFiles. See *MFile Generation* (on page 127)
- Start the SLEE. See *Starting the SLEE* (on page 130)

Replicating Data to the VWS

Follow these steps to enable replication between the SMS and VWS, and to perform initial synchronization of the data.

Step	Action
1	In the Service Management SystemUI, select **Operator Functions > Node Management**. **Result:** You see the **All Nodes** tab on the Node Management screen. 
2	Select the **Table Replication** tab.

Step	Action



3 Click **Create Config File**.

4 Click **OK**.

5 On the VWS nodes, open a shell session and review the output in the **updateLoader** log file. This file is located at **/IN/service_packages/CCS/tmp/**.

Example command

```
tail -20f /IN/service_packages/CCS/tmp/updateLoaderWrapper.log
```

Example output

```
Node 351 sms comparison / resync cient ready.
Sep 29 15:09:36.750197 updateLoader (4369)  NOTICE: Update Loader replication
process started (node 351)
Canceling any current client action.
Sep 29 15:09:36.753543 updateLoader (4369)  NOTICE: Reached master node 1 at
'192.168.44.40'
RES: Wed Sep 29 15:09:39 2010: Node 351, started processing 781 SMS and 0 SCP
records.
RES: Wed Sep 29 15:09:39 2010: Node 351, resynchronization pass 1, started
processing of 781 SMS and 0 SCP records.
Sep 29 15:09:39.282806 smsCompareResyncClient (4383) NOTICE: Beginning
resynchronisation for node 351.
RES: Wed Sep 29 15:09:39 2010: Node 351, resynchronization pass 1, finished
processing 781 of 781 SMS and 0 of 0 SCP records.
Sep 29 15:09:39.803041smsCompareResyncClient (4383) NOTICE: Ending
resynchronization for node 351. Resynchronization was successful.
RES: Wed Sep 29 15:09:39 2010: Node 351, finished processing 781 of 781 SMS and 0
of 0 SCP records, resync completed successfully.
Sep 29 15:09:40.827498 updateLoader (4369) NOTICE: Resynchronization Finished.
Processing Queued Updates
Node 351 SMS comparison/resync client ready.
```

Checking eserv.config

This table lists the configuration parameters that you should review in **eserv.config** on the VWS node. It is located at **/IN/service_packages/**. For more information, see **eserv.config** *configuration file* (on page 122).

Refer to *Voucher and Wallet Server Technical Guide* for details about **eserv.config** on the VWS.

To make changes, log in as the user root and edit the **eserv.config** file.

Parameter	Description
`cmnPushFiles = [ "-h", "host"]`	Set this parameter to an IP address or hostname of the SMS that will be used by the VWS to transfer files, such as CDRs, to the SMS. You should set this parameter in the following sections of **eserv.config**: • `CCS.ccsVWARSExpiry` • `CCS.ExpiryMessages` • `CCS.notificationPlugin` • `BE.cmnPushFIles` **Note:** You should use the default host "usms.CdrPush", and ensure that this hostname resolves to the correct SMS IP address through the **/etc/hosts** file. See *Setting IP Addresses and Hostnames* (on page 89).
`BE.serverId`	Set this parameter to the ID of the domain to which this VWS belongs. To determine the domain IDs, log on to the SMS as the user smf_oper, and enter the following SQL query: **`sqlplus /`** **`SQL> select domain_id, name from ccs_domain;`** **`DOMAIN_ID NAME`** **`--------- --------`** **`1 TESTVWS`**
`BE.amPrimary`	Set this parameter to: • True - if this is the primary VWS in the domain • False - if this is the secondary VWS
`BE.triggering.scps`	Set this parameter to a comma separated list of IP:port combinations for all xmlTcap interfaces on SLC nodes. **Example** `scps = ["10.1.0.10.3072","10.1.0.20:3072"]`
`BE.triggering.osd_scps`	Set this parameter to a comma separated list of IP:port combinations for all OSD interfaces on the SLC nodes that are used for sending notification SMS messages. **Example** `osd_scps = ["10.1.0.10.2222","10.1.0.20:2222"]`
`BE.beVWARS.plugins`	The entry `"ccsVWARSReservationExpiry.so"` must only be included on the primary VWS. You must stop the VWS and remove this line from the list of plug-ins.

SLEE.cfg Configuration

The **SLEE.cfg** file is located on both primary and secondary VWS nodes in the **/IN/service_packages/SLEE/etc/** directory.

It includes the following configuration for the ccsSLEEChangeDaemon interface:

```
INTERFACE=ccsSLEEChangeDaemon ccsSLEEChangeD.sh /IN/service_packages/CCS/bin 1 EVENT
```

The ccsSLEEChangeDaemon should run on the primary VWS node only. Edit **SLEE.cfg** on the secondary VWS to ensure that the SLEE does not try to run this interface from the secondary VWS. You should comment out the following line:

```
# INTERFACE=ccsSLEEChangeDaemon ccsSLEEChangeD.sh /IN/service_packages/CCS/bin 1
EVENT
```

Note: Attempts by the SLEE to run ccsSLEEChangeDaemon from the secondary VWS node will result in recurring alarms being generated.

Rereading Configuration for inittab Processes

Follow these steps to force the system to reread the configuration for inittab processes on the VWS.

Step	Action
1	Log in to the VWS as the user `root`.
2	Cycle between inittab run level 2 and run level 3. Set the inittab run level to 2 by entering the following command: **`init 2`**
3	Check the run level by entering: **`who -r`** **Example output** `run-level 2 Jan 13 10:46 2 0 3`
4	Set the inittab run level to 3 by entering: **`init 3`**
5	Check the run level by entering: **`who -r`** **Example output** `run-level 3 Jan 13 10:46 3 1 2`

MFile Generation

Introduction

MFiles are files which are generated on the Voucher and Wallet Server (VWS) nodes, and provide a fast lookup for a subset of the data in the E2BE database. MFiles can be generated to provide either CLI-DN rating data or event data.

Following the NCC installation and after any rating change, you must compile new MFiles for each VWS node. You compile MFiles on the **MFile Generation** tab in the Service Management screen.

Note: For more information, see *Charging Control Services User's Guide*.

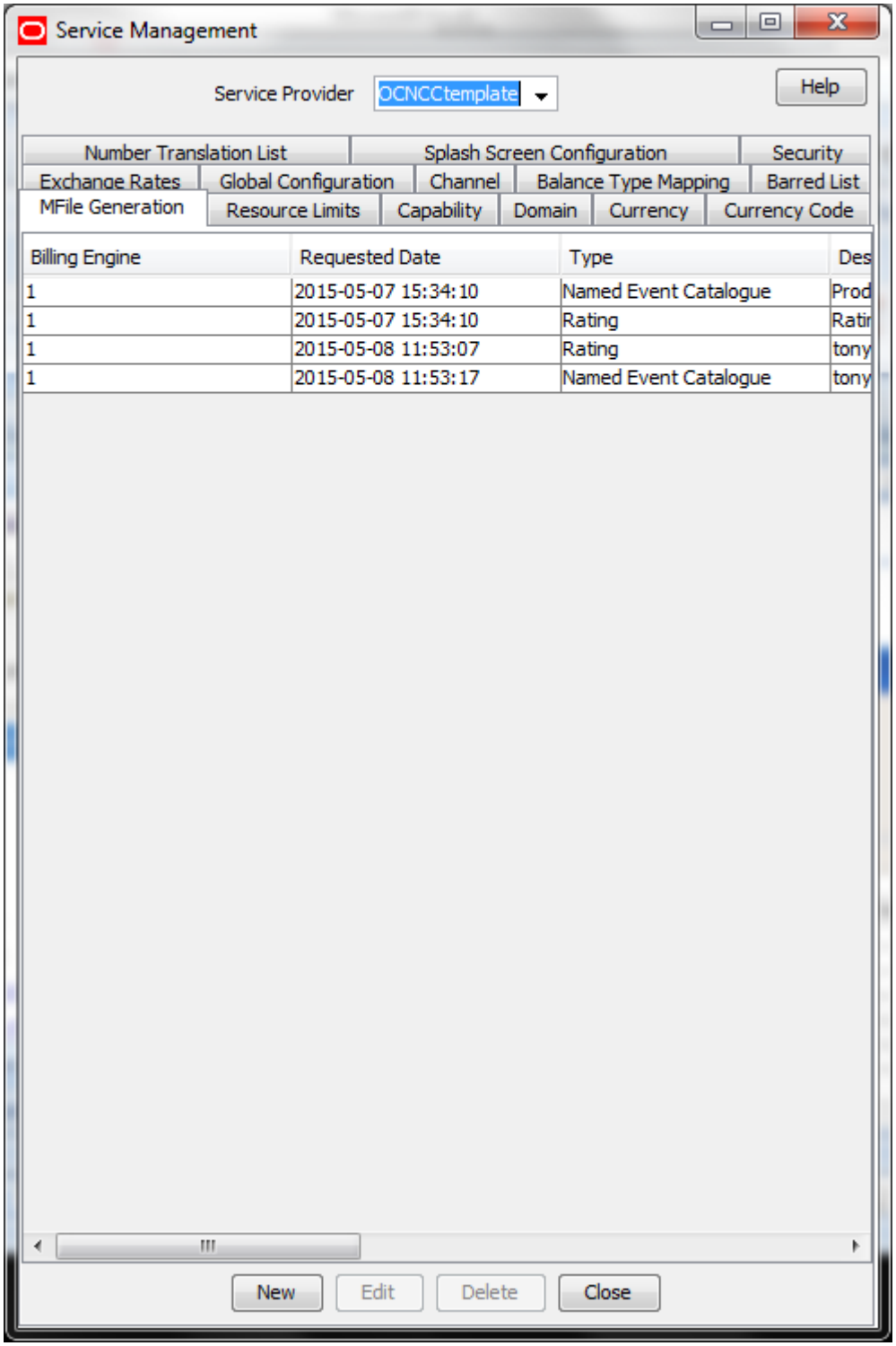
Accessing the MFile Generation Tab

Follow these steps to access the **MFile Generation** tab in the Service Management window.

Step	Action
1	Open the Service Management System main screen if it is not already open. See *Opening SMS Using Webstart* (on page 106) for more information.
2	Select **Services > Prepaid Charging > Service Management** and select the **MFile Generation** tab.

MFile Generation Tab

Here is an example **MFile Generation** tab.



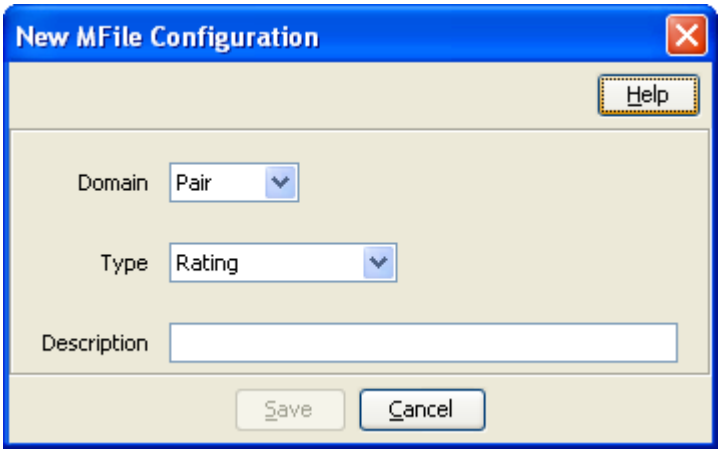
MFile Fields

This table describes the function of each field.

Field	Description
Domain	The Voucher and Wallet Server pair you will send the MFile to. This field is populated by the **Domain** tab. This field cannot be edited once it is initially saved.
Description	The description of the MFile.
Request Date	The date the MFile was last requested to run. **Note:** This field is only available on the Edit MFile screen.
Type	Whether the MFile is for: • Rating • Named event catalogue

Compiling MFiles

Follow these steps to compile MFiles.

Step	Action
1	On the **MFile Generation** tab, click **New**. **Result:** You see the New MFile Configuration screen. 
2	Select the name of the primary Domain from the **Domain** drop down list.
3	Select `Rating` from the **Type** drop down list.
4	Enter a description such as **`Initial install`** in the **Description** field.
5	Click **Save**. **Result:** The ccsMFileCompiler on the VWSs within the chosen domain will build up a new MFile and notify the VWS processes.
6	Repeat these steps to create MFiles for **Type** `Named Event Catalogue`.
7	Repeat these steps to create the MFiles for any other configured VWS domain.

Starting the SLEE

Starting the SLEE on the VWS

All critical application processes on the VWS node run in the SLEE.

To manually start the SLEE on the VWS node, log on as the user `NCC_runtime user` and enter the following command:

```
/IN/bin/slee-ctrl start
```

To restart the SLEE, enter the following command as the user `NCC_runtime user`:

```
/IN/bin/slee-ctrl restart
```

SLC Node Configuration

Checking acs.conf on the SLC

This table lists the configuration parameters that you should review in **acs.conf** on the SLC node. The **acs.conf** file is located in the **/IN/service_packages/ACS/etc/** directory.

To edit the **acs.conf** file you must be logged in as the user `NCC_runtime user`.

For more information on **acs.conf**, see *acs.conf configuration file* (on page 123).

Parameter	Description
acsStatsMaster masterStatsServer acsStatsLocal masterStatsServer	Set both parameters to an IP address or hostname of the SLC running the acsStatsMaster, normally the primary SLC node. See *Setting IP Addresses and Hostnames* (on page 89). **Note:** You should use the default setting of `acsStatsMaster` and ensure that this hostname resolves to the correct SLC IP address in the **/etc/hosts** file.

Messaging Manager Configuration

Introduction

The Messaging Manager (MM) application handles receiving, routing, and sending SMS messages through a variety of protocols. This section explains how to implement a basic initial configuration of MM to enable:

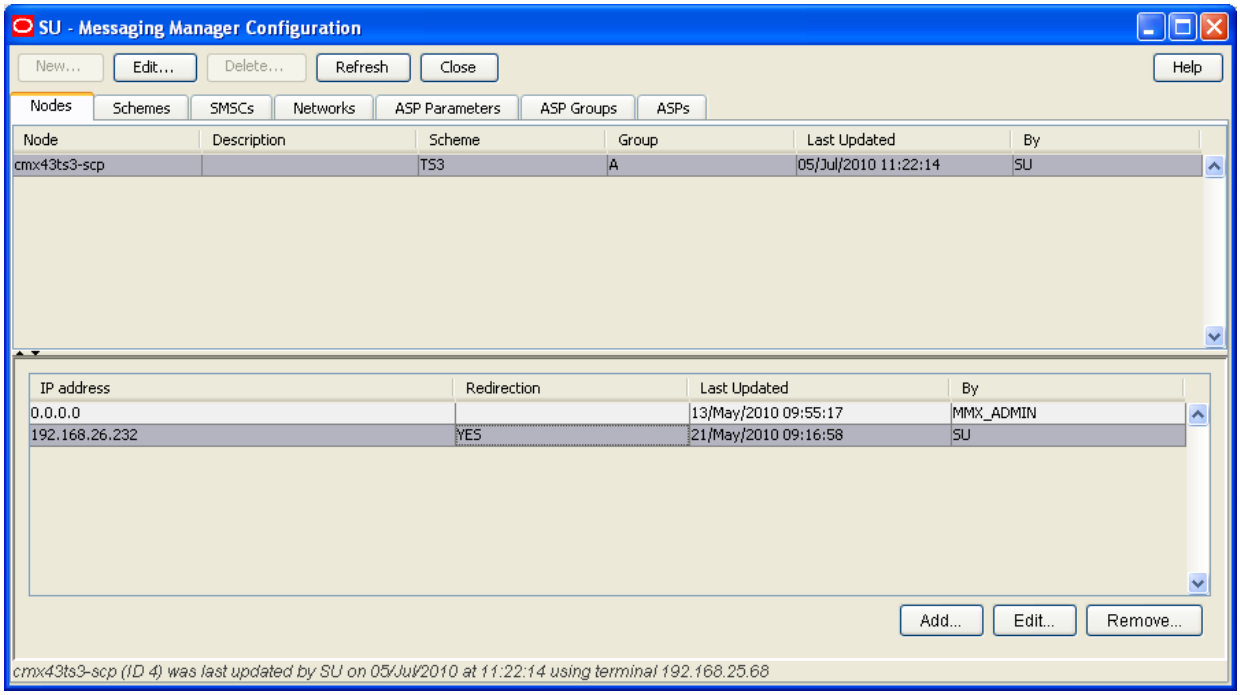
- Inbound SMS messages to be received through EMI, SMPP or MAP (MO_FwdSM).
- All inbound SMS messages to trigger the prepaid charging services to charge the sender.
- SMS messages to be routed using FDA (First Delivery Attempt). The FDA will be attempted using MAP. If this fails, then the SMS will be submitted to the SMSC using the MAP, SMPP or EMI protocol. MMX routing node should be added as per the instructions described in the Messaging Manager Technical Guide.

For more information on configuring MM, see *Messaging Manager User's Guide* and *Messaging Manager Technical Guide*.

Accessing the Messaging Manager Configuration Screen

Follow these steps to open the Messaging Manager Configuration screen.

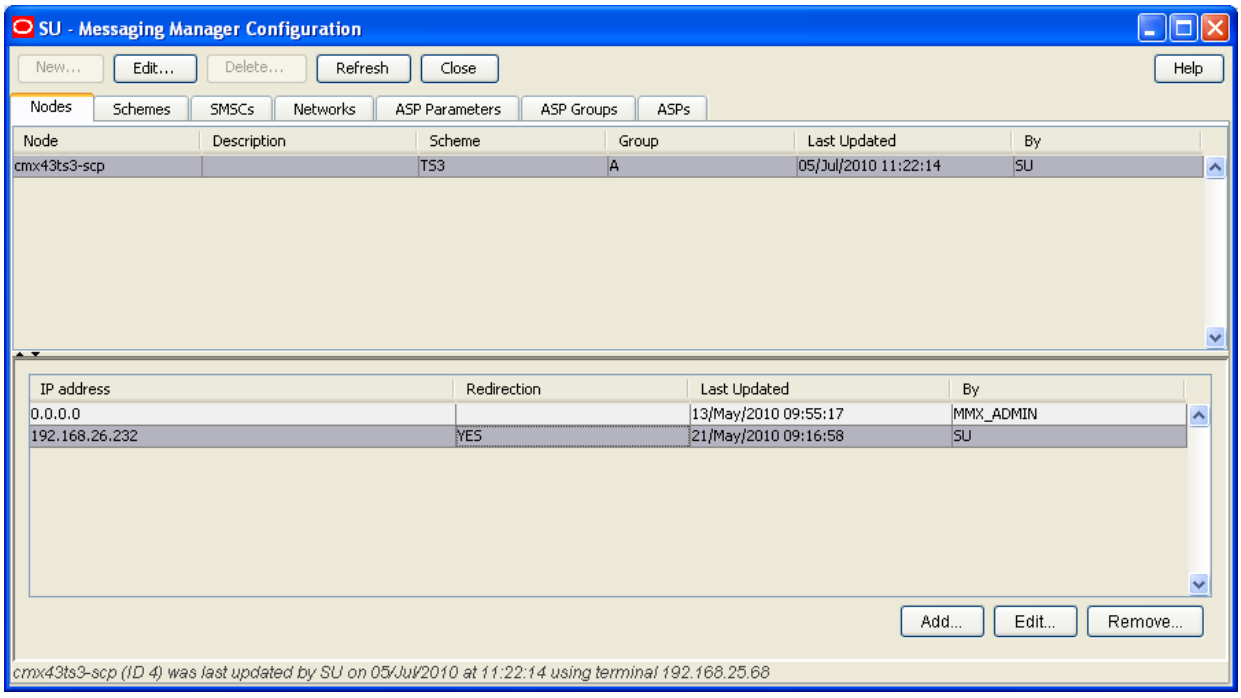
Step	Action
1	On the Service Management System main menu, select the **Services** menu.
2	Select **Messaging Manager**, then **Configuration.** **Result:** You see the Messaging Manager Configuration screen.



Viewing the Nodes

Follow these steps to view the MM nodes.

Step	Action
1	Select the **Nodes** tab on the Messaging Manager Configuration screen. **Result:** You see the MM nodes listed on the tab.



Messaging Manager Scheme Configuration

Introduction

The **Schemes** tab in the Messaging Manager Configuration screen allows you to manage all the routing definitions for the Messaging Manager configuration.

A scheme is a set of rules that define how to treat and route messages.

You specify rules for multiple protocols to define:

- Paths to use
- Connections to use
- Billing domain to use
- Filtering to use
- Actions to take

PrepaidPack Schemes

The MM PrepaidPack scheme is automatically created when you install the Prepaid Charging Service Template (PCST).

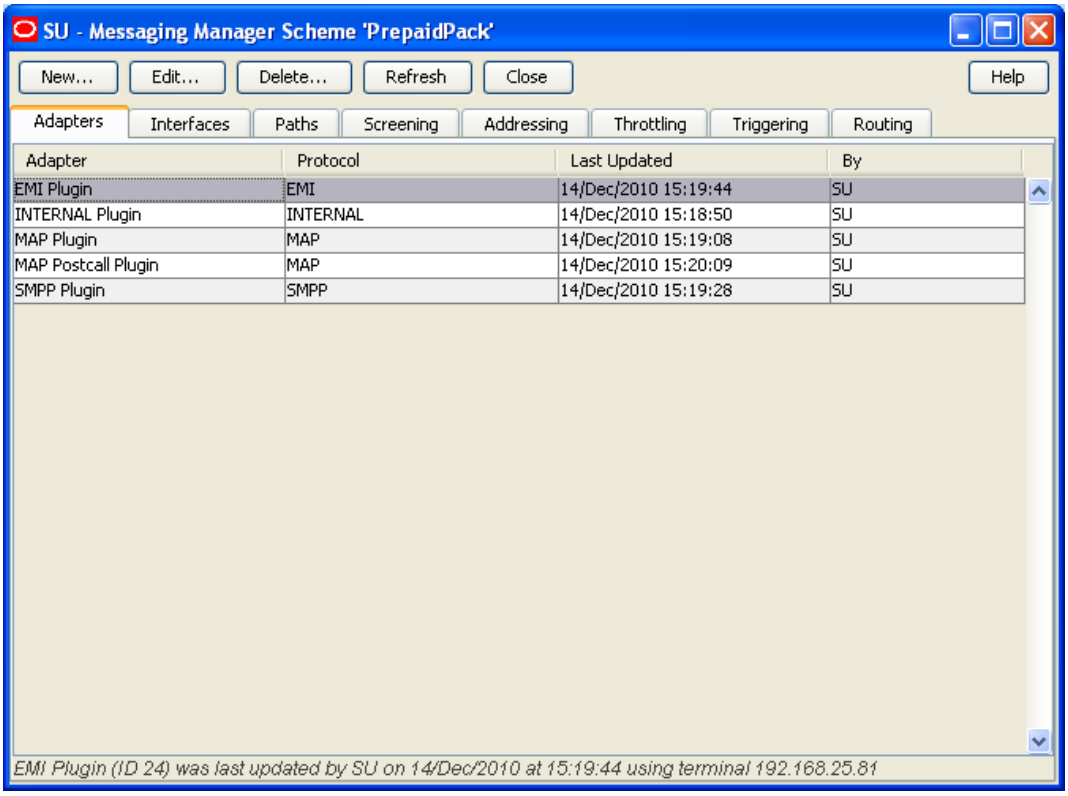
You will need to perform some additional configuration for these schemes. The additional configuration tasks are described in this section.

Opening the Scheme

Follow these steps to open the template scheme that you want to configure.

Step	Action
1	Select the **Schemes** tab in the Messaging Manager Configuration screen.
2	In the table on the **Schemes** tab, select the scheme record to open. Select `PrepaidPack`.

Step	Action
3	Open the record, by performing one of the following actions: • Double-click on the record in the table • Click **Open**. **Result:** You see the Messaging Manager Scheme screen for the selected scheme record.



Scheme Tabs

The Scheme screen enables you to configure the scheme details.

This table describes the tabs on the screen and tells you whether any configuration is required.

Tab	Description	Configuration
Adapters	Defines the adapters which route traffic to and from this scheme. Entries in the **eserv.config** file identify which adapters will be loaded by Messaging Manager at startup. The link between **eserv.config** and the adapter configuration values is made on this tab.	No changes required.
Interfaces	Defines the interfaces which are available to this scheme.	No changes required.
Paths	Defines the paths available to this scheme.	See *Paths Configuration* (on page 134).
Screening	Defines the anti-spam rules for the Scheme.	Screening is not used in this configuration.
Addressing	Defines the addressing rules for the scheme.	Addressing has been pre-configured so that all inbound SMS messages

Tab	Description	Configuration
		are assigned a domain named "SMSMO", while all internally generated SMS messages are assigned a domain named "Notification SMS".
Throttling	Reports summary of all the domain throttling values.	Throttling is not used in this configuration.
Triggering	Defines the triggering rules for the scheme.	See *Configuring Triggering Rules* (on page 135).
Routing	Defines the routing rules for the scheme.	See *Configuring Routing Rules* (on page 136).

Paths Configuration

A number of paths have been pre-configured for the service template schemes. This table lists the possible configuration for each path.

Path	Configuration
To SMSC using EMI	For sending SMS messages to an SMSC using the EMI protocol. If you do not require this scenario: • Select the path and click **Edit** • Deselect the **Enabled** check box • Click **Save** If you do require this scenario: • Select the path • In the Connection panel, select the connection labeled "To SMSC using EMI" • In the Connection panel, click **Edit** • In the **Remote Listen** field, configure the SMSC TCP/IP address and port Messaging Manager will use to connect to the SMSC • In the **Remote username** and **Remote password** fields configure the username and password MM will use to log into the SMSC. • Click **Save**
To SMSC using SMPP	For sending SMSs to an SMSC using the SMPP protocol. If you do not require this scenario: • Select the path and click **Edit** • Deselect the **Enabled** check box • Click **Save** If you do require this scenario: • Select the path • In the Connection panel, select the connection labeled "To SMSC using SMPP" • In the Connection panel, click **Edit** • In the **Remote Listen** field, configure the SMSC TCP/IP address and port MM will use to connect to the SMSC • In the **Remote username** and **Remote password** fields configure the username and password MM will use to log into the SMSC. • Click **Save**

Path	Configuration
Internal_DR INTERNAL_SME	These paths are used internally between MM and other NCC components. No configuration is required.
To SMSC using MAP	For sending SMS messages to an SMSC using the MAP protocol. If you do not require this scenario: • Select the path and click **Edit** • Deselect the **Enabled** check box • Click **Save** If you do require this scenario: • Select the path • In the Connection panel, select the connection labeled "SMSC" • You can configure the SSN and PC or GT values of the SMSC in the corresponding fields. MM will set these values in outgoing MAP messages to reach this SMSC. • Click **Save**

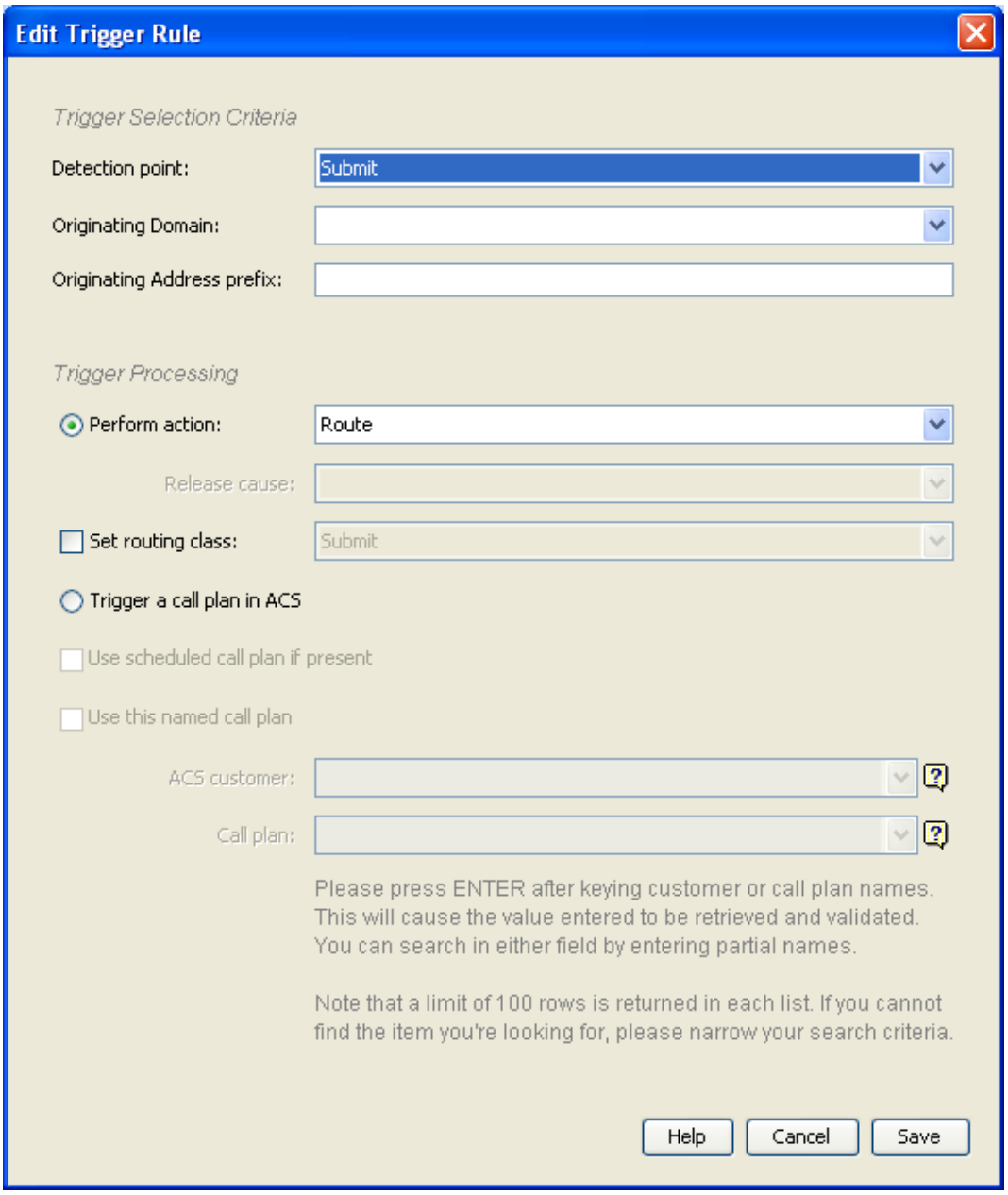
Configuring Triggering Rules

Triggering for all inbound SMS messages has been pre-configured to trigger the template service. In general, all other internally generated SMS messages will be routed to their destination.

Follow these steps to configure whether or not direct delivery (FDA) is attempted for inbound SMS messages.

Step	Action
1	Select the **Triggering** tab in the Messaging Manager Scheme screen.
2	From the table on the tab, select the `Submit` detection point.
3	Select the rule for `Orig.Domain = SMSMO` in the PrepaidPack scheme.
4	Click **Edit**. **Result:** The Edit Trigger Rule screen appears.

Step	Action



5 Select the **Set routing class** check box.

6 Select one of the following options from the **Set routing class** drop down list:

- Submit - if no FDA is required. SMS messages will be sent to the SMSC
- FDA - if FDA is required. MM will first attempt to deliver SMS messages directly before sending them to the SMSC

7 Click **Save.**

Configuring Routing Rules

Routing has been pre-configured so that the SMS messages sent to the SMSC are sent using the MAP path (using the MAP protocol). If required you can change this to route SMS messages using the EMI or SMPP path.

Follow these steps to configure routing for the selected service template using EMI or SMPP.

Step	Action
	Select the **Routing** tab in the Messaging Manager Scheme screen.
1	Select the `Submit` routing class. **Result:** All rules for the selected routing class are displayed in the table on the tab.
2	Select a rule in the table.
3	Click **Edit**. **Result:** The Edit Routing Rule screen applicable to the routing class for the selected record appears.
4	Remove the path named `To SMSC using MAP` from the rule. In the Path table in the **Paths Sequencing** section of the Edit Routing Rule screen, select the path `To SMSC using MAP` and click **Remove**.
5	From the **Paths sequencing** drop down list, select either the EMI or SMPP path by selecting one of the following paths: • `To SMSC using EMI` • `To SMSC using MAP`
6	Click **Add**.
7	Click **Save** to save the routing rule to the configuration database.
8	Repeat these steps for each rule.
9	Click **Close** to close the scheme.

MM SMSC Configuration and Node Mapping

Introduction

To complete Messaging Manager (MM) configuration for the Prepaid Charging Service Template (PCST), you should:

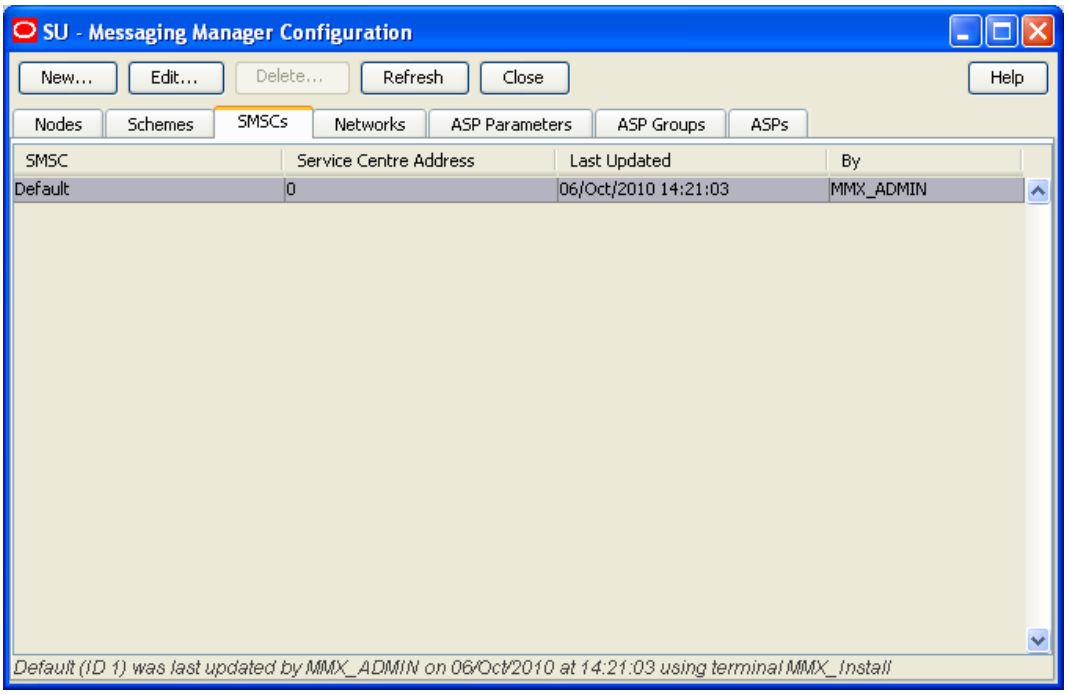
- Configure the default SMSC
- Map the Messaging Manager nodes to the `PrepaidPack`

Configuring Default SMSC

Follow these steps to configure the default SMSC.

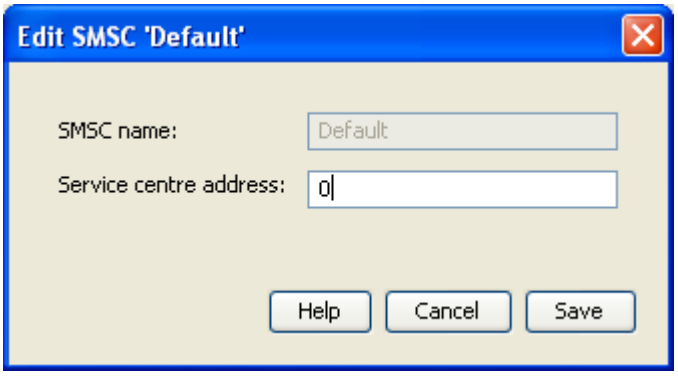
Step	Action
1	Select the **SMSCs** tab in the Messaging Manager Configuration screen. **Result:** You see the available SMSCs listed on the tab.

Step	Action



2 Select the `Default` SMSC record in the table and click **Edit**.

Result: You see the Edit SMSC 'Default' screen.



3 In the **Service centre address** field, enter the address to set in outbound MAP messages.

4 Click **Save**.

Mapping Nodes to Service Template Schemes

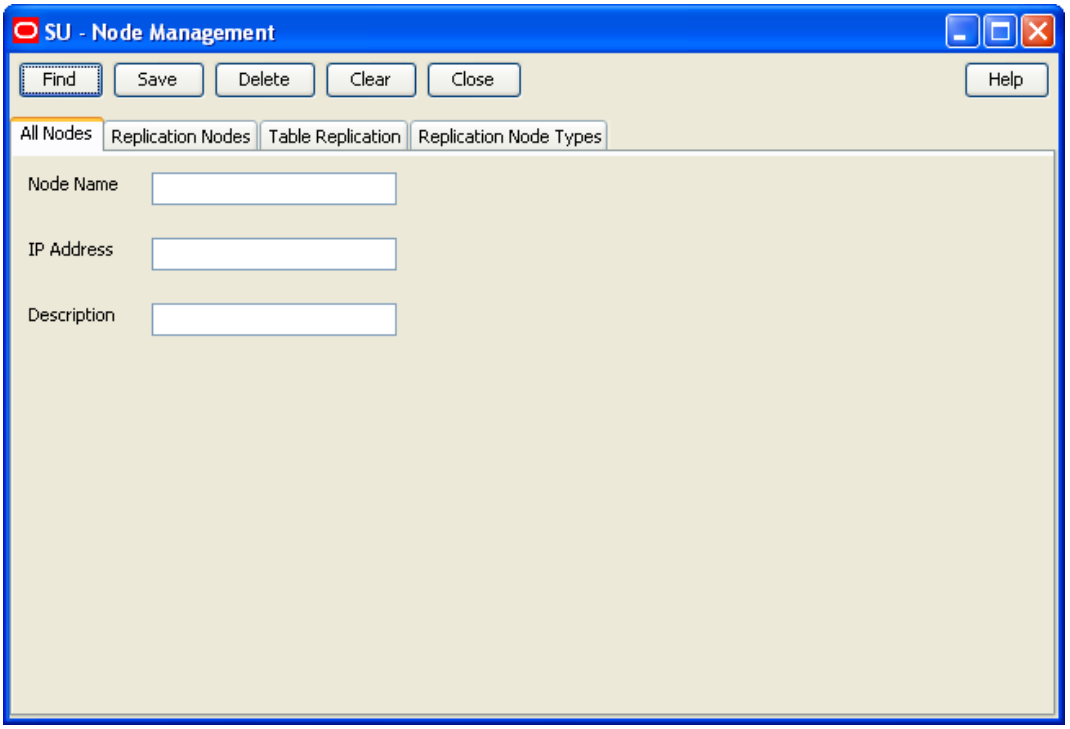
Follow these steps to map MM nodes to the required service template scheme.

Step	Action
1	Select the **Nodes** tab in the Messaging Manager Configuration screen. **Result:** You see the available MM nodes listed on the tab. For an example screen, see *Viewing the Nodes* (on page 131).
2	Select the first node in the table and click **Edit**.
3	In the Edit Node <*node name*> screen, select the service template **Routing Scheme**.
4	In the table, select the IP address for the NIC_A interface. This will be the IP address this SLC will use for EMI and SMPP connections.

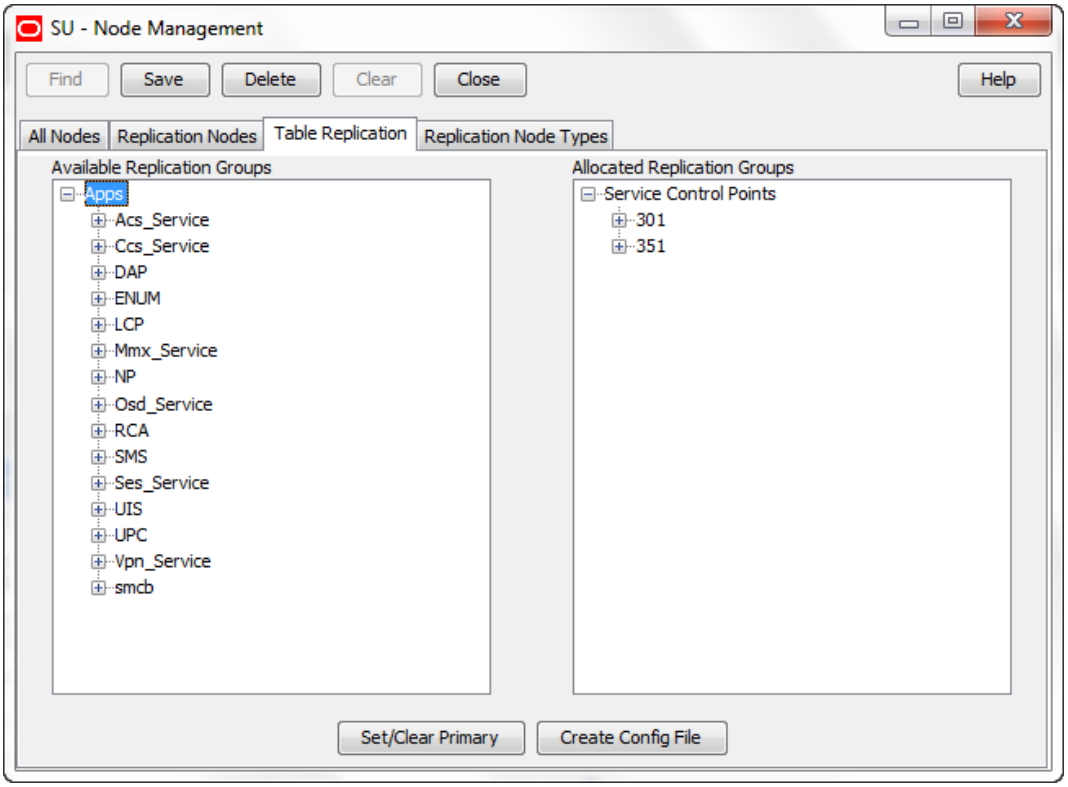
Step	Action
5	Click **Save**.
6	Repeat these steps for each MM node.

Replicating Data to the SLC

Follow these steps to enable replication between the SMS and SLC and perform initial synchronization of the data.

Step	Action
1	Open the Service Management System screen. **Note:** If the SMS UI is already running from previous tasks, close the running instance first and then start a new instance. To start a new instance, select **Logout & Exit** from the **File** menu in the Service Management System screen.
2	Select **Operator Functions > Node Management** in the Service Management System screen. **Result:** You see the **All Nodes** tab on the Node Management screen. 

Step	Action
3	Select the **Table Replication** tab.



4	Click **Create Config File**.

Note: If you have already created a replication configuration file as part of another task and you have not changed the replication configuration, then you do not need to re-create the replication configuration file.

5	Click **OK**.
6	On the SLC node, open a shell session and review the output in the **updateLoader.log** file. This file is located at **/IN/service_packages/SMS/tmp/updateLoader.log**.

Example output

```
# tail -20f /IN/service_packages/SMS/tmp/updateLoader.log

RES: Wed Sep 29 15:09:39 2010: Node 301, started processing.
RES: Wed Sep 29 15:09:39 2010: Node 301, resynchronization pass 1, started
processing.
Sep 29 15:09:39.282806 smsCompareResyncClient (1052) NOTICE: Beginning
resynchronization for node 301.
RES: Wed Sep 29 15:09:39 2010: Node 301, resynchronization pass 1, finished
processing 0 SMS and 0 SCP records.
Sep 29 15:09:39.803041smsCompareResyncClient (1052) NOTICE: Ending
resynchronization for node 301. Resynchronization was successful.
RES: Wed Sep 29 15:09:39 2010: Node 301, finished processing 0 SMS and 0 SCP
records, resync completed successfully.
Sep 29 15:09:40.827498 updateLoader (858) NOTICE: Resynchronization Finished.
Processing Queued Updates
Node 301 SMS comparison/resync client ready.
Sep 29 15:09:40.872190 updateLoader (858) NOTICE: Finished Processing Queued
Updates
```

Configuring xmsTrigger.sh on the SLC

You must update the **xmsTrigger.sh** file to add the Messaging Manager node name configuration for the SLC node.

Follow these steps to update **xmsTrigger.sh**.

Step	Action
1	Log in to the SLC node as the user root.
2	Edit the **xmsTrigger.sh** script to add the Messaging Manager node name in the *exec* line.

SIGTRAN Configuration

Introduction

The NCC SIGTRAN component provides SIGTRAN M3UA and SUA capabilities for sending and receiving traffic. The NCC template configuration defines four default M3UA Sigtran stack instances. These are for:

- Inbound CAMEL traffic
- Inbound INAP traffic
- Inbound USSD traffic
- Inbound and outbound MAP traffic

Each stack is a separate instance of the m3ua_if process, controlled by individual startup scripts and configuration files and started from the SLEE. You will need to edit each startup script to change the settings to match the target sigtran network.

For more information on SIGTRAN, please refer to the SIGTRAN specific user documentation.

SIGTRAN Startup Scripts and Configuration Files

This table lists the startup scripts and configuration files for the sigtran SLEE interfaces.

Note: All startup scripts are located in the **/IN/service_packages/SLEE/bin** directory on the SLC. All configuration files are located in the **/IN/service_packages/SLEE/etc** directory on the SLC.

SLEE Interface	Protocol	Startup Script	Configuration File
m3uaCapIf	CAMEL	**m3ua_CAP_if.sh**	**m3ua_CAP.config**
m3uaInapIf	INAP	**m3ua_INAP_if.sh**	**m3ua_INAP.config**
m3uaUssdIf	USSD	**m3ua_USSD_if.sh**	**m3ua_USSD.config**
m3uaMmxIf	MAP	**m3ua_MMX_if.sh**	**m3ua_MMX.config**

Startup Script Parameters

The startup scripts are used to configure SCCP (for example, Global Titles, SSNs) and maximum traffic rates.

This table describes the mandatory parameters which must be configured.

Parameter	Description	Default Value
retgt	Sets the default SCCP Origination Global Title Address. The format depends on the GT type: • 1 = "1,No*a,Address_Digits*" • 2 = "2,*Trans_TypeAddress_Digits*" • 3 = "3,*Trans_Type,Num_Plan,Address_Digits*" • 4 = "4,*Trans_Type,Num_Plan,Noa,Address_Digits"* **Example** "4,0,1,4,123456789" - replace 123456789 with the GTA to be used for each SLC/stack	"4,0,1,4,123456789"
retni	Sets the National Indicator in a return address. • 0 - to set the NI to 0 (ITU). • 1 - to set the NI to 1 (ANSI).	0
retpc	Sets the default SCCP Origination Point Code. If 0, then no Point Code is set	0
retri	Sets the default SCCP Origination Address's routing indicator. • 0 - route on GT • 1 - route on PC	0
retssn	Sets the default SCCP Origination Address SSN value.	CAMEL: 146 INAP: 242 USSD: 8 MAP: 8
ssns	A comma separated list of SCCP subsystem numbers (SSNs) that this stack will register to.	CAMEL: 146 INAP: 242 USSD: 8 MAP: 8
rejectlevel	Sets the maximum number of new inbound transaction attempts (TCAP_BEGIN) per second that will be accepted by this stack.	CAMEL: 400 INAP: 50 USSD: 50 MAP: 200

Configuration File Parameters

The configuration files are used to configure SCTP and M3UA.

This table describes the mandatory configuration file parameters that you should configure.

Parameter	Description	Default Value
opc	Local point-code for this SLC/stack.	
stpPCs	List of the SG-STPs (signaling gateways) to which outbound traffic will be routed.	[1,2]
remote_host	For each signaling gateway, the primary and secondary SCTP IP address (or hostname) to be used to connect to this SG.	["sg1_sig1", "sg1_sig2"]
remote_port	SCTP port on the SG to connect to.	2900

Parameter	Description	Default Value
local_host	For each signaling gateway, the primary and secondary SCTP IP address (or hostname) to be used on the SLC to connect to this SG.	["hostname_sig1", "hostname_sig2"]
local_port	SCTP port on the SLC to connect from.	

eserv.config Configuration on the SLC

Checking eserv.config File Parameters

The **eserv.config** file on the SLC defines configuration for NCC. It is located at **/IN/service_packages/eserv.config**.

For more information on **eserv.config**, see **eserv.config** *configuration file* (on page 122).

You should review the configuration parameters listed in the following table in the **eserv.config** file. You must log in to the SLC as the user root to edit the configuration.

Parameter	Description

BeClient.clientName	Set to a unique name on each SLC node.
	Example configuration
	`BeClient = {`
	`  clientName = "slc`*X*`-ccsBeClient"`
	`}`
	Where *X* is a unique number per SLC node.

CCS.smcbMacroNodes.HomeCountryCode	Set this to the country code of the HPLMN.
	Example configuration
	`CCS = {`
	`  smcbMacroNodes = {`
	`  HomeCountryCode = "44"`
	`  }`
	`}`

CCS.ccsMacroNodes.BSAnnBalanceTypes.acsCustomerId	Change the parameter value to the ID of the 'OCNCCtemplate' ACS Customer. To determine the ACS Customer ID enter the following SQL command: **`select id from acs_customer where name = 'OCNCCtemplate';`**
CCS.ccsMacroNodes.BSAnnBalanceTypes.balTypeIds	Change the parameter value to the ID of the General Cash Balance. To determine the General Cash Balance ID enter the following SQL command: **`select id from ccs_balance_type where acs_cust_id =`** *`ID`* **`and name = 'General Cash';`** Where: • *ID* is the ACS Customer ID

Parameter	Description

XMS.xmsTrigger.adapters.GT
XMS.xmsTrigger.adapters.SCA
	Set these values to the GT and SCA which will be used in inbound MAP messages addressed to this SLC node.
	Example configuration
	`adapters = [`
	`{`
	`GT = "5114406267"`
	`SCA = "5114406267"`
	`}`
	`]`
	Note: Set these parameters in all the adapters sections of xmsTrigger.

RIMS.MAP.GT RIMS.MAP.SCA	Set these values to the GTA and SCA that will be used in outbound MAP SRI_SM messages sent out by Messaging Manager for the FDA functionality.

LCP.sriPlugin.gmscAddress
LCP.atiPlugin.gsmScfAddress
	Set these values to the GT that will be set as the originating address in outbound SRI and ATI messages used for location based capabilities.
	Example configuration
	`LCP = {`
	`sriPlugin = {`
	`gmscAddress = "441234567890"`
	`}`
	`atiPlugin = {`
	`gsmScfAddress=441234567890`
	`}`
	`}`

Rereading Configuration for inittab Processes

Follow these steps to force the system to reread the configuration for inittab processes on the SLC.

Step	Action
1	Log on to the SLC as the user root.
2	Cycle between inittab run level 2 and run level 3. Set the inittab run level to 2 by entering the following command: **`init 2`**
3	Check the run level by entering: **`who -r`** **Example output** `run-level 2 Jan 13 10:46 2 0 3`
4	Set the inittab run level to 3 by entering: **`init 3`**
5	Check the run level by entering: **`who -r`** **Example output** `run-level 3 Jan 13 10:46 3 1 2`

Configuring and Starting the SLEE

SLEE Configuration File

The Service Logic Execution Environment (SLEE) is configured in the **SLEE.cfg** file located in the **/IN/service_packages/SLEE/cfg** directory.

For information on the SLEE, see *Service Logic Execution Environment Technical Guide*.

SLEE Commands

All critical application processes on the SLC run in the SLEE.

To manually start/restart/check the status of SLEE, log in as the user `NCC_runtime user`, and enter the command:

```
/IN/bin/slee-ctrl start
```

To restart the SLEE:

```
/IN/bin/slee-ctrl restart
```

To check the status of the SLEE, and see a list of the processes that are running, enter:

```
/IN/bin/slee_ctrl status
```

Chapter 9

Verifying the NCC Installation

Overview

Introduction

This chapter explains how to verify that the Oracle Communications Network Charging and Control (NCC) applications work correctly following the installation.

In this chapter

This chapter contains the following topics.

About Verifying the Installation

Introduction

Verify the NCC installation to ensure the system works correctly after installation. This chapter describes how to set up NCC and the tests that you should run to verify the installation. These tests cover the basic features of the installation.

Prerequisites

Before you start verifying the installation, you must ensure that all:

- Nodes are running
- Post-installation tasks are completed

Note: If you have the Application Management Pack for Communications available in your Oracle Enterprise Manager installation, the availability test will be automatically reported after discovery of the nodes. Otherwise the following manual steps can be performed:

On the SMS Node

Check that the SMS processes are running by running the following commands:

```
ps -ef | grep smsNamingServer
ps -ef | grep smsTaskAgent
ps -ef | grep smsMaster
ps -ef | grep ccsBeOrb
```

Check the Oracle listener is running by running the following command:

```
lsnrctl status
```

To verify the SLC and VWS nodes on SMS:

Step	Action
1	Log in to SMS UI as super user.
2	Click the **Operators** tab and select **Node Management.**
3	In the **All Nodes** screen, enter the node details in the **Node Name** field. The node name can be either SLC or VWS.
4	In the **Replication Nodes** screen, enter the node number in the **Node Number** field.
5	Click **Find**. The **Find Replication Node** dialogue box appears.
6	Click **Search**. **Result:** The available nodes details are displayed.

On the SLC Node

Check that the SLC processes are running by running the following commands:

```
ps -ef | grep slee_acs
ps -ef | grep replicationIF
ps -ef | grep diameterBeClient
ps -ef | grep BeClient
```

On VWS Node

Check that the SLC processes are running by running the following commands:

```
ps -ef | grep beServer
ps -ef | grep beVWARS
ps -ef | grep beSync
ps -ef | grep beGroveller
```

About Collecting Diagnostic Data with RDA HCVE

Overview

Remote Diagnostic Agent (RDA) is an Oracle standard tool that you use to collect diagnostic data about your NCC system. When you submit a service request (SR) to Oracle Technical Support, you must also provide an RDA output file. The RDA output file provides a comprehensive view of your system configuration and contains diagnostic data used by Oracle Technical Support to diagnose problems. This minimizes the number of requests from Oracle Technical Support for additional information, which can reduce the service request resolution time.

RDA includes a Health Check Validation Engine (HCVE) module that checks your NCC installation for known issues and common practices that impact performance, availability, and functionality. When you run HCVE, it generates a detailed report in both HTML and text formats that detail possible issues it has found on your system. You can then use the report for preventive maintenance to avoid any service disruption.

HCVE Validations on NCC Systems

RDA HCVE performs a variety of checks of your NCC system, such as ensuring that:

- Sufficient memory and disk space is available.

- The appropriate packages and scripts are installed and are configured correctly.
- The appropriate flags and parameters are set.
- acsDbCleanup.sh is configured correctly.
- The log files are set up correctly.
- The NCC system is configured to startup and shutdown the Oracle database appropriately.
- The appropriate permissions for running scripts are set correctly.

HCVE Validations on NCC Databases

RDA HCVE performs a variety of checks of your NCC database, such as ensuring that:

- The user running HCVE has sufficient privileges
- There are no invalid objects in the Oracle Database instance
- Database parameters, such as **_job_queue_process**, are set to appropriate values

Downloading and Installing RDA

Follow these steps to download and install the RDA software:

Step	Action
1	Go to the My Oracle Support Web site: http://support.oracle.com
2	In the **Knowledge Base Search & Browse** section, enter `314422.1` in the **Enter Search Terms** field, and then click **Search**.
3	In the search results, click the **Remote Diagnostic Agent (RDA) - Getting Started** link. **Result:** The Remote Diagnostic Agent (RDA) - Getting Started page is displayed.
4	In the **RDA Bundle** section of the page, click the link for the appropriate operating system.
5	Follow the directions in the **Installation Instructions** section of the page to install the RDA software.

Running HCVE on Your NCC System

Follow these steps to collect data about your NCC system:

Step	Action
1	Log in as the root user.
2	Go to the directory in which you installed RDA. **Note:** The default RDA installation directory is **/IN/service_packages/SUPPORT/rda**.
3	Run data collection by entering the following command: `./rda.pl -dT hcve:Pncc44os_sol`
4	Answer the prompts. **Result:** HCVE generates an output file.
5	Send the output file to Oracle Technical Support.

Running HCVE on NCC Databases

Follow these steps to collect data about your NCC database:

Step	Action
1	Log in as the oracle user.
2	Go to the directory in which you installed RDA. **Note:** The default RDA installation directory is **/IN/service_packages/SUPPORT/rda**.
3	Run data collection by entering the following command: `./rda.pl -dT hcve:Pncc44db_gen.xml`
4	Answer the prompts. **Result:** HCVE generates an output file.
5	Send the output file to Oracle Technical Support.

Appendix A

NCC OUI Installer Screens

Overview

This appendix describes the information you need to provide for each screen when you install Oracle Communications Network Charging and Control (NCC) in interactive mode. You can also access the information by clicking Help during installation.

Note: This document does not substitute for NCC installation instructions. You should read all chapters in NCC Installation Guide in preparation for installing NCC, including "*NCC System Requirements* (on page 9)" for information you need to collect in preparation for installation, and "*Installing NCC* (on page 57)" for installation procedures.

NCC OUI Installer Screens

Installation Inventory

Specify the name and location of the directory where all Oracle installations are done.

Field	Description
Inventory Directory	Enter the name and the full path to the directory where all Oracle installations are done.
Operating System Group	Select the primary Oracle inventory group.

Installation Location

Specify the name and location of the directory in which to install NCC.

Field	Description
Application Home Path	Enter the full path to the **/IN** directory in which to install NCC.

Installation Type

Select the installation type.

Field	Description
SMS	Installs the NCC Service Management System (SMS) application and the SMS database. You use the SMS GUI to configure and manage NCC.
SLC	Installs the NCC Service Logic Controller (SLC) application and the SLC database. You use SLC to provide the logic to manage the calls, sessions, messages in NCC. **Note:** Ensure that SMS is installed before installing SLC.

Field	Description
SLC With Test Tools	Installs the NCC Service Logic Controller (SLC) application, the SLC database, and the SLC test tools. **Note:** Ensure that SMS is installed before installing SLC With Test Tools.
VWS	Installs the NCC Voucher and Wallet Server (VWS) application and VWS database. The Voucher and Wallet Server manages charging, vouchers, balances, and subscribers. **Note:** Ensure that SMS is installed before installing VWS.

Oracle User

Enter the Oracle database user details.

Field	Description
Oracle DB owner	Retain the default, **oracle**, which is the user name with permissions to create the Oracle database instance.
Oracle DB group	The OS group which owns the Oracle database. For example ‘dba’.

Application User

Enter the NCC runtime user details.

Field	Description
Application owner	The NCC_runtime_user i.e. the OS user that will run the application.
Application group	The NCC OS group. Fixed to ‘esg’.

Database Location

Select one from the provided options.

Option	Description
The database, schema and application will all be installed	Select this option to install all items on the same node.
The database already exists and both the schema and application will be installed	Select this option if you have already created the database including datafiles on this or a remote node but not the database schema or application.
The database and schema already exists and only the application will be installed	Select this option if the database and schema already exists on this or a remote node and you want to only install the application.

Database Datafiles

Database Server Paths

Specify the location of the base directory and the Oracle home directory.

Field	Description
Base directory	Enter the name and the full path to the **oracle** base directory in which the database creation scripts are installed. The **oracle** base directory is the directory in which the Oracle database is installed.
Oracle home	Enter name and the full path to the Oracle Database home directory in which Oracle 19*c* database is installed.

Datafile and Redolog Paths

Specify the location of the datafile and redo log directories.

Field	Description
Datafile directory	Enter the full path to the directory where the oracle datafiles are stored.
Redo log directory	Enter the full path to the directory to store the database redo log files.

Database User Password

Specify a password for the database schema user accounts.

Field	Description
Oracle SID	Oracle SID
Database user (smf, scp or e2be_admin)	Database username
Oracle database password	Enter the password for the Oracle database administrative accounts.
Confirm password	Re-enter your password to confirm.

Database Type Selection

Select one from the provided options.

Option	Description
Standard Database	Select this option to install traditional database.
RAC/Multi-tenant Database	Select this option to install multi-tenant database. For example, select this option for 26ai database installation.

Oracle Client Path

Specify the Oracle Database Client home directory.

Field	Description
Oracle client home	Enter the full path to the Oracle Database Client home directory.

Pre-existing Database Details

Specify the hostname, username, and password for the existing database connection.

Field	Description
Oracle SID	Enter the Oracle SID.
Database hostname	Enter the hostname where the database is located.
Database user (smf, scp or e2be_admin)	Enter the database username.
Oracle database password	Enter the password for the Oracle database administrative accounts.
Database Port	Enter the port that is required to connect to the database host.
Service database hostname	Enter the fully qualified service DB hostname. For 26ai database, enter <Database name>.<remote database host short name> Example: <smf|scp|e2be>.<remote database host short name>

SMS GUI

Enter the information for SMS GUI.

Field	Description
Screen superuser password	Enter the password for the SMS GUI administrator user account.
Confirm password	Enter the password again for confirmation.
Timezone	Enter the time zone in which the date and time are displayed in the SMS GUI.

PI Admin

Enter the information for Provisioning Interface (PI) configuration.

Field	Description
PI admin password	Enter the password for PI administrator user account.
Confirm password	Enter the password again for confirmation.

SMS EDR Paths

Enter the path to the directories in which the SMS event data record (EDR) files are stored.

Field	Description
CDR Loader Input directory	Retain the default path to the directory of a single file system to store CDR input files.
CDR Loader Output directory	Retain the default path to the directory of a single file system to store CDR output files.

Default Template

Select the option to install default template.

Field	Description
Install PCST	Check the box to install Prepaid Charging Service Template (PCST).

Default Currency

Enter the details of default system currency.

Field	Description
System Currency	Select the currency name from the Name drop down box. **Note**: Only valid currency names are available from the list.
Base Value	Enter the ratio of subunits to main units of currency in the Base field. Example: 100 cents per euro = a ratio of 100.
Big Symbol	Enter the symbol that represents the main unit of the currency in the Big Symbol field (for example, € for euros).
Little Symbol	Enter the symbol that represents the subunit of the currency in the Little Symbol field (for example, c for cents).
Separator	Enter the separator used to separate the main unit from the subunit of the currency in the Separator field. Example: In the currency of: Euros - the separator is a comma (for example, 3,20) Dollars - the separator is a decimal point (for example, $4.00)

Replication

Enter the information of the SMS host from which the current node is replicated.

Field	Description
SMS Host name	Enter the qualified hostname for the SMS server used to configure the clients that will connect to the SMS server.

VWS Config

Enter the information Voucher and Wallet Server (VWS) configuration.

Field	Description
SMS EDR Input directory	Enter the name and the full path to the directory in which the SMS event data record (EDR) input files are stored.
Primary VWS node	Select to install the primary node of a VWS pair.

Appendix B

Maintaining a Remote Database

If the SMS node is on a remote database, the following scripts (which require DBA privileges) should be run on the database node, or equivalent schema management for partitioning needs to be implemented:

- smsAddArchiveLog.sh
- hotbackup.sh
- archbackup.sh
- oraLockMonitor.sh
- fragmentation_install_oui.sh
- CCSPART_uninstall.sh
- CCSPART_create_schema.sh
- CCSPART_maintenance.sh
- CCSPART_statistics.sh
- CCSPART_capacity_monitor.sh
- CCSCPART_check_oracle.sh
- CCSCPART_statistics.sh
- CCSCPART_add_week.sh
- CCSCPART_capacity_monitor.sh
- CCSCPART_restart_job_processes.sh
- CCSCPART_install.sh
- CCSCPART_rman_exclude.sh
- CCSCPART_maintenance.sh
- CCSCPART_uninstall.sh
- CCSCPART_drop_week.sh
- CCSCPART_list_partitions.sh
- CCSVCHRPART_uninstall.sh
- CCSVCHRPART_statistics.sh
- CCSVCHRPART_capacity_monitor.sh
- CCSVCHRPART_maintenance.sh
- CCSVCHRPART_create_schema.sh

Installing Network Charging and Control on a Remote Database Using the OUI Installer (For 19c)

This section describes how to install Network Charging and Control using a remote database by deploying the database schemas and applications with the Oracle Universal Installer and completing the required configuration and verification tasks.

Install the SMS, SLC, and VWS schemas on a dedicated remote database server using the OUI. Then install each application component (SMS, SLC, VWS) on separate nodes. Before you begin, you must prepare the remote database server, set required environment variables, assign directory permissions, configure network files, and create the required Oracle Wallet credentials.

Prerequisites

Before starting the installation, ensure that you have completed all pre-installation tasks described in *NCC Pre-Installation Tasks* (on page 43)

Linux Asynchronous I/O Configuration

For installations using Linux and Oracle Database versions 10.2 through 12.1, you might need to set the maximum number of asynchronous I/O requests allowed by the operating system.

If you are installing the database schema on a remote database server, perform the following steps on the remote database server.

1. Install the database schema and application on the remote server using OUI installer in a server. After this installation, treat that server as the remote database host for all subsequent nodes. See *NCC Pre-Installation Tasks* (on page 43) for details.
2. If you're installing using Linux, set the maximum number of asynchronous I/O requests. If you use Oracle Database 10.2 to 12.1, edit `/etc/sysctl.conf` and add:

   ```
   fs.aio-max-nr = 3145728
   ```

   Then run:

   ```
   /sbin/sysctl -p /etc/sysctl.conf
   ```

Installing the Database and Schema on the Remote Server Using the OUI Installer

1. Before installing each component, export the appropriate ORACLE_SID:
   - Before installing SMS:
     `export ORACLE_SID=SMF`
   - Before installing SLC:
     `export ORACLE_SID=SCP`
   - Before installing VWS:
     `export ORACLE_SID=E2BE`
2. Install the SMS database and schema on the remote database server, then install the SMS application on its designated server.
   You must fully complete the installation of both the SMS database schema and the SMS application before you attempt to install the SLC or VWS components. See Installing Applications Using the OUI Installer section for more information.

3. During SLC and VWS Database and Schema installation, on the Replication Configuration screen, enter the SMS application node name in the **SMS Hostname** field where the SMS application is installed.

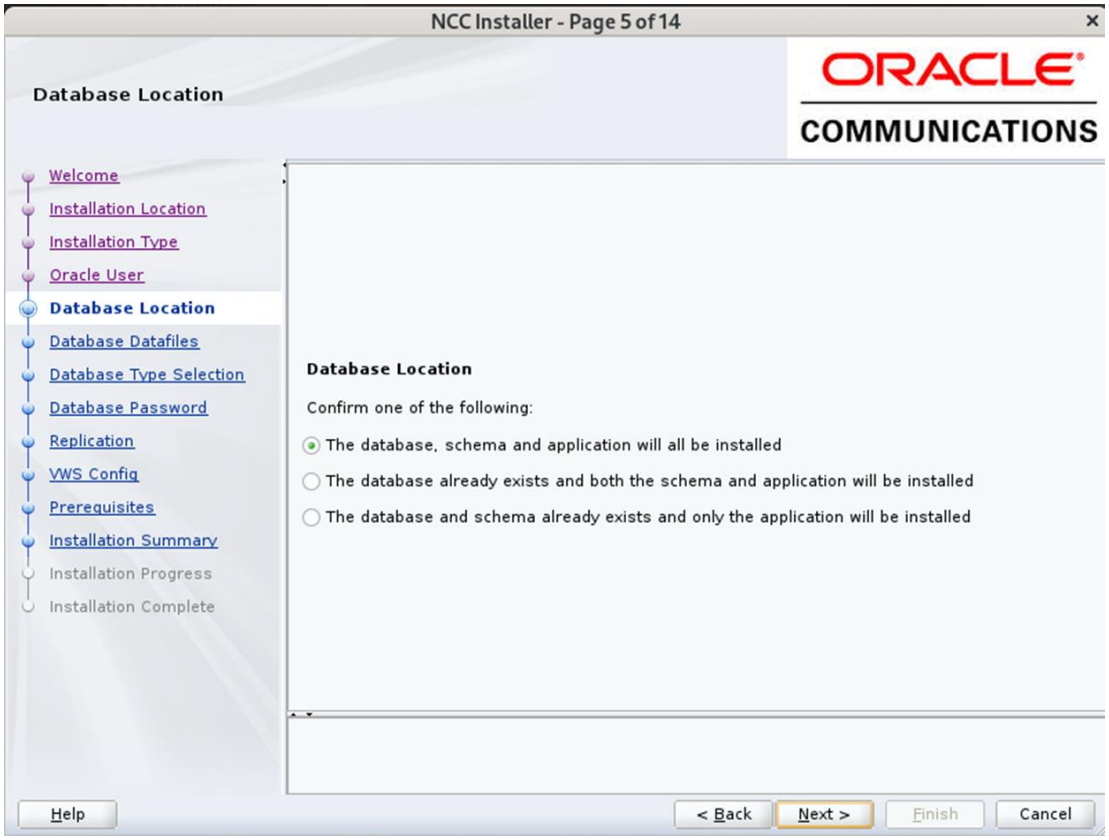
Installing SMS Database and Schema

Follow the steps below to install SMS database and schema:

1. Log in to the remote database server as the LDAP user.
2. Launch the OUI installer.
3. On the Database Installation Mode screen, select **Database Location** in the left pane.

The Database Location window appears.

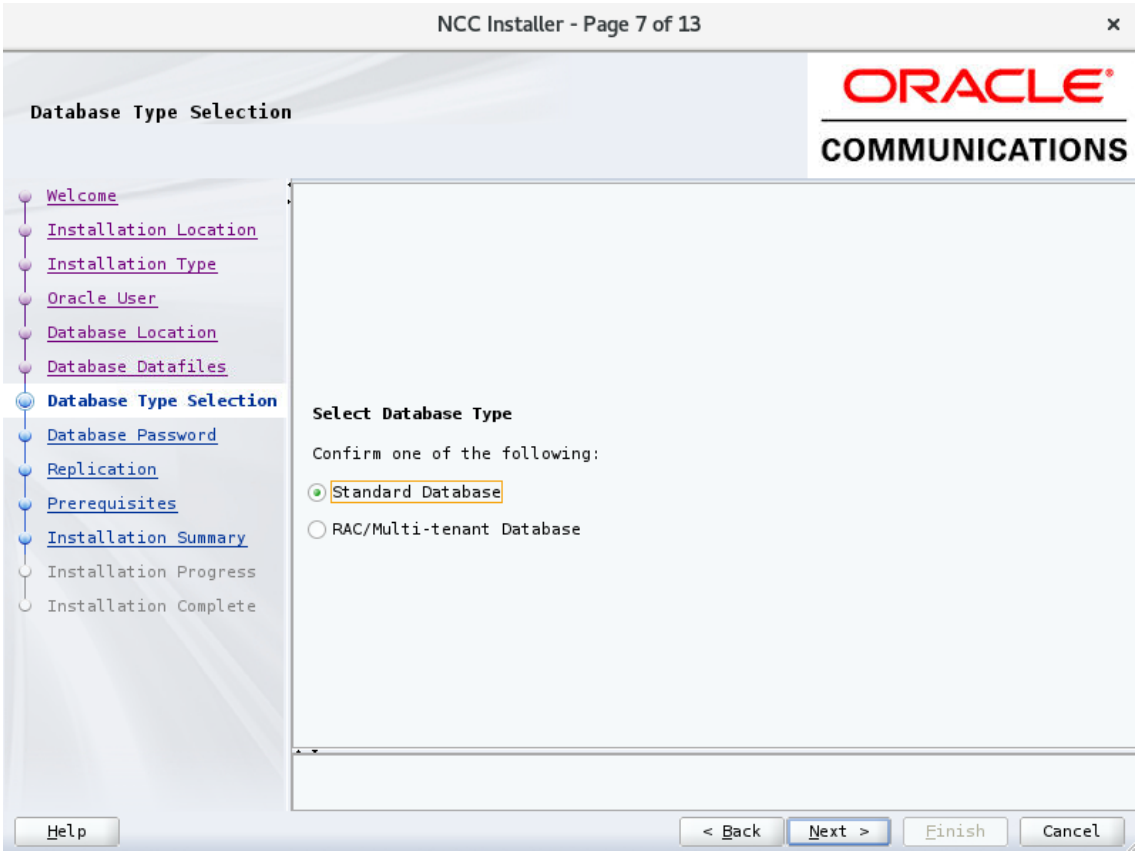
4. In the Database Location window, select **The database, schema and application will all be installed**:



5. In the left pane, select **Database Type Selection**.

The Selection Database Type window appears.

6. In the Select Database Type window, select the database type as **Standard Database** and complete the SMS installation:



Renaming Installation Directories

Follow the steps below to rename the installation directories:

1. After completing the SMS installation on the remote server, rename the `IN` directory:
   - Rename `IN` to `IN_SMS`.
2. Install the SLC database and schema using OUI, and then rename the directory:
   - Rename `IN` to `IN_SLC`.
3. Install the VWS database and schema using OUI, and then rename the directory:
   - Rename `IN` to `IN_VWS`.

Consolidating Database Files on the Remote Database Server

After completing the SMS, SLC, and VWS database and schema installations, perform the following steps on the remote database server:

1. Rename `IN_SMS` back to `IN`, or create a symbolic link:

   ```
   ln -s IN_SMS IN
   ```

2. Copy the SLC database files:

   ```
   Copy SCP directory from /IN_SLC/oracle/datafiles to /IN/oracle/datafiles
   ```

3. Copy the VWS database files:

```
Copy E2BE directory from /IN_VWS/oracle/datafiles to /IN/oracle/datafiles
```

4. Change ownership of all database-related files:

```
chown oracle:dba *
```

Apply this ownership change to all files (database files, control files, and related files) in the following directories:

- `/IN/oracle/datafiles/SMF`
- `/IN/oracle/datafiles/SCP`
- `/IN/oracle/datafiles/E2BE`

Updating Ownership Under /IN/service_packages

On the remote database server, update ownership for the following directories under `/IN/service_packages`:

1. CCSPART
   - Set owner and group to `oracle:esg` for the directory and all files and subdirectories.
2. SMS
   - Set owner and group to `smf_oper:esg` for all files and subdirectories.
3. CCSVCHRPART
   - Set owner and group to `oracle:esg` for the directory and all files and subdirectories.
4. CCS
   - Set owner and group to `smf_oper:esg` for all files and subdirectories.
5. Copy the following files:
   - Copy `variables_vws.sh` from the `etc` directory under `IN_VWS` to `/IN/etc`.
   - Copy `variables_scp.sh` from the `etc` directory under `IN_SLC` to `/IN/etc`.

Other modules under `/IN/service_packages` can be removed or retained. However, the modules listed above are mandatory because they are required to run cron jobs and because the profile files located in these directories are required.

Updating tnsnames.ora and listener.ora on the Remote Database Server

Update the `tnsnames.ora` and `listener.ora` files located under `/IN/etc` on the remote database server. If a secondary VWS instance exists, update that instance as well. After updating these files, restart the SMS, SLC, and VWS databases and restart the listener. If any required database instance does not start, update the `ORACLE_SID` entry in the `listener.ora` file.

Sample tnsnames.ora:

```
# TNS alias for the SMF database. SMF =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = <Remote_database_server_hostname>) (PORT
= 1521))

(CONNECT_DATA = (SERVER = DEDICATED)

(SID = <ORACLE_SID_OF_SMS>)

)

)

SCP =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = <Remote_database_server_hostname>) (PORT
= 1521))

(CONNECT_DATA = (SERVER = DEDICATED)

(SID = <ORACLE_SID_OF_SLC>)

)

)

E2BE =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = <Remote_database_server_hostname>) (PORT
= 1521))

(CONNECT_DATA = (SERVER = DEDICATED)

(SID = <ORACLE_SID_OF_VWS>)

)

)
```

Sample listener.ora:

```
LISTENER = (DESCRIPTION =

(ADDRESS_LIST =

(ADDRESS = (PROTOCOL = TCP)(PORT = 1521))

)

)

SID_LIST_LISTENER = (SID_LIST =

(SID_DESC =

(SID_NAME = <ORACLE_SID_SMS>)

(ORACLE_HOME = /u01/app/oracle/product/19.0.0)
```

```
 )
 )
 (SID_LIST = (SID_DESC =
 (SID_NAME = <ORACLE_SID_SLC>)
 (ORACLE_HOME = /u01/app/oracle/product/19.0.0)
 )
 )
 (SID_LIST = (SID_DESC =
 (SID_NAME = <ORACLE_SID_VWS>)
 (ORACLE_HOME = /u01/app/oracle/product/19.0.0)
 )
 )
 LOG_LEVEL_LISTENER = OFF
 LOGGING_LISTENER = OFF
 CONNECT_TIMEOUT_LISTENER = 10
 STARTUP_WAIT_TIME_LISTENER = 0
 TRACE_LEVEL_LISTENER = OFF
 ADMIN_RESTRICTIONS_LISTENER=ON
```

Creating the Oracle Wallet on the Remote Database Server

Follow the steps below to create the Oracle wallet on the remote database server:

1. Create the wallet directory:

```
mkdir -p /IN/wallet
```

2. Change to the wallet directory:

```
cd /IN/wallet
```

3. Create the wallet with auto-login enabled:

```
  orapki wallet create -wallet . -auto_login
```

4. Create credentials for each schema:

```
  mkstore -wrl /IN/wallet -createCredential E2BE E2BE_ADMIN manager
mkstore -wrl /IN/wallet -createCredential SCP SCP manager
    mkstore -wrl /IN/wallet -createCredential SMF SMF manager
```

5. Set the wallet permissions:

```
sudo chmod -R 750 /IN/wallet
```

6. Restart the listener after completing wallet configuration.

Stopping Database Instances on the Remote Database Server

Follow the steps below to stop database instances on the remote database server:

1. Log in to the remote database server as the LDAP user.
2. Switch to the oracle user:

```
su – oracle
```

3. Stop the listener:

```
lsnrctl stop
```

4. Shut down the SMF instance:

```
export ORACLE_SID=SMF; echo $ORACLE_SID; sqlplus /
as sysdba

shutdown immediate
```

5. Shut down the SCP instance:

```
export ORACLE_SID=SCP; echo $ORACLE_SID; sqlplus /
as sysdba

shutdown immediate
```

6. Shut down the E2BE instance:

```
export ORACLE_SID=E2BE; echo $ORACLE_SID; sqlplus /
as sysdba

shutdown immediate
```

Starting Database Instances on the Remote Database Server

Follow the steps below to start database instances on the remote database server:

1. Log in as the LDAP user and switch to the oracle user.
2. Start the SMF instance:

```
export ORACLE_SID=SMF; echo $ORACLE_SID; sqlplus /
as sysdba

startup pfile='/u01/app/oracle/product/19.0.0/dbs/initSMF.ora'
```

3. Start the SCP instance:

```
export ORACLE_SID=SCP; echo $ORACLE_SID; sqlplus /
as sysdba

startup pfile='/u01/app/oracle/product/19.0.0/dbs/initSCP.ora'
```

4. Start the E2BE instance:

```
export ORACLE_SID=E2BE; echo $ORACLE_SID; sqlplus /
as sysdba
```

```
startup pfile='/u01/app/oracle/product/19.0.0/dbs/initE2BE.ora'
```

5. Start the listener:

```
lsnrctl start
```

Configuring Maintenance Cron Jobs on the Remote Database Server

Configure the following cron jobs for the Oracle user on the remote database server. If these cron jobs are not already present, you must configure them:

CDR Partitions

```
30 * * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSPART/bin/CCSPART_capacity_monitor.sh ) >
  /IN/service_packages/CCSPART/tmp/ CCSPART_capacity_monitor.sh.log 2>&1

30 7 * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSPART/bin/CCSPART_log_cleaner.sh ) > /IN/service_packages/CCSPART/tmp/
  CCSPART_log_cleaner.sh.log 2>&1

30 1 * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSPART/bin/CCSPART_maintenance.sh ) > /IN/service_packages/CCSPART/tmp/
  CCSPART_maintenance.sh.log 2>&1

0 2 * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSPART/bin/CCSPART_statistics.sh ) > /IN/service_packages/CCSPART/tmp/
  CCSPART_statistics.sh.log 2>&1
```

Voucher Partitions

```
40 * * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSVCHRPART/bin/CCSVCHRPART_capacity_monitor.sh ) > /IN/service_packages/
  CCSVCHRPART/tmp/CCSVCHRPART_capacity_monitor.sh.log 2>&1

20 7 * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSVCHRPART/bin/CCSVCHRPART_log_cleaner.sh ) > /IN/service_packages/
  CCSVCHRPART/tmp/CCSVCHRPART_log_cleaner.sh.log 2>&1

30 2 * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
  CCSVCHRPART/bin/CCSVCHRPART_maintenance.sh ) > /IN/service_packages/
  CCSVCHRPART/tmp/CCSVCHRPART_maintenance.sh.log 2>&1

    0 3 * * * ( . /IN/service_packages/CCS/.profile ; /IN/service_packages/
    CCSVCHRPART/bin/CCSVCHRPART_statistics.sh ) > /IN/service_packages/
    CCSVCHRPART/tmp/CCSVCHRPART_statistics.sh.log 2>&1
```

Installing Applications Using the OUI Installer

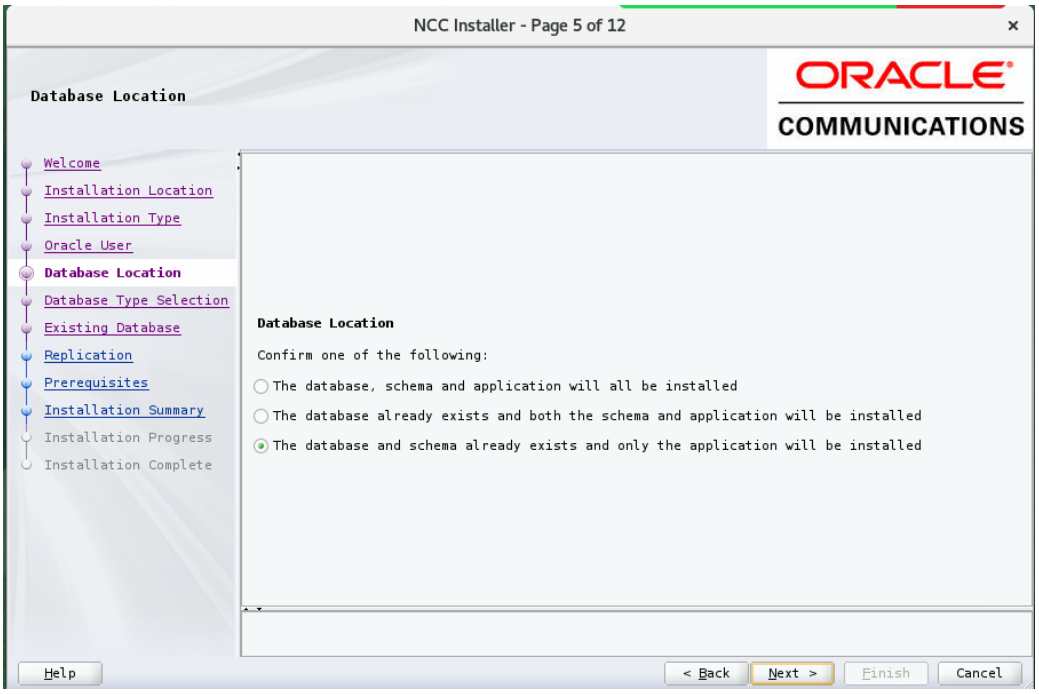
Follow the steps below to install the SMS, SLC, and VWS applications on three different application nodes using the OUI installer:

1. Log in as the LDAP user on each application server.
2. Launch the OUI installer.
3. On the Database Installation Mode screen, select **Database Location** in the left pane.

   The Database Location window appears.

4. In the Database Location window, select **The database and schema already exist and only the**

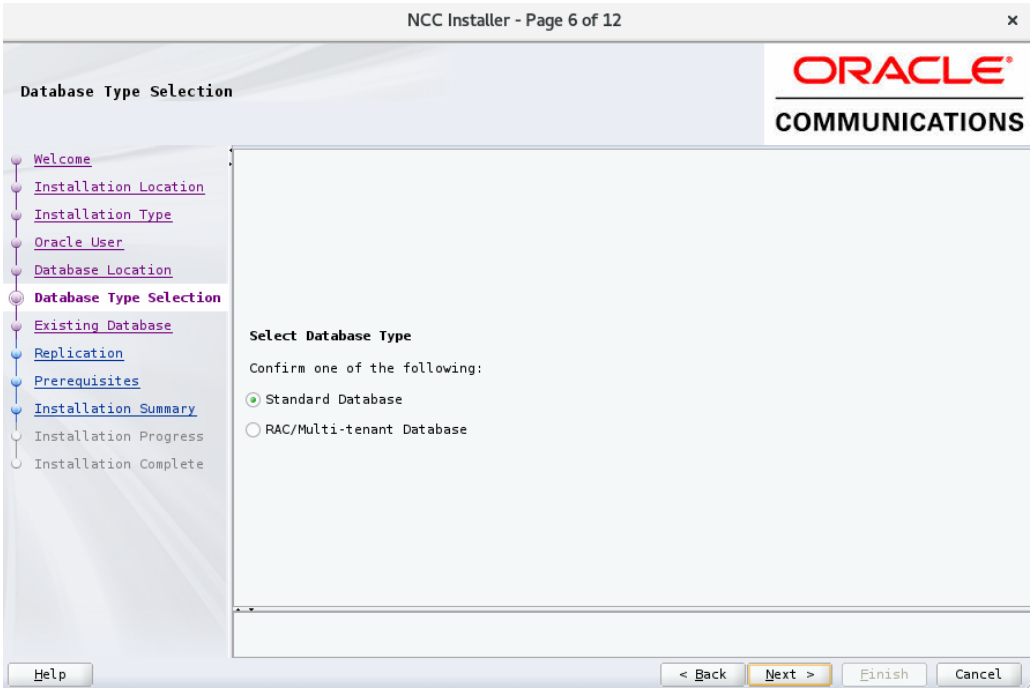
application will be installed:



5. In the left pane, select **Database Type Selection**.

The Select Database Type window appears.

6. In the Select Database Type window, select the database type as **Standard Database**:



7. On the pre-existing database details page, enter the remote database server hostname in the **Database Hostname** field and complete the installation.

8. On each application server, verify the database connectivity configuration files located under

/IN/etc by performing the following checks:

a. Ensure that the tnsnames.ora file contains the correct remote database host name (<Remote_database_server_name>).

b. Verify that the entries are appropriate for the specific application node.

The following is an example of tnsnames.ora on the SMS application node:

```
# TNS alias for the SMF database. SMF =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = <Remote_database_server_name>)
  (PORT = 1521))
(CONNECT_DATA = (SERVER = DEDICATED) (SID = <ORACLE_SID>)
)
)
```

Note:

- On the SMS application node, the tnsnames.ora file must contain only the SMF entry. It must not include SLC or VWS (E2BE) entries.
- On the SLC application node, the tnsnames.ora file must contain only the SLC (SCP) entry. It must not include SMF or VWS (E2BE) entries.
- On the VWS application node, the tnsnames.ora file must contain only the VWS entry. It must not include SMF or SLC entries.
- On the remote database server, the tnsnames.ora file must contain all required entries for SMS, SLC, and VWS.

9. Verify that the listener.ora file on the remote database server is correctly configured. See *Updating tnsnames.ora and listener.ora on the Remote Database Server* (on page 161) for more details.

Use the following example for reference:

```
LISTENER = (DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP)(PORT = 1521))
)
)
SID_LIST_LISTENER = (SID_LIST =
(SID_DESC =
(SID_NAME = <ORACLE_SID>)
(ORACLE_HOME = /u01/app/oracle/product/19.0.0)
)
)
LOG_LEVEL_LISTENER = OFF
LOGGING_LISTENER = OFF
```

```
CONNECT_TIMEOUT_LISTENER = 10
STARTUP_WAIT_TIME_LISTENER = 0
TRACE_LEVEL_LISTENER = OFF
ADMIN_RESTRICTIONS_LISTENER = ON
```

10. Repeat the verification on the SLC and VWS application servers to ensure their configurations match the requirements described above.

Verifying Remote Database Access from Application Server

Follow the steps below to check that the application server can connect to the remote database before and after installing NCC:

1. Before you start the installation, check that the application server can connect to the remote database using a database username and password.

2. Log in to the server where you plan to install Network Charging and Control as the `smf_oper` user or the `oracle` user.

3. Run the following command to test the connection to the remote database:

   Syntax

   ```
   sqlplus
      "<username>/<password>@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(
      PROTOCOL=TCP)

   (HOST=<remote database
      hostname>)(PORT=1521)))(CONNECT_DATA=(SERVER=DEDICATED)

    (SID=<ORACLE_SID)))"
   ```

   Update the values in the command as needed:

   - Database username and password
   - Remote database host name
   - Database SID (`SMF`, `SCP`, or `E2BE`)

   This check confirms that the database is reachable before installation and does not use TNS configuration files.

Verifying Connectivity Using TNS Aliases

Note: Run these checks only after the NCC installation finishes**,** because the required TNS files are created during installation.

Follow the steps below to check database connectivity using TNS aliases after installation:

1. Log in to each application node as the `smf_oper` user to check the database connection using the connected strings in the `tnsnames.ora` file.

2. Run the following commands to test the connections:

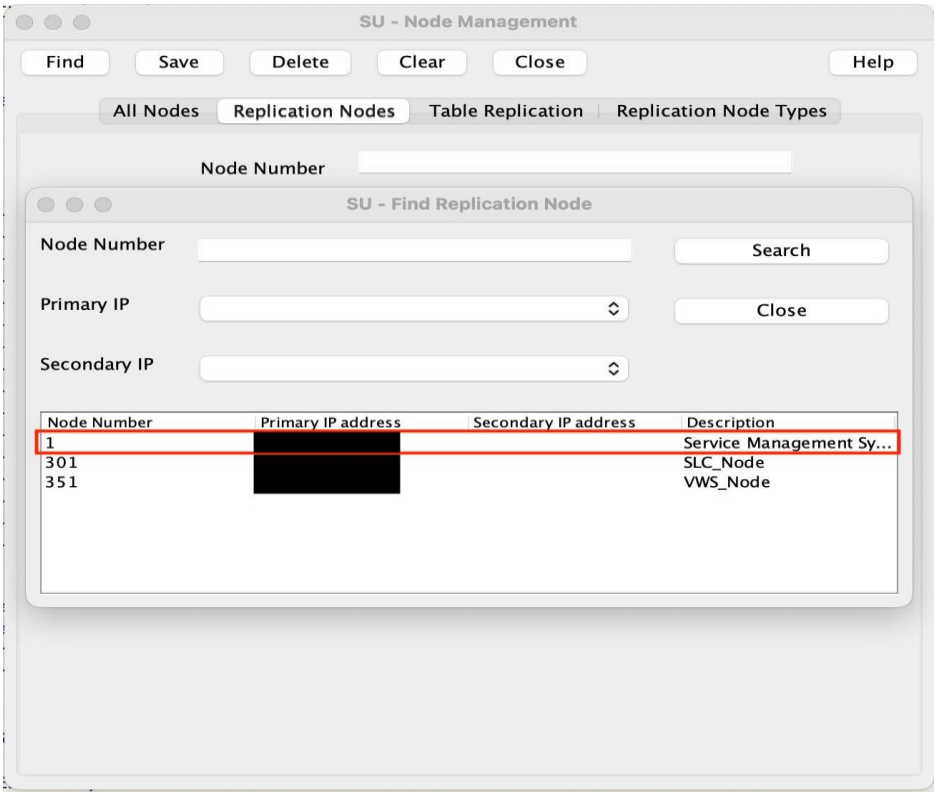
```
sqlplus /@SMF

sqlplus /@SCP

sqlplus /@E2BE
```

Launching the SMS GUI

Note: In the SMS GUI:

- Check that all application node addresses appear in the Node Management screen.
- On the Replication Nodes tab, make sure the **Node Number** for the SMS application node is set to **1**.

The following figure shows the Replication Nodes tab in the Node Management screen:



To launch the SMS GUI, follow the steps below:

1. Open the `smsGui.sh` or `smsGui.bat` file located in the `/IN/html` directory on the SMS application node.
2. Verify that the file contains the correct remote database host name in the required fields. If the information is missing or incorrect, update the file before proceeding.
3. Set the `databaseHost` parameter so that it points to the remote database server where the database is installed:

```
-Djnlp.sms.databaseHost=<Remote_database_server_name>:<port>:<ORACLE_SID>
```

4. Configure the secure database connection parameter as follows:

```
-
Djnlp.sms.secureConnectionDatabaseHost="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS
=(PROTOCOL=TCPS)
(HOST=<Remote_database_server_name>)(PORT=2484)))
(CONNECT_DATA=(SERVICE_NAME=SMF)))"
```

These parameters are mandatory for successfully launching the SMS GUI when the database is hosted on a remote database server.