Cisco ASR 5000 Series Subscriber Service Controller Installation and Administration Guide

Version 12.1

Last Updated December 21, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23965-04

Cisco ASR 5000 Series Subscriber Service Controller Installation and Administration Guide

CONTENTS

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis.

This preface includes the following sections:

- Conventions Used
- Contacting Customer Support
- Additional Information

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents text that appears on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter at the CLI, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* *`slot_number`* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**.

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[**`keyword`** or *`variable`*]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support alternative variables. These “options” are documented within braces or brackets by separating each variable with a vertical bar. These variables can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Go to http://www.cisco.com/cisco/web/support/ to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Cisco ASR 5000 Installation Guide*
- *Cisco ASR 5000 System Administration Guide*
- *Cisco ASR 5x00 CDMA Command Line Interface Reference*
- *Cisco ASR 5x00 eHRPD / LTE Command Line Interface Reference*
- *Cisco ASR 5x00 GPRS / UMTS Command Line Interface Reference*
- *Cisco ASR 5x00 Thresholding Configuration Guide*
- *Cisco ASR 5x00 SNMP MIB Reference*
- *Web Element Manager Installation and Administration Guide*
- *Cisco ASR 5x00 AAA Interface Administration and Reference*
- *Cisco ASR 5x00 GTPP Interface Administration and Reference*
- *Cisco ASR 5x00 Release Change Reference*
- *Cisco ASR 5x00 Statistics and Counters Reference*
- *Cisco ASR 5x00 Gateway GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 HRPD Serving Gateway Administration Guide*
- *Cisco ASR 5000 IP Services Gateway Administration Guide*
- *Cisco ASR 5x00 Mobility Management Entity Administration Guide*
- *Cisco ASR 5x00 Packet Data Network Gateway Administration Guide*
- *Cisco ASR 5x00 Packet Data Serving Node Administration Guide*
- *Cisco ASR 5x00 System Architecture Evolution Gateway Administration Guide*
- *Cisco ASR 5x00 Serving GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 Serving Gateway Administration Guide*
- *Cisco ASR 5000 Session Control Manager Administration Guide*
- *Cisco ASR 5000 Packet Data Gateway/Tunnel Termination Gateway Administration Guide*
- Release notes that accompany updates and upgrades to the StarOS for your service and platform

Chapter 1
Subscriber Service Controller (SSC) Overview

This chapter provides an overview of the Subscriber Service Controller (SSC) which provides extended centralized PCRF and SPR functionality in Cisco PCC solution and manages data related to service usage and subscriber profile for IP-CAN session.

SSC is an integral part of Cisco's Policy Control and Charging (PCC) solution. It is designed to be used in conjunction with Intelligent Policy Control Function (IPCF) on Cisco© chassis and the Policy Provisioning Tool (PPT) on Cisco© UCS or Solaris platform.

This chapter contains following sections:

PCC Solution Elements

This section provides a brief overview of PCC solution components.

The Cisco Policy and Charging Control (PCC) solution includes following functional entities:

- Intelligent Policy Control Function (IPCF)
- Subscriber Service Controller (SSC)
- Policy Provisioning Tool (PPT)

Intelligent Policy Control Function (IPCF)

This section briefly describes IPCF.

IPCF provides policy control and charging rule functions in a core network. IPCF acts as a Policy Charging and Rules Function (PCRF) supplemented with usage monitoring capability that enables policies around data consumption. IPCF interfaces with Policy Charging and Enforcement Function (PCEF) over standard **Gx** interface.

Cisco IPCF is compliant with 3GPP standard in operator's core network. It performs following key functions:

- Derive and authorize the QoS information for the service data flow for session as well as bearer use.
- Select appropriate charging criteria and mechanism apt for data usage.
- Provide network control regarding the service data flow detection and gating.
- Ensure that the PCEF user plane traffic treatment is in accordance with user's subscription profile.
- Correlate service and charging information across PCEF and Application Function (AF).

Important: For more information on IPCF function and supported interfaces, refer *Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide*.

Subscriber Service Controller (SSC)

This section briefly describes SSC.

SSC provides the SPR functionality for the Cisco PCC solution that is compliant with 3GPP R8, and uses an extended implementation of 3GPP Sh messaging for exchanging static as well as dynamic subscriber profile data with IPCF. SSC allows the enforcement of aggregate rules supporting volume usage across groups of subscribers sharing common account. It also provides optional decision center functionality.

SSC provides a centralized and simplified policy management for the network. It interfaces with IPCF over **Sp** interface which is based on standard **Sh** protocol, for subscriber profile and usage related transactions. SSC also supports a proprietary interface to receive event notification data from IPCF.

Policy Provisioning Tool (PPT)

This section briefly describes PPT.

The PPT is a GUI-based policy and profile management tool in the PCC solution that allows operators to perform subscriber policy provisioning and management functions.

The PPT interfaces with IPCF as well as SSC to provide centralized policy management interface for operators.

Important: For more information on PPT function and supported interfaces, refer *PolicyProvisioning Tool Installation and Administration Guide*.

SSC Introduction

SSC is an application that complements and extends the functionality of PCRF in Cisco PCC solution.

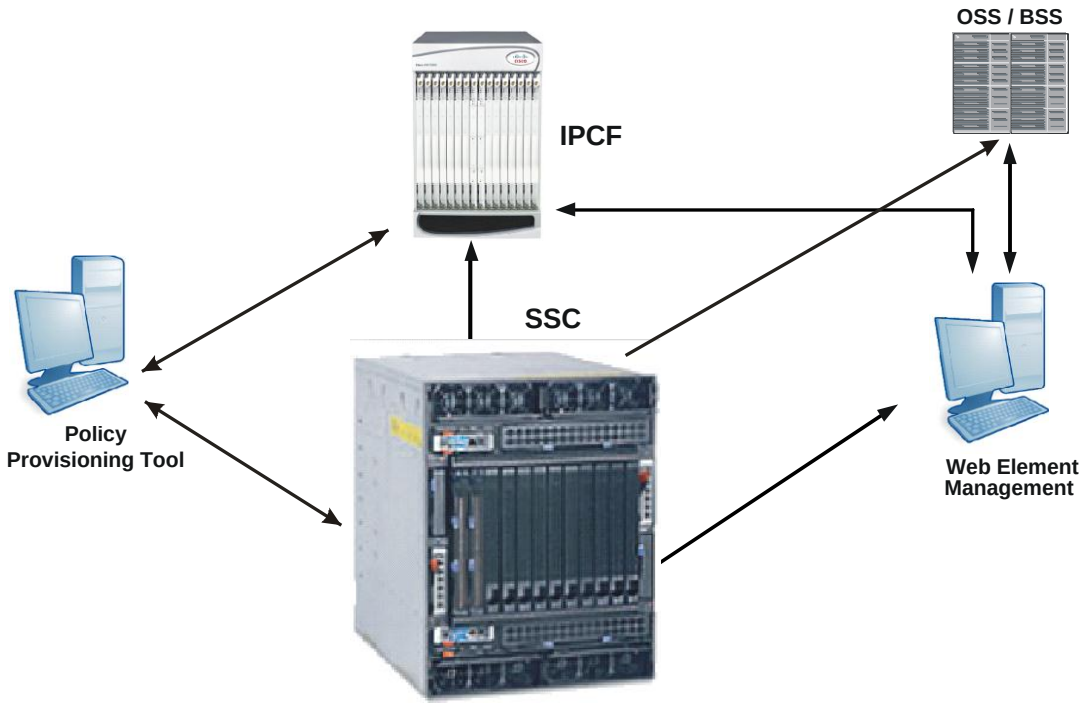
SSC uses Policy Charging and Rules Function (PCRF) along with Subscriber Profile Repository (SPR) data store, to implement the usage control policies in a centralized manner. It also handles account details as well as session state information of the subscriber. SSC can manage the event notification function for PCC, by sending e-mails or text messages to subscribers. SSC provides storage facility for subscriber profile along with centralized management of subscriber policy and service usage for your deployment.

SSC works in conjunction with IPCF for PCC functionality and interfaces with PPT and other components of PCC solution to provide following functionality:

- An intelligent database for service policies by acting either as a standalone SPR or a high-transaction SPR front end for dynamic policy tracking.
- A centralized policy software application engine complementing IPCF for advanced converged and co-related session handling.
- Customized integration with IPCF for managing subscriber usage plans.
- An event notification module that enables user interactions using e-mail and text messages.
- Policy events and statistics management, which can be used for operational monitoring and analysis of subscriber service usage.
- Centralized storage of subscriber, subscription and operator specific preferences along with centralized policy management.
- Managing subscriber service usage.
- Bulk loading of subscriber profile data using Comma Separated Value (CSV) files.
- Provisioning of policy as well as usage monitoring functions for multiple IPCF systems in your network.
- Provisioning of application interfaces with Operations Support System (OSS) or Billing Support System (BSS) as well as with IPCF and PPT components of PCC solution, for subscriber profile and service usage information.
- Exchanging profile and service usage data with Customer Relationship Management (CRM) systems, using **Ud** interface, if CRM is storing data in different database format.

Following figure describes high level overview of a deployment scenario involving SSC along with other components of PCC solution.

Figure 1. SSC Deployment Scenario



The multi-layer distributed architecture of SSC provides carrier grade reliability, by ensuring high availability of the subscriber and subscription data, for the deployment. SSC architecture ensures that there is no single point of failure that may render your deployment unstable for operations. This is achieved by supporting geographical redundancy for disaster recovery.

In a typical SSC deployment a Cisco UCS or IBM Blade Center chassis can contain multiple instances of database manager (RDBMS) along with multiple instances of SSC application and its corresponding In Memory Database (IMDB) application. The IMDB pushes data to RDBMS. Sensitive data such as provisioning information can be pushed immediately where as other information that is being cached can be pushed to database using time-based policies.

SSC Deployment and Interfaces

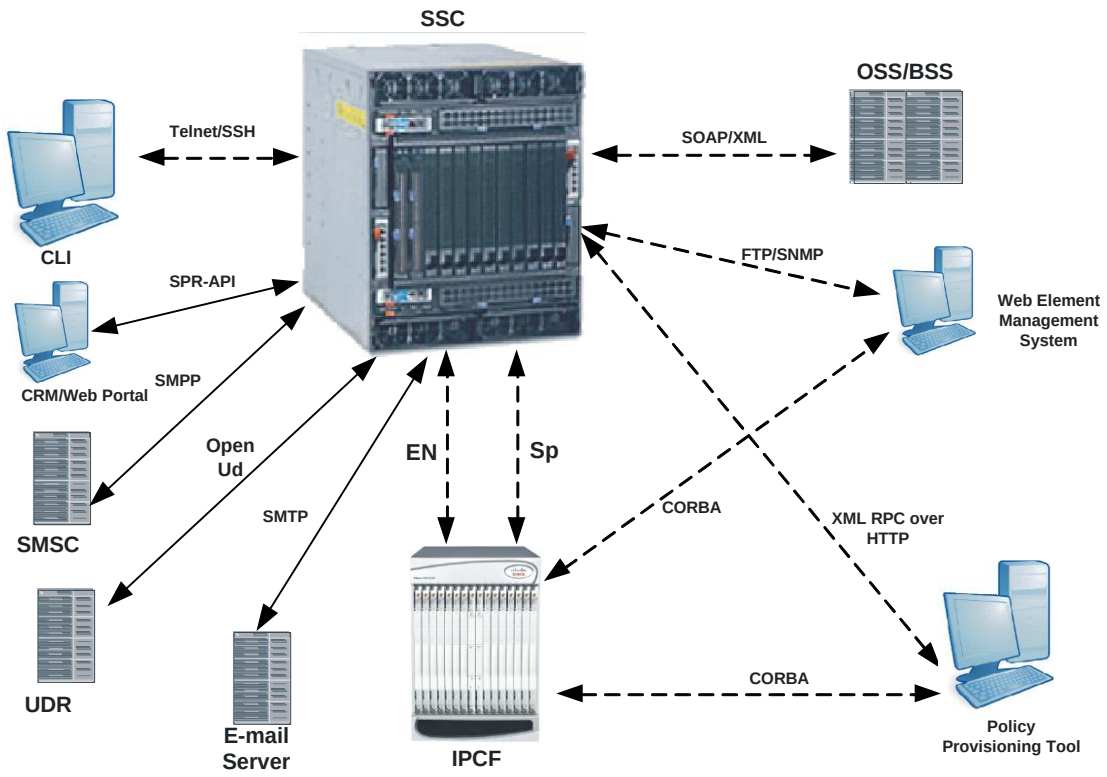
This section describes SSC deployment in a network and various interfaces it uses to communicate with other components of PCC solution and external applications in the network.

SSC in PCC Environment

In a given PCC environment SSC can be deployed along with other components of Cisco PCC solution, such as IPCF and PPT.

Following figure describes a network scenario where SSC is deployed with other PCC components and external applications.

Figure 2. SSC Deployment Scenario



Interfaces

SSC supports following network interfaces for communication with PCC components and other external applications such as OSS, BSS or CRM:

- **Sp**: This interface is used by SSC to communicate with IPCF for subscriber profile operations. Such as getting or updating the subscriber profile, periodically or at the end of session. Subscribing to profile change notifications, the Sp interface is also used by SSC to query data related to usage and balance. Sp interface uses

a standard Sh protocol. SSC uses Sp interface to exchange information such as QoS profile, dynamic rules and time of day objects with IPCF.

- **XML-RPC over HTTP**: This interface is used by SSC to exchange information with PPT application. This interface is used over HTTP protocol. SSC uses the XML-RPC interface to exchange information such as data plans, SMS and e-mail notification templates, subscription tires and dynamic profile attributes with PPT application.
- **SOAP/XML**: This interface is used by SSC to connect to external Operation Support Systems (OSS) or Billing Support Systems (BSS) and exchange profile and usage data.
- **FTP/SNMP**: This interface is used by SSC to connect to Web Element Manager (WEM) and exchange SNMP traps for SSC as well as administrative data.
- **SMTP**: This interface is used by SSC to send the e-mails containing event notification information, to subscribers thru an e-mail server.
- **SMPP**: This interface is used by SSC to send the text messages containing event notification information, to subscribers thru the Short Message Service Center (SMSC).
- **Telnet or SSH**: These interfaces are used by SSC to provide administration and configuration functionality using Command Line Interface (CLI). These are deployed over RS-232 connection.
- **Open Ud**: This interface allows SSC to query data from other nodes or LDAP servers including User Data Repository (UDR). It allows SSC to integrate in the network by supporting transactions with multiple third party databases.Using this interface data can be written or read from existing Light weight Directory Access Protocol (LDAP) or 3GPP R9 Ud compliant databases. SSC can act as Ud server or Ud client for other PCC solution components. When acting as Ud server, SSC allows other components of PCC solution such as CRM and OSS or BSS to query data stored in SSC. It can also send notifications to these components when this data is updated. When acting as Ud client, SSC can query and fetch data from other PCC solution components.
- **Management Interface**: This interface is used by SSC for configuration and scheduling of nodes in a deployment cluster. The system controller component of this interface is used for configuration and management of the SSC deployment. The scheduler component is used to push the SSC performance data to Web Element Manager (WEM). The log daemon component is used to log important SSC host parameters.
- **EN**: This is the Event Notification interface and used by SSC to receive a notification trigger from IPCF upon execution of certain actions, such as provisioning rules to Policy Charging and Enforcement Function (PCEF). SSC can communicate with primary and backup interface for notifying the event to subscriber using either e-mail or SMS. Primary interface is used for delivering the notification, where as backup interface can be used as a temporary provision in case of failure of primary interface.

SSC System Requirements

This section identifies the minimum system requirements for SSC.

Hardware Requirements:

You can use either Cisco Unified Computing System (UCS) C210 M2 General Purpose Rack Mounted server, or an IBM Blade Center for SSC deployment.

Cisco UCS C210 M2 Requirements:

- 2 Intel Xenon X5670 series processors.
- 96 Gb of DDR3 Memory.
- Small Form Factor (SFF) SAS or SATA disk drivers,1 TB or more.

Important: Refer *Cisco UCS C210 M2* documentation, for detailed system requirements.

IBM Blade Center Requirements:

- IBM Blade Center HT Chassis, embedded Cisco 3110G GE, FC.
- IBM Blade HS22, E5645 6C 2.40GHz, 96GB, 300GB.
- IBM DS3500 Storage Array 1.8TB.

Important: Refer*IBM Blade Center* documentation for detailed Blade server system requirements regarding IBM Blade Center HT chassis and IBM HS22 blade.

Software Requirements:

SSC 14.0 Software for Database Manager and PCC functions on Cisco UCS or IBM Blade Center platform. Cisco MITG SSC RHEL v5.5 is a 64- bit operating system customized to run on selected hardware platform.

Important: The Cisco MITG SSC RHEL v5.5 OS is a custom image that contains only those software packages required to support compatible Cisco MITG software applications. Users must not install any other applications on servers running the Cisco MITG RHEL v5.5 OS. For detailed software compatibility information, refer *Cisco MITG RHEL v5.5 OS Application Note*.

Licenses

This section identifies licensing requirements for SSC.

SSC is a licensed Cisco product. Separate feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

Licenses may be required for following SSC software components:

- SSC Software for Database Manager.
- SSC Software for PCC functions.

Licenses may be required for following session categories:

- SSC session license for SPR.
- SSC session license for decision center.

Features and Functionality

This section describers the features and functions supported by SSC.

Following features are described in this section:

- Bulk Load Provisioning
- Event Notification Management
- Redundancy and Fault Tolerance
- Service Usage Management
- Subscriber Database Geo-redundancy
- SSC Application High Availability in Multi Host Cluster Deployment
- SSC Bulk Statistics Support
- SSC RAC Support
- Usage Monitoring Functions

Bulk Load Provisioning

This section briefly describes bulk load provisioning for subscriber profile.

SSC database needs to provision subscriber profiles, so that IPCF can process the policy rules using these profiles from SSC and enable the subscriber specific policy control. SSC provides a mechanism to bulk load this profile data, provided that such data is available in specified CSV format as shown below.

```
<MSISDN,IMSI,TIER_NAME,ENABLE_EMAIL,SUB_EMAIL,ENABLE_SMS,SUB_STATUS,PLAN_NAME,SUB
_OPT_OUT,BILL_START_DT,SUB_TYPE,SUB_ORDER,SUB_START_DT,FLAG_LIST >
```

The bulk load script **Bulk_load_sub** is located in *localhome/ssc/tool*s folder. You need to execute this script with administrative user privileges, ensuring that Oracle is up and running during the provisioning process.

Important: For more information, refer *Bulk Loading Subscriber Data* topic, from *Before You Begin SSC Administration* section in *SSC Administration* chapter of this guide.

Depending upon composition of the subscriber profile, CSV file may contain fields similar to following fields:

- **Mobile Subscriber ISDN Number (MSISDN)**: A character data type that indicates subscriber's MSISDN.
- **International Mobile Subscriber Identity (IMSI)**: A character data type that indicates subscribers IMSI.
- **Tire Name**: A character data type that indicates the subscription tire associated with this subscriber.
- **Enable E-mail**: A numeric data type that indicates e-mail is being used to send the notifications to this subscriber.
- **Sub E-mail**: A Character data type that indicates e-mail address of the subscriber.
- **Enable SMS**: A numeric data type that indicates SMS is being used to send notifications to this subscriber.

- **Sub status**: A numeric data type that indicates current status of the subscriber. Value 1 indicates active status value 0 indicates in-active status. Depending upon your business model, you can use additional values to indicate current status of the subscriber.
- **Service or Data Plan Name**: A character data type that identifies name of service or data plan associated with the subscriber.
- **Sub Opt Out**: This is a numeric data type.
- **Billing Start Date**: A date data type that indicates the date on which billing is started for this subscriber.

Following is a sample of bulk load in CSV format for above mentioned configuration:

```
77777777777777,777777777777777,GOLD,0,Bye,0,10,VOD,1,21-Apr-2012,10,1,22-Apr-
2012,URL=Rediff;URL=Facebook;URL=Google
```

Where URL is attribute name and Rediff,Facebook,Google are attribute values.

Important: It is recommended that SSC Administration Console should not be used for subscriber provisioning, the provisioning should carried out using bulk upload script and CSV file.

Event Notification Management

This section briefly describes the event notification support.

SSC uses event notification module to provide usage and policy notifications to the subscriber. These notifications are mostly related with subscriber's service usage scenario or policy changes imposed by PCC rules that might affect subscriber. SSC generates this information by exchanging subscriber profile as well as usage information with other components of PCC solution such as IPCF or PPT as well as with OSS and BSS systems.

SSC event notification module receives change triggers from service usage as well as policy management modules of IPCF. Change triggers are the events on whose execution, notifications are sent to subscribers regarding changes in their service usage or profile status. Notifications can be sent as an SMS or e-mail using subscriber's Mobile Subscriber ISDN Number (MSISDN) or registered e-mail id.

Change triggers can be on-line or off-line events. Examples of on-line events are:

- Start of subscriber session.
- Termination of subscriber session.
- When a threshold is breached.

Examples of off-line events are:

- A plan is activated or de-activated for a subscriber.
- A plan is associated or de-associated with a subscriber.
- When a plan is recharged by a subscriber.

You can use event notifications to inform subscribers, regarding changes in their service usage or profile status. SSC initiates these notifications after confirming changes in subscriber profile. SSC allows customizing as well as throttling of notification messages as per the category of message and capacity of notification gateway.

Important: A notification template can contain maximum 2000 characters.

SSC can generate event notifications even if the subscriber session is not active i.e. subscriber is not connected using a PDP context. Such notifications are needed in following scenarios:

- A plan is activated or de-activated for the subscriber.
- A plan is associated or de-associated with the subscriber.
- Usage top-up is completed for the subscriber.

Event Notification Templates

This section briefly describes the event notification templates.

You can use event notification templates to inform subscribers regarding specific network or service related events or thresholds that may affect their service usage or billing.

Following scenarios may warrant a notification to be sent to the subscriber:

- Subscriber belongs to a specific class such platinum or gold, and as per his or her profile in Subscriber Profile Repository (SPR) is entitled to receive specific notifications.
- Subscriber is using specific service or class of service such as VoIP restricted tariffs.
- Detection of specific event regarding usage pattern of this subscriber, such as usage of specific application or application class such as Skype or VoIP.
- Subscriber is about to cross the threshold of the Fair Usage Policy (FUP) for their subscribed services.

SSC allows you to choose event specific notification method. For certain events you can send the notification thru e-mail to subscriber's registered mail address, for remaining categories of events you can send notification thru SMS to subscriber's registered number.

Depending upon your access privilege, you can customize these templates.

Important: Notification templates can be configured using PPT application, a component of PCC solution.

Redundancy and Fault Tolerance

This section briefly describes inherent redundancy and fault tolerance of SSC architecture.

SSC provides carrier grade reliability by ensuring that there is no single point of failure in the system. It also supports the geographical redundancy for any catastrophic failures that may render the system unstable. SSC also supports high availability of database, providing multiple levels of high availability and data preservation capacity.

Multi-layered, distributed SSC architecture ensures that process faults are contained, by providing the capability to re-start the process with minimum or no service impact. In a multi-host geo-redundant deployment, SSC can replicate all subscriber and session processing tasks with its corresponding peer SSC instances using active- active model.

In a clustered deployment, more than one SSC instances can be active on multiple blade servers. At least two blade servers can be configured as active –standby database system using shared storage or disk arrays.

Service Usage Management

This section briefly describes service usage management.

SSC along with IPCF provides policy control for subscribers based on their usage of various services that are being offered.

SSC stores subscriber account information such as profile and service usage data, along with subscription tires and plans. SSC acts as a centralized location for managing subscriber's service usage. This information is synchronized between SSC and IPCF using Sp interface and Sh protocol. If service usage is shared between multiple Policy Charging Control (PCC) sessions, then SSC performs session binding using, Mobile Subscriber ISDN Number (MSISDN) or suitable subscription account attribute such as group id.

SSC provides subscriber profile information such as International Mobile Subscriber Identity (IMSI), MSISDN as well as subscriber group. It also provides service usage associated with the subscriber as well as subscriber status flags such as whether the subscriber is a VIP or is blacklisted. This information is used by IPCF for monitoring the service usage of subscribers.

Subscriber Database Geo-redundancy

This section briefly describes the geo-redundancy feature available for the subscriber data stored in SSC.

The geo-redundancy feature allows SSC to be deployed in more than one, geographically distant sites and ensures availability of subscriber data in case of catastrophic failure at any of these sites. Same version of an SSC instance can be deployed in an active–standby mode by using distant geographic sites, and by sharing the database.

For the subscriber data stored in SSC, this feature supports failover to a redundant data storage site. Geo-redundancy utilizes a database technology supported by the RDBMS that allows maintaining stand-by or secondary database repository for the primary database. This feature also uses active-active cache of the In Memory Database (IMDB) application that is being used to provide the database grid.The IMDB application always fetches data from the primary data base. The stand-by database is always running in a limited mode and periodically being synchronized with primary database.

Important: Currently database redundancy is supported using the stand-by database either at local site in cluster configuration or at a geographically distant site. Both categories of stand-by database instances cannot co-exist in a given deployment.

In a multi-host environment, geo-redundancy feature supports the failure detection and recovery of:

- SSC application processes such as log daemon, scheduler and various controller as well as manager processes such as Udr controller and Udr manager.
- Database and IMDB private interface processes.
- Network related processes such as Sh link monitoring.

For IBM Blade Center platform with one chassis per site, GR feature supports following configurations:

- Two sites each with one blade, one for active or primary database and other for secondary or stand-by database.
- Two sites each with two blades, primary site with primary database and an active-stand-by IMDB pair. Secondary site with secondary database and an active-stand-by IMDB pair.
- Two sites with two blades, primary site with database Real Active Cluster (RAC) as primary database and an active-stand-by IMDB pair. Secondary site with database RAC as stand-by database and an active stand-by IMDB pair.

For UCS rack mounted servers, GR feature supports a configuration with two sites, each with one UCS C series server. A primary site for primary database and a secondary site for secondary database.

SSC Application High Availability in Multi Host Cluster Deployment

This feature briefly describes High Availability (HA) implementation in an SSC cluster.

High Availability (HA) can be implemented for an SSC cluster deployment. It ensures availability of subscriber data by managing failure detection and recovery of all the components of SSC deployment such as:

- **SSC Application Software**: Application failure detection and recovery is implemented using heart beat daemon. SSC components send heart beats at a configured interval. The daemon re-starts a component if it fails to receive any heart beat from that component in defined consecutive intervals. SSC application components such as Sh, event, ud and profile controller as well as system controller, scheduler and log daemon can be made highly available using this method
- **In Memory Database (IMDB) Application**: IMDB failure detection and recovery is implemented using the second blade in active –standby mode. The data base blade hosts database and IMDB in active mode, where as the application blade hosts IMDB in standby mode. Automatic failover is performed in case of un-availability of active IMDB node. Active sessions are maintained in IMDB and are replicated between active and stand by nodes.

  Caution: In the current release, IMDB failure recovery requires manual intervention in form of attaching working blade to grid and cleaning up entries in database, this may introduce a down time of up to 60 minutes.

- **SSC Persistent Database (RDBMS)**: In a two node active stand-by configuration, persistent data in the database is protected by performing periodic back-ups.
- **Hardware such as UCS or IBM Blade center Blades**: In a blade failure scenario, the recovery is implemented using Red Hat Cluster. In case of un-availability of application blade, the application is migrated to the data base blade using floating IPs that is transparent to other PCC components such as IPCF.

SSC Bulk Statistics Support

This section briefly describes the bulk statistics frame-work provided by SSC.

SSC provides a bulk statistics framework which can be used to record various system related statistics such as counters, gauges and fixed value strings from various SSC schema of your deployment.

This framework can be used for recording as well as monitoring of such bulk statistics.

The user can configure and monitor bulk statistics for following SSC schema:

- **ShApp Schema**: Bulk statistics schema for Sh application.
- **EnApp Schema**: Bulk statistics schema for Event Notification application.
- **ProfApp Schema**: Bulk statistics schema for Profile application.

Statistical counters provide a snapshot of the system at any given instant. The bulk statistics collected over a regular and configurable time interval can be used for administering SSC deployment as well as for troubleshooting purpose. User can compare values of such counters on a discrete time line specified by the sampling period, to diagnose the system health.

By default the Bulk statistics is stored in a *.txt* file and then can be transferred to Web Element Manager (WEM) to parse and archive for further analysis where WEM provides graphical interface for data representation.

SSC RAC Support

This section briefly describes the RAC support in the enhanced architecture. This support is required for High Availability (HA) and Geo Redundancy (GR) features.

The limiting factor for HA and GR features in the previous SSC architecture was the single instance of Oracle database, which used to act as a single point of failure. This has been mitigated by incorporating RAC support. Enhanced SSC architecture supports Oracle Real Application Cluster (RAC). The RAC allows Oracle database to run any packaged or custom application un-changed across the server pool. It provides a facility to add more servers and instances to the pool without taking users off-line.

In previous SSC architecture, the data base could become single point of failure as well as performance bottle neck as it used to be deployed on a single blade in any of the site. With the RAC feature, Oracle de-couples the database instance i.e. the processes and memory structure that are running on the server to access the data from the data files i.e. the physical structure that is actually storing the data. A clustered database can now be accessed by multiple database instances running on separate servers.

Important: In a non-RAC deployment, when the database server fails in the first site the fail-over occurs in the second site. In a RAC deployment, after failure of one database instance another data base instance from the same site takes over.

Usage Monitoring Functions

This section briefly describes the usage monitoring capabilities of SSC.

SSC acts as a centralized repository for data pertaining to subscriber profile, policy and service usage. As per your network configuration and business model, you can configure SSC to exchange this data between IPCF and various Operation Support Systems (OSS) as well as Billing Support Systems (BSS). Thus extending the data monitoring capacity of IPCF.

OSS software applications are used to administer operational processes related to network infrastructure and services such as QoS monitoring, network and server performance. OSS applications also provide logical or element and physical or network management of the deployed resources. Provisioning function can also be handled by OSS applications. BSS software applications are used to administer external business operations such as billing, rating, sales or customer management. BSS application can also be used to administer customer databases.

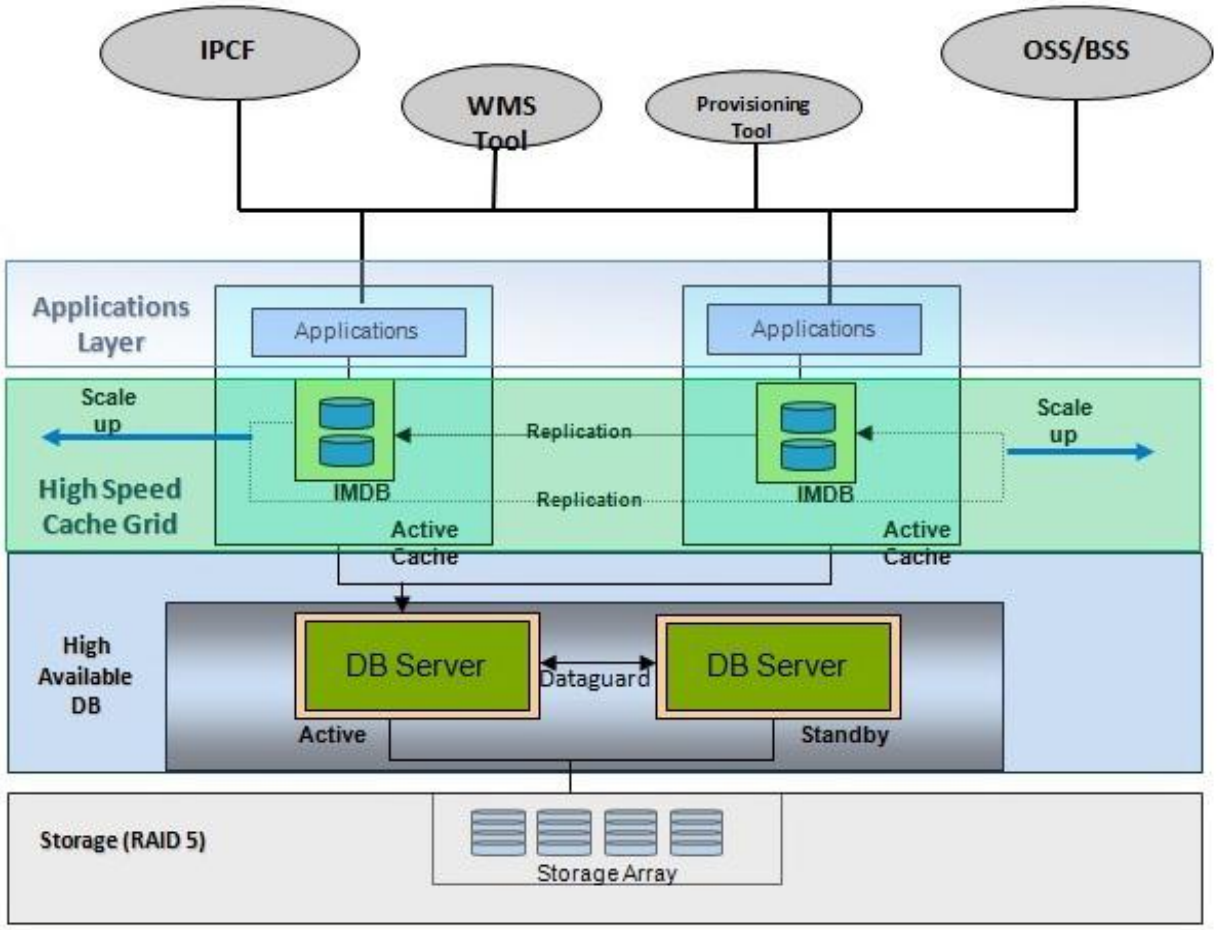
SSC Architecture

Following layers constitute a multi-layered and distributed SSC architecture:

- Data storage layer containing storage arrays.
- Highly Available (HA) database layer containing clusters of database servers in active –standby mode, on the top of data storage layer.
- High speed cache grid layer providing fault tolerance and higher transaction rates for the database on the top of HA database layer.
- An application layer that is used by various components of PCC solution such as IPCF, PPT as well as OSS or BSS to access data from the database.

Following figure describes layered architecture for multi host, highly available SSC deployment running on Cisco UCS or IBM Blade center platforms:

Figure 3. SSC Architecture



Main components of the SSC are:

- **Database**: SSC stores the subscriber data using RDBMS servers in highly available i.e. active- standby mode. Database can be configured using local hard disk or an external storage array.
- **Applications**: SSC provides various application interfaces such as **Sp**, **SOAP-XML** and **Open Ud**. Using these interfaces applications such as CRM,OSS, BSS or other components of PCC solution such as IPCF and PPT exchange data with SSC. Users with administrative privilege can use a console based User Interface (UI) to administer an SSC deployment.

SSC application layer is made up of various processes or tasks such as:

- **System Management Controller (SysCtrl) and System Manager (SysMgr) Tasks**: These manage resource sharing for individual hosts as well as entire SSC deployment.
- **Heart Beat daemon (HBd)**: This task monitors all SSC processing tasks and re-starts a failed task in case of a process failure.
- **Logging Daemon (Logd)**: This task controls log generation for the SSC deployment.

How SSC Works

This section briefly describes the working of SSC.

SSC manages subscriber's profile as well as service usage information using following data objects:

- **Subscriber Profile**: A subscriber profile identifies various subscription plans associated with subscriber along with their privileges and entitlements that can be availed by the profile owner.
- **Subscription Plan**: A subscription plan identifies the treatment regarding the service usage to be made available to the user of your network. A subscription plan can be categorized as data plan, service plan, service pack or add-on for the plan.
- **Usage Account**: A usage account stores current status of the subscriber's service usage, using service units such as volume and time.

Depending upon your business model and network configuration, SSC keeps track of other subscriber attributes such as, current service usage or last visited country. SSC is modeled on Subscriber Profile Repository (SPR). In a PCC deployment an SSC provisions:

- Static as well as dynamic attributes of subscriber profile.
- Data or service plans along with service packages and add-on.
- Notification information.
- Subscription tires.

SSC performs this provisioning using a combination of following methods:

- SSC console.
- PPT application using XML-RPC interface.
- External LDAP using Ud interface.
- SPR provisioning APIs using SOAP/XML.
- Bulk-loading of subscriber profiles using shell script and CSV files.
- Auto provisioning templates.

Different PCC component applications such as IPCF, PPT, WEM and OSS or BSS access application layer of SSC using appropriate interfaces. These applications exchange different categories of data such as subscriber profile or service usage as well as system management data with SSC. This data is accessed from the database that is deployed in a cluster environment using Storage Area Network (SAN).

SSC provides a console based administrative interface to manage the subscriber, subscription and services related data for the Cisco PCC solution. This interface can be used to:

- Start and stop specified SSC components in the system.
- Manage interfaces with other application components of a PCC solution, for sharing data.
- View the logs generated by the system.
- View application counters.
- Monitor overall system health using various processes.
- Set-up and fine tune various parameters for the system components.

SSC Data Model

This section briefly describes schematic considerations of the database containing subscriber and subscription information.

SSC database schema categorizes the subscriber, subscription and service related information. Depending upon your business model and deployment architecture the data model can have following components:

- **Subscriber Group Profile**: A subscriber group profile contains group name, subscriber Id such as IMSI or MISDIN, e-mail address, a flag to enable e-mail, and a flag to enable SMS.
- **Subscriber Profile**: A subscriber profile is a separate component it is not a part of subscriber group profile. It contains subscriber profile Id such as IMSI or MSISDN, subscriber name, subscription tire and other executable profile attributes.

  Current version of SSC supports a flexible subscriber profile schema that can be extended using dynamic attributes. These attributes can later on be used to configure appropriate policy condition rules and identify the subscriber individually as either white listed or black listed.
- **Data Plan**: A data plan contains subscriber profile Id, plan Id, volume usage, time usage, start date, end date, and a flag to enable notifications.
- **Service Plan**: A service plan contains subscriber profile Id, plan Id, volume balance, time balance, recharge day, recharge duration, and usage monitoring key.
- **Service Pack**: This is a subscribe able service plan. A service pack is associated with a data plan subscription.
- **Threshold**: A threshold contains threshold id, template id, absolute and percentage value of service usage.
- **Notification Template**: A notification template contains notification template id, subscriber id such as MSISDN and e-mail address.
- **Area**: This is the smallest configurable entity. An area can be defined using network entities such as MCC, MNC, LAC.
- **Region**: A region contains one or more areas. A single region can accommodate maximum sixteen areas.
- **Region List**: A region list contains one or more regions.

These components are related with each other as follows:

- A single subscriber group profile can be associated with multiple data plans as well as multiple subscriber profiles.
- A single subscriber profile can be associated with multiple data plans.
- A single data plan can be associated with multiple service plans.
- A single service plan can be associated with multiple thresholds.
- A threshold is associated with a single notification template.

SSC Startup

This section briefly describes startup process for an SSC instance.

Following steps describe the start-up of an SSC instance:

1. Heart Beat daemon (HBd) is spawned on management application blade, all instance ids of applications or facilities will be on management blade.
2. Heart Beat daemon then initiates Logd and SysCtrl (instance id – 1) on management blade.

3. SSC startup script starts HBd on all sscblade<*number*>, with instance id starting from 2 up to *n*-2.
4. HBd then spawns Logd and SysMgr on slave blades.
5. When SysMgr is up and running, it notifies SysCtrl with its own facility id, instance id, and blade server name on private network (sscblade<*number*>).
6. In response SysCtrl sends the list of SSC components to SysMgr. SysCtrl keeps track of which applications are on which blade.

   SysCtrl accepts the information regarding which component is running on which blade(s), from console user interface.

   This configuration information is stored in SSC configuration database. SysCtrl refers to this configuration and uses it to start application on blades.
7. SysMgr then requests HBd to start list of applications. **HBd** starts AppMgr along with all the mentioned components, and informs status to SysMgr.
8. SysMgr then informs SysCtrl about failure or success of application start-up.

Important: In a cluster deployment, SSC start-up script can be executed from any blade. In case of a node failure, high availability of various SSC tasks such as SysCtrl, ShCtrl, Logd and Scheduler is ensured by the cluster deployment.

Supported Standards and References

This section lists supported standards and references for SSC.

The SSC complies with the following standards for PCC functionality:

- 3GPP References

3GPP References

- 3GPP TS 23.203 V8.6.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.4.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.4.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- 3GPP TS 29.214 V8.5.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 8)
- 3GPP TS 29.328 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents (Release 8)
- 3GPP TS 29.329 V7.3.0 (2006-09): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Sh Interface based on the Diameter protocol; Protocol details (Release 7)
- 3GPP TS 23.335 V9.2.0 (2010-09): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; User Data Convergence (UDC); Technical realization and information flows; Stage 2 (Release 9)
- 3GPP TS 32.182 V9.0.0 (2010-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; User Data Convergence (UDC); Common Baseline Information Model (CBIM) (Release 9)

Chapter 2
SSC Installation

This chapter provides information and procedures to install and configure Subscriber Service Controller (SSC), a component of Cisco Policy Charging and Control (PCC) solution.

SSC provides a Graphical User Interface (GUI) based installer that can be used for single host as well as cluster installation. This installer performs installations of necessary database storage infrastructure as well as database related applications such as In Memory Database (IMDB) application, that are required to maintain the database gird for the cluster deployment of SSC. SSC installer creates the users and groups with appropriate access privileges that are required to administer the SSC deployment. The installer updates required environment variables as well as provides necessary scripts for post installation configuration and administration tasks.

SSC installation chapter provides network planning as well as cluster deployment guide lines, along with procedures for enabling High Availability (HA) and Geo Redundancy(GR) features for a cluster deployment as well as adding and removing a node from an existing SSC cluster. This chapter briefly describes the SAN storage infrastructure installation prerequisites and procedures for the data base that is being used by the SSC deployment.

This chapter also provides un-installation information for the SSC deployment. SSC Installation chapter includes following sections:

Before You Begin

This section includes the information that is required for initiating the installation procedure. It contains following sub-sections:

- Pre- installation Checklist
- Hardware Requirements
- RHEL File System Partitioning Guide Lines
- Users and Groups
- Environment Variables
- Network Configuration For Cluster Installation

Pre- installation Checklist

You must verify following requirements before starting the installation procedure.

- IBM blades and chassis or Cisco UCS C210M2 is available and properly mounted.
- Latest versions of firm-ware and Basic Input Output System (BIOS) are installed on blades.
- X-windows application such as Xming or Xterm is installed and active on the machines where SSC is being installed.
- X11 forwarding is enabled in the putty configuration. Xterm application can be started from the shell and the DISPLAY variable is set correctly.
- The Cisco MITG SSC RHEL v5.5. The 64- bit operating system customized to run on selected hardware platform is installed on blades.
- Prior to installation for a multi host set-up with High Availability (HA) and Geo Redundancy (GR) features, the file */localhome/oracle/.ssh/known_hosts* is deleted. On the host where SSC installation is complete, entry of the current host from this file is removed.

  For example if SSC installation is completed for host 1and host 2and it is being performed on host 3. Then verify that the file */localhome/oracle/.ssh/known_hosts* on host 1 and host 2 **does not** have any entry for **host 3**. Remove such entry from host1 and host 2 if it exists.
- Hostname is same as the interface name that is used to connect to the database, for e.g. if hostname of the box is datablade1 then “ping datablade1” resolves to the IP address on which IPCF will connect to SSC.
- Ensure that execution of **hostname** command returns short host name and not the FQDN by setting the parameter HOSTNAME in the file *etc/sysconfig/network* to short host name and executing the command **sysctl kernel.hostname =<short_hostname>**.
- SSH is set-up between the host machines on which the SSC is being deployed.
- NTP daemon is properly configured. The server parameter in the file *etc/ntp/conf* has correct address of the NTP server. The OPTIONs parameter in the file e*tc/sysconfig//ntpd* is set to **-x-u ntp:ntp – p /var/run/ntpd.pid**
- IP map for management, database and application interfaces for SSC clearly defines the ethernet interfaces such as eth0, eth1, eth2 that are being used by SSC.

- During installation you can access the *var/log/messages* file for any SSC installation related errors. You can use troubleshooting information to resolve these errors. After resolving them use **Previous** and **Next** buttons to re-execute the failed steps in the installation procedure.

Important: Refer to relevant IBM blade center or Cisco UCS C210M2 documentation for system hardware details.

Hardware Requirements

This section lists the recommended hardware requirements for single host as well as cluster installation.

Following are the recommended hardware requirements:

- **Processors**: Up to 2 x Dual-core Intel Xeon Processor up to 3.0GHz.
- **Memory**: 96GB Fully Buffered DIMM. Minimum: 16GB.
- **Hard drives**: 140GB, minimum 40GB.
- **Networking**: Dual Gigabit Ethernet up to 8 ports. Minimum - 2 ports for single host installation, 4 ports for cluster installation.
- **Max cache** : 4MB L2 shared cache.
- **Front side bus**: 1333 MHz.

Important: Hardware requirements may vary as per SSC deployment configuration.

RHEL File System Partitioning Guide Lines

This section lists guidelines for RHEL partitioning.

Following are the recommended values:

- **Root (/)**: Hosts the root file system. Minimum Requirement is 2Gb.
- **localhome (/localhome)**: Hosts SSC application. In some deployments it can host primary data base along with application. Minimum requirement is 80 Gb.

  Important: The partition size scales as per number of subscribers in the database.

- **Storage Array(/u01)**: This is a separate file system over the storage array to host raw file system of the database.

Users and Groups

This section lists various users and their groups created by the SSC installer. Following table lists their names and descriptions.

Table 1. SSC Users and Groups

Sr.No	User Name	Group Name	Description
1	sscadmin	sscadmin, oinstall,timesten,dba	A Linux administrative user for SSC application. Who can administer SSC application, log onto all databases that are associated with this software installation using DBA privileges. Start or stop database services and perform other database related activities.
2	Policy_Operator		An SSC application user, who can manage policies.
3	Sys_Operator		An SSC application user, who can manage SSC application.
4	Sys_Admin		An application user, who can act as a super user for SSC application.

If the groups **oinstall**, **timesten** and **dba** does not exist on the host, then create these groups by using command *#groupadd <group_name>* by logging in with root administrative privileges.

Environment Variables

This section describes the environment variables required for SSC installation. Following table lists required environment variables along with their description.

Table 2. Environment Variables

Sr.No	Variable Name	Description
1	$SSC_HOME	Stores the path of the directory where SSC is installed by the user.
2	SSC_BIN	Stores the path of the directory where SSC binaries are available.
3	*database*_HOME	Stores home directory path for *database*.
4	*IMDB_App*_HOME	Stores home directory path for the In Memory Database (IMDB) application.

Network Configuration For Cluster Installation

This section describes guidelines to design network configuration for cluster installation.

A blade cluster contains multiple blades. In a cluster installation you need to install SSC components on all the blades in a cluster. As per your IP map you can install the SSC application, primary and stand-by database along with the IMDB application on respective blades.

This section contains following sub sections:

- Network Configuration
- Sample 3 Node Cluster IP Plan

Network Configuration

This section briefly describes the network configuration required for the SSC deployed in a cluster environment.

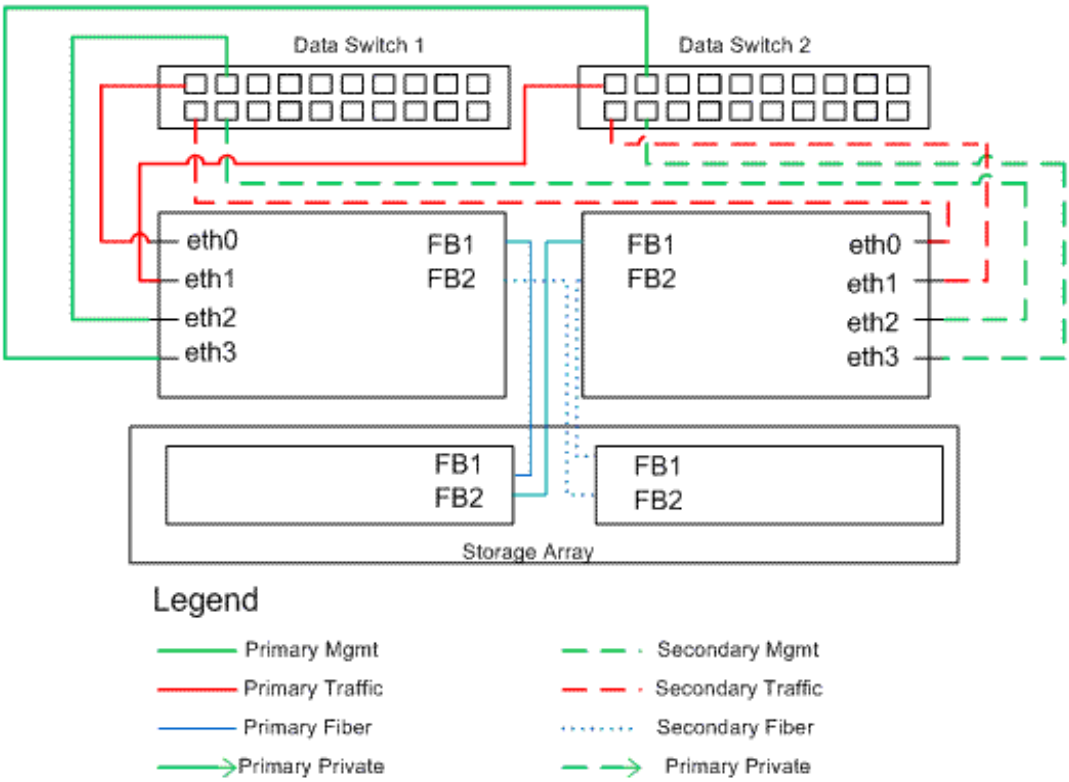
While configuring the network you need to ensure that the database remains available even if one of the blades is not accessible for some time.

You can create such a highly available clustered database solution by installing SSC components across various blades using network interfaces. You need to configure these interfaces in such a way that they are highly available from the ethernet interface as well as from the cabling prospective.

Important: Before proceeding with SSC cluster installation you need to define a detailed **IP map** that co-relates the SSC management and application interfaces as well as primary and standby databases with available IP addresses for entire SSC deployment. During installation you must ensure that eth0 is selected as a management interface. The IP map should list Blade, Eth Interface associated with the blade, Alias or blade name, validations and description.

Following figure describes a default network configuration for an SSC cluster with two blades.

Figure 4. Network Configuration for a Cluster



To provide a highly available clustered database solution, SSC services, In Memory Database (IMDB) and RDBMS use various interfaces across the blades. These interfaces need to be highly available from the Ethernet interface and cabling perspective.

This can be achieved by constructing three VLANs in high availability configuration mode. During the installation process you need to provide IP address of the host for each interface.

These three VLANs are:

- **Traffic VLAN**: It carries data traffic for the SSC cluster. Maximum bandwidth should be configured for this VLAN. It serves the Sh, En and SPR API interfaces along with a standby interface for the Oracle database.
- **Management VLAN**: It carries management traffic for the SSC cluster and used for following interfaces:
  - UI access to SSC.
  - SSH access to the blades for SSH login for installation and troubleshooting.
  - Web access to IBM chassis management console.
- **PPT Interface** : It provides access to PPT server component to exchange information related to data plans, notification templates, subscription tires, dynamic profile attributes, area, region and region lists with the PPT application component of Cisco PCC solution.
- **Private VLAN**: It provides Inter-Process Communication (IPC) between the application nodes as well as carries the private traffic between IMDB instances.

Sample 3 Node Cluster IP Plan

This section briefly describes a three node cluster IP plan and associated interfaces for the SSC deployment.

A cluster IP plan describes:

- Deployment of SSC install set components on the blades.
- Ethernet Interface usage.

Following is the deployment of SSC install set components on three blades:

- **Blade one** hosts SSC application as well as primary database.
- **Blade two** hosts only SSC application.
- **Blade three** hosts only SSC application.

Following ethernet (eth) interfaces are used in this deployment:

- Eth0: For management VLAN. This IP address needs to be configured manually.
- **Eth1**: for the traffic VLAN
- **Eth2**: for the private VLAN for IMDB
- **Eth3**: for the private VLAN for IPC

To install SSC in a cluster environment:

- Ensure that you have configured the network and have a detailed IP map as described in the previous section.
- Ensure that all the binaries required for installation are present on all blades in the cluster.
- Select the blade or host on which to install primary database.
- Create In Memory Database Application (IMDB) grid for primary database.
- Select the blade on which to install the secondary database.
- Synchronize primary database with secondary database.
- Initiate SSC and bind the controllers using SSC console.

Access Installation Files

The SSC installer constitutes five zip files namely:

- `ssc_<version>_rhel_x86_qa1.zip`
- `ssc_<version>_rhel_x86_qa2.zip`
- `ssc_<version>_rhel_x86_qa3.zip`
- `ssc_<version>_rhel_x86_qa4.zip`
- `ssc_<version>_rhel_x86_qa5.zip`

Important: SSC installer also includes a binary file for upgrading SSC along with above mentioned files.

Copy and extract these files in a temporary directory.

During the installation use **`tail`** command to view SSC installation logs being created in `/var/log/messages` file, to verify the success or failure of commands being executed by the SSC installer.

After installation refer to the installation summery captured in `Subscriber_Services_Controller_InstallLog.log` file which is located in `/localhome/install` folder.

Important: For the cluster installation, the installer executable must be available on all the blades where you want to install the SSC.

If there are any failures in system logs then, fix those errors by referring to *Troubleshooting* chapter, and re-execute the installation steps using **Previous** and **Next** buttons, provided by installer GUI.

Single Host Installation

This section describes the procedure to install SSC on a single host.

Installing SSC on a single host

Perform following procedure for a single host installation:

Step 1 On Linux host login as a user with root administrative privileges.

Step 2 Locate the SSC installer archive files as explained in previous section.

Step 3 Extract all zip files that constitute the SSC installer.

Step 4 Initiate the installation process by issuing following command:

```
/. start.sh
```

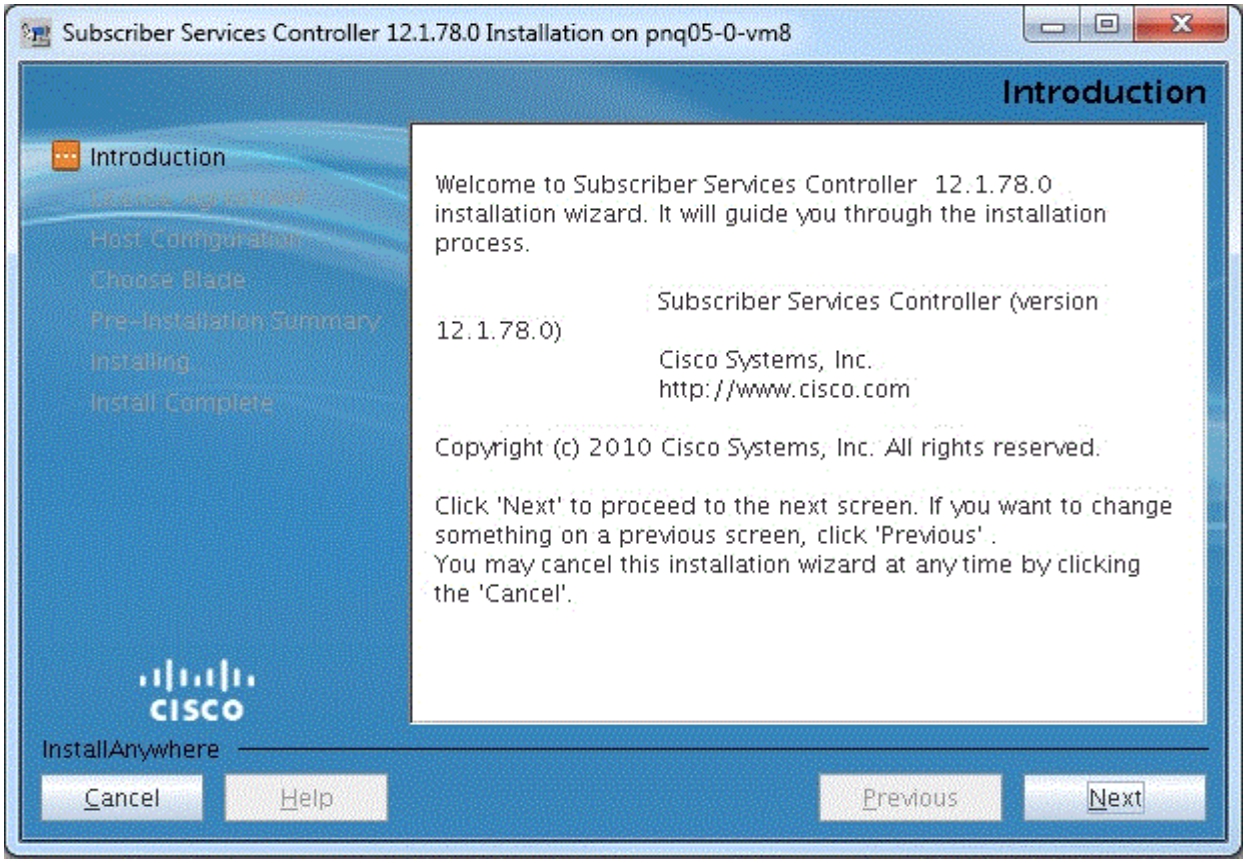
Important: As the SSC installer is a GUI based installer, ensure that x windows application such as Xming or Xterm is active and running, before you execute the **`start`** script.

The installer displays following messages:

```
SSC installation config directory is /tmp/sscCurrent directory is
/root/tools/SSC/SC_12.1.225Extracting installdata.tar in /localhome/install.
Please wait ....Extracting Sinstalldata.tar in /localhome/install. Please wait
....Extracting upgradedata.tar in /localhome/installChange setup.bin as
executableCalling setup binPreparing to install...Extracting the JRE from the
installer archiveExtracting the installation resources from the installer
archive...

Configuring the installer for this system's environment...Launching installer...
```

Step 5 SSC Installer displays the **Introduction** screen.

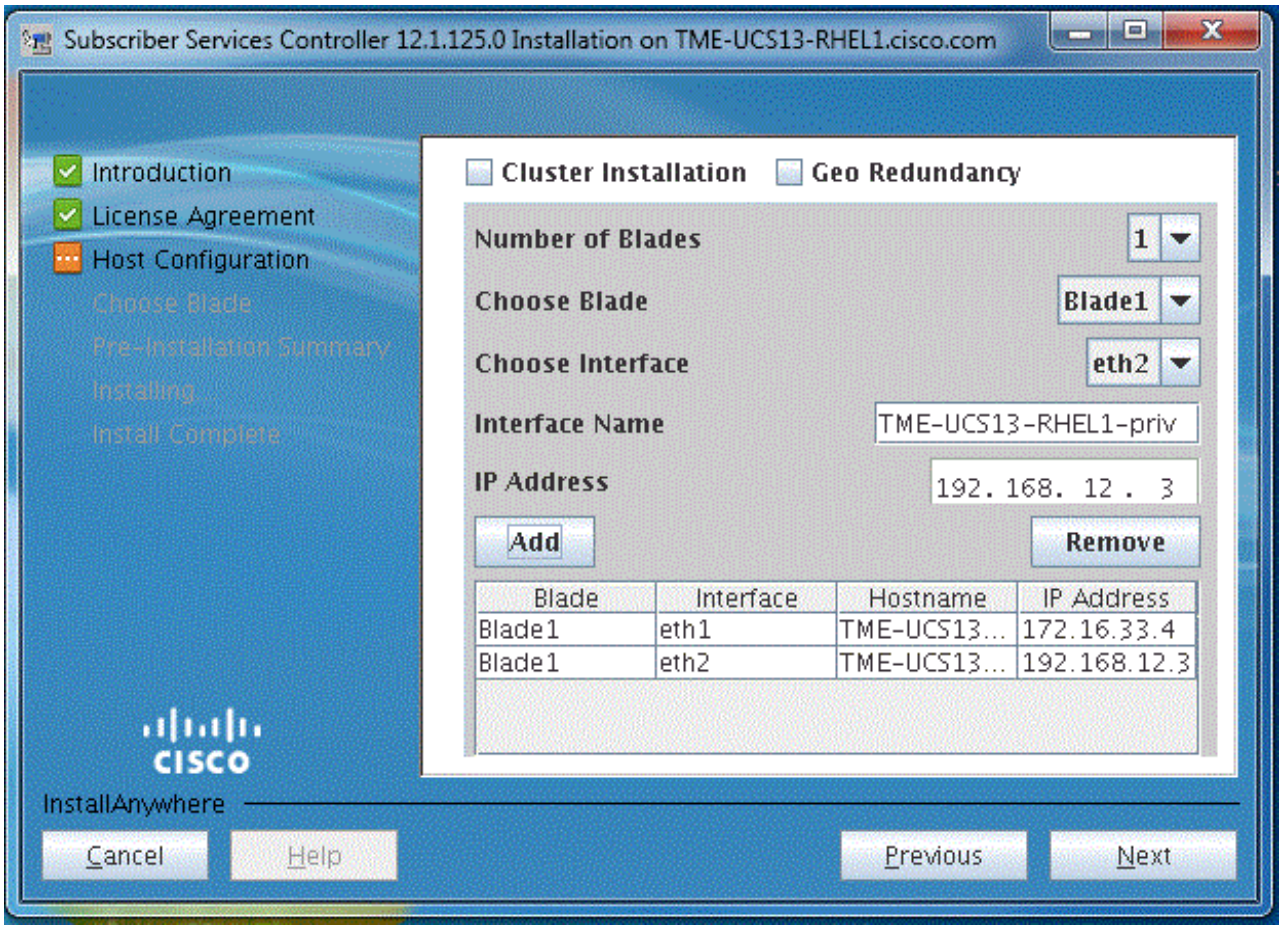


Step 6 Click **Next**

SSC Installer displays License Agreement screen. Select the option **I accept terms of license agreement**.

Step 7 Click **Next**

SSC Installer displays **Cluster Installation** screen. As this installation is for single host. Select **Number of Blades** as 1. The **Choose Blade** field displays the available blade. Using **Choose Interface** field select the interface for this blade.



Important: In a single host as well as cluster installation do not change the value of Eth0, as this is the interface that is being used to connect to the box, otherwise connection to the installer will be lost. IP addresses assigned to all the Ethernet interfaces are stored in *../etc/hosts* and in *../etc/sysconfig/networking-scripts/ifcfg-eth.*

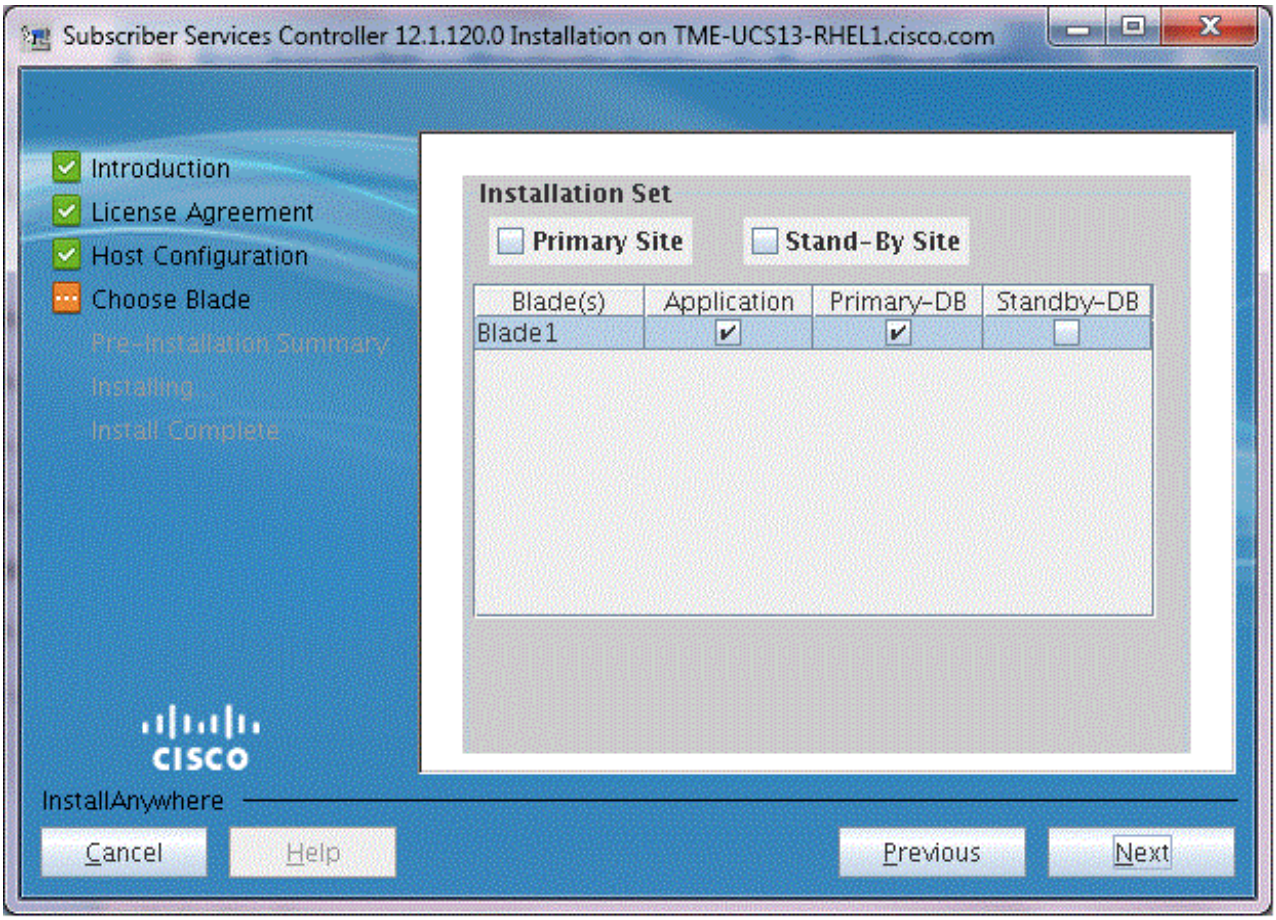
Step 8 Click **Add** to add this interface

Add interfaces for database and application, as per your network configuration strategy and IP map.

Important: For multi node cluster installation refer Cluster Installation section.

Step 9 Click **Next**

SSC Installer displays **Installation Set** screen. The options **Primary** and **Stand-by** site are applicable only if you are implementing geo redundancy feature. Select whether you want to install Application, Primary Database or Secondary Database components from SSC installation set on the available blades.



Primary Site and **Stand-by** site options are used to implement the geo redundancy feature. In a multi-host cluster environment, if you are implementing the geo-redundancy, then as per your IP map specify whether you want to use this SSC installation as primary site or as a stand-by site.

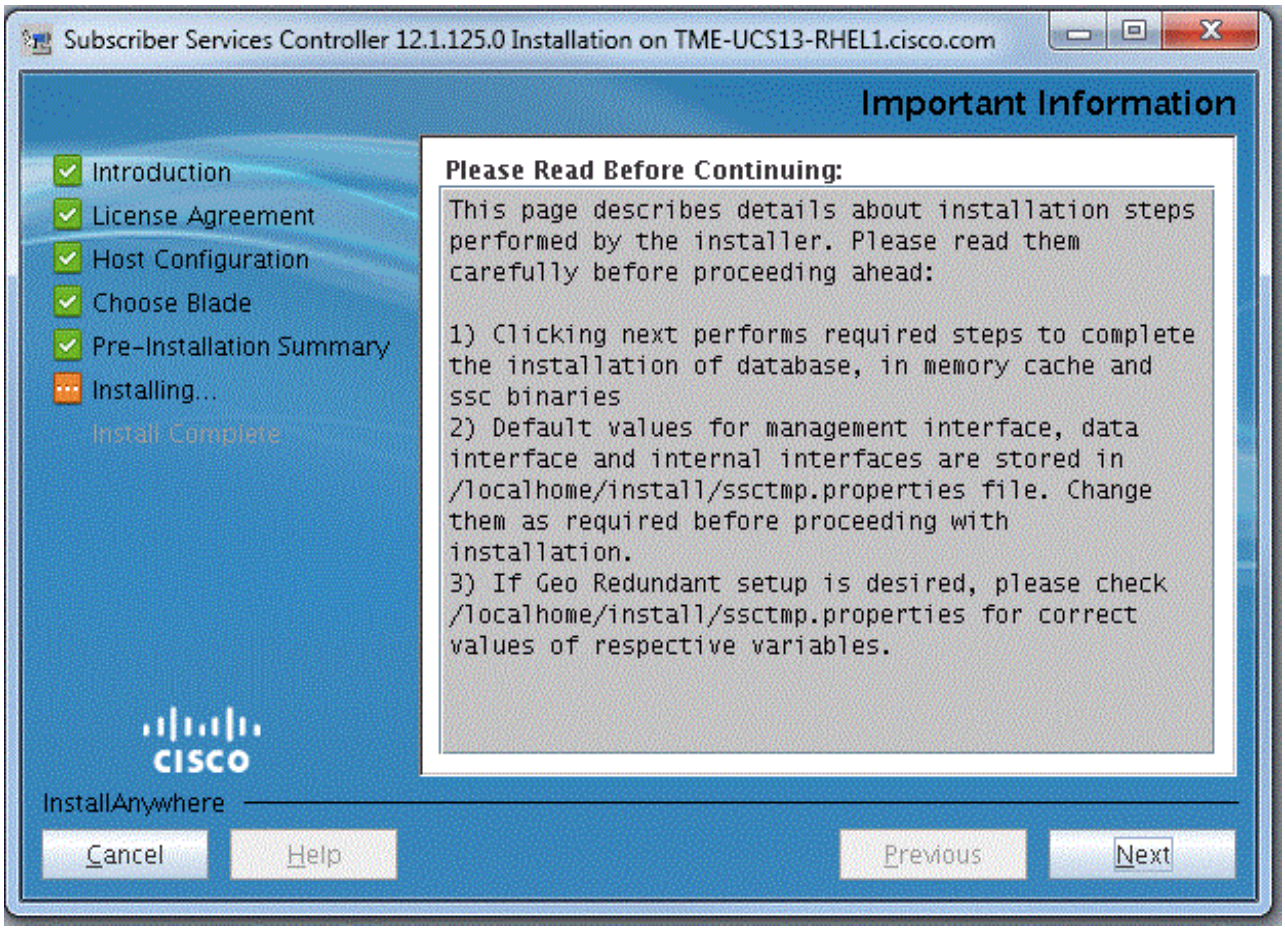
> ***Important:*** Primary and standby databases cannot be configured on same blade.

Step 10 Click **Next**

Following step completes the installation of SSC database. Installer configures database and IMDB instances. After installing selected Installation Set, SSC installer creates database schema and IMDB cache.

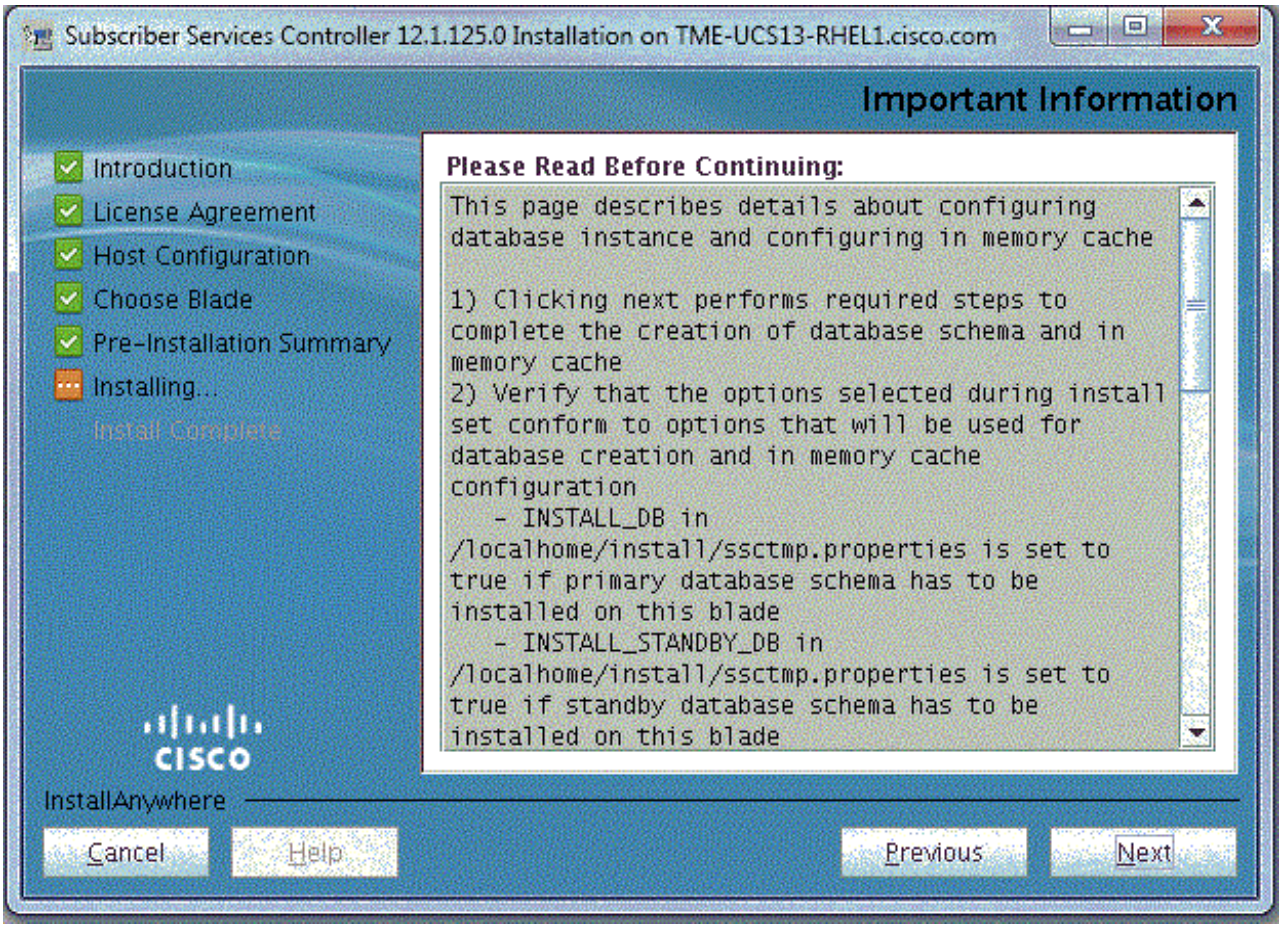
You need to check the *ssctmp.properties* file. You can edit this file as per your requirements. Refer following note as a guide line:

> ***Important:*** Ensure that INSTALL_DB in `/localhome/install/ssctmp.properties` is set to true, if database schema is to be installed on this blade. *`database`*`_DB_HOST in /localhome/ssc/install/spr_install/createSSC_grid.cfg` is set to the host name of box where primary database instance is created. `IMDB_* in /localhome/SSC/install/spr_install/cratessc_grid.cfg` is set to the host names of the boxes that need to be part of the IMDB grid. **InstanceName** in `/localhome/ssc/etc/system.cfg` is set to the database instance that is to be configured on this box.



Step 11 Click **Next**

Following step completes the creation of database schema and IMDB configuration.



Step 12 SSC Installer configures Kernel Parameters, sets network configuration files, adds users and groups. Time required to configure these parameters depends upon your hardware and the options that you have selected. During this period the **Next** button will be grayed out. Click **Next** when that button is available.

If any errors or suggested changes regarding certain configurations are displayed by the SSC installer, then resolve such errors before proceeding with installation. Refer *Troubleshooting* chapter for more information.

Step 13 SSC Installer displays **Pre- Installation Summary** screen.

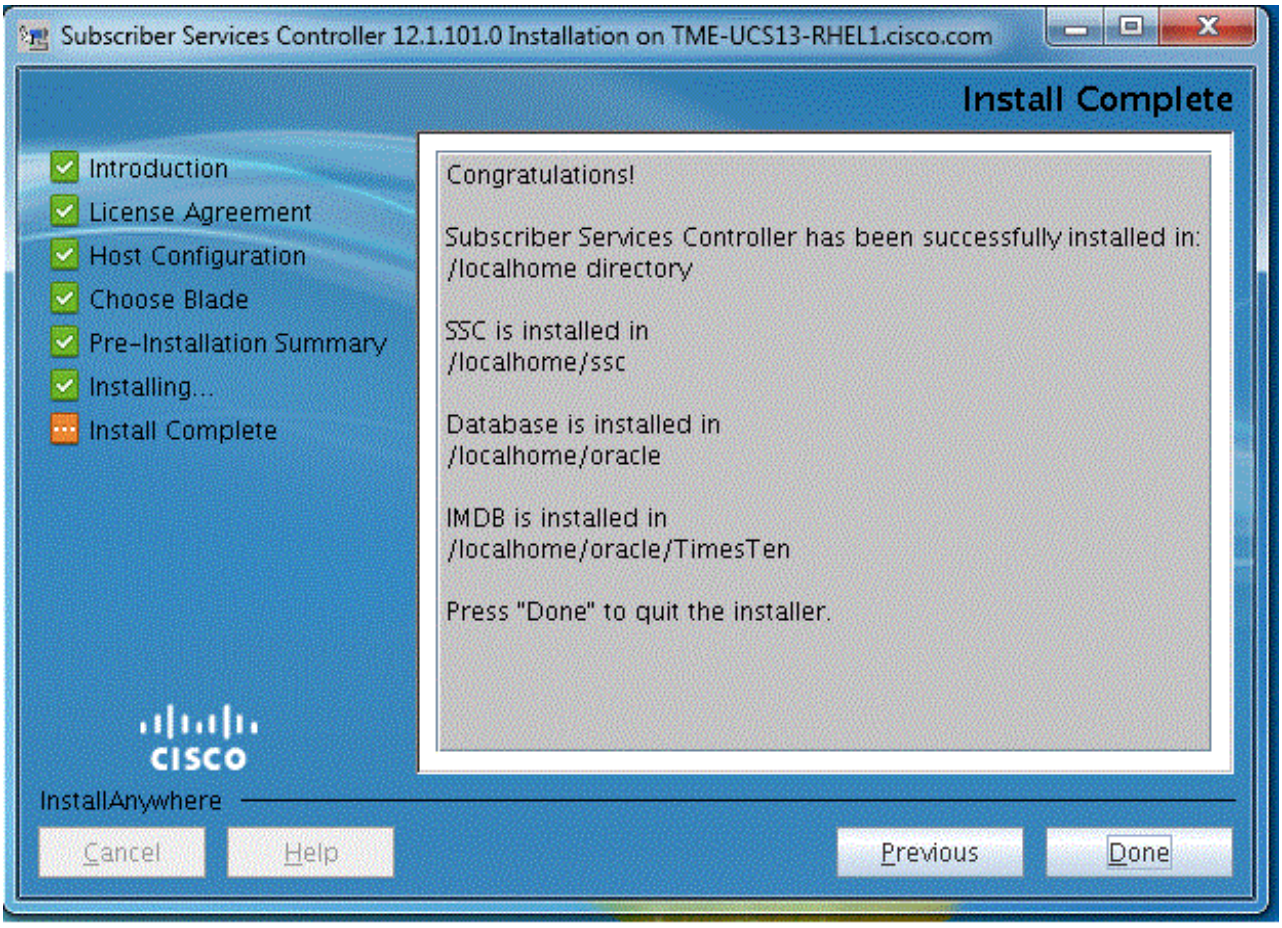
Step 14 Click **Install**.

SSC Installer displays Important Information such has important steps that are being performed by the installer. Number of users that are being created. Along with a list of manual steps that need to be performed to complete the SSC installation.

The installer waits for user input. You need to check and edit the */localhome/install/ssctmp.properties* file as per your SAN and geo-redundancy requirements.

Step 15 Click **Next**

SSC Installer displays **Installation Complete** screen, when SSC application is installed on your system. After installation refer to overall summary of installation steps along with success or failure indicators in */localhome/install/Subscriber_Services_Controller_InstallLog.log*



Important: After successful installation, **maintenance** mode is **enabled** for the SSC deployment which affects the execution of cron jobs. Refer *Controlling Maintenance Mode* in Before You Begin section of SSC Administration chapter.

Salient Installation

A user with root administrative privileges can use the *sscinstall.sh* script to perform the silent SSC installation using parameter values from the file *ssctmp.properties*.

Installing SSC Using Script

This section briefly describes the non-GUI or script based installation.

Perform following procedure to saliently install SSC:

Step 1 Log in with root administrative privileges.

Important: Before proceeding with salient installation, ensure that X11 forwarding option is disabled.

Important: The **sscinstall.sh** script performs silent installation using parameter values from the file *ssctmp.properties*, before proceeding with installation ensure that interface values and other parameters are updated in this file for the respective node as per your network plan.

Step 2 Create a place holder directory, outside the */localhome* directory.

Step 3 Copy all the zip files of SSC installer archive to this directory.

Important: Refer section *Accessing Installation Files* for more information.

Step 4 Extract all the installation zip files and access **Silent Installation** directory.

Step 5 Execute the script **./sscinstall.sh** to perform silent installation.

SAN Based Disk Installation

This section briefly describes SAN installation and configuration for the SSC deployment.

SAN installation and configuration is required for multi host, cluster deployments that support HA and GR features. This section includes following sub-sections:

- Prerequisites and Assumptions
- User Group and ASM Directory Creation
- SAN Disk Configuration
- ASM Libraries Configuration
- ASM Disk Value Creation
- Oracle Infrastructure Installation

Prerequisites and Assumptions for SAN Infrastructure

This section lists the prerequisites and assumptions for the SAN infrastructure installation.

Following are the prerequisites:

- Linux kernel version is 2.6.18-194.el5.
- Any previously installed Oracle infrastructure has been removed.
- Using root administrative privilege and commands from */usr/sbin/getenforce*. It is possible to check the status of SELinux parameter. This status should be Disabled. It can be changed by accessing the */etc/selinux/configset* file.

Following are the assumptions:

- SAN is connected to the Linux machine that is hosting SSC Oracle database.
- SAN disks have the RAID -5 configuration and are represented as devices in /dev directory.
- During SSC grid installation the primary database is to be installed on the first node.

User, Group and ASM Installation Library Directory Creation

This section briefly describes account and ASM directory creation.

This section briefly describes how to create user, group and ASM installation library. This section includes following sub-sections:

- Adding a Group
- Creating Oracle User
- Resetting Password for the Oracle User
- Creating ASM Installation Directory and Setting System Limits

Adding a Group

This section describes how to add various groups. Using root administrative privileges you need to create following groups for installing SAN infrastructure:

- oinstall
- oracle
- timesten
- dba

Use the command `cat/tec/group ! grep "^<groupname>` to check the existence of groups listed above. If these groups does not exist then create them using following commands with root administrative privileges:

- `groupadd oinstall`
- `groupadd oracle`
- `groupadd timesten`
- `groupadd dba`

Creating Oracle User

This section describes how to create an Oracle user. To create an Oracle User:

- **Ensure that localhome directory exists**: If it does not exist then create it and change its permission using the commands , `mkdir /localhome` and `chmod 775/localhome`.
- **Ensure that localhome/oracle directory exists**: If it does not exist then create it and change its permission using commands `mkdir/localhome/oracle` and `chmod 775 .`
- **Ensure that the user oracle exists**: By using following command with root administrative privileges, `Cat/etc/passwd |grep "^oracle"`. If it does not exist then crate it using following command, `USERADD -C Database software owner -d/localhome/oracle -g oinstall -G oracle,timesten,dboracle`.
- **Ensure that ownership of /localhome/oracle is changed** : By using the command .

Resetting Password of Oracle User

This section describes how to reset the password for Oracle user. To rest the password:

- Log in with root administrative privileges.
- Enter the command .
- Specify new user password using which the oracle user can access the system.

Creating ASM Installation Directory and Setting System Limits

This section describes how to configure the ASM installation directories and set system limits. To create installation directories:

- Log in with root administrative privileges.
- Enter command `mkdir/oracleinfra`
- Enter command `chown oracle:oinstall/oracleinfra`

System limits need to be set for providing maximum number of open file descriptor as well as process for the user oracle. To set system limits execute following commands:

- `echo "oracle soft nofile 4096" >>/ etc/security /linits.conf`
- `echo "oracle hard nofile 65536 >> /etc/security/limits.conf`
- `echo oracle soft nproc 16384 >> /etc/security/limits.conf`
- `echo oracle hard nproc 16384 >> /etc/security/limits.conf`

SAN Disk Configuration

This section briefly describes how to configure volumes for SAN disk.

Ensure that multi-pathing in SAN is enabled and following parameters are set as described:

- Ensure that device-mapper multioath 0.4.7-34.el5 rpm is installed. By using command `#rpm-qa ! grep multipath`.
- Ensure that multi-pathing is enabled by checking value of MULTIPATH parameter, by using following command `# cat/etc/sysconfig/mkinitrd/multipath`.
- Using **fdisk** command create three disk volumes such as **/dev/sdd1**, **/dev/sdd2** and **/dev/sdd3** and identify where to configure SAN disk.

If volume **/dev/sdd1** is identified for SAN configuration. Enter command `#fdisk/dev/sdd1`

Ensure parameter settings as described below:

- The number of cylinders for the disk is set to 364722. As this number is larger than 1024 it may cause problems for boot-time and partitioning software from other operating system.
- Use option (m for help):n
- Use option action
- Use option e for extended
- Use option p for primary partition (1-4)
- Specify partition number (1-4):1
- First cylinder (1-36472, default 1):1
- Last cylinder or + size or sizeM or sizeK (1-36472, default 36472):12000

> ***Important:*** This value should be approximately one third of 36472 hence it is 12000.

For second volume ensure following parameters:

- Use option (m for help):n
- Use option action
- Use option e for extended
- Use option p for primary partition
- Specify parathion number (1-4):2
- First cylinder(12001-36472, default 12001):

> ***Important:*** Using default value 12001.

- Last cylinder or +size or +sizeM or +sizeK (12001-36472, default 36472):24000

For third volume ensure following parameters:

- Use option (m for help):n
- Use option action
- Use option e for extended

- Use option p for primary partition
- Specify parathion number (1-4):3

> **Important:** The system might respond as Invalid parathion number for type 3.

- Use option action
- Use option e for extended
- Use option p for primary partition
- Specify parathion number (1-4):3
- First cylinder (24001-36472, default 24001):

> **Important:** Using default value 24001

- Last cylinder or +size or +sizeM or +sizeK(24001-36472, default 36472):

> **Important:** Using default value 36472

Complete the configuration using command, Command (m for help) w.

ASM Libraries Configuration

This section describes how to configure ASM libraries.

The Automatic Storage Management (ASM) feature simplifies the database administration task, by reducing the kernel resources such as number of open file descriptors. The ASM allows the DBA to directly manage the disks for stand-alone or clustered instances that are allocated to Oracle database, instead of managing individual database files. All the Oracle files and directories are included in the disk groups. ASM can automatically perform the load balancing operations.

Log in with root administrative privileges and execute the command `#/etc/init.d/oracleasm configure`.

Ensure that following values are set for the parameters of this command:

- Default user to own the driver interface []:oracle
- Default group to own the driver interface []:dba
- Start Oracle ASM library driver on boot (y/n)[n]:y
- Scan for Oracle ASM disks on boot (y/n)[y]”y

The command configures ASM libraries and displays following output:

- Writing Oracle ASM library driver configuration :done
- Initializing the Oracle ASMLib driver: [ok]
- Scanning the system for Oracle ASMLib disks: [ok]

ASM Disk Volumes Creation

This section describes ASM disk value creation.

This section briefly describes the procedure to create ASM disk volumes when:

- Multi-pathing is enabled.
- Multi-pathing is disabled.

Creating ASM Disk Volumes when Multi-pathing is Enabled

This task describes how to create the disk volume when multi-pathing is enabled.

To create the disk volumes when multi-pathing is enabled:

Step 1 Edit the file */etc/sysconfig/oracleasm* and set the parameters are described.

Following are the recommended values for parameters:

- ORACLEASM_ENABLED=true
- ORACLEASM_UID=oracle
- ORACLEASM_GID=dba
- ORACLEASM_SCANBOOT=true
- ORACLEASM_SCANORDER=""
- ORACLEASM_SCANEXCLUDE="sd*"
-

Step 2 Change current directly to */dev/mapper* directory and list files and directories present in it.

Ensure that there exist entries for each partition.

Step 3 Create the ASM disk volumes for three previously configures disk volumes.

Following are the recommended command parameter values:

- `# /etc/init.d/oracleasm createdisk ASMDISK1 /dev/mapper/mpath0p1 - Marking disk "ASMDISK1" as an ASM disk [ok]:`
- `# /etc/init.d/oracleasm createdisk ASMDISK2 /dev/mapper/mpath0p2 - Marking disk "ASMDISK2" as an ASM disk: [ok]`
- `# /etc/init.d/oracleasm createdisk ASMDISK3 /dev/mapper/mpath0p3 - Marking disk "ASMDISK3" as an ASM disk: [ok]`

Step 4 If due to some reasons above mentioned command fails then use first `deletedisk` and then `cretedisk` commands.

Use these commands in following sequence:

- `#/etc/init.d/oracleasm createdisk ASMDISK1 /dev/sdd1` - Marking disk "ASMDISK1" as an ASM disk: [ok]
- `# /etc/init.d/oracleasm deletedisk ASMDISK3 /dev/mapper/mpath0p3` - Removing ASM disk "ASMDISK3":[ok]
- `# /etc/init.d/oracleasm createdisk ASMDISK3 /dev/mapper/mpath0p3` - Marking disk "ASMDISK3" as an ASM disk: [ok]

Creating ASM Disk Volumes when Multi-pathing is Disabled

This task describes how to create the ASM disk volumes when multi-pathing is disabled.

To create ASM disk volumes when multi-pathing is disabled:

Step 1 Follow step 1 as described in previous procedure.

Step 2 Follow step 2 as described in previous procedure.

Step 3 Create the ASM disk volumes for three previously configures disk volumes.

Following are the recommended command parameter values:

- `#/etc/init.d/oracleasm createdisk ASMDISK1 /dev/sdd1` - Marking disk "ASMDISK1" as an ASM disk: [ok]
- `#/etc/init.d/oracleasm createdisk ASMDISK2 /dev/sdd2` - Marking disk "ASMDISK2" as an ASM disk: [ok]
- `#/etc/init.d/oracleasm createdisk ASMDISK3 /dev/sdd3` - Marking disk "ASMDISK3" as an ASM disk: [ok]

Step 4 If due to some reasons above mentioned command fails then use first`deletedisk` and then `cretedisk` commands.

Following are the recommended command parameter values:

- `#/etc/init.d/oracleasm createdisk ASMDISK3 /dev/sdd3` - Marking disk "ASMDISK3" as an ASM disk: [FAILED]
- `#/etc/init.d/oracleasm deletedisk ASMDISK3 /dev/sdd3` - Removing ASM disk "ASMDISK3": [ok]
- `#/etc/init.d/oracleasm createdisk ASMDISK3 /dev/sdd3` - Marking disk "ASMDISK3" as an ASM disk:[ok]

Oracle Infrastructure Installation

This section briefly describes how to install the Oracle storage infrastructure for the SSC deployment.

Infrastructure Installation Pre-requisites

Following are the prerequisites for Oracle installation:

- You can access the system with Oracle user privileges.
- DISPLAY environment variable is set correctly, by verifying that X11 forwarding option is selected for the ssh session with the host.
- The directory */localhome/inastall/installdata/oracle/griddirectory* exist.

Verifying Existence of /oracle/griddirctory

This section briefly describes how to create the */localhome/install/installdata/oracle/griddirectory* if it does not exists. Verify existence of this directory before proceeding with infrastructure installation. If it does not exists then:

- If */localhome/install* directory is also not present, the create it first by using command *mkdir –p /localhome/install.*
- Ensure that root is the owner of the above mentioned directory and group as well as world have read and execute permissions for it.
- Down load all five SSC installation zip archives and extract them.

- After extracting all the zip files ensure that you have following tar files , installdata1.tar, installdata2.tar, installdata3.tar, installdata4.tar and installdata5.tar. Copy all these tar files to */localhome/install* directory and extract all the tar files in this directory.
- The */localhome/install/installdata*directory will be created after extraction of all these inastalldata tar files.
- The *localhome/install/installdata*directory contains following tar files oracle1.tar, oracle2.tar, oracle3.tar and oracle4.tar
- Extract all the oracle.tar files from *localhome/install/installdata*directory to create the */localhome/install/installdata/oracle/griddirectory*.
- Ensure that the */localhome/install* directory and its sub-directories have read and execute permissions for group and world user groups.

Installing Oracle Infrastructure Software

To install oracle infrastructure software:

Step 1 After ensuring that DISPLAY environment variable is set as explained in previous section. Execute the export commands.

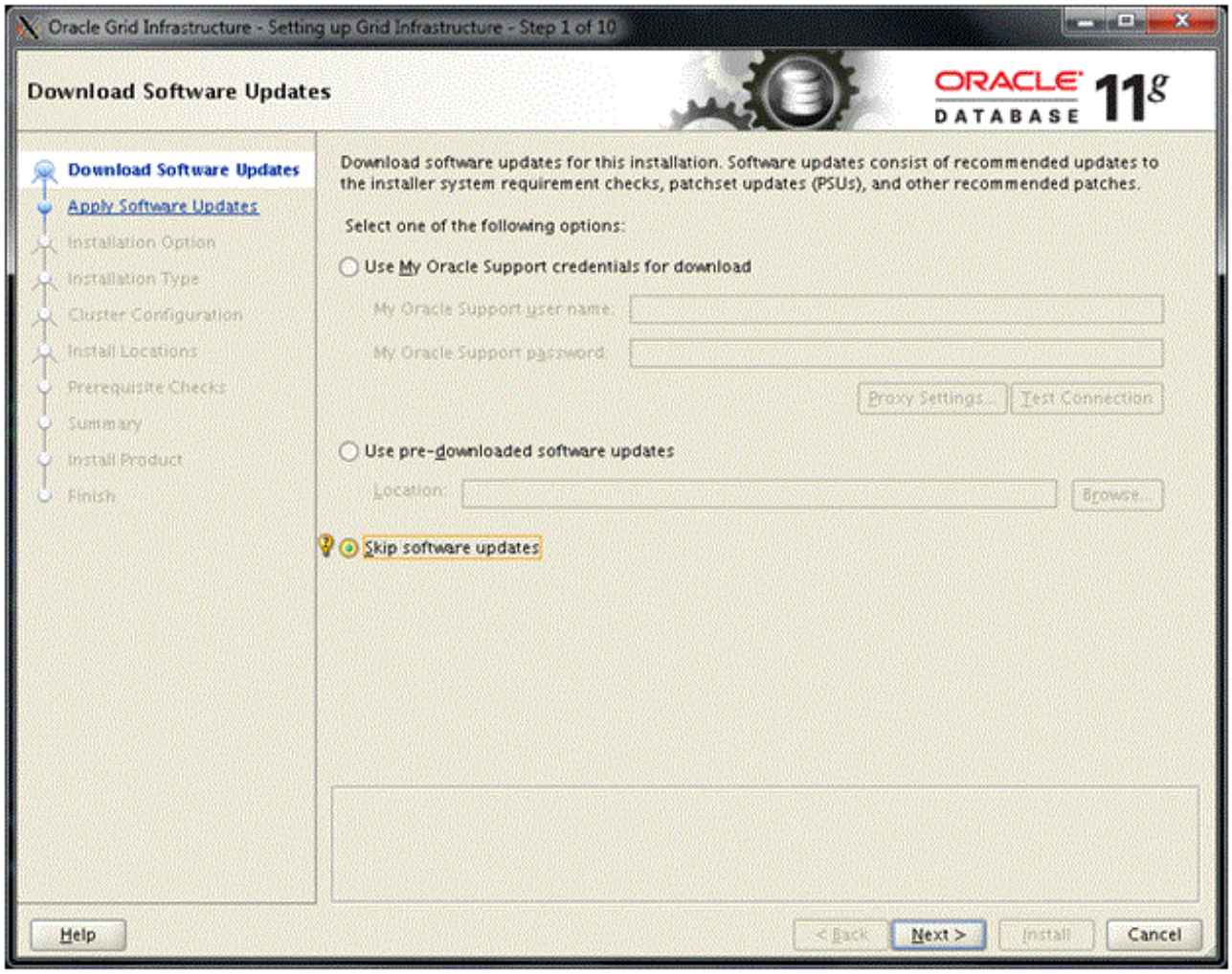
Following export commands need to be executed before initiating the installer:

- `export ORACLE_HOME=/oracleinfra/product/11.2.0/grid`
- `export ORACLE_BASE=/oracleinfra/base`
- `export PATH =/oracleinfra/product/11.2.0/grid/bin:$PATH`
- `cd/localhome/install/installdata/oracle/grid`

Step 2 Initiate the installer by issuing following command `./runInstaller`.

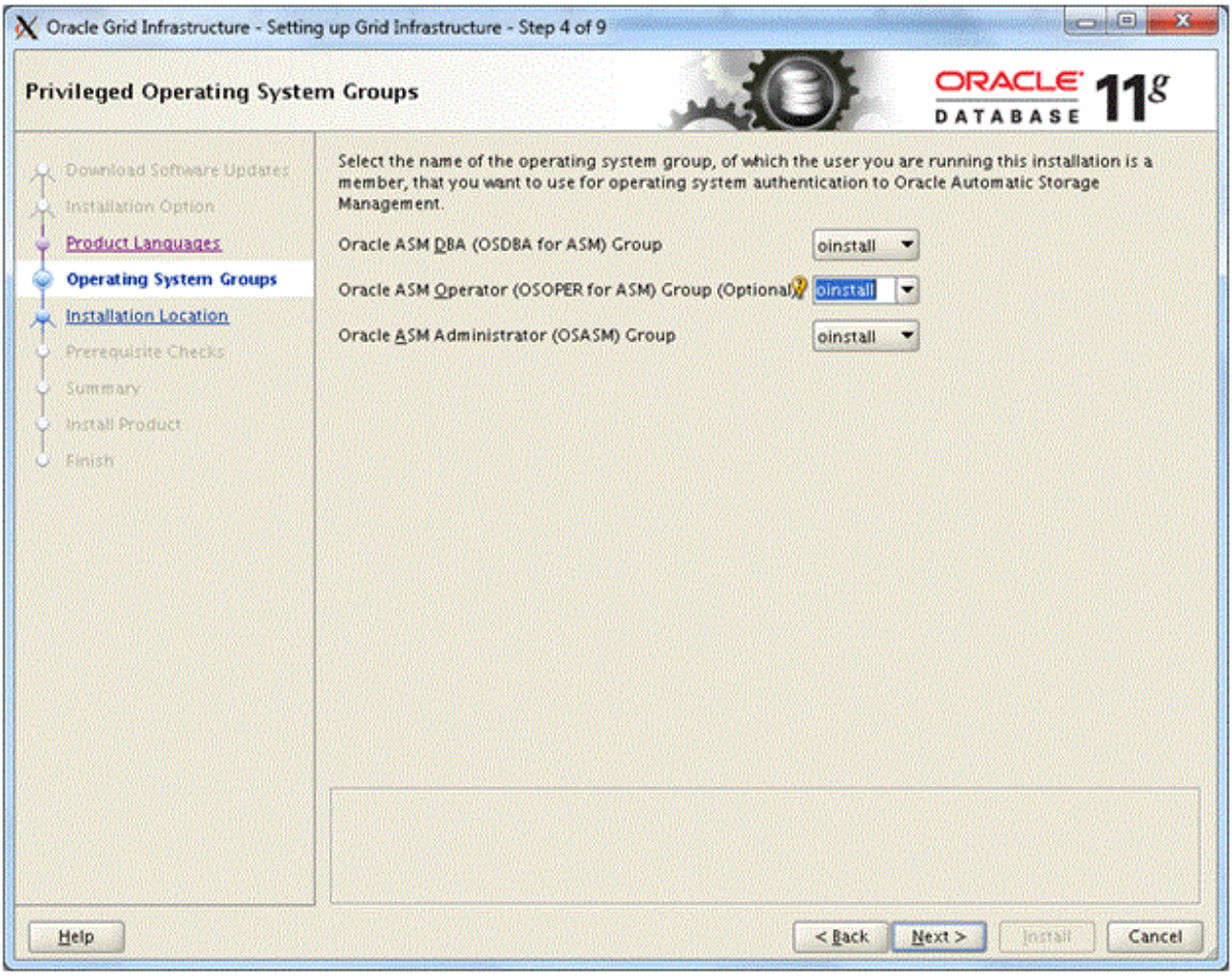
Installer may display a warning message indicating auto check for display colors, ignore such warning message by clicking **yes** .

Step 3 Installer displays **Download Software Updates** screen . Select the option **Skip software updates** and click **Next**.



Step 4 Installer displays **Select Installation Option** screen. Select the option **InstallOracle_Grid infrastructure Software Only**. Click **Next** to specify the product Language. In the **Select Product Languages** screen select **English**.

Step 5 Click **Next** Installer displays **Privileged Operating System Groups** screen.



Select **oinstall** from the drop-down lists for all three groups. The installer may display warning indicating that one and the same account is selected for operator, administrator and DBA groups, ignore this warning by clicking **yes**.

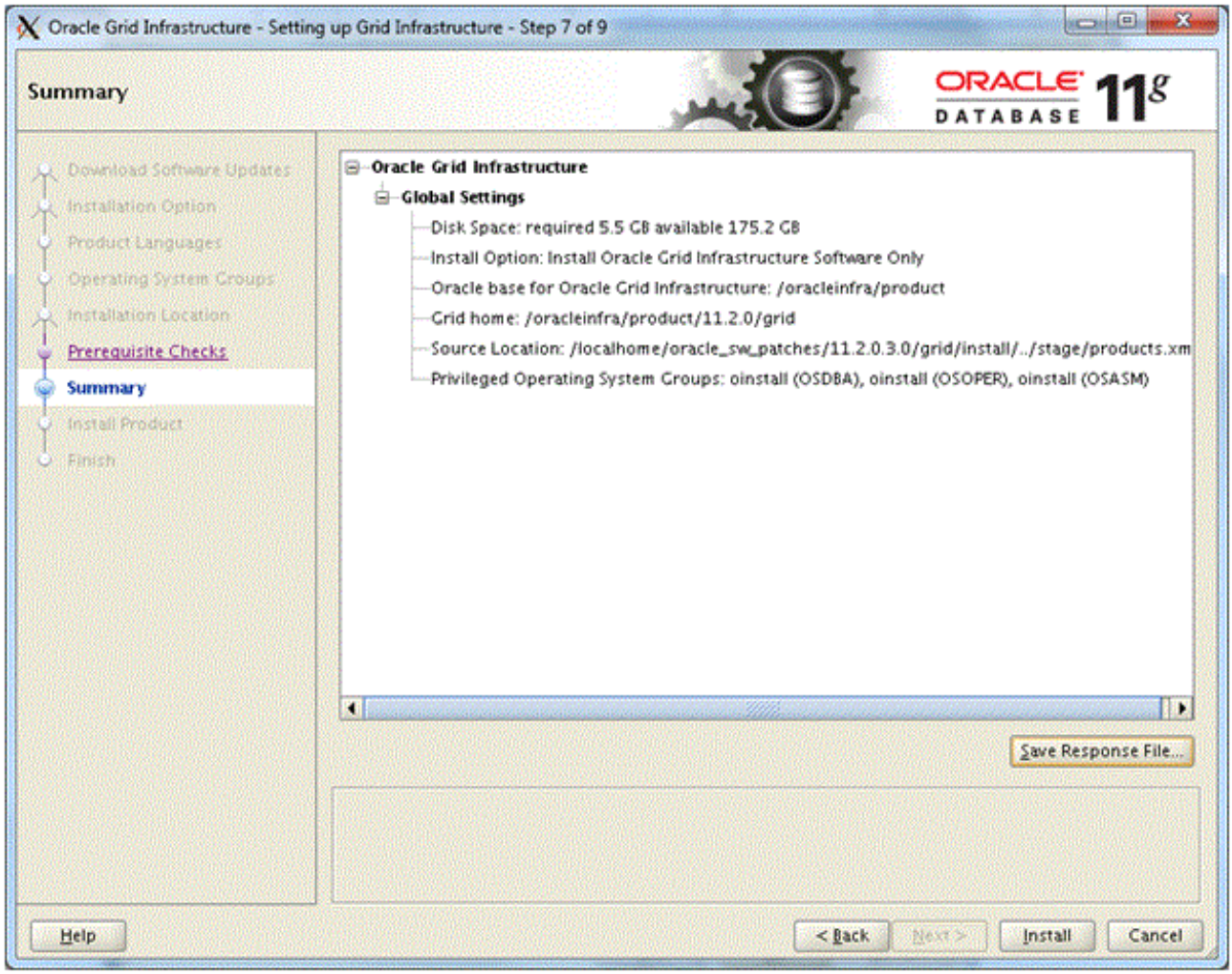
Step 6 Click **Next** installer displays **Specify Installation Location** screen. For **Oracle Base** specify the directory */oracleinfra/base*. For **Software location** specify the directory */oracleinfra/product/11.2.0/grid*.

The installer may display a warning indicating that grid infrastructure software for the cluster should not be under an oracle base directory. Ignore this warning by clicking **yes**.

Step 7 Click **Next** the installer displays Create Inventory screen. Specify */oracleinfra/oraInventory* directory as the **Inventory** directory. Click **Next** the installer performs prerequisite checks while displaying Perform Prerequisite Checks screen.

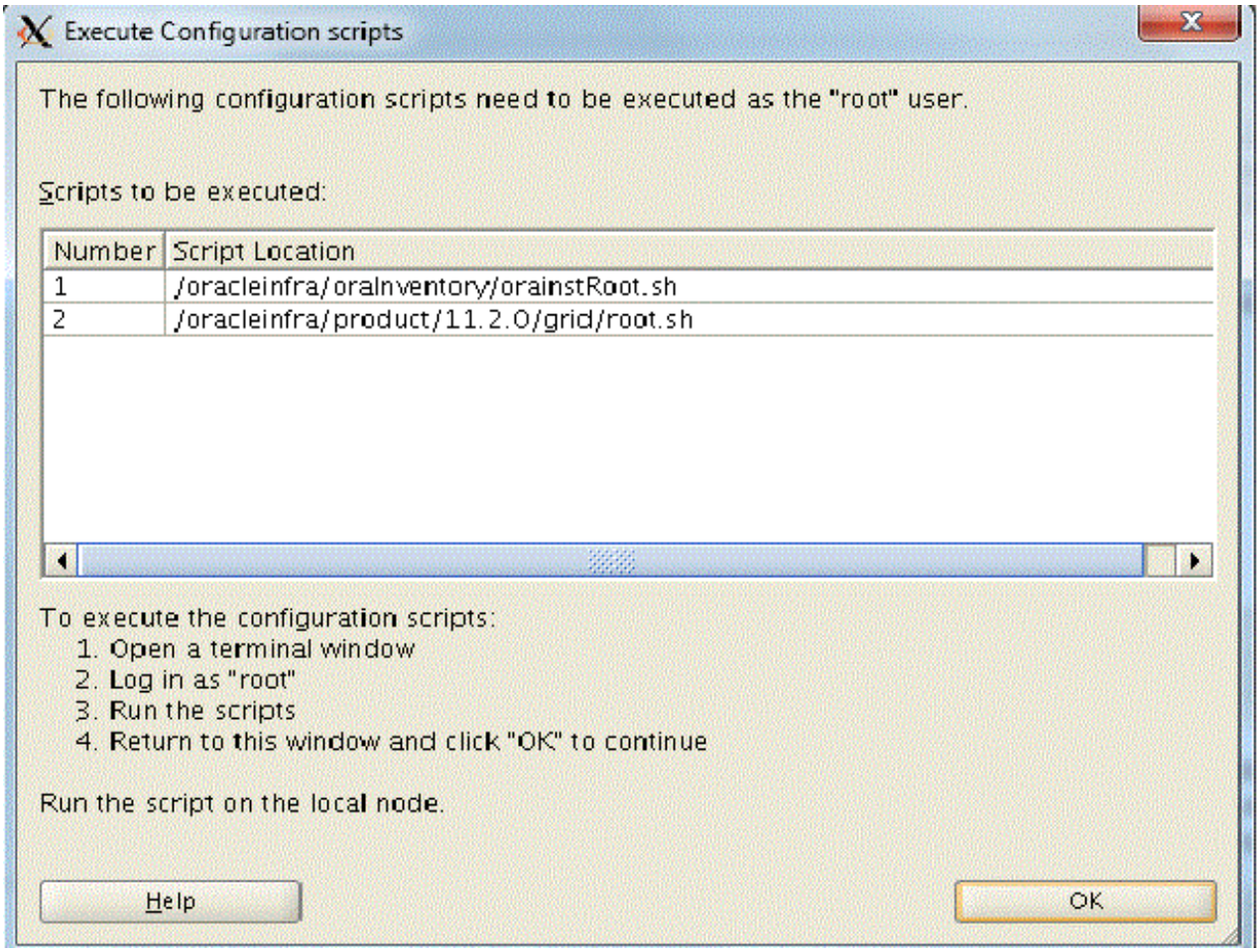
Some prerequisite checks may fail. In such scenario, click more details link and try to fix the errors using provided information. If any warning messages are displayed then select **yes** option to continue installation.

Step 8 After completing the prerequisites the installer displays summary of the selected option. Ensure that the options areas per your requirement. Save this configuration information using **Save Response** option .Click **Install** to initiate the installation.



Step 9 Installer displays the **Install Product** screen indicating status of grid infrastructure packages that are being installed for the cluster.

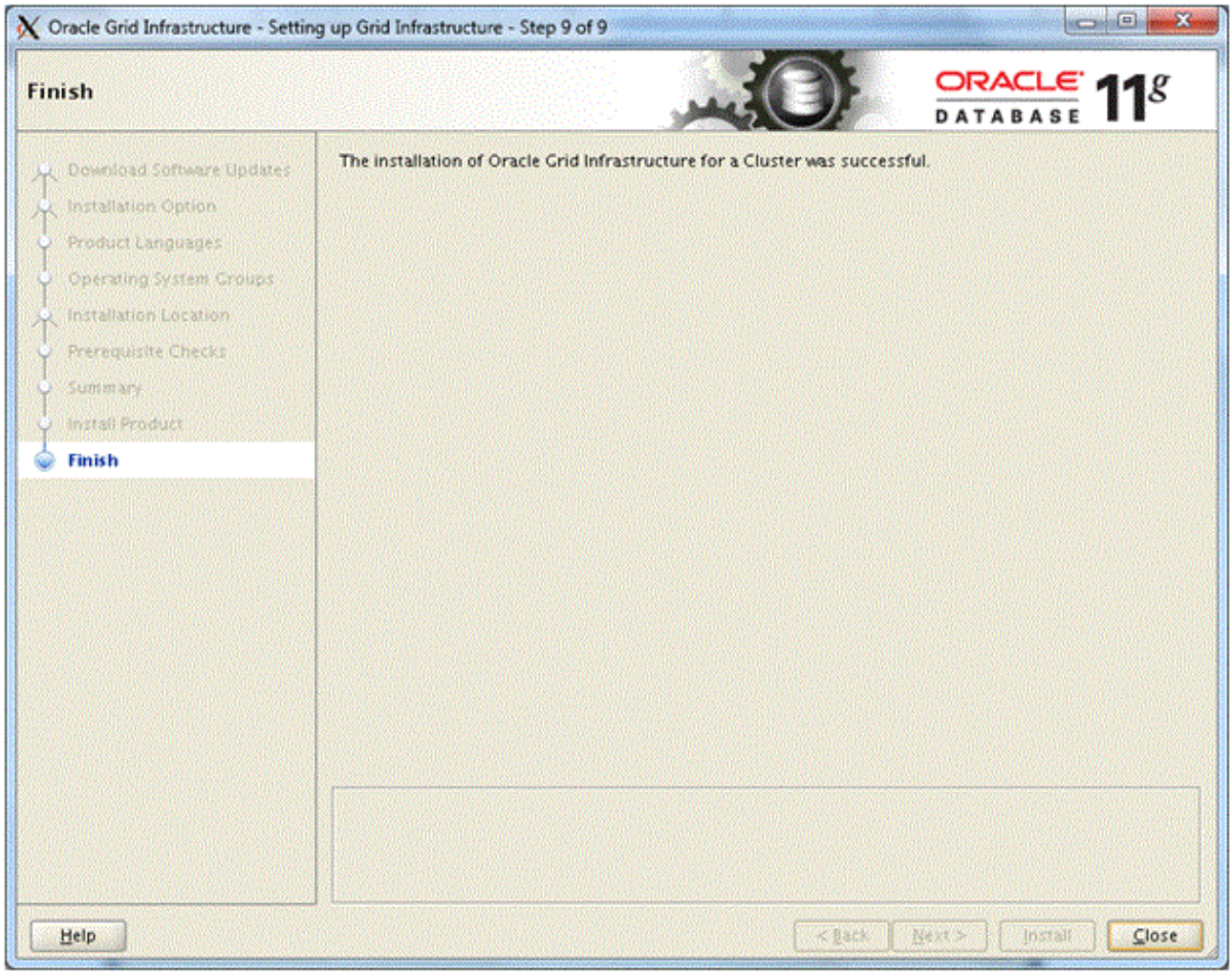
Step 10 Installer displays E**xecute Configuration scripts** screen. When this screen appears, then log-into a separate window and execute the scripts displayed on the screen. After competing their execution access the screen again and click **OK** and then **Close**.



These scripts set the environment variables, execute generic as well as product specific root actions. As a root user:

- Issue following command to configure grid for stand-along server –
  ```
  /oracleinfra/product/11.2.0/grid/perl/bin/perl -
  I/oracleinfra/product/11.2.0/grid/perl/lib -
  I/oracleinfra/product/11.2.0/grid/crs/install
  /oracleinfra/product/11.2.0/grid/crs/install/roothas.pl
  ```
- Issue following command to configure grid for a cluster - /oracleinfra/product/11.2.0/grid/crs/config/config.sh

Step 11 After successful installation the installer displays **Finish** screen.



To configure grid infrastructure for a stand-along server issue the command

```
#/oracleinfra/product/11.2.0/grid/perl/bin/perl -
I/oracleinfra/product/11.2.0/grid/perl/lib -I/oracleinfra/product/11.2.0/grid/crs/install
/oracleinfra/product/11.2.0/grid/crs/install/roothas.pl
```

Installation logs can be accessed using */localhome/oracle/app/orainventory/logs/location* directory or in the log directory at Oracle inventory location.

SAN Infrastructure Un-installation

This section describes how to un-install the SAN infrastructure.

Un-installing SAN Infrastructure

To un-install SAN infrastructure:

Step 1 Log in with database administrative privileges and access the un-installation script by issuing following commands:`$export ORACLE_HOME=/oracleinfra/product/11.2.0/grid$cd $ORACLE_HOME/deinstalldeinstall]$./deinstall`

Specify following parameters:

- Specify the ASM Diagnostic Destination as :/oracleinfra/product/diag/asm/+asm/+ASM
- Specify the diskgroups that are managed by this ASM instance such as ASMDISK1,ASMDISK2,ASMDISK3

Important: De-configuring ASM drops all the diskgroups at cleanup time. Specify **y**when prompted.

Step 2 Installer displays **Check Operation Summary**. Specify **y** when prompted.

Summary displays grid infrastructure directories created by Oracle infrastructure. It also specifies where the un-installation log files will be stored.

Step 3 If in the previous step you have selected to proceed with un-installation, then the installer displays **Clean Operation Start** Information.

The installer proceeds to remove listener and naming methods configurations and maintains un-installation logs in /localhome/oracle/app/oraInventory/logs directory.

Step 4 Issue following command with root administrative privileges, from the blade on which the Oracle infrastructure is installed:`/tmp/deinstall2011-05-13_01-05-01-PM/perl/bin/perl -I/tmp/deinstall2011-05-13_01-05-01-PM/perl/lib -I/tmp/deinstall2011-05-13_01-05-01-PM/crs/install /tmp/deinstall2011-05-13_01-05-01-PM/crs/install/roothas.pl -force -delete -paramfile /tmp/deinstall2011-05-13_01-05-01-PM/response/deinstall_Ora11g_gridinfrahome1.rsp`

Important: Press Enter to proceed with un-installation.

Step 5 Log into the blade as root user and execute ***.rsp** i.e. the output file mentioned in previous step.

Info installer displays messages indicating successful deletion of Oracle configuration stack and removal of associated temporary directories

Step 6 With root administrative privileges issue following command `#oracleasm listdisks`.

This command lists the ASM disk partitions such as ASMDISK1 and ASMDISK2.

Step 7 Delete each ASM disk parathion by issuing command `#oracleasm deletedisk <Disk ParationName>`

Cluster Installation

This section briefly describes how to install SSC cluster, configure high availability in a multi host deployment and add or remove a node from cluster.

Primary Node Installation - Cluster Setup

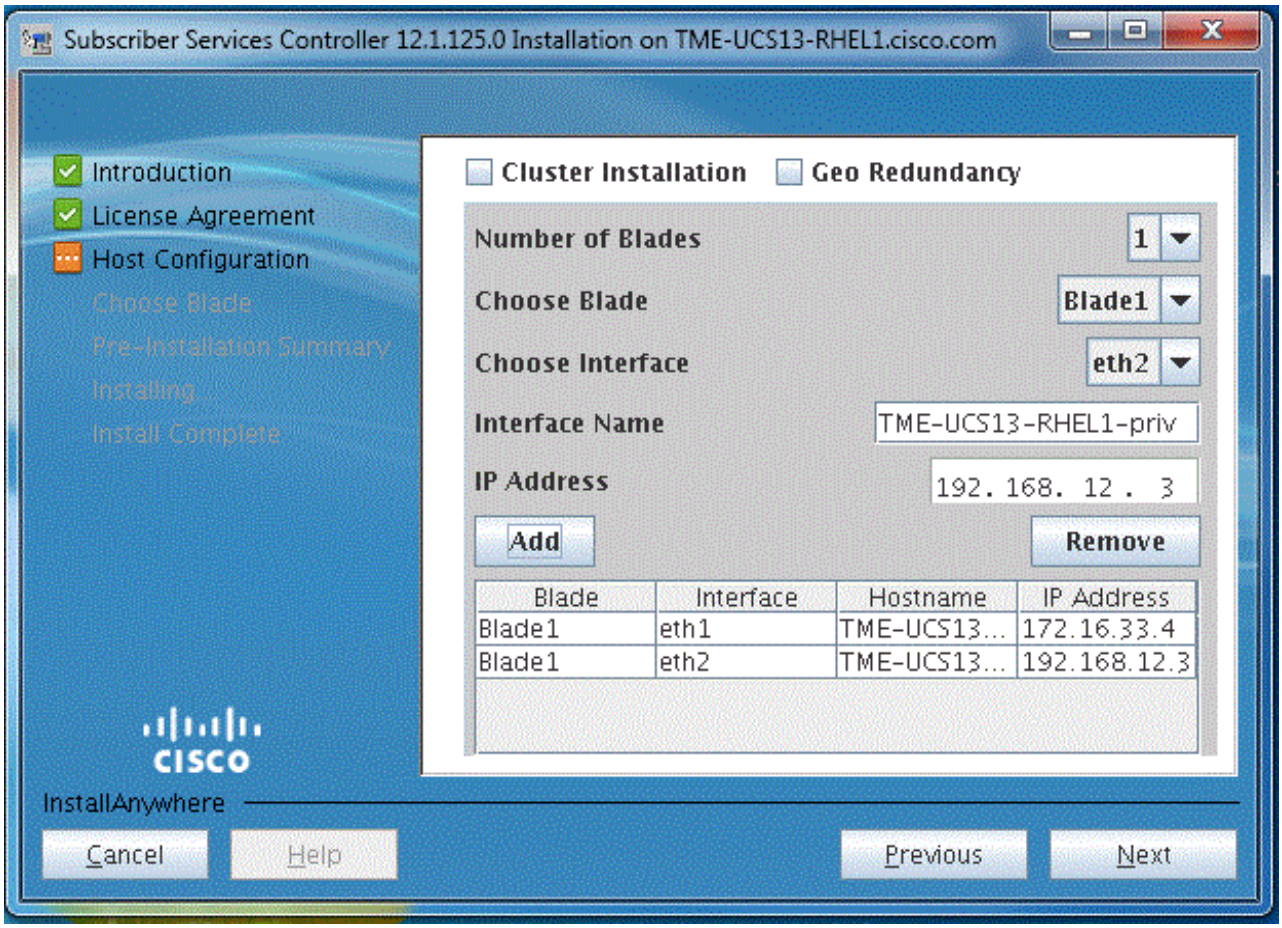
Before proceeding with cluster installation ensure that:

- All the nodes on both sites are reachable to each other by providing host names as well as by their IP addresses.
- Version of SSC components namely SSC application, IMDB and database on all nodes is same.
- Physical memory on both the nodes where IMDB and standby database is being installed is identical.

Ensure that you have a cluster plan, before initiating the cluster installation. A plan also helps in maintenance of the cluster when you need to add or remove a node from cluster.

Refer to the installation procedure documented in the section Installing SSC on a Single Host. On each host or blade, follow this procedure from *step 1* up to the cluster installation step.

Following figure displays the cluster installation screen:



While performing the cluster installation, on each blade:

Step 1 Select the check box Cluster Installation. Select **Number of Blades** as 2.

You can specify the **Cluster Name** to identify the unique cluster, otherwise installer assigns a default cluster name SSCCLUSTER. Ensure that the cluster name is same on all the nodes in a given cluster.

Using**Choose Interface** field you can specify the Ethernet interfaces from eth0 up to eth5 for each blade. Refer your IP map and network planning for assigning the interfaces. If you do not have NIC bonding then you have to configure only eth1, eth2 and eth3 interfaces as eth4 and eth5 interfaces are reserved for NIC bonding. Use **Add** and **Remove** buttons to add or remove a network interface.

Step 2 Click **Next** after completing the network configuration for primary node.

Step 3 SSC Installer displays **Installation Set** screen. Refer step 9 in the Single Host Installation section to view this screen. Select the blade to be configured on this host. Select components **Application** and **Primary Db**.

Step 4 Click **Next**, the installer displays **Installation Slot Information** screen. Specify the **Slot** number for each blade and press **Enter**.

Ensure that all the blades have respective slot numbers. By default the blade number should match the slot number.

Important: The installer displays an error message Slot interface can neither be empty nor be null, if the slot numbers are not provided.

Step 5 Click **Next** button SSC installer displays **Pre-Installation Summary** screen. Refer step 13 in the Single Host Installation section to view this screen. It displays information such as available and used space, product name and install folders.

Step 6 Before initiating installation, the installer displays **Important Information** screen. Refer step 11 in the Single Host Installation Section to view this screen. Update appropriate parameters of *ssctmp.properties* file located in *localhome/ssc/install* folder.

Update the file */localhome/ssc/etc/system.cfg* ensure that parameter **SscInstanceMode** is set to MASTER

Following are the suggested values for important parameters of *ssctmp.properties* file for Primary node:

- INSTALL_SAN_ENABLED = false (If this is a local disk installation otherwise set it to True for SAN installation.
- INSTALL_EXT_PROFILE_INTERFACE = <change to floating IP>
- INATALL_EXT_EVENT_INTERFACE = <change to floating IP>
- ISTALL_EXT_MGT_INTERFACE = <change to floating IP>
- INSTALL_EXT_SH_INTERFACE = <change to floating IP>

On the next screen, SSC installer halts for user input, before clicking **Next** update required parameters in file *./localhome/ssc/install/spr_install/createSSC_grid.cfg*.

Step 7 Login as database (Oracle) user, and updated the file *../localhome/ssc/install/spr_install/createSSC_grid.cfg*

Following are the suggested values specification of IMDB data store parameters:

- IMDB_HOST_1 = < First IMDB host name>
- IMDB_HOST_2 = < Second IMDB host name>
- IMDB_HOST_3 =

- IMDB_HOST_4 =
- IMDB_HOST_5 =
- IMDB_HOST_6 =
- IMDB_HOST_7 =
- IMDB_HOST_8 =
- IMDB_HOST_9=
- IMDB_HOST_10 =

Following are the suggested values for specification of active standby pair parameters:

- INSTANCE = 1
- IMDB_AS_PAIR_1= 1:2:9990:9991
- IMDB_AS_PAIR_2 =
- IMDB_AS_PAIR_3 =
- IMDB_AS_PAIR_4 =
- IMDB_AS_PAIR_5 =
- IMDB_AS_PAIR_6=

Secondary Node Installation - Cluster Setup

In a two node cluster, SSC Application is installed on the second note. Refer to previous task Primary Node Installation – Cluster Setup.

Step 1 Refer Cluster Installation Set-up screen displayed in the previous task. Specify cluster installation information for the second node.

Step 2 Click **Next** after completing the network configuration for secondary node.

Step 3 SSC installer displays **Installation Set** Screen. Select **Application** for blade 2.

Step 4 Click **Next**. SSC installer displays the **Pre-Installation Summary** screen. It displays information such as available and used space, product name and installation folders.

Step 5 Before initiating the installation, SSC installer displays **Important Information** screen. Update appropriate parameters of *ssctmp.properties* file located in *localhome/ssc/install* folder.

Following are the suggested values for secondary node:

- INSTALL_SSC_INSTANCE_ID=2
- INSTALL_DB_INSTANCE_NAME=SSC
- INSTALL_DB=false
- INSTALL_SAN_ENABLED=false (false if local disk otherwise set it to true if SAN installation)
- INSTALL_HA_ENABLED=1
- INSTALL_EXT_PROFILE_INTERFACE=<Change to floating IP>
- INSTALL_EXT_EVENT_INTERFACE=<Change to floating IP>
- INSTALL_EXT_MGMT_INTERFACE=<Change to floating IP>

- INSTALL_EXT_SH_INTERFACE=<Change to floating IP>

Step 6 Login as database (Oracle) user, and updated the file *../localhome/ssc/install/spr_install/createSSC_grid.cfg*

- IMDB_HOST_1 = < First IMDB host name>
- IMDB_HOST_2 = < Second IMDB host name>
- IMDB_HOST_3 =
- IMDB_HOST_4 =
- IMDB_HOST_5 =
- IMDB_HOST_6 =
- IMDB_HOST_7 =
- IMDB_HOST_8 =
- IMDB_HOST_9=
- IMDB_HOST_10 =
- INSTANCE = 1
- IMDB_AS_PAIR_1= 1:2:9990:9991
- IMDB_AS_PAIR_2 =
- IMDB_AS_PAIR_3 =
- IMDB_AS_PAIR_4 =
- IMDB_AS_PAIR_5 =
- IMDB_AS_PAIR_6=

Adding a Node to Cluster

This section describes the configurations required on a node to add it to a cluster.

While installing components of SSC application, before initiating the installation, installer displays important information. Refer step 5 of the section Primary Node Installation - Cluster Setup. Perform following configurations to add this node to cluster:

- ORACLE_DB_HOST parameter in the file */localhome/ssc/install/spr_install/createSSC_grid.cfg* is set to the host name of the machine where primary database is installed.
- IMDB_DB_* parameter in the file */localhome/ssc/install/spr_install/crateSSC_grid.cfg* is set as per the cluster plan.
- InstanceName parameter in the file /*localhome/ssc/etc/system.cfg* is set to the database instance configured.

Important: Increment the instance Id for every node or blade that is being added to the cluster. Instance id for the master blade is reserved to 1.

Removing a Node from Cluster

You may require removing a node from the SSC cluster for maintenance or trouble shooting purpose. This section describes how to remove a node from a cluster.

Step 1 Shutdown all components of SSC application from the node that you want to remove form the cluster.

Step 2 Login to the node as the database (oracle) user.

Step 3 Access IMDB (TimesTen) application by issuing following command:`ttIsql "UID=cacheuser;PWD=timesten;DSN=<Your InstanceName from etc/system.cfg>;OraclePwd=oracle`

Step 4 Execute the *GridDetach* script by issuing following commend:`Call ttGridDetach ()`

Step 5 Exit IMDB command prompt.

createSSC_grid.cfg Parameters

This section briefly describes important parameters of crateSSC_grid.cfg file.

A cluster deployment involves multiple SSC installations or nodes. Features such as High Availability (HA) and Geo Redundancy (GR) can be implemented in an SSC cluster deployment using the database and IMDBgrid. *cerateSSC_Grid.cfg* file stores parameters that are used to enable these features. This file is located in */localhome/ssc/install/spr_install* directory.

In a cluster deployment following TimesTen (IMDB) and log related parameters need to be defined appropriately:

- **T10CacheCleanupRetryCount**: This indicates the maximum retry attempts for the cleanup of the cache information for a failed TimesTen site. Minimum one and by default 12 retries are allowed for the clean-up attempt. During a fail-over the cache information of the failed TimesTen (IMDB) site is cleaned to delete the event logs for the updates and hence to avoid filling up the disk space. This parameter indicates number of clean-up attempts.
- **T10CacheCleanupRetriesSleepTime**: This indicates the sleep time in seconds between two consecutive retry attempts for the clean-up of the TimesTen cache information. The default sleep time is 5 seconds. During a fail-over the cache information of the failed TimesTen (IMDB) site is cleaned to delete the event logs for the updates and hence to avoid filling up the disk space. This parameter indicates default interval between two successive attempts.
- **T10HealthCheckCountForTimeout**: This indicates the maximum retries allowed for the health check to be performed for the timeout error encountered. This parameter covers the scenario in which the failover is in progress for the failed TimesTen site and simultaneously the database monitoring script is checking the TimesTen health. This parameter indicates maximum retries allowed for the health check. Minimum and default values for this parameter are 1 and 3 respectively.
- **ArchiveLogKeep**: This parameter indicates time in hours. It is referred by the archive log clean-up script when the data base is in archive log mode. The archive log cleanup job retains archive logs on both primary as well as standby database for the period specified by this parameter. This parameter is to be configured as per available disk space. The default value is one hour.

Configuring HA in Cluster

This section briefly describes how to configure high availability feature.

Configuring High Availability (HA) in Cluster

Important: For a single host SSC deployment, High Availability (HA) is not supported, however failure detection and recovery mechanisms exist for application processes, database, IMDB and network link for such deployment.

In a multi-host SSC deployment, High Availability ensures availability of SSC application in case of node, network or power failure. High Availability is implemented using RedHat Cluster Suit (RHCS). The RHCS protects SSC components or services in case of network disruption.

Important: Before attempting the HA configuration for both Cisco UCS and IBM Blade Center, you need to ensure that the hardware is configured for recovery from **eth** card failure.

Depending upon your deployment configuration, RHCS can protect following SSC services and related IP addresses in case of network description:

- Services that are used for managing SSC deployment such as System controller, Log daemon and Scheduler.
- Sh controller.
- Event controller.
- Profile controller.
- Ud controller.

In a cluster deployment high availability can be configured by setting some parameters values in the file*/localhome/install/ssctmp.properties*. Ensure that before starting installation of cluster RPMs, the keys *RPM-GPG-KEY-redhat-beta* and *RPM-GPG-KEY-redhat-release* are imported.

To configure high availability:

Step 1 Install the RPMs.

Ensure that following RPMs are installed:

- Cluster_Administration-en-US-5.2-1.noarch.rpm
- cluster-cim-0.12.1-2.el5.x86_64.rpm
- cluster-snmp-0.12.1-2.el5.x86_64.rpm
- cman-2.0.115-29.el5.x86_64.rpm
- cman-devel-2.0.115-29.el5.x86_64.rpm
- luci-0.12.2-10.el5.x86_64.rpm
- modcluster-0.12.1-2.el5.x86_64.rpm
- rgmanager-2.0.52-3.el5.x86_64.rpm
- ricci-0.12.2-10.el5.x86_64.rpm

- system-config-cluster-1.0.57-3.noarch.rpm

Step 2 Enable High Availability (HA) feature by setting parameter INSTAL_HA_ENABLED parameter to 1.

This parameter is located in */localhome/istall/ssctmp.properties* file.

Step 3 Set floating point IPs for Sh, Management, Event and Profile Controller interfaces.

Update following parameters in the file in */localhome/istall/ssctmp.properties*:

- INSTALL_EXT_PROFILE_INTERFACE=<Change to floating IP >
- INSTALL_EXT_EVENT_INTERFACE=<Change to floating IP >
- INSTALL_EXT_MGMT_INTERFACE=<Change to floating IP >
- INSTALL_EXT_SH_INTERFACE=<Change to floating IP >

Step 4 Set Management Module details.

By updating the file in */localhome/istall/ssctmp.properties* as follows:

- INSTALL_MM_IP=<MM hostname or IP address>
- INSTALL_MM_USER=USERID
- INSTALL_MM_PWD=PASSW0RD

Important: You need to change the user id and password only if you have changed them during chassis set-up, otherwise keep the default values.

Geo Redundancy Setup

This section briefly describes how to enable geo redundancy feature, enable it along with cluster and how to install a secondary node in the site.

Important: Currently the Geo Redundancy (GR) feature is available only for the deployments that are using IBM Blade Center platform for hosting SSC database and application.

The geo redundancy feature allows you to deploy SSC in two geographically distinct sites, namely:

- Primary site.
- Stand-by site.

Geo Redundancy(GR) future supports failover to stand-by site for the subscriber data in case of catastrophic failure of primary site. This is achieved by using a database technology supported by RDBMS that allows maintaining a redundant repository for primary database.

The network bandwidth required between two geo-redundant sites, is a function of Transactions Per seconds (TPS). As with increased TPS, the generation rate of Oracle redo log files also increases.

Important: Following function captures this co-relation, Required bandwidth in Mbps = ((redo rate bytes per sec/0.7)* 8). Note that the bandwidth is expressed in Mbps not MBs. For example, for 3000 Sh and 500 SPR API TPS with one logical SSC. The **minimum required** and **recommended** bandwidth is **10 MB** and **50 MB** respectively.

Following are the prerequisites for enabling Geo Redundancy (GR) feature:

- All nodes from both sides are reachable to each other.
- No local stand by database is configured on any of the geo redundant site, as the stand by data base will be installed on one of these sites.
- All SSC nodes participating the geo-redundant configuration contain same version of the SSC product components i.e. SSC application, IMDB and database.
- Primary and stand-by sites have independent IMDB grids, and only the IMDB grid of active site is up, this is important as both the grids are attached to same database.
- Physical memory on both the nodes where active and stand-by pair for the GR feature is to be configured, must be same.

At both primary and secondary sites, the SSC installer can be used to:

- Enable only geo redundancy feature.
- Enable geo redundancy with cluster.
- Install a secondary node on a site in a cluster setup.

Important: While enabling any one of these geo-redundancy options on a **stand-by** site, follow same procedures but use the data base and ssctmp.properties as well as c*reateSSC_Grid.cfg* parameters for the stand-by site.

Enabling Geo Redundancy

This task describes how to configure geo redundancy feature without cluster. It assumes you have detailed IP map that describes the network planning.

Step 1 Refer your IP map. Follow the procedure to install single host up to step 7 – The cluster installation and geo redundancy screen.

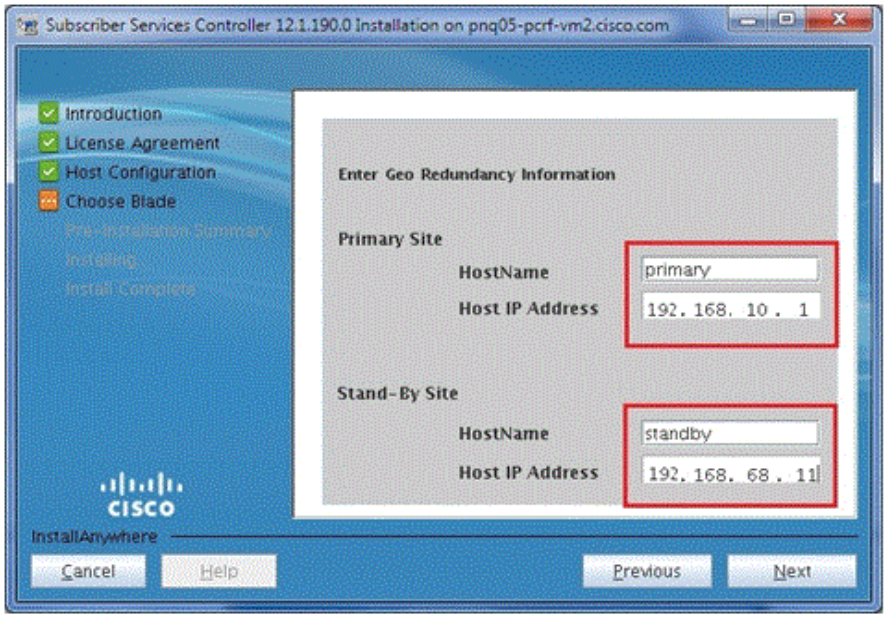
Step 2 Select Geo Redundancy feature.

The **Number of Blades** and **Chose Blade** fields will be already populated. As Geo Redundancy feature is being enabled without cluster, keep **Cluster Installation** and **Cluster Name** fields blank.

Configure the Network using **Choose Interface** option. If NIC bonding is not available then configure interfaces eth1, eth2 and eth3 only, as the interfaces eth4 and eth5 are used for NIC bonding.

Step 3 Click **Next** after completing the network configuration. SSC installer displays the **Installation Set** screen. Select options **Primary Site**, **Application** and **Primary Db**.

Step 4 Click **Next**, SSC installer displays **Geo Redundancy Information** screen.



Provide the **Host Name** and **IP Address** for **Primary** as well as **Stand-by** sites. Verify the ping results from each machine.

Step 5 Click **Next**. The installer waits for user input. Verify that the file */localhome/install/ssctmp.properties* contains following parameters.

Recommended values for the parameters are as follows:

- INSTALL_SSC_INSTANCE_ID=1
- INSTALL_DB_INSTANCE_NAME=SSC
- INSTALL_DB=true
- INSTALL_STANDBY_DB=false
- INSTALL_GEO_REDUNDANCY=true
- INSTALL_PRIMARY_INSTANCE=true
- INSTALL_STANDBY_INSTANCE=false
- INSTALL_PRIMARY_HOST_NAME=<primary db host>
- INSTALL_PRIMARY_HOST_IPADDR=<primary ip address>
- INSTALL_STANDBY_HOST_NAME=<standby db host>
- INSTALL_STANDBY_HOST_IPADDR=<standby ip address>
- INSTALL_SAN_ENABLED=false (false if local disk otherwise set it to true if SAN installation)
- INSTALL_IMDB_GRID=SPRGRIDPRI

Important: ignore the parameters INSTALL_GEO_REMOTE_SITE_ID and INSTALL_GEO_SITE_ID if present.

Step 6 Click **Next** the SSC installer displays Important Information screen and wait for usr input. Update parameters in the file */localhome/ssc/install/spr_install/crateSSC_grid.cfg*

Following are the recommended values:

- ORACLE_DB_HOST=<Primary DB Short Hostname>
- IMDB_HOST_1=<Primary site IMDB node short host name>
- SBY_DB_HOST_1=<Standby DB Short Hostname>

Step 7 In the crateSSC_grid.cfg set the SITE FAILOVER as per requirement. It is not recommended to disable this flag.

Following are the recommended values for the parameters:

- #For failover on any TimesTen blade or Oracle database failure.
- SITE_FAILOVER=ALWAYS
- #For failover of majority of TimesTen blade or Oracle database failure.
- SITE_FAILOVER=DBONLY
- #For no failover (default)
- SITE_FAILOVER=DISABLED

Step 8 In */localhome/ssc/install/spr_install/crateSSC_grid.cfg* set the flag *T10HealthCheckCountForTimeout* as required.

If the db site monitoring script is checking the health of TimesTen (IMDB), then value of this parameter specifies number of times the health check needs to be done. If this parameter is not defined or wrongly defined then the check is performed only once.

Step 9 Update the file *localhome/ssc/etc/system.cfg*

Following are the recommended values for the parameters:

- SiteName=PRIMARY

- InstanceName=SSC
- SscInstanceId=1

Step 10 Perform remaining installation steps.

Enabling Geo Redundancy with Cluster

This task describes how to configure geo redundancy with clustering enabled. It assumes you have detailed IP map that describers the network planning.

Step 1 Refer your IP map. Follow procedure to install single host up to step 7 – The cluster installation and geo redundancy step.

Step 2 Select **Cluster Installation** as well as **Geo Redundancy** options. Select N**umber of Blades** as 2. Specify the **Cluster Name**. Ensure that same cluster name is used across all nodes. Default cluster name is SSCCLUSTER.

Configure network using **Chose Interface** option and your IP map as described in previous task.

Step 3 After completing network configuration, click **Next**. SSC installer displays the **Installation Set** screen. Select options **Primary Site**, **Application** and **Primary Db**.

Important: Installation on multiple nodes is not supported. Select only blade that is to be configured on this host.

Step 4 Click **Next**, SSC installer displays **Geo Redundancy Information** screen. Provided the **Host Name** and **IP address** for **Primary** as well as **Stand- By** sties. Verify the ping results from each machine.

Step 5 Click **Next**. The installer waits for the user input. Verify that the file */loalhome/install/ssctmp.properties* contains following parameters.

For recommended parameter values refer step 5 of previous task.

Step 6 Click **Next** the installer displays Important Information screen. Login as Oracle user and edit the file */localhome/ssc/install/spr_install/createSSC_grid.cfg*

Following are the recommended values for dome of the parameters of this file:

- SBY_DB_HOST_1=<Standby DB short hostname>
- ORACLE_DB_HOST=<Primary DB short host name>
- IMDB_HOST_1=<Primary site IMDB node short host name>
- IMDB_HOST_2=<Primary site IMDB node short host name>
- IMDB_HOST_3=
- IMDB_HOST_4=
- IMDB_HOST_5=
- IMDB_HOST_6=
- IMDB_HOST_7=
- IMDB_HOST_8=
- IMDB_HOST_9=

- IMDB_HOST_10=
- INSTANCE=1
- IMDB_AS_PAIR_1=1:2:9990:9991
- IMDB_AS_PAIR_2=
- IMDB_AS_PAIR_3=
- IMDB_AS_PAIR_4=
- IMDB_AS_PAIR_5=
- IMDB_AS_PAIR_6=

Important: Refer section *Configuring HA Cluster* for enabling high availability feature.

Step 7 In */localhome/ssc/install/spr_install/crateSSC_grid.cfg* set the flag *T10HealthCheckCountForTimeout* as required.

If the db site monitoring script is checking the health of TimesTen (IMDB), then value of this parameter specifies number of times the health check needs to be done. If this parameter is not defined or wrongly defined then the check is performed only once.

Step 8 Update the file *localhome/ssc/etc/system.cfg*

Following are the recommended values for the parameters:

- SiteName=PRIMARY
- InstanceName=SSC
- SscInstanceId=1

Step 9 Perform remaining installation steps.

Installing a Secondary Node on a Site in cluster Setup

Primary node on the primary site has been installed successfully.

Step 1 Refer your IP map. Follow procedure to install single host up to step 7 – The cluster installation and geo redundancy step.

Step 2 Select **Cluster Installation** as well as **Geo Redundancy** options. Select N**umber of Blades** as 2. Specify the **Cluster Name**. Ensure that same cluster name is used across all nodes. Default cluster name is SSCCLUSTER.

Configure network using **Chose Interface** option and your IP map as described in previous task.

Step 3 After completing network configuration, click **Next**. SSC installer displays the **Installation Set** screen. Select options **Primary Site**, **Application** and **Primary Db**.

Important: Installation on multiple nodes is not supported. Select only blade that is to be configured on this host.

Step 4 Click **Next**, SSC installer displays **Geo Redundancy Information** screen. Provided the **Host Name** and **IP address** for **Primary** as well as **Stand- By** sties. Verify the ping results from each machine.

Step 5 Click **Next**. The installer waits for the user input. Verify that the file */loalhome/install/ssctmp.properties* contains following parameters.

Following are the recommended values for the parameters:

- INSTALL_SSC_INSTANCE_ID=2
- INSTALL_DB_INSTANCE_NAME=SSC
- INSTALL_DB=false
- INSTALL_STANDBY_DB=false
- INSTALL_GEO_REDUNDANCY=true
- INSTALL_PRIMARY_HOST_NAME=<primary db host>
- INSTALL_PRIMARY_HOST_IPADDR=<primary ip address>
- INSTALL_STANDBY_HOST_NAME=<standby db host>
- INSTALL_STANDBY_HOST_IPADDR=<standby ip address>
- INSTALL_SAN_ENABLED=false (false if local disk otherwise set it to true if SAN installation)
- INSTALL_IMDB_GRID=SPRGRIDPRI

Step 6 Click **Next** the installer displays Important Information screen. Login as Oracle user and edit the file */localhome/ssc/install/spr_install/createSSC_grid.cfg*

Following are the recommended values for important parameters:

- ORACLE_DB_HOST=<Primary DB short host name >
- SBY_DB_HOST_1=<Standby DB short hostname>
- IMDB_HOST_1=<Primary site IMDB node short host name>
- IMDB_HOST_2=<Primary site IMDB node short host name>
- IMDB_HOST_3=
- IMDB_HOST_4=
- INSTANCE=1
- IMDB_AS_PAIR_1=1:2:9990:9991
- IMDB_AS_PAIR_2=
- IMDB_AS_PAIR_3=

Important: Refer section *Configuring HA Cluster* for enabling high availability feature.

Step 7 Update the flag SITE_FAILOVER in the file */localhome/ssc/install/spr_install/createSSC_grid.cfg* as per requirement. It is recommended to not to set is as DISABLED.

Following are recommended values for this flag:

- #For failover on any TimesTen blade or Oracle database failure.
- SITE_FAILOVER=ALWAYS
- #For failover of majority of TimesTen blade or Oracle database failure.
- SITE_FAILOVER=DBONLY
- #For no failover (default)

- SITE_FAILOVER=DISABLED

Step 8 In */localhome/ssc/install/spr_install/crateSSC_grid.cfg* set the flag *T10HealthCheckCountForTimeout* as required.

If the db site monitoring script is checking the health of TimesTen (IMDB), then value of this parameter specifies number of times the health check needs to be done. If this parameter is not defined or wrongly defined then the check is performed only once.

Step 9 Ensure that the file */localhome/ssc/install/spr_install/createSSC_grid* is identical on both primary as well as secondary nodes.

Step 10 Update the file *localhome/ssc/etc/system.cfg*

Following are the recommended values for the parameters:

- SiteName=PRIMARY
- InstanceName=SSC
- SscInstanceId=2

Step 11 Perform remaining installation steps.

Database Migration

This section describes procedures required to migrate SSC data.

Database migration includes following tasks:

- Exporting Database Schema From One SSC Instance to Another
- Migrating a Single Host SSC installation to multi-host
- Installing SSC Instance on SAN Connected Blade
- Exporting SPR database
- Importing SPR Database on Newly Installed SAN Enabled Blade.
- Completing Migration

Exporting Database Schema From One SSC Instance to Another

This section describes the procedure to export database schema from instance SSC1 on host 1 to another SSC instance SSC2 on host 2.

To export database schema from SSC1 to SSC2:

Step 1 Shut down the IMDB and SSC application instance on host 1. Ensure that there is no activity happening on host1database.

Step 2 Log-in to host 1 as database administrative user and create a working directory under /home directory by issuing following command `$mkdir dbdump`

Ensure that you have sufficient disk space for the export operation.

Step 3 From the home directory execute following command:`exp system/sscsystem@SSC1 FILE=scc_dump.dmp log=scc_export_dump.log STATISTICS=none direct=Y owner=spradm`

Step 4 Verify connectivity of host 2 database from host 1 by issuing following command:`$tnsping SSC2`

If you are not able to ping SSC2 database from hosit1, then FTP the dump file on host2 server.

Step 5 Shutdown the IMDB and SSC applications on host2

Step 6 Ensure that no activity is happening on host 2 database. Execute the clean up script on SSC2 database by issuing following command:`./cleanuo_all.sh <SID>`

Step 7 and then execute the following command: `select 'DROP SEQUENCE ' || SEQUENCE_NAME || ';' seq from USER_SEQUENCES`

Step 8 Execute the output of SQL statement mentioned in the previous step to drop all the sequences.

Step 9 Ensure that there are no sequences by executing following SQL command: `SELECT COUNT(*) FROM USER_SEQUENCES`

A zero count for this SQL indicates that there are no sequences.

Step 10 Execute the output of following SQL statement to drop all the object types: `SELECT 'DROP TYPE ' || OBJECT_NAME || ' VALIDATE;' A FROM USER_OBJECTS WHERE OBJECT_TYPE = 'TYPE`

Step 11 Ensure that there are no object types by executing following SQL command: `SELECT COUNT(*) FROM USER_OBJECTS WHERE OBJECT_TYPE = 'TYPE'`

A zero count for this SQL indicates that there are no object types.

Step 12 Execute following SQL statement:`SELECT 'ALTER TABLE ' || TABLE_NAME || ' DISABLE CONSTRAINT ' || CONSTRAINT_NAME || ';' A FROM USER_CONSTRAINTS WHERE CONSTRAINT_TYPE = 'R'`

Execute the output of this SQL statement to disable foreign keys.

Step 13 Ensure that the foreign key constraints are disabled by issuing following SQL statement:`SELECT CONSTRAINT_NAME, STATUS FROM USER_CONSTRAINTS WHERE CONSTRAINT_TYPE = 'R'`

Step 14 import the data on the host2 that is in the SSC2 application instance by issuing following command: `imp system/sscsystem@SSC2 FILE=scc_dump.dmp log=scc_import_dump.log FROMUSER=spradm TOUSER=spradm IGNORE=y STATISTICS=none buffer=99999`

Step 15 Login to SSC2 database using sqlplus by issuing the following command: `sqlplus spradm/spr_adm@SSC2`and then execute following command:`SELECT 'ALTER TABLE ' || TABLE_NAME || ' ENABLE CONSTRAINT ' || CONSTRAINT_NAME || ';' A FROM USER_CONSTRAINTS WHERE CONSTRAINT_TYPE = 'R';`

Execute the output of this SQL command to enable foreign keys.

Step 16 Execute the following SQL command:`SELECT CONSTRAINT_NAME, STATUS FROM USER_CONSTRAINTS WHERE CONSTRAINT_TYPE = 'R';`

From the output of this SQL command ensure that the status of foreign key constraints is enabled.

Step 17 Truncate the session tracker table by issuing following command `TRUNCATE TABLE SPR_SESSION_TRACKER`

Step 18 Gather SSC2 database statistics by first log-in to the database by issuing following command: `sqlplus system/sscsystem@SSC2`and then collect the schema statistics by issuing following command:`execute dbms_stats.gather_schema_stats('SPRADM',60)`

Step 19 Initiate the IMDB for SSC2.

Migrating a Single Host SSC installation to multi-host

This section describes the procedure to migrate a single host SSC installation to multi-host installation.

Following are prerequisites for migration:

- You have full filled prerequisites of SSC installation.
- Blades with SAN set-up are available.
- Live single host SSC instance is available with disk based SPR database.
- Both the blades, one with live SSC instance and another with SAN connection are housed in same IBM blade center chassis.

Step 1 Installing SSC instance on a blade connected with SAN.

Step 2 From the blade with active SSC instance, exporting SPR database.

Step 3 On newly installed SAN enabled blade importing the SPR database.

Step 4 Configuring Sh and other components for SAN based SPR after it has been brought –up with positive results, for the test call in the previous step.

Step 5 Un-installing SSC on earlier blade of disk based SPR.

Step 6 Installing SSC on the blade from where it was un-installed.

Step 7 Completing the migration process.

Installing SSC Instance on SAN Connected Blade

Perform following procedure to install SSC instance on SAN connected blade.

Step 1 Perform cluster installation.

Step 2 Provide the IP addresses of both blades i.e the current blade as well as a blade that has active SSC instance with disk based SPR.

Step 3 Select for the primary database on the current blade.

Step 4 In *ssctemp.properites* chose for SAN based installation and HA enabled options.

Step 5 In *createGrid.cfg* for the stand-by database give the name of blade with disk based SPR.

Step 6 Complete the installation

Exporting SPR database

Perform following procedure to export SPR data base.

Step 1 Access the blade with active SSC instance.

Step 2 Shut down SSC application.

Step 3 Export SPR database schema.

Step 4 Start SSC application.

Importing SPR Database on Newly Installed SAN Enabled Blade.

Perform following procedure to import SPR database on SAN enabled blade.

Step 1 Upgrade IMDB application to appropriate version.

Step 2 Start IMDB application.

Step 3 Upgrade SSC instance to appropriate version.

Step 4 Edit *etc/system.cfg* and set value of the parameter **HaEnabled** to 0.

Step 5 Start SSC.

Step 6 Ensure that sample profile is exported correctly.

Step 7 Bind Sh controller. Ensue it is working properly by trying test call for a sample subscriber profile.

Step 8 If results of the test mentioned in previous step are positive, then un-bind Sh controller, shut down SSC and in system.cfg change value of the parameter HaEnabled to 1. Start SSC application.

Step 9 If test results are negative then troubleshoot the issues with SAN based SPR.

Completing Migration

Perform following procedure to complete single host to multi-host migration.

Step 1 Confirm that grid is attached properly with two entries one for each blade.

Step 2 Confirm that standby database is replicating from active database.

Step 3 Ensure that the files /etc/cluster/cluster.conf and etc/host are identical for both blades.

Step 4 Start SSC application.

RAC Support

This section briefly describes the RAC support along with RAC-HA installation prerequisites and procedures.

This section contains following sub-sections:

- RAC Overview
- RAC-HA Installation Prerequisites
- RAC-HA Primary Node Installation
- RAC-HA Secondary Node Installation

RAC Overview

This section briefly describes the RAC support in the enhanced architecture.

Enhanced SSC architecture supports Oracle Real Application Cluster (RAC). The RAC allows Oracle data base to run any packaged or custom application un-changed across the server pool. It provides facility to add more servers and instances to the pool without taking the users offline. In the previous SSC architecture, the data base can become single point of failure as well as performance bottle neck as it is installed on a single blade in any site.

With RAC Oracle de-couples the Oracle instance i.e. the processes and memory structures that are running on the server to access the data, from the data files i.e. the physical structure that is actually storing the data. A clustered database can be accessed by multiple instances running on separate servers.

Important: In a non-RAC deployment, when the data base server fails in the first site the fail-over occurs in the second site. In a RAC deployment failure of one database instance fail-over does not occurs in second site, as another database instance form the first site takes over.

RAC –HA Installation Prerequisites

This section briefly describes RAC-HA installation prerequisites.

Following are the RAC-HA installation prerequisites:

- The Virtual IPs (VIPs) used in the installation should be registered in the DNS and they must be on the same sub-net as the public host network addresses. Each Configured VIP requires an un-used and resolvable IP address.
- RAC installation needs seven partitions on the sheared disk. Partition the shared disk as described in the following table.

Table 3. RAC-HA Partition Table

Partition Name	Partition Type	Partition Content (Size of Partition in %)
/dev/sde1	Primary	Data disk, Redo logs, Control file 1 (25%)
/dev/sde2	Primary	Index disk, Redo logs, Control file 2 (15%)

Partition Name	Partition Type	Partition Content (Size of Partition in %)
/dev/sde3	Primary	System file disk, Control file 3 (5%)
/dev/sde4	Extended	
/dev/sde5	Logical Extended 1	Flashback file disk (10%)
/dev/sde6	Logical Extended 2	Archive file disk (35%)
/dev/sde7	Logical Extended 3	Cluster file disk (5%)
/dev/sde8	Logical Extended 4	Cluster file disk (5%)

Primary Node Installation – RAC HA

This section briefly describes primary node installation procedure for RAC – HA deployment. *Refer RAC-HA Prerequisites* as well as *Before You Begin* section of this chapter, before proceeding with RAC-HA set-up.

Installing Primary Node for RAC-HA

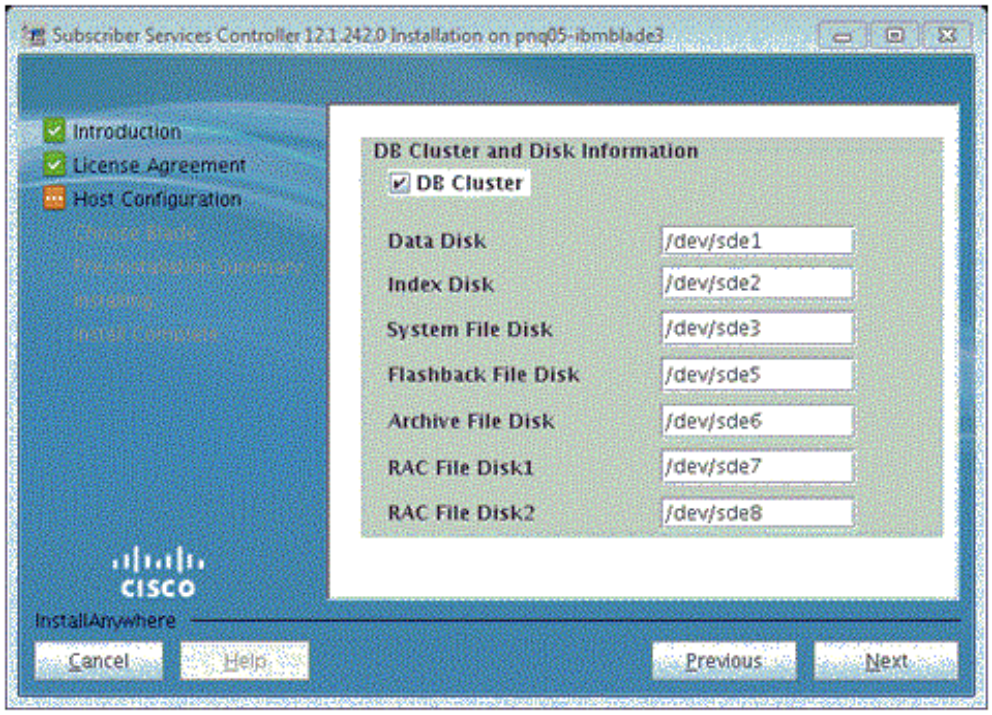
To install primary node for RAC-HA:

Step 1 Follow the procedure mentioned in the section, *Installing SSC on a Single Host* upto **step 7**, the **Cluster Installation** step to **Add** or **Remove** the **Network Configuration**.

Ensure that:

- Number of Blades is 2 as this is a two node setup. In the Choose Blade field, the blade number on which this installation is being performed is selected.
- Cluster Name is same for all the nodes in a cluster.
- In the Choose Interface field there are 6 entries viz eth0 upto eth5 for each blade. Refer you IP map and network planning section for choosing the interface and the interface name.
- If you do not have NIC bonding then you need to configure only et1, et2 and eth3. The Ethernet cards et4 and eth5 can be used for NIC bonding if they are not being used as management interface.

Step 2 Click **Next** to configure **DatabaseCluster** and **Disk Information** for the RAC-HA set-up. Specify the disk partitioning information refer table tiled *RAC-HA Partition* from previous section.



Step 3 Click **Next**to specify the **Virtual IP Address**. Provide Virtual IP address and the interface names for both the blades.

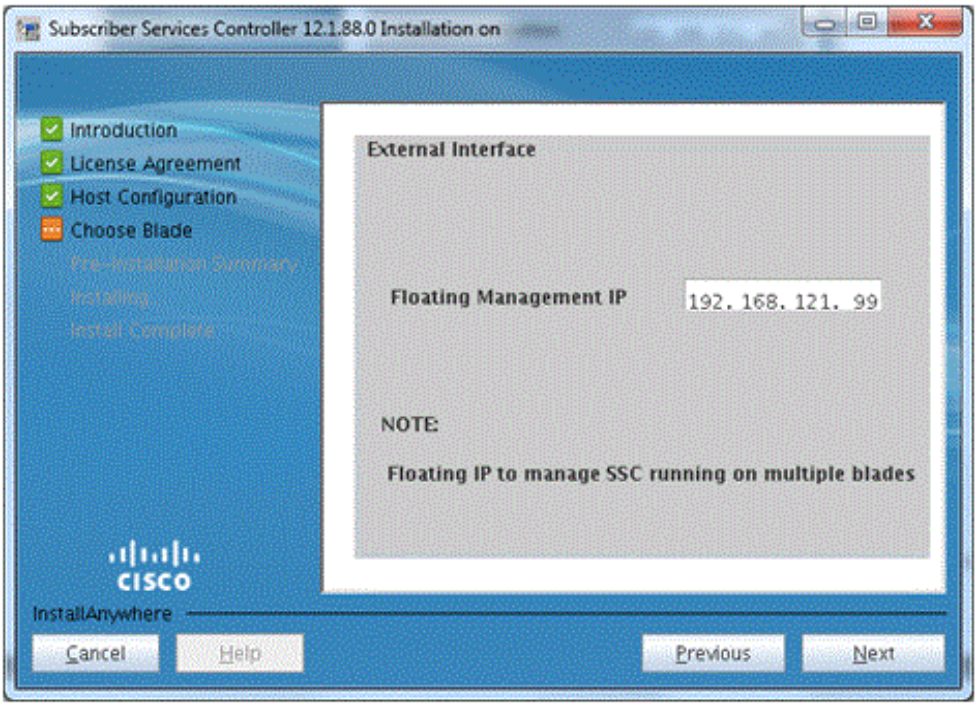
Step 4 Click **Next** to specify the **Installation Set.** Select **Application** and **Primary Database**, along with the blade on which you want to install this application. Refer step 9 of the procedure Installing SSC on single host.

> ***Important:*** Installation on multiple nodes is not supported in the current release.

Step 5 Click **Next** to specify the **Slot Numbers** for the blade.

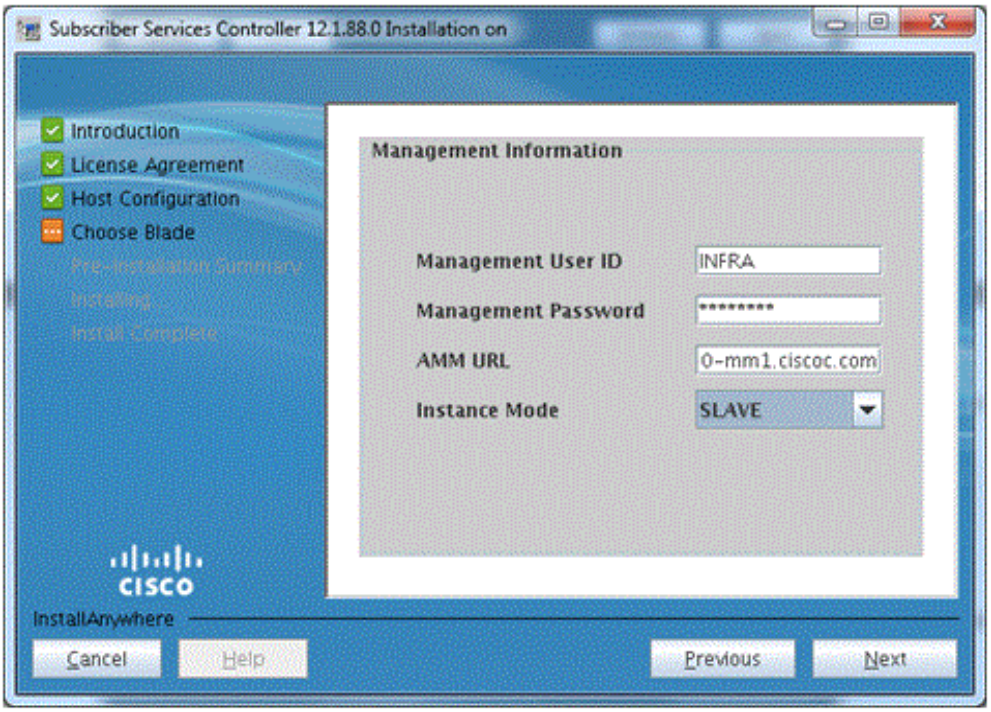
> ***Important:*** If you are not aware of the slot numbers, then specify slot number 1 for blade 1 and slot number 2 for blade 2 respectively.

Step 6 Click **Next** to specify the **Floating Point Management IP**.



The Floating Point Management IP is used to manage the SSC instance running on multiple blades.

Step 7 Click **Next** to specify the **Management Information**.



The management information includes:

- Management user Id

- Management Password
- AMM URL
- Instance Mode - Select the instance mode as Master for Primary Node installation for RAC-HA.

Step 8 Click **Next** to specify the **Port Details** for the TimesTen **Active** and **Standby** node.

Step 9 Click **Next** to view the **Pre-Installation Summary** panel.

It includes following information:

- Product Name
- Install Folder
- Link Folder
- Available as well as required disk space in bytes.

Step 10 Click **Next** to view the important information. Read the information regarding the interface values. Access the **ssctmp.properties** file from */localhome/install* folder. Set value of INSTALL_SAN_ENSBLED parameter to true.

Step 11 Click **Next** whenever the installer prompts and complete the installation.

Secondary Node Installation RAC-HA

Perform the task described in the previous section on the second node. In step 4 while specifying the I**nstallation Set**, select only **Application** for blade 2.

SSC Uninstallation

The section lists the procedure to un-install SSC.

The un-installation wizard removes SSC application along with all database records and deletes the database schema.

Important: If your SSC cluster deployment is using multiple hosts or blades, then you need to run this un-installation wizard on each such host.

Un-installing SSC

Perform following procedure to un-install the SSC:

Step 1 Log in as a user with root administration privileges.

Step 2 Ensure that your **X windows** application such as Xterm or Xming is active and running. If **Putty** application is being used to access SSC Console, then ensure that the Putty setting **Enable X11 forwarding** is selected.

Step 3 Access SSC installation directory by issuing following command

```
cd../localhome/install/uninstall
```

Step 4 Execute the script **`uninstallSSC`**, by issuing following command

```
./uninstallSSC.sh
```

Step 5 SSC initiates the GUI based un-installer.

Step 6 Click **Next**, the un-installer first stops and then removes SSC related database and applications, by executing the clean-up scripts and displaying appropriate messages.

Step 7 Click **Done** to exit SSC un-installer.

Step 8 You can access detailed log of SSC un-installation process in **`../var/log/messages`**file.

Important: After executing un-installation wizard, you can ensure that the un-installation was complete, by checking that processes related to database, IMDB and SSC application are not active.

Chapter 3
SSC Administration

This chapter provides information and procedures to administer SSC node in PCC deployment.

SSC is an element of Cisco Policy Charging and Control (PCC) solution. SSC acts as an intelligent database for policy services. By acting as a centralized policy software application engine, SSC complements IPCF for converged session handling.

Depending upon the configuration of SSC deployment, administering SSC system involves tasks related to monitoring and administering the interfaces for **Sh**, Event Notification (EN) and User Data Repository (UDR) applications. SSC uses these interfaces to exchange the subscriber profile or service usage data with respective components of PCC solution as well as with external OSS or BSS. SSC administration also involves tasks related to administering subscriber profile, service plans and data store related to profile and plans.

SSC administration also involves tasks related to security, audit and troubleshooting for the SSC deployment.

This chapter discusses pre-requisites for SSC administration, and covers following sections for SSC administration:

SSC Administration Overview

This section briefly describes SSC administration and monitoring tasks.

In an SSC node deployment scenario all tasks can be divided in following major groups:

- Administering SSC Node.
- Provisioning Subscriber and Subscription Information.
- Monitoring Performance of SSC Node.
- Monitoring Security of SSC Node.

Administering SSC involves tasks such as administering users, managing the interfaces for various applications such as event notification module, that interact with SSC as well as configuring and monitoring alarms, logs and statistics generated by deployment.

Provisioning subscriber and subscription information includes tasks related to provisioning subscriber profile, notifications and related database objects using methods such as bulk load, SPR APIs, PPT application and Ud interface for external LDAPs. Depending upon your business model SSC can be configured to provision following:

- Static subscriber profile
- Dynamic subscriber profile
- Data or service plans and related add-on
- Subscription tire
- Notification template.

As per the deployment requirement SSC can use any of the following provisioning methods or their combination:

- SSC console.
- PPT application using XML-RPC interface.
- External LDAP using Ud interface.
- SPR provisioning APIs using SOAP/XML.
- Subscriber Profile Bulk load using shell script and CSV files.
- Auto provisioning.

Provisioning also includes tasks related to administering profile and usage policy for the subscriber. Tasks such as monitoring and administering subscriber profile and groups as well as subscription plans and data stores related to profile and policy fall under this category.

> ***Important:*** Profile, plans, group and data store administration tasks are available only when you log-in to SSC Administration Console as a policy administrator or as a user whose credentials include policy administration credentials. For more information refer *User Administration* section.

Monitoring performance of SSC node includes tasks such as, monitoring system logs and system statistics as well as monitoring system resources using threshold policies.

Monitoring security of SSC node involves tasks such as managing system password, viewing system, SPR and event log audit records, viewing system session information.

Before You Begin SSC Administration

This section includes pre-requisites that must be satisfied and tasks that must be performed before you begin to administer SSC.

This section includes following sub-sections:

- Pre-requisites for SSC Administration
- Controlling Maintenance Mode
- Accessing SSC Administration Console
- Checking Status of SSC Application
- Starting SSC Application
- Checking Status of IMDB Application
- Bulk Loading Subscriber Profile Data

Pre-requisites for SSC Administration

This section describes the pre-requisites for administering an SSC.

Following are the pre-requisites for administering SSC:

- Status of the database, that is being used by the SSC to store subscriber, subscription and policy related data, must be active.
- Status of IMDB application that is being used by SSC to provide the database grid for the cluster deployment, must be active.
- Status of SSC application must be active.

> ***Important:*** You can verify the status of database and the IMDB, by executing the script `sscdbstatus.sh` located in the `localhome/ssc/install/spr_install/tools` directory.

- If SSC is deployed in the cluster mode then all the blades in a cluster must be accessible.
- Sh controller is bound with the host machine as per your IP map, so that SSC application can communicate with other components of PCC solution, such as PPT.
- Profile controller is bound with the host machine as per your IP map, so that SSC application can communicate with other components of PCC solution, such as PPT.

Ensuring Accessibility of Blade Cluster

Before initiating the administrative tasks for an SSC cluster deployment ensure that the blade cluster is accessible.

To ensure accessibility of a blade cluster:

Step 1 Ping the host names by referring IP map and ensure that the individual host or blades are reachable.

Step 2 Check status of the SSC instance on all the blades in cluster. The status should be active on all the blades.

Step 3 Check status of the database, on the blades that are configured as primary or secondary database using the `dbstatus.sh` script. Database status should be active.

Binding Sh controller

For SSC to communicate with other components of PCC solution, Sh controller needs to be bound with the host machine as per your IP map.

To bind Sh controller:

Step 1 Login to the host with root administrative privileges.

Step 2 Invoke system administrative privileges for the SSC node by issuing following command:

```
su - sscadmin
```

Step 3 Execute SSC administration script by issuing following command:

```
./sscadm
```

SSC Administration Console window appears.

Step 4 Press **1** to access System Administration options.

Step 5 Press **L** to access to access List Hosts option.

If multiple hosts are available, then select the host machine with which you want to bind the Sh controller.

Step 6 Press **c** to access Interface Management option.

Step 7 Specify the number indicating the Sh controller, for **Enter Option**.

SSC Administration Console binds the Sh controller with the host machine and displays appropriate message.

Binding Profile controller

For SSC to communicate with other components of PCC solution, Profile controller needs to be bound with the host machine as per your IP map.

To bind profile controller:

Step 1 Login to the host with root administrative privileges.

Step 2 Invoke system administrative privileges for the SSC node by issuing following command:

```
su - sscadmin
```

Step 3 Execute SSC administration script by issuing following command:

```
./sscadm
```

SSC Administration Console window appears.

Step 4 Press **1** to access System Administration options.

Step 5 Press **L** to access to access List Hosts option.

If multiple hosts are available, then select the host machine with which you want to bind the Sh controller.

Step 6 Press **c** to access Interface Management option.

Step 7 Specify the number indicating the profile controller, for **Enter Option**.

SSC Administration Console binds the profile controller with the host machine and displays appropriate message.

Controlling Maintenance Mode

This section briefly describes the maintenance mode for the SSC deployment.

During installation, upgrade or trouble shooting, you may need to work on the deployment by manually executing some scripts. An SSC deployment contains various cron jobs and background processes that may interrupt such manual script execution.This can be avoided by using the **Maintenance** mode. By default this maintenance mode is enabled after successful completion of installation or upgrade procedure.

You need to:

- Enable the maintenance mode to verify the deployment set-up after any installation or upgrade operation.
- Disable the maintenance mode after completion of installation, upgrade or troubleshooting activities. This is required for proper functioning of cron jobs and background processes.

Enabling or Disabling Maintenance Mode

To enable to disable the maintenance mode:

Step 1 Log in with database administrative privileges.

Step 2 Access the directory */localhome/ssc/tools*.

Step 3 Execute the script **maintenanceMode.sh**.

Following options are available for this script:

- **Status**: To view current status of the maintenance mode.
- **Disable**: To disable the maintenance mode.
- **Enable**: To enable the maintenance mode.
- **Help**: To access more information about usage.

Accessing SSC Administration Console

This section describes the prerequisites and procedure to access the SSC administration console.

You can access the SSC Administration Console provided that you satisfy following pre-requisites:

- SSC has been installed successfully either as a single host or in cluster mode.
- You have root administrative privileges for the host or the cluster of blades.
- You have system administrative privileges for the SSC installation.

Important: PuTTY window must be maximized, if PuTTY application is being used to access SSC console.

Using SSC Administration Console

Before initiating the administrative tasks for an SSC cluster deployment using the SSC Administration Console, ensure that you can access this console.

To access SSC administration console:

Step 1 Login to the host with root administrative privileges.

Step 2 Invoke system administrative privileges for the SSC node by issuing following command:

```
su - sscadmin
```

Step 3 Execute SSC administration script by issuing following command:

```
./sscadm
```

SSC Administration Console window appears.

Step 4 Specify login and password of appropriate user level.

The console displays appropriate status messages in the message window.

Checking Status of SSC Application

This section describes the procedure to view the status of SSC application.

Viewing Status of an SSC Application

All SSC components run as independent processes. SSC allows you to check the status of each such process.

To view status of an SSC application:

Step 1 Login with SSC Administrative privileges.

Step 2 Check the status of SSC application instance by issuing following command:

```
./sscadm status
```

SSC displays current status of its various components such as Heart beat daemon, Login daemon, System manager and Scheduler. For each process the running status indicates that corresponding component is active and running.

Important: You can also use the system status option from the SSC Administration Console to view current status of SSC service instance.

Starting SSC Application

This section describes the procedure to start an instance of SSC application.

Starting an SSC Application Instance

All SSC components run as independent processes. SSC provides a script to start or stop an application instance.

To start an SSC application instance:

Step 1 Login with SSC Administrative privileges.

Step 2 Start SSC application instance by issuing following command:

```
./sscadm start
```

SSC initiates its various components such as Heart beat daemon, Login daemon, System manager and Scheduler.

Step 3 Use **`status`** command to ensure that all SSC components are started successfully.

Important: You can also use the system status option from the `SSC Administration Console` to view current status of SSC service instance as well as to start or stop an instance.

Checking Status of IMDB Application

This section describes the procedure to check status of IMDB application.

Viewing Status of IMDB Application

In a cluster deployment of SSC, the In-Memory Data Base (IMDB) application provides a grid that can be used to access the database. Hence, all the instances of this application needs to be active and running for normal functioning of an SSC cluster.

To view status of an IMDB application:

Step 1 Get the names of IMDB instances, by starting the SSC instance if it is not active by issuing following command:

```
./sscadm start
```

Step 2 Access the file `localhome/ssc/etc/system.cfg` from SSC installation directory.

Step 3 Note the names of IMDB and database instances from the file mentioned in previous step.

Step 4 To ensure that these instances are active, login with SSC administrative privileges.

Step 5 Check the status of IMDB instances by issuing following command:

```
./<IMDB_App>status
```

SSC displays a list of active connections to the data store. For each active connection it displays Type of connection, Process Id (PID), Context and Name of the connection along with its Connection Id (ConId). Names of database and IMDB application instances will be displayed here, if these instances are active.

Step 6 Ensure that a message that indicates that replication agent is running, is displayed while verifying the status of IMDB application using following command:

```
<IMDB_App> status
```

Bulk Loading Subscriber Profile Data

This section describes procedures to bulk load subscriber profile data for standalone as well as GR/HA SSC deployments.

Bulk Loading Subscriber Profile Data For a Standalone SSC Deployment

This section briefly describes how to execute bulk load operation for a stand alone SSC deployment.

SSC provides a script to bulk load subscriber profile data, if such data is available in CSV format. Refer to *Bulk Load Provisioning* feature in *Overview* chapter for more information regarding structure and nomenclature of the CSV file containing profile data. Enhanced SSC architecture increases the provisioning speed by providing an independent process that caters to provisioning load.

Important: It is recommended that SSC Administration Console should not be used for subscriber provisioning, the provisioning should carried out using bulk upload script and CSV file.

To bulk load subscriber profile data for a standalone SSC deployment:

Step 1 Add subscription tires, plans and mail or SMS flags referring to CSV file stricture.

Step 2 Login to the SSC deployment with privileges of Oracle user and execute the following command: `sh /localhome/ssc/tools/maintenanceMode.sh enable`.

Step 3 If you want to start with fresh Oracle data base then truncate the database by executing the script `/localhome/ssc/install/spr_install/tools/cleanup.sh SSC`.

Important: Execute this step if you want to remove all the existing data from Oracle tables.

Step 4 Login to the deployment with SSC administrative privileges and stop the SSC application by using the command: `. /sscadm stop`.

Step 5 Login to SSC deployment as Oracle user and access Times Ten prompt by executing following command : `ttisql "DSN=<Data Store ame>;UID=cacheuser;PWD=timesten;OraclePWD=oracle"`.

Step 6 Execute following set of commands to pause auto-refresh for the RO cachegroups:

Important: This step is to be followed for the standalone SSC deployment with less than 1 million subscribers.

Use auto refresh by executing following commands:

- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUBSCRIPTION_TIER SET AUTOREFRESH STATE PAUSED`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_MSISDN_IMSI SET AUTOREFRESH STATE PAUSED`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUBSCRIBER_MASTER SET AUTOREFRESH STATE PAUSED`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUB_PLAN_BUNDLE SET AUTOREFRESH STATE PAUSED`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUB_USAGE SET AUTOREFRESH STATE PAUSED`

Step 7 Copy the .csv data file that you want to upload to the SSC deployment into */localhome/ssc* directory.

Step 8 Login as a root user and access the directory */localhome/ssc* and execute the command : `run ./tools/bulk_load_sub -f <cav file name>`.

Step 9 After completing the upload access the upload process logs from the file */localhome/oracle/incommingdata/bload*. Records indicating unsuccessful upload will be indicates by ***.bad** file name.

Step 10 After completing the upload process, ensure that Oracle tables are populated with the subscriber records, by accessing *localhome/ssc* directory and executing following files with root user privileges.

> ***Important:*** This step is to be followed for the standalone SSC deployment with greater than 1 million subscribers.

Execute following files:

- `./tools/dumpDbData -c --table spr_sub_plan_bundle --src oracle`
- `./tools/dumpDbData -c --table spr_msisdn_imsi --src oracle`
- `./tools/dumpDbData -c --table spr_sub_flag --src oracle`
- `./tools/dumpDbData -c --table spr_sub_usage --src oracle`
- `./tools/dumpDbData -c --table spr_subscriber_master --src oracle`

Step 11 Ensure that the database grid is attached properly, by logging in with Oracle user privileges and executing following command: `/localhome/ssc/install/spr_install/tools/sscdbstatus.sh SSC`

Step 12 Start the SSC application by logging with SSC administrative privileges and executing the command: `./sscadm start`.

Step 13 Disable the maintenance mode by logging in with Oracle user privileges and executing the command: `sh /localhome/ssc/tools/maintenanceMode.sh --disable`.

Bulk Loading Subscriber Profile For GR-HA SSC Deployment

This section briefly describes how to execute a bulk load operation for a Geo Redundant (GR) and Highly Available (HA) SSC deployment.

SSC provides a script to bulk load subscriber profile data, if such data is available in CSV format. Refer to *Bulk Load Provisioning* feature in *Overview* chapter for more information regarding structure and nomenclature of the CSV file containing profile data. Enhanced SSC architecture increases the provisioning speed by providing an independent process that caters to provisioning load.

The bulk load procedure for GR-HA SSC deployment differs slightly from the bulk load procedure for standalone SSC deployment.

> ***Important:*** It is recommended that SSC Administration Console should not be used for subscriber provisioning, the provisioning should carried out using bulk upload script and CSV file.

To bulk load subscriber profile data for a GR-HA enabled SSC deployment:

Step 1 Refer step 1 of the previous task.

Step 2 For all the nodes first enable maintenance mode and then disable automatic database failover.

- Enable maintenance mode using following command: `sh /localhome/ssc/tools/maintenanceMode.sh --all --enable`.
- Disable automatic database failover using following command:`/localhome/ssc/tools/failoverFlag.sh --disable` .

Important: Execute this command first on the primary node and then on the secondary node.

Step 3 Refer step 3 of the previous task.

Step 4 Login to the deployment with SSC administrative privileges and stop the SSC application by using the command: `./sscadm stop`.Stop SSC application on primary as well as secondary node.

Step 5 Login to SSC deployment as Oracle user and access Times Ten prompt by executing following command : `ttisql "DSN=<Data Store ame>;UID=cacheuser;PWD=timesten;OraclePWD=oracle"`

Step 6 Execute following set of commands to pause auto-refresh for the RO cachegroups:

Important: This step is to be followed for the standalone SSC deployment with less than 1 million subscribers.

Use auto refresh by executing following commands:

- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUBSCRIPTION_TIER SET AUTOREFRESH STATE PAUSED.`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_MSISDN_IMSI SET AUTOREFRESH STATE PAUSED.`
- `LTER CACHE GROUP CACHEUSER.TT_SPR_SUBSCRIBER_MASTER SET AUTOREFRESH PAUSED.`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUB_PLAN_BUNDLE SET AUTOREFRESH STATE PAUSED.`
- `ALTER CACHE GROUP CACHEUSER.TT_SPR_SUB_USAGE SET AUTOREFRESH STATE PAUSED.`

Step 7 Refer step 7 of the previous task.

Step 8 Refer step 8 of the previous task.

Step 9 Refer step 9 of the previous task.

Step 10 After completing the upload process, ensure that Oracle tables are populated with the subscriber records, by accessing *localhome/ssc* directory and executing following files with root user privileges.

Important: This step is to be followed for the standalone SSC deployment with greater than 1 million subscribers.

Execute following files:

- `./tools/dumpDbData -c --table spr_sub_plan_bundle --src oracle`
- `./tools/dumpDbData -c --table spr_msisdn_imsi --src oracle`
- `./tools/dumpDbData -c --table spr_sub_flag --src oracle`
- `./tools/dumpDbData -c --table spr_sub_usage --src oracle`
- `./tools/dumpDbData -c --table spr_subscriber_master --src oracle`

Step 11 Ensure that the database grid is attached properly, by logging in with Oracle user privileges and executing following command: `/localhome/ssc/install/spr_install/tools/sscdbstatus.sh SSC`

Ensure that the command is executed on primary as well as secondary node.

Step 12 Start the SSC application by logging with SSC administrative privileges and executing the command: `./sscadm start`

Ensure that the command is executed on primary as well as secondary node.

Step 13 Disable Maintenance mode and enable failover.

- Disable maintenance mode using following command: `sh /localhome/ssc/tools/maintenanceMode.sh --all --disable`.
- Enable automatic database failover using following command:`/localhome/ssc/tools/failoverFlag.sh --enable .`

Administering SSC Using Console

This section describes the procedures and methods to use the SSC Administration Console, to perform administrative tasks for SSC.

The SSC Administration Console displays current status of an SSC instance as well as starts or stops the SSC instance and displays appropriate messages.

Important: PuTTY window must be maximized, if PuTTY application is being used to access SSC console.

This section includes following sub-sections:

- System Status Monitoring
- User Administration
- Interface Management
- SSC Logs Administration
- SNMP Traps and Alarms Configuration
- Bulk Statistics Configuration
- Subscriber Profile Repository (SPR) Configuration
- Configuration Management
- Profile Controller Configuration
- Policy Provisioning Tool (PPT) Configuration
- SSC Home or Roaming Feature Configuration

System Status Monitoring

This section describes procedures to view current status of the system along with active tasks related to SSC components and application interfaces as well as message routing table.

Depending upon access privileges for the SSC instance, you can perform following tasks:

- Verifying System Status
- Viewing Active SSC System Tasks
- Viewing Message Routing Table

Verifying System Status

This section describes how to view system status and start or stop the system.

Viewing System Status

This section describes the procedure to verify the SSC system instance status on SSC node and to start/stop the instance.

To viewing system status:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **a** to monitor the status of SSC instance.

Step 5 Press **V** to view the current status of the system. It indicates whether this instance of SSC is running or it has stopped.

If SSC instance is stopped and you want to start it, press **s** key. If SSC instance is running and you want to stop it, press the **t** key.

Viewing Active SSC System Tasks

This section describes how to view active tasks associated with an SSC instance.

Viewing Active Tasks Associated with SSC System Instance

An SSC instance is active when all tasks or processes associated with that instance are active.

To view active SSC system tasks:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **K** to monitor the status of processes associated with SSC instance.

SSC Administration Console displays the list of SSC base and common component as well as SPR, Ud and event component processes such as sn_hbd, sn, sn_appmgr, sn_shctrl, sn_udctrl, sn_enctrl respectively along with their process id and current status as running or not –running.

Viewing Message Routing Table

This section describes how to view the message routing tables.

Viewing Message Routing Tables

A message routing table displays available routes for a message.

To view message routing tables:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **R** to access the message routing table for SSC instance.

SSC Administration Console displays the message routing table.

Important: Depending upon your access privilege, more routing table information can be generated using the script **dumprtbl** available in */localhome/ ssc /tools* directory.

User Administration

This section describes the procedures to administer the users.

SSC provides pre-defined roles that can be assigned to a user. Each of this user role has different access privileges.

Depending upon your deployment configuration following roles can be assigned to users:

- **Policy Administrator (PA)**: This role can perform administration tasks for Subscriber Profile Repository (SPR). This role can also add, delete or modify data in the database.
- **Policy Operator (PO)**: This role can only view subscriber profile and related data in the database.
- **System Administrator (SA)**: This role can perform all the tasks related to SSC application and deployment specific configurations.
- **System Operator (SO)**: This role can only view the system configuration.

Depending upon access privileges you can perform following tasks:

- Viewing Existing Users
- Adding New User
- Deleting Existing User
- Resetting User Password

Viewing Existing Users

This section describes how to view existing users who can access an SSC instance.

Viewing Existing Users with Assigned Roles

This section describes the procedure to view the existing users who can access SSC node, as well as their configured roles.

To view existing users:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **b** to access the user administration options.

Step 5 Press **V** to view the user roles configured for your deployment.

Step 6 Specify the role, to generate a list of users who can access this instance of SSC using the selected role

SSC Admin Console displays the list of the users associated with this role.

Adding New User

This section describes how to add a new user.

Adding a New User With Assigned Role

This section describes the procedure to add a User with its assigned role to an SSC node.

To add a new user to an SSC node:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **b** to access the user administration options.

Step 5 Press **N** to add a new user.

Step 6 Specify the name of the user.

Step 7 Specify the password which can be used by this user to access the SSC node.

Step 8 Specify the role that is to be associated with this user.

SSC Administration Console displays the message that the user has been added.

Deleting Existing User

This section describes how delete a user from an SSC node.

Deleting an Existing User From SSC Node

This section describes the procedure to delete a user from an SSC node.

To delete a user from an SSC node:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **b** to access the user administration options.

Step 5 Press **t** to delete an existing user.

Step 6 SSC Administration Console invokes the delete user action.

Step 7 Specify the name of the user that you want to delete.

SSC Administration Console deletes the user and displays appropriate message.

Resetting User Password

This section describes how to re-set a user's password.

Resetting a User Password

This section describes the procedure to re-set a user's password.

To re-set the password of an existing user:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **b** to access the user administration options.

Step 5 Press **R** to access change password option.

Step 6 Specify the name of the user whose password you want to change.

Step 7 Specify the **New** password.

SSC Administration Console changes the password of the user and displays appropriate message.

Interface Management

This section describes the procedures to administer the host machines and application interfaces that are used by various applications to exchange data with SSC.

SSC uses various network interfaces such as **Sp**, **XML-RPC** or **FTP** to exchange the subscriber profile and session information with other components of the Policy Charging and Control (PCC) solution such as Intelligent Policy Control Function (IPCF), Policy Provisioning Tool (PPT) or Operation Support System (OSS) or Billing Support System (BSS).

Binding an interface with SSC, indicates SSC to associate a task such as **Sh** application or profile application or event application with a particular server or host machine. If SSC deployment has multiple hosts, then multiple options will appear for binding interfaces.

Binding an interface does not associate an IP address with the task. For associating the IP address with a task, you need to configure IP address for that individual component. For example IP address for **Sh** application is specified in **Sh** configuration, where as the bind interface option is used to select the host machine to run the **Sh** application.

Depending upon SSC deployment configuration, SSC needs to interact with various application interfaces. The bind interface option allows binding of an SSC application interface or one of the SSC components with the host machine.

SSC interface management involves following tasks:

- Listing Hosts
- Listing Interface Bindings
- Binding an Interface
- Un-binding an Interface
- View Status

Listing Hosts

This section describes how to list machines that are hosting SSC application.

Listing SSC Host Machines

This section describes the procedure to list machines that are hosting SSC application.

To list hosts:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **c** to access the interface management options.

Step 5 Press **L** to view the list of hosts configured for SSC node.

SSC Administration Console displays information of the hosts machines available for this deployment.

Listing Interface Bindings

This section describes how to list interface bindings

Listing Interface Bindings of SSC Components

This section describes the procedure to list interface bindings used by various components of SSC application.

To list interface bindings:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **c** to access the interface management options.

Step 5 Press **t** to view the list of bindings configured for SSC node.

SSC Administration Console displays the bindings configured for this deployment.

Binding an Interface

This section describes how to bind an application interface of any SSC component with the host machine.

Binding SSC Application Interface With Host Machine

This section describes the procedure to bind an SSC application interface with a host machine.

To bind an interface:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **c** to access the interface management options.

Step 5 Press **i** to bind the interface.

SSC Administration Console displays the bindings configured for this deployment.

Step 6 Specify the details of binding between the host machine and SSC component.

SSC Administration Console binds the interface to the host machine and displays appropriate message.

Important: SSC displays appropriate warning message, if some other SSC related task or application is already associated with this machine that you are currently attempting to bind with additional SSC related task or application.

Un-binding an Interface

This section describes how to un-bind an SSC application interface from the host machine.

Un-binding SSC Application Interface From Host Machine

This section describes the procedure to un-bind an SSC application interface from its host machine.

To un-bind an interface:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **c** to access the interface management options.

Step 5 Press **u** to delete the binding of this interface.

SSC Administration Console severs the connection between interface and host machine and displays appropriate message.

Important: This option allows you to un-bind an SSC application interface or SSC component from the host machine and isolate that host machine for troubleshooting or maintenance purpose.

View Status

This section describes how to view the availability status of the SSC interfaces.

Viewing Binding Status of the Interfaces Configured on Host Machine.

This section describes the procedure to view status of SSC application interfaces.

To view interface status:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **c** to access the interface management options.

Step 5 Press **S** to access view status option. .

SSC Administration Console displays a list of configured interface, or it displays appropriate error message.

Step 6 Select the interface whose status you want to monitor.

SSC Administration Console displays the binding status for the selected interface.

SSC Logs Administration

This section provides information about SSC logs.

SSC logs can be used to monitor the availability of various application interfaces and host machines as well as for the troubleshooting issues associated with deployment.

SSC logs are categorized as:

- **Event logs**: SSC records information related to events that affect subscriber profile or their service usage. These logs are used to troubleshoot the issues related to profile and service usage of the subscriber. Event logs consist of e-mail and SMS notifications that have been generated by SSC and sent to the subscriber.

  Following is an example of an event log entry:

  ```
  Timestamp:12-APR-2011 16:31, Module Id:SPR Audit, Event Id: Create Data
  Plan(15), client_context session_id: 45668734556, user_name: policyadmin,
  Request: plan_name: plan-2, Response: result_code :0
  ```

  Event logs are stored in a database. Depending upon access privilege, and deployment configuration. You can access these logs using SPR API as well as purge these logs as per requirements.

  Important: Event logs are also known as audit logs.

- **System logs**: SSC also records information related to deployment infrastructure such as web servers and active sessions. System logs are mostly used for administering SSC node and troubleshooting issues related to hardware and software infrastructure of SSC node, such as web servers and associated sessions. System logs can be used to troubleshoot issues related to system performance by analyzing errors and access information related to web servers and AXIS framework.

  System process logs are stored in file **sn_SSC.log**. This file can be rotated based on time, size or number of entries, to prevent the log files from growing infinitely. Refer section *Changing SSC Log Sink Settings* for more information.

  Following is an example of a system log entry:

  ```
  11-May-03+14:59:05.226 [sysmgr:1 (24703/18752)] [sysctrl_callback.cpp:329]
  [info sysmgr 7505] Logged in: user name - SA, role - 10, session id -
  1498446599
  ```

Important: For more information about system logs, refer to the section *Monitoring System Logs*.

SSC uses event or audit logs to record information related to:

- System configuration events.
- Subscriber Profile Repository (SPR) provisioning events.
- Subscriber notification logs.
- Specific logs that are being triggered by the Intelligent Policy Control Function (IPCF) to record specific events related to SSC.

SSC can log e-mail and SMS event notifications that have been generated and sent to the subscriber. The event notification log records time, user id and details of the notification. Subscriber's preferences determine the events that are being logged. Following events implicitly generate the notifications:

- Recharge of a data or usage plan.
- Crossing the threshold associated with the usage of a plan.
- Resetting of user account at the start of billing cycle.

Important: Billing cycle re-set dates for subscribers and usage threshold levels for configured data plans can be defined using Policy Provisioning Tool (PPT).

IPCF triggers logging in SSC by provisioning the event log actions using event notification (EN) interface between IPCF and SSC.

SSC logs administration involves following tasks:

- Changing Sink Settings
- Changing Debug Level
- Changing Session Log Level
- Viewing Logging Level Configuration
- Managing Syslog

Changing Sink Settings

The log sink is used to send the SNMP alarms. It is used by the central logging server residing on the management blade. This section describes how to change sink settings.

Changing SSC Log Sink Settings

This section describes the procedure to change sink settings while capturing SSC logs.

To change sink settings:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **d** to access log configuration options.

Step 5 Press **K** to access sink settings.

Step 6 Specify maximum size for the individual log file. The range is from 1 to 50 Mb. Maximum size defines upper limit for the size of a log file in MegaBytes (MB).

Step 7 Specify maximum duration between successive samples. The range is from 1 to 360 minutes. SSC creates a new log file after set duration time is lapsed.

Step 8 Specify Maximum count. The range is between 0 to 50. Maximum count defines the number of files in which the logs are recorded in rotation.

Important: Count zero indicates that the files will not be rotated while recording the logs.

Step 9 Specify log verbosity as detail, brief or normal. Log verbosity defines the degree of details that are to be recorded while logging values for this parameter.

SSC Administration Console updates the sink setting for the log as per the values specified in steps 6 to 9.

Changing Debug Level

This section describes how to change debug levels of the logs that are being captured.

Changing Debug Level For SSC Node

This section describes the procedure to change the Debug level on SSC node.

To change debug level:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **d** to access log configuration options.

Step 5 Press **L** to access debug level settings.

Step 6 SSC Administration Console displays existing logging configuration. The log categories correspond to the SSC processes for deployment.

Step 7 Specify the log category for which you want to change the log level.

Step 8 Specify the log level. Valid values for the log levels are info, critical, notice, emergency, trace, alert, warning, error and debug.

SSC Administration Console assigns updated logging level to the selected logging category.

Changing Session Log Level

This section describers how to change the session log level.

Changing Session Log Level For SSC Node

This section describes the procedure to change the session log level on SSC node.

To change session log level:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **d** to access log configuration options.

Step 5 Press **S** to change the existing level of session logs.

Step 6 Specify new logging level.

Available levels for session logs are Debug, Info, Warning, Critical and Error.

Step 7 Specify whether you want to enable or disable the console capture.

SSC Administration Console updates session log configuration and displays appropriate message.

Viewing Logging Level Configuration

This section describes how to view logging level configuration.

Viewing Configured Logging Level For SSC Node

This section describes the procedure to view configured logging levels.

To view log level configuration:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **d** to access log configuration options.

Step 5 Press **V** to view existing log configuration.

SSC Administration Console displays the default/configured log level.

Important: Currently available logging levels are Debug, Information, Warning, Critical and Error.

Managing Syslog

Syslog protocol is used by SSC network devices such as blades, to send event messages to a logging server, such messages are sent upon activation of associated triggers and used device monitoring and trouble shooing purpose. This section describes how to manage syslog.

Enabling or Disabling Syslog Storage

This section describes the procedure to manage syslog information by enabling or disabling the syslog storage.

To enable or disable the syslog storage:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **d** to access log configuration options.

Step 5 Press **M** to access manage syslog option.

Step 6 SSC Administration Console displays whether the syslog option is enabled or disabled, and allows you to change that status by specifying **y** or **n**.

Step 7 If in the previous step, you chose to enable this option then you need to specify name or IP address of the remote computer where you want to store the syslog.

Step 8 Specify root password for this computer.

Step 9 SSC Administration Console enables or disables the storage and displays appropriate message in the message window.

SNMP Traps and Alarms Configuration

This section describes the procedures to view and configure the SNMP traps and alarms.

Simple Network Management Protocol (SNMP) traps or alarms, provide information about the network status to system administrators. Alarms can also be used for troubleshooting the issues. Alarms are classified as critical, warning and informational.They mostly indicate the status of various SSC hardware and software components such as chassis, blades, power, I/O and storage modules.

An SSC instance can be configured to generate alarms for following events:

- Crashing and restarting of processes.
- Crossing or clearing the threshold by resources.
- Status change of peers from active to in-active and vice versa.

SNMP traps are sent to the configured SNMP traps receiver. These traps are also stored in the file `sn_SSC.log`. In the log file the traps can be identified by the keyword alarm.

SNMP traps and alarms configuration involves following tasks:

- Configuring SNMP Traps and Alarms Parameters
- Verifying SNMP Traps and Alarms Configuration

Important: For detailed descriptions of SSC traps and alarms, refer to *Cisco ASR 5000 Series SNMP MIB Reference*. For alarms related to other software or hardware components of the solution such as CRM/OSS/BSS or IBM Blade Center HT chassis or Cisco UCS C210M1, refer to respective documentation.

Configuring SNMP Traps and Alarms Parameters

This section describes how to configure SNMP traps and alarms.

Configuring SNMP Traps and Alarms

This section describes the procedure to configure SNMP traps and alarms.

To set SNMP traps and alarms parameters:

Step 1 Login with SSC administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **e** to access SNMP configuration options.

Step 5 Press **i** to view existing SNMP configuration.

Step 6 Specify the IP address and Port number of the SNMP sever for which you are configuring alarms.

Verifying SNMP Traps and Alarms Configuration

This section describes how to verify SNMP traps and alarms configuration.

Viewing SNMP Traps and Alarms Configuration

This section describes the procedure to verify SNMP traps and alarms configuration.

To view SNMP traps and alarm configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **e** to access SNMP configuration options.

Step 5 Press **V** to view existing SNMP configuration.

SSC Administration Console displays existing SNMP collection server configuration. Such as Port number and server IP address.

Bulk Statistics Configuration

This section describes the procedures to configure the bulk statistics parameters on SSC node.

Depending upon SSC configuration, system statistics can record the information such as:

- Service level statistics for SSC, IMDB and database services.
- Database layer parameters.
- **Sh** protocol parameters.

- Subscriber Profile Repository (SPR) API parameters.

Bulk statistics records counters, gauges and fixed value strings for various application schema that are associated with SSC, such as:

- **Sh** application.
- Event notification application.
- Profile application.

A counter records incremental data cumulatively and rolls over when the limit value is reached. This limit depends upon the data type of the counter. SSC can perform various calculations and record the historical information in form of peak, average or total counters. A gauge records a single value representation of a single instance. A gauge can be used to track particular events in time.

Bulk statistics parameters are useful indicators of system performance.

SSC can be configured to save this information at periodic intervals. This information can be saved in a local directory or on a remote server using FTP.

Bulk statistics configuration for an SSC instance involves following tasks:

- Configuring Bulk Statistics Parameters
- Enabling Bulk Statistics Collection
- Verifying Bulk Statistics Configuration

Important: Refer to appendices for available event notification, profile and Sh application, bulk statistics schema.

Configuring Bulk Statistics Parameters

This section describes how to configure bulk statistics parameters.

Configuring Bulk Statistics Parameters for SSC Deployment

This section describes the procedure to configure bulk statistics parameters.

To set bulk statistics parameters:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **f** to access statistics configuration options.

Step 5 Press **n** to configure bulk statistics parameters.

Step 6 Provide Sample Interval in minutes.

Important: Sample interval indicates the time in minutes after which the counters are sampled and written to the file.

SSC Administration Console displays a message indicating completion of statistical configuration.

Enabling Bulk Statistics Collection

This section describes how to enable bulk statistics collection on an SSC node.

Enabling Bulk Statistics Collection For SSC Deployment

This section describes the procedure to enable bulk statistics collection on an SSC node. Depending upon your deployment configuration, this option may not be available.

To enable bulk statistics collection:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **f** to access statistics configuration options.

Step 5 Press **r** to enable or disable the bulk statistics configuration depending on available status.

SSC Administration Console displays the following message:

```
The bulk statistics feature is disabled. Do you want to enable it? (y/n)
```

Step 6 Press **y** to start the Bulk statistics collection on SSC node or Press **n** to stop the Bulk statistics collection on SSC node.

Verifying Bulk Statistics Configuration

This section describes how to verify bulk statistics configuration.

Viewing Bulk Statistics Configuration

This section describes the procedure to verify Bulks Statistics collection configuration on SSC node.

To view the bulk statistics configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **f** to access statistics configuration options.

Step 5 Press **V** to view existing configuration for bulk statistics.

SSC Administration Console displays existing bulk statistics configuration parameters such as Sampling interval (in min), FTP interval (in minutes), password, user name, FTP server and the location of the bulk statistics configuration file indicated by the field, Place file at.

Subscriber Profile Repository (SPR) Configuration

This section describers the procedures to access and view the SPR data storage and configure the subscriber identifier in SPR.

SSC uses Subscriber Profile Repository (SPR) data storage along with centralized Policy Charging and Rules Function (PCRF) to implement usage control policies for subscribers. Depending upon your system configuration and services that are being offered, an SPR includes information related to subscriber profile, entitlements and rate plans. SPR can be a standalone database or it can be integrated with exiting subscriber database such as Home Subscriber Server (HSS). An SPR can store information related to subscriber's profile and activity or session state.

SPR can store following profile related information:

- IMSI
- Initial subscriber quality of Service (QoS) profile identifier.
- MSISDN
- Mobile 3GPP QoS as defined in home Location Register (HLR)

SPR can store following activity or state related information:

- Home location
- Current subscriber QoS profile
- Current subscriber class Id
- Service event Id
- Remaining balance
- Usage parameters such as volume or time that are being tracked for this service event.
- Active event queue and usage history

After configuring identifier for the subscriber, the SPR provisioning can accomplished using following methods:

- Bulk loading subscriber profile.
- Using SPR APIs and web services.
- Using XML-RPC interface to communicate with PPT and exchanging parameters such as subscription tires and dynamic profile attributes.

SPR configuration using SSC console involves following tasks:

- Configuring Subscriber Identifier in SPR
- Verifying Subscriber Identifier in SPR

Configuring Subscriber Identifier in SPR

This section describes how to configure subscriber identifier in SPR.

Configuring Identifier For SPR Subscriber

This section describes the procedure to configure subscriber identifier in SPR.

To configure SPR subscriber identifier:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **g** to access SPR configuration option.

Step 5 Press **S** to configure identifier for the SPR subscriber.

Step 6 Specify subscriber identifier, use MSIDN, NAI or IMSI associated with this subscriber as his or her unique identifier.

SSC Administration Console configures the identifier for this subscriber and displays appropriate message.

Verifying Subscriber Identifier in SPR

This section describers how to verify a subscriber identifier in SPR.

Verifying Identifier For SPR Subscriber

This section describes the procedure to verify subscriber identifier in SPR.

To verify SPR subscriber identifier:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **g** to access SPR configuration option.

Step 5 Press **V** to view the identifier for SPR subscriber.

SSC Administration Console displays the identifier associated with this subscriber. The identifier is either MSISDN, NAI or IMSI associated with this subscriber.

Configuration Management

This section describes how to manage SSC system configuration.

Depending upon your access privilege for an SSC node, you can configure:

- Users that can access this deployment with pre-defined privileges.
- Sh, EN, Ud and other interfaces for exchanging data with other applications such as PPT, IPCF and CRM.
- Binding of SSC host machine with various application host machines that need to exchange data with SSC.
- System logs that store values for system parameters.
- SNMP alarms or traps for various system parameters.
- Bulk statistics, counters or thresholds that can be used for administering as well as troubleshooting the SSC node.

Configuration management for an SSC instance involves following tasks:

- Saving Configuration
- Loading Configuration

SSC system configuration is saved in XML format. **Save Configuration** option is used to save or export existing system configuration to an XML format.Whereas **Load Con figuration** option is used to import a system configuration from XML format, by deleting existing system configuration and loading or using new or imported configuration.

Saving Configuration

This section describes how to save system configuration.

Saving SSC System Configuration

This section describes the procedure to save system configuration.

To save configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **i** to access configuration management option.

Step 5 Press **S** to save existing configuration.

Step 6 Specify the filename, along with its relative path from the SSC home directory.

Admin Console saves the configuration in a file at specified location and displays appropriate message.

Loading Configuration

This section describes how to load any available system configuration.

Loading SSC System Configuration

This section describes the procedure to load previously saved system configuration.

To load a saved configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **i** to access configuration management option.

Step 5 Press **L** to load an existing SSC system configuration from the file.

Step 6 Provide SSC configuration file name which you want to load in SSC system from the existing saved configurations in local directory.

SSC Administration Console loads the system configuration described in the file and displays appropriate message.

Profile Controller Configuration

This section describes the procedure to configure the Profile Controller on SSC node.

The profile controller component manages web services using SOAP /XML interfaces that are used to exchange data with external OSS and BSS.

Profile controller configuration contains following tasks:

- Configuring Profile Controller
- Verifying Profile Controller Configuration

Configuring Profile Controller

This section describes how to configure a profile controller on an SSC node.

Configuring Profile Controller For SSC Node

This section describes the procedure to configure a profile controller.

To configure the profile controller:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **j** to access profile controller configuration option.

Step 5 Press **S** to set profile controller configuration.

Step 6 Specify the IP address of the machine that is hosting the profile controller application.

Step 7 Specify the port that is to be used to communicate with profile controller application.

SSC Administration Console configures the profile controller or displays appropriate error message.

Verifying Profile Controller Configuration

This section describes the procedure to verify the Profile Controller configuration on SSC node.

Verifying Profile Controller configuration For SSC Node

This section describes the procedure to verify the configuration of profile controller.

To verify the Profile Controller configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **j** to access profile controller configuration option.

Step 5 Press **V** to view existing profile configuration.

Step 6 SSC Administration Console displays the IP address of the machine hosting the profile controller and the port which can be used to connect to it.

Policy Provisioning Tool (PPT) Configuration

This section describes the procedure to configure the Policy Provisioning Tool (PPT) for SSC deployment.

Policy Provisioning Tool (PPT) is a component of Cisco PCC solution. PPT is a web based client –server application that provides a wizard based interface to configure usage and monitoring policies using various SSC objects such as subscription tires and data plans as well as various IPCF objects such as QoS profile and dynamic rules and PCEF objects such as APN, rules and rule bases. In a PCC deployment PPT may need to communicate with multiple SSC instances. PPT uses XML-RPC protocol for communication with SSC.

PPT application configures subscriber as well as network usage and monitoring policies using following SSC objects:

- Data plans.
- SMS and e-mail notification templates.
- Subscription tires.
- Dynamic profile attributes.

Depending upon your deployment configuration multiple SSC instances may exchange information with a PPT instance or vice versa. PPT configuration for an SSC instance includes following tasks:

- Viewing PPT Configuration
- Configuring PPT Controller (PPTCtrl)
- Adding PPT Peer
- Deleting PPT Peer

Viewing PPT Configuration

This section describes how to view existing PPT configuration.

Viewing PPT Configuration For SSC Node

This section describes the procedure to view existing PPT configuration.

To view PPT configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **k** to access PPT configuration option.

Step 5 Press **V** to view existing configuration.

SSC Administration Console displays authentication information for PPT controller as well as PPT peer machine configuration parameters such as ip address, name, user name and password.

Configuring PPT Controller (PPTCtrl)

The PPT controller component communicates with external Policy Provisioning Tool (PPT) application using XML-RPC as the communication tool.

Configuring PPT Controller For SSC Node

This section describes the procedure to configure a PPT controller for SSC node.

To configure PPT controller:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **k** to access PPT configuration option.

Step 5 Press **P** to configure PPT controller.

Step 6 Specify whether you want to authenticate the PPT instance.

SSC Administration Console configures authentication for PPT controller.

Adding PPT Peer

This section describes how to add a PPT peer.

Adding PPT Peer For SSC Node

This section describes the procedure to add a PPT peer for SSC node.

To add a PPT peer:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **k** to access PPT configuration option.

Step 5 Press **T** to add a PPT peer machine.

Step 6 Specify the name for PPT peer.

Step 7 Specify the user name that can used to access this PPT peer.

Step 8 Specify password to access this machine

Step 9 Specify the client IP address of the PPT peer machine, with which this SSC instance will be communicating.

SSC Administration Console configures PPT client and displays appropriate error message.

Deleting PPT Peer

This section describes how to delete a PPT peer.

Deleting PPT Peer From SSC Deployment

This section describes the procedure to delete a PPT peer from SSC deployment.

To delete a PPT peer:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **1** to access System Administration options.

Step 4 Press **j** to access PPT configuration option.

Step 5 Press **r** to delete an existing PPT peer machine.

Step 6 Specify the name of PPT peer machine with which you want to sever communication from this SSC instance.

SSC Home or Roaming Feature Configuration

This section briefly describes how to view and set the home or roaming configuration for the SSC Node.

A home region can be associated with the subscriber profile. Differentiated billing can be provided to subscribers depending upon their usage of the network services from either home region or while they are roaming outside their configured home region.

Important: For more information, refer Roaming Determination Support feature, from the Features and Functionality section of the Overview chapter.

Setting Home or Roaming Configuration for SSC Node

This section describes the procedure to set home or roaming configuration for the SSC node.

To set home or roaming configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access System Administration options.

Step 4 Press **L** to access SSC configuration option.

Step 5 Press **S** to access current setting for home or roaming feature.

SSC Administration Console displays the current setting of the Home or Roaming feature for this SSC node. You can enable or disable this feature by specifying **y** or **n**.

Viewing Home or Roaming Configuration for SSC Node

This section describes the procedure to view home or roaming configuration for the SSC node.

To view home or roaming configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access System Administration options.

Step 4 Press **L** to access SSC configuration option.

Step 5 Press **V**to view current setting for home or roaming feature.

SSC Administration Console displays the current setting of the Home or Roaming feature for this SSC node.

Important: By default the home or roaming feature is disabled for the SSC node.

Sh Application Configuration

This section describes the procedures to administer the Sh application.

SSC uses **Sp** interface to query data related to service usage and balance as well as to exchange subscriber profile information with IPCF. Sp interface uses a standard **Sh** protocol to exchange the XML data with IPCF.

The Sh protocol:

- Works as an interface between SSC and IPCF.
- Is a diameter based interface.
- Requests subscription information related to IP-CAN transport level policies from the SSC database, based on IMSI or MSISDN.

In an SSC deployment a single **Sp** endpoint can be simultaneously connected to multiple SPR peer servers, for providing load balancing and high availability of profile and usage database. This is achieved by either configuring primary and secondary SPR servers or by using round robin mechanism. Sh application configuration is used for configuring Sh servers and peers for the SSC deployment. This configuration can be used to provide better connection management between the servers and peers. It can also be used to provide load balancing for Sh messages in the deployment. Enhanced SSC architecture supports hierarchal comparison of the SPR attributes. It also provides information about data type and tag attributes.

While administering Sh application you can perform following tasks:

- Sh Server Configuration
- Sh Peer Configuration

Sh Server Configuration

This section describes the configuration of Sh servers.

While configuring Sh server you perform following tasks:

- Configuring Sh Server
- Deleting Sh Server Configuration
- Verifying Sh Server Configuration

Configuring Sh Server

This section describes how to configure an Sh server.

Configuring Sh Server Host Machine

This section describes the procedure to configure an Sh server.

To configure Sh Server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`

Step 3 Press **2** to access Sh App Admin options.

Step 4 Press **b** to access Sh Server Config options.

Step 5 Press **S** to configure the Sh server.

Step 6 Specify the host name of the machine on which you want to configure the Sh server.

Step 7 Specify the realm for the server.

Step 8 Specify the IP address for this host machine.

Step 9 Specify the port that will be used by this server for communicating Sh protocol related messages.
SSC Administration Console configures the servers and displays appropriate message.

Deleting Sh Server Configuration

This section describes how to delete an Sh server configuration.

Deleting Sh Server Configuration Form Host Machine

This section describes the procedure to delete an **Sh** server configuration.

To delete Sh Server Configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access Sh App Admin

Step 4 Press **b** to access Sh Server Config options.

Step 5 Press **S** to configure the Sh server.

Step 6 Press **t** to access the Delete Sh Server option.

Step 7 Press **Y** if you want to delete the Sh server.
SSC Administration Console deletes the Sh server and displays appropriate message.

Caution: Deleting an Sh server deletes all the peers associated with this server.

Verifying Sh Server Configuration

This section describes how to verify the**Sh** sever configuration on SSC node.

Verifying Sh Server Configuration For SSC Instance

This section describes the procedure to verify existing **Sh** server configuration.

To verify Sh Server Configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access Sh Application Administration (Sh App Admin) option.

Step 4 Press **V** to view existing server and peer configuration for Sh application.

SSC Administration Console displays Name, IP address, Port number for Sh server and peers along with its realm indicated by associated .com.

Important: If Sh server is already configured for your deployment, then SSC Administration Console displays the host name of the machine on which this server is configured.

Sh Peer Configuration

This section describes the configuration of Sh peer server.

While configuring Sh peer servers you perform following tasks:

- Adding Sh Peer
- Viewing Sh Peer
- Removing Host Machine From Sh Peer Configuration

Adding Sh Peer

This section describes how to add an Sh peer.

Adding Host Machine to Sh Peer Configuration

This section describes the procedure to add an **Sh** peer.

To add Sh peer Configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access Sh Application Administration (Sh App Admin) option.

Step 4 Press **c** access Sh peer configuration (Sh Peer config) options.

Step 5 Press **P** to add Sh peer machine.

Step 6 Specify the Name, Realm and IP address for the Sh peer.

SSC Administration Console configures the peer and displays appropriate message.

Viewing Sh Peer

This section describes how to view an Sh peer.

Viewing Sh Peer Configuration

This section describes the procedure to view existing **Sh** peer configuration.

To view Sh peer Configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access Sh Application Administration (Sh App Admin) option.

Step 4 Press **c** access Sh peer configuration (Sh Peer config) options.

Step 5 Press **V** to access view peers option.

SSC Administration Console displays Sh peer machines configured for your deployment

Important: If your session has timed out then, you need to log out and again log in to view Sh peer configuration.

Deleting Sh Peer

This section describes how to delete an Sh peer.

Removing Host Machine From Sh Peer Configuration

This section describes the procedure to delete an **Sh** peer.

To delete Sh peer Configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access Sh Application Administration (Sh App Admin) option.

Step 4 Press **c** access Sh peer configuration (Sh Peer config) options.

Step 5 Press **t** to delete an Sh peer.

Step 6 Specify the Name of the Sh peer, that you want to delete.

Step 7 Press **Y** to delete the Sh peer.

SSC Administration Console deletes the peer and displays appropriate message.

Administering User Data Repository (UDR)

This section describes the procedures to administer **Ud** interface.

Subscriber Profile Repository (SPR) stores the subscriber profiles. These profiles are essentially a set of attributes indexed by subscriber identity such as International Mobile Subscriber Identity (IMSI) or Mobile Subscriber ISDN Number (MSISDN). Subscriber profiles can be accessed using various protocols such as Sh, LDAP or SOAP/XML over an Sp interface. If the SPR is implemented using Universal Data Collection (UDC) schema, then User Data Repository (UDR) serves as SPR for such SSC deployments. In such case the profiles are accessed using **Ud** interface.

The Ud interface can be used to:

- Exchange data between SSC and HLR or HSS.
- Facilitate introduction of SSC in an existing deployment.

Ud interface of SSC allows you to introduce SSC in your network and exchange the subscriber profile data with other components of Policy Charging and Control (PCC) solution, such as Customer Relationship Management (CRM), Operation Support System (OSS) or Billing Support System (BSS). This is possible even if these components are storing data in different database formats, provided that the **Ud** capabilities or Light weight Directory Access Protocol (LDAP) is supported by the data stores that are exchanging the data with SSC.

An SSC instance can be configured as:

- **Ud Server**: In this capacity SSC can allow other components of PCC solution to query the profile database. Acting as a server SSC can send the notifications to these component applications when profile data is updated.
- **Ud Client**: In this capacity SSC can query and fetch data from other components of PCC solution.

This section includes following sub- sections:

- Configuring Server
- Configuring Search Query
- Configuring Attribute Map
- Configuring Ud Client
- Configuring Ud Policy
- Configuring Usage Policy
- Configuring UDR Controller
- Configuring Ud Client for CRM
- Configuring an Update Query

Configuring Server

This section describes the procedures to configure UDR server.

SSC can act as an **Ud** server, while exchanging the data with other PCC solution components such as CRM and can allow these components to query as well as modify the subscriber usage and profile data stored in SSC.

UDR server configuration involves following tasks:

- Adding a UDR Server

- Deleting UDR Server
- Viewing UDR Server Configuration

Adding a UDR Server

This section describes the procedure to add an UDR server.

To add UDR server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **a** access UDR server configuration option.

Step 5 Press **S** to add an UDR server to your deployment.

Step 6 Specify UDR server Id, such as ip address or Fully Qualified Domain Name (FQDN).

Important: Server Name or Id should be alphanumeric and less than 32 characters in length.

Step 7 Specify primary IP of the UDR Server.

Step 8 Specify Primary UDR server port.

Step 9 Specify secondary IP of the UDR server.

Step 10 Specify secondary server UDR port.

Step 11 Specify whether you want this server to be **Ud** compliant, by entering y for yes or n for no.

Step 12 Specify the user name for the UDR.

Step 13 Specify password for this UDR server.

Step 14 Specify the UD service url, that is to be used for accessing this server.

SSC Administration Console configures the UDR server and displays appropriate message.

Deleting UDR Server

This section describes the procedure to delete an UDR server.

To delete a UDR server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **a** access UDR server configuration option.

Step 5 Press **t** to delete an existing UDR server.

SSC Administration Console deletes the UDR server and displays appropriate message.

Viewing UDR Server Configuration

This section describes the procedure to view configuration of an existing UDR server.

To view UDR server configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **a** access UDR server configuration option.

Step 5 Press **V** to view configuration of an existing UDR server.

SSC Administration Console displays information such as primary and secondary UDR server Ids, corresponding IP addresses. It also displays whether the given server is **Ud** compliant or not.

Configuring Search Query

This section describers the procedures to configure a UDR search query, when an SSC instance is acting as a UDR client to query and fetch data from other PCC components.

UDR search query configuration involves following tasks:

- Adding UDR Search Query
- Viewing UDR Search Query
- Deleting UDR Search Query

Adding UDR Search Query

This section describes the procedure to add an UDR search query.

To add a UDR search query:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **b** access UDR search query configuration option.

Step 5 Press **S** to add a new search query for the UDR server.

Step 6 Specify the search query Id.

Important: Name or id of the search query should be alphanumeric and less than 32 characters in length.

Step 7 Specify Base Domain Name (DN) for this query. The query will be executed on this domain only.

Step 8 Specify the search filter. This is the search criteria.

Step 9 Specify the output parameters for this query.

Step 10 Specify whether you want to execute this query or not.

Step 11 Specify the server Id of the UDR server, on which to execute this query.

SSC Administration Console configures the UDR search query and displays appropriate message.

Viewing UDR Search Query

This section describes the procedure to view an existing UDR search query.

To view UDR search query:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **b** access UDR search query configuration option.

Step 5 Press **e** to view an existing search query.

SSC Administration Console displays the list of all existing search queries. For each search query it displays query id, search filter, associated server id, whether this query is to be executed or not and what are the query output parameters.

Deleting UDR Search Query

This section describes the procedure to delete an existing UDR search query.

To delete a UDR search query:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **b** access UDR search query configuration option.

Step 5 Press **t** to delete an existing search query from the UDR server.

SSC Administration Console deletes the search query and displays appropriate message.

Configuring Attribute Map

This section describers the procedures to configure an attribute map Between User Data Repository (UDR) and SSC schema.

An attribute map defines the relationship between attribute types in hierarchical LDAP schema and corresponding columns in the tables of a relational database schema. The map also contains rules that define the procedures for copying or transforming an attribute while exchanging the information between two different data sets.

Attribute map configuration involves following tasks:

- Adding UDR-SSC Attribute Map
- Viewing UDR-SSC Attribute Configuration
- Deleting UDR-SSC Attribute Map

Adding UDR-SSC Attribute Map

This section describes the procedure to add an UDR- SSC attribute map.

To add UDR-SSC attribute map:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **c** to access UDR attribute map configuration option.

Step 5 Press **S** to add a new attribute map for UDR-SSC.

Step 6 Specify attribute Id, that you want to map with a column in a relational database schema table.

Step 7 Specify the LDAP attribute that you want to map with an SSC attribute.

Step 8 Specify the SSC attribute that you want to map with an LDAP attribute.

Step 9 Specify table name that maps LDAP and SSC attributes for the UDR.

SSC Administration Console adds the **Ud** attribute map and displays appropriate message.

Viewing UDR-SSC Attribute Configuration

This section describes the procedure to view existing UDR -SSC attribute configuration.

To view attribute configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **c** to access UDR attribute map configuration option.

Step 5 Press **V** to view existing attribute maps. These maps display relationship between LDAP and SSC attributes.

SSC Administration Console displays UDR attribute id along with LDAP and SSC UDR attributes and the name of SSC table where these attributes are mapped.

Deleting UDR-SSC Attribute Map

This section describes the procedure to delete an existing UDR-SSC attribute map.

To delete UDR-SSC attribute map:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **c** to access UDR attribute map configuration option.

Step 5 Press **t** to delete an entry from UDR-SSC attribute map.

Step 6 Specify id of the attribute that you want to remove from the LDAP-UDR attribute map.

Step 7 Confirm that you want to delete this attribute configuration.

SSC Administration Console deletes the mapping for UDR-LDAP attribute map from the table and displays appropriate message.

Configuring Ud Client

This section describers the procedures to configure an UDR client.

SSC can also act as an **Ud** client or a front end application for the User Data Repository (UDR) and support multiple target databases. It can read data from LDAP or 3GPP R9 compliant **Ud** databases.

UDR client configuration involves following tasks:

- Viewing UDR Client Configuration
- Setting UDR Client Configuration

Viewing UDR Client Configuration

This section describes the procedure to view the configuration of a UDR client.

To view UDR client configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **d** to access UDR client configuration option.

Step 5 Press **V** to view configuration of all existing UDR clients.

SSC Administration Console displays the front-end Id and the service name for all the UD clients configured for your system.

Setting UDR Client Configuration

This section describes the procedure to set the configuration of a UDR client.

To set UDR client configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **d** to access UDR client configuration option.

Step 5 Press **C** to configure UDR client.

Step 6 Specify the front-end id. This indicates the front end which you want to set SSC front end.

Step 7 Specify the service name or subscription, whose information will be exchanged with SSC using this front end.

SSC Administration Console configures new **Ud** client and displays appropriate message.

Configuring Ud Policy

This section describes the procedures to configure **Ud** polices.

Ud policies are used by the Sh Manager component of SSC to send a message to LDAP interface manager component that fetches the profile from SSC's LDAP interface.

Following pre-defined **Ud** policies are available:

1. **Fetch always**: This policy will always fetch the user profile, irrespective of its availability in the destination database.
2. **Fetch if absent**: This policy will fetch the user profile if it is not available in the destination database.

UDR policy configuration involves following tasks:

- Viewing UDR Policy
- Setting UDR Policy

Viewing UDR Policy

This section describes the procedure to view an existing UDR policy.

To view UDR policy:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **e** to access Ud policy configuration option.

Step 5 Press **p** to view existing UDR policies.

Setting UDR Policy

This section describes the procedure to set a UDR policy.

To set UDR policy:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **e** to access Ud policy configuration option.

Step 5 Press **Y** to set UDR policy.

Step 6 Specify the number, to indicate the policy that you want to set. For example select **1** to specify fetch always or **2** specify fetch if absent as a UDR policy.

SSC Administration Console configures the **Ud** policy and displays appropriate message.

Configuring Usage Policy

This section describes the procedures to configure policy for exchanging service usage data with UDR.

SSC can receive the service usage related data from User Data Repository (UDR) servers. You can configure a policy either to update the service usage data in SSC from UDR server or to ignore such data from the UDR server.

Usage policy configuration involves following tasks:

- Viewing Usage Policy
- Setting Usage Policy

Viewing Usage Policy

This section describes the procedure to view usage policy.

To view usage policy:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **f** to access usage policy configuration option.

Step 5 Press **P** to view existing usage policies for receiving the usage data from User Data Repository (UDR) to SSC.

SSC Administration Console displays the configured usage data exchange policy between SSC and UDR.

Setting Usage Policy

This section describes the procedure to set usage policy.

To set usage policy:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **f** to access usage policy configuration option.

Step 5 Press **Y** to configure policy for updating usage data from UDR.

Step 6 Specify the usage policy number. Select **1**to receive updated usage data from UDR or select **2**if you do not want SSC to receive current usage data from the UDR server.

SSC Administration Console configures usage policy for UDR data and displays appropriate message.

Configuring UDR Controller

This section describes the procedures to configure UDR controller.

Some CRM deployments communicate with other PCC components using LDAP or Ud interface. SSC can communicate with such deployments by acting as a UDR controller for them. It allows CRM to query or modify the subscriber profile and usage data stored in the SSC data base. By acting as UDR controller, SSC also allows CRM component to register for change notifications from SSC.

UDR controller configuration involves following tasks:

- Viewing UDR Controller Configuration
- Setting UDR Controller Configuration

Viewing UDR Controller Configuration

This section describes the procedure to view configuration of an existing UDR controller.

To view UDR controller configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **g** to access UDR controller configuration option.

Step 5 Press **V** to view configuration of an existing UDR controller.

SSC Administration Console displays UDR controller parameters such as, Base DN, password, IP address, Port number and User Name.

Setting UDR Controller Configuration

This section describes the procedure to set configuration of a UDR controller.

To set UDR controller configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **g** to access UDR controller configuration option.

Step 5 Press **C** to set the controller configuration.

Step 6 Specify IP address for UDR controller.

Step 7 Specify the port number which will be used by this UDR controller for communication.

Step 8 Specify the Base DN for this controller.

Step 9 Specify the user name which will be used to access this controller.

Step 10 Specify the password required to access this controller.

SSC Administration Console configures the controller with parameters and displays appropriate message.

Configuring Ud Client for CRM

This section describes the procedures to configure a **Ud** client to exchange data with Customer Relationship Management (CRM) application.

Configuring **Ud** client for CRM, involves following tasks:

- Configuring Ud Client for CRM
- Viewing Ud Client Configuration

Configuring Ud Client for CRM

This section describes the procedure to configure a Ud client for CRM.

To configure UD client for CRM:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **i** to configure a **Ud** client for CRM.

Step 5 Press **C** to access the configuration option for this client.

Step 6 Specify Id for the front end for this CRM client.

Step 7 Specify the URL which is required to access this front end.

Step 8 Specify the port number that will be used for communicating with this front end of CRM client.

SSC Administration Console configures the **Ud** client and displays appropriate message.

Viewing Ud Client Configuration

This section describes the procedure to view configuration of a Ud client.

To view Ud client configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **i** to configure a **Ud** client for CRM.

Step 5 Press **V** to view existing configuration for CRM Ud client.

SSC Administration Console displays Id for the front end and the URL that is to be used to access this CRM client, along with the port number that is to be used for communicating with this client.

Configuring an Update Query

This section describers the procedures to configure an update query for a UDR server.

Update query configuration involves following tasks:

- Adding Update Query
- Viewing Update Query
- Deleting Update Query

Adding Update Query

This section describes the procedure to add an update query.

To add an update query:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **j** to access update query configuration option.

Step 5 Press **U** to add a new update query for the UDR server.

Step 6 Specify the update query Id.

Step 7 Specify Base Domain Name (DN) for this query. The query will be executed on this domain only.

Step 8 Specify the search filter. This is the search criteria.

Step 9 Specify the output parameters for this query.

Step 10 Specify whether you want to execute this query or not.

Step 11 Specify the server Id of the UDR server, on which to execute this query.

SSC Administration Console configures the update query and displays appropriate message.

Viewing Update Query

This section describes the procedure to view an existing update query.

To view an update query:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **j** to access update query configuration option.

Step 5 Press **p** to access view update query option.

SSC Administration Console displays a list of all the configured update queries. For each query it displays all the configuration parameters explained in the previous section.

Deleting Update Query

This section describes the procedure to delete an existing update query.

To delete an update query:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access UDR Administration option.

Step 4 Press **j** to access update query configuration option.

Step 5 Press **r** to delete an existing update query for the UDR server.

Step 6 Specify the id of an update query that you want to delete.

SSC Administration Console deletes the update query, and displays appropriate message.

Administering Event Notification Application

This section describes the procedures to administer an event notification application.

Event notifications are used to generate and send the notifications to subscribers. These notifications are mostly related to subscribers service usage and policy changes that may affect the subscriber.

This section includes following sub-sections:

- Configuring Event Notification Server
- Configuring SMTP Server
- Configuring SMPP Server
- Configuring E-mail Layout
- Configuring Interface Monitor

Configuring Event Notification Server

This section describers the procedures to configure an event notification server.

Event notification server is used by SSC to communicate with other components of PCC solutions such as IPCF that want to use the event notification functionality provided by SSC. Notification server can also be used to handle load balancing among SMTP and SMPP servers used by the event notification module.

Event notification server configuration involves following tasks:

- Configuring Event Notification Server Instance
- Viewing Event Notification Server Instance

Configuring Event Notification Server Instance

This section describes the procedure to configure an event notification server instance.

To configure an event notification server instance:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **a** to access event notification server configuration option.

Step 5 Press **S** to configure an event notification server.

Step 6 Specify server IP address.

Step 7 Specify server port to communicate with this server.

SSC Administration Console displays the IP address and port for all configured event notification servers.

Viewing Event Notification Server Instance

This section describes the procedure to view an event notification server instance.

To view an event notification server instance:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **a** to access event notification server configuration option.

Step 5 Press **V** to view existing server configuration.

SSC Administration Console displays the IP address and port for all configured event notification servers.

Configuring SMTP Server

This section describes the procedures to configure an SMTP server.

Simple Mail Transfer Protocol (SMTP) is a standard used by Internet Protocol (IP) networks to transmit e-mails. SMTP is used by mail servers and Mail Transfer Agents (MTAs) to send or receive mails. Mail client applications use SMTP to send messages to servers. SSC allows you to configure SMTP servers that can be used to send event notification related messages as e-mails.

SMTP server configuration involves following tasks:

- Configuring Primary SMTP Server
- Configuring Secondary SMTP Server
- Viewing SMTP Server Configuration

Configuring Primary SMTP Server

This section describes the procedure to configure primary SMTP server.

To configure primary SMTP server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **b** to access SMTP server configuration option.

Step 5 Press **P** to configure primary SMTP server.

Step 6 Specify the server IP address.

Step 7 Specify the port used to communicate with this server.

Step 8 Specify the e-mail throttle rate. This indicates maximum number of e-mails that can be sent per second.

SSC Administration Console configures the server or displays appropriate error message.

Configuring Secondary SMTP Server

This section describes the procedure to configure secondary SMTP server.

To configure secondary SMTP server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **b** to access SMTP server configuration option.

Step 5 Press **S** to configure secondary SMTP server.

Step 6 Specify IP address of the machine that is hosting secondary SMTP server.

Step 7 Specify the port used to communicate with this server.

Step 8 Specify e-mail throttle rate. This rate indicates maximum number of e-mails that can be sent per second.

SSC Administration Console configures the secondary SMTP server or displays appropriate error message.

Viewing SMTP Server Configuration

This section describes the procedure to view configuration of existing SMTP servers.

To view SMTP server configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **b** to access SMTP server configuration option.

Step 5 Press **V** to view existing SMTP server configuration.

SSC Administration Console displays IP address, port that is to be used for communication with this server, and e-mail throttle rate for all the configured primary as well as secondary SMTP servers.

Configuring SMPP Server

This section describes the procedures to configure an SMPP server.

Short Message Peer to Peer (SMPP) protocol is used for exchanging SMS messages between Short Message Service Centers (SMSCs) and external short messaging entities. SSC allows you to configure SMPP servers that can be used to send event notifications and related messages as an SMS.

Type Of Numbering (TON) and Numbering Plan Indicator (NPI) are mandatory for supporting connection with SMPP server. Different combinations of TON and NPI values are supported while sending SMS to SMSC using SMPP interface. SMPP server configuration can be used to configure both source as well as destination TON and NPI values.

SMPP server configuration involves following tasks:

- Configuring Primary SMPP Server
- Configuring Secondary SMPP Server
- Viewing SMPP Server Configuration

Configuring Primary SMPP Server

This section describes the procedure to configure primary SMPP server.

To configure primary SMPP server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **c** to access SMPP server configuration option.

Step 5 Press **P** to configure primary SMPP server.

Step 6 Specify client system Id. This indicates unique identification number of client system or subscriber system. This is supplied by SMPP provider.

Step 7 Specify password to access the machine hosting SMPP server.

Step 8 Specify system type. This indicates the category of client (or subscriber) system. Maximum 8 characters are allowed to indicate the system type.

System type is always SMPP for an SMPP server.

Step 9 Specify the service type. This indicates the category of service being used by the subscribers receiving this notification. Maximum 8 characters are allowed to indicate the service type.

Service type is the event, regarding which the notification is being sent thru SMS.

Step 10 Specify the IP address or FQDN of the SMPP primary server. This indicates the IP address or Fully Qualified domain Name (FQDN) of the machine that is hosting the SMPP server.

Step 11 Specify server port. This indicates the port number that is to be used for communicating with the machine that is hosting SMPP server.

Step 12 Specify source address. This indicates IP address of the SMPP server.

Step 13 Specify server response time in seconds. This indicates the time by which the machine hosting the event notification server should acknowledge or drop the event request.

Step 14 Specify enquire link time in seconds. This indicates time by which the link is accessible.

Step 15 Specify event throttle rate. This rate indicates maximum number of SMSs that can be sent per second.

SSC Administration Console configures primary SMPP server or displays appropriate error message.

Configuring Secondary SMPP Server

This section describes the procedure to configure secondary SMPP server.

To configure secondary SMPP server:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **c** to access SMPP server configuration option.

Step 5 Press **S** to configure secondary SMPP server.

SSC Administration Console configures parameters for secondary SMPP server, as per step 6 to step 15 of previous section – Configuring primary SMPP server.

Viewing SMPP Server Configuration

This section describes the procedure to view configuration of SMPP servers.

To view SMPP server configuration:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **c** to access SMPP server configuration option.

Step 5 Press **V** to view existing SMPP server configuration.

SSC Administration Console displays configured values of SMPP server parameters, mentioned in sections configuring primary and secondary SMPP servers.

Important: This information is displayed for all configured SMPP servers i.e. for primary as well as secondary servers.

Configuring E-mail Layout

This section describes the procedures to configure an e-mail layout.

E-mail layout configuration involves following tasks:

- Configuring E-mail Parameters
- Viewing E-mail Parameters

Configuring E-mail Parameters

This section describes the procedure to configure e-mail parameters.

To configure e-mail parameters:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **d** to access e-mail parameters configuration option.

Step 5 Press **P** to configure e-mail parameters.

Step 6 Specify e-mail footer.

Step 7 Specify e-mail header.

Step 8 Specify sender's e-mail address.

SSC Administration Console configures e-mail parameters or displays appropriate error message.

Viewing E-mail Parameters

This section describes the procedure to view mail parameters.

To view e-mail parameters:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **d** to access mail parameters configuration option.

Step 5 Press **V** to view existing e-mail parameters.

SSC Administration Console displays the header, footer and sender's e-mail address that will be used for sending the event notification thru e-mail

Configuring Interface Monitor

This section describers the procedures to configure and view interface parameters for event notification interface.

SSC allows you to configure and view the retry count and retry interval for event notification interface.

Interface monitor configuration involves following tasks:

- Configuring Retry Parameters for Event Notification (EN) Interface
- Viewing Retry Parameters for Event Notification (EN) Interface

Configuring Retry Parameters for Event Notification (EN) Interface

This section describes the procedure to configure retry parameters for an EN interface.

To configure retry parameters for an EN interface:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **e** to access interface monitor configuration option.

Step 5 Press **C** to configure the retry parameters for EN interface.

Step 6 Specify interface retry count.

Step 7 Specify interface retry interval.

SSC Administration Console configures interface monitoring parameters.

Viewing Retry Parameters for Event Notification (EN) Interface

This section describes the procedure to view retry parameters, configured for an EN interface.

To view an event notification server instance:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **4** to access Event notification Application Administration (EventAppAdmin) options.

Step 4 Press **e** to access interface monitor configuration option.

Step 5 Press **V** to view existing retry parameters for the EN interface.

SSC Administration Console displays interface retry count and interface retry interval configured for the EN interface.

Monitoring SSC Performance Using Console

This section describes the procedures to use the SSC Administration Console, to monitor the performance of SSC system.

This section includes following sub-sections:

- Monitoring System Log
- Monitoring System Statistics
- Monitoring Resources
- Monitoring Threshold Policies

Monitoring System Log

This section describes the procedures to monitor the system logs.

SSC node, logs certain system parameters periodically. System logs record information about the web servers used in the deployment along with session and system information. These logs can be used for troubleshooting issues related to both system hardware and related operating system software used by the SSC node.

Depending upon the deployment configuration, these logs can be:

- stored locally in files on the SSC host machines.
- using system **syslog**, these logs can be stored on some external server.

Important: System logs are different from event logs. Refer *SSC Logs Administration*, for more information on event logs.

System logs are categorized as:

- System Log
- Session Log
- Web Server Log.

The web server logs are further categorized as:

- **Web server error logs**: These contain the errors encountered while accessing the web server. These are stored in error.log file in `../localhome/ssc /3rdparty/apapche/logs` directory.
- **Web server access logs**: These contain access details for the web server. These are stored in access.log file in `../localhome/ssc/3rdparty/apache/logs` directory.
- **AXIS framework log**: These contain SSC framework related information. These are stored in libaxis.log file in `../localhome/ssc/3rdparty/axis/modules/logging` directory.

System logs monitoring involves following tasks:

- Accessing System Log
- Accessing Session Log
- Accessing Web Server Log

Accessing System Log

This section describes the procedure to access system logs.

To access system log:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **a** to access system log option.

Step 5 Press **S** to view system logs.

SSC Administration Console displays the locations where system process logs as well as system start-up and internal log files are created.

Important: The file `sn-SSC.log` contains system process logs and the file `startup.log` contains system start-up and internal logs.

Accessing Session Log

This section describes the procedure to access session log.

To access session log:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **n** to access session log option.

SSC administration Console displays location of the session log file.

Important: The file `session_`*`xxxxx`*`.log` contains the session log, where *`xxxxxx`* is concatenation of the date on which the logs are generated and a system generated number. For example a file `session_2010122117346.log` stores the session logs for 21st December 2010.

Accessing Web Server Log

This section describes the procedure to access web server log.

To access web server log:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **w** to access web server log option.

SSC administration Console displays location of the web server log files.

Monitoring System Statistics

This section describes the procedures to monitor the system statistics.

SSC node stores certain system parameters at periodic time interval. These parameters can be used to monitor the system performance as well as for troubleshooting purpose.

Depending upon your access privilege following system statistics views are available:

- **Summary View**: This view generates a summary of important statistical parameters.
- **By Process View**: The SSC node spawns different processes such as SysMgr, AppMgr, EnCtrl and ShCtrl for the installed SSC components. This view displays the statistical parameters related to the selected process.
- **Refresh View**: This view updates the statistical information on the UI with latest available values for the selected parameters.
- **Clear Stats View**: This view clears the displayed values of bulk statistics parameters.

Monitoring system statistics involves following tasks:

- Viewing System Statistics by Summary
- Viewing System Statistics by Process
- Clearing System Statistics View
- Refreshing System Statistics View

Viewing System Statistics by Summary

This section describes the procedure to view system statistics summary.

To access system statistics by summary:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **b** to access system statistics option.

Step 5 Press **s** to access the summary view.

SSC Administration Console displays a summary of system statistics. It displays current values of important statistical parameters related to different SSC processes such as Sh and event notification applications, UDR controller, that are active for this SSC instance.

Viewing System Statistics by Process

This section describes the procedure to view system statistics associated with various SSC processes.

To access system statistics by process:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **b** to access system statistics option.

Step 5 Press **P** to access system statistics related to specific processes.
SSC Administration Console displays active processes associated with this instance of SSC.

Step 6 Specify the number associated with process, whose statistics you want to view.

Step 7 enter N if you want to view IPC statistics, V for verbose display or B for basic display.

Step 8 Specify the instance, whose statistical parameters you want to view.
SSC Administration Console displays available data or appropriate error message.

Clearing System Statistics View

This section describes the procedure to clear the displayed statistics.

To clear system statistics view:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **b** to access system statistics option.

Step 5 Press **t** to clear the displayed statistics.
SSC Administration Console displays active process related to this SSC instance.

Step 6 Specify the process for which you want to clear the bulk statistics.
SSC Administration Console clears the statistics related to this process.

Refreshing System Statistics View

This section describes the procedure to refresh the displayed statistics.

To refresh system statistics view:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **b** to access system statistics option.

Step 5 Press **R** to refresh existing view.

SSC Administration Console displays updated values for the bulk statistics.

Important: The refresh view option will work only when you have selected summary or by process view options.

Monitoring System Resources

This section describes the procedures to monitor the system resources using thresholds.

Threshold is a concept used to monitor a system, such as SSC, for conditions that could potentially introduce errors or cause outage. In most cases these conditions are temporary, such as high CPU utilization or inconsistency in the processes associated with scheduler or heart beat daemon and are resolved quickly.

However continuous occurring of such conditions in large number and during specific time interval may indicate larger issues.

Thresholds help to identify such conditions and allow administrators to take preventive actions.

Depending upon the system configuration following threshold models are supported:

- **Alert**: A resource is monitored and alert condition occurs when value associated with this resource reaches or exceeds the configured high threshold within specified polling interval. An alert is then generated and sent at the end of polling interval.
- **Alarm**: For a resource, both high and low thresholds are defined, alarm condition occurs when resource value reaches or exceeds high threshold value, in such case alarm is generated and sent at end of polling interval. This alarm is cleared if during the next polling interval the resource value equals or falls below the low threshold value.

Thresholds can be used for system administration as well as troubleshooting purpose.You can configure threshold percentage for certain system resources such as processes associated with CPU usage, logging or scheduling.

As per the deployment configuration and your access privileges, you can view or configure the thresholds associated with following:

- System resources.
- System processes.
- Applications.

As per your deployment system resources can be further categorized as:

- CPU
- SWAP

As per your deployment, active SSC processes associated with this SSC instance can be categorized as:

- Heart Beat Daemon (HbD)
- Log Daemon (LogD)
- System Manager (SysMgr)
- Scheduler
- Sh Controller (ShCtrl)
- Application Manager (AppMgr)
- Event Notification Controller (EnCtrl)

- Profile Controller (ProCtrl)
- UDR Manager(UdrMgr)

As per your deployment the applications associated with this SSC instance can be categorized as:

- Maximum active Sh sessions.
- Maximum input queue size for application manager per blade.
- Maximum input queue size for application manager across the system.

System resource monitoring involves following tasks:

- Viewing Thresholds
- Configuring Thresholds
- Viewing System Status

Viewing Thresholds

This section describes the procedure to view thresholds.

To view thresholds:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **C** to access resource monitor option.

Step 5 Press **V** to view existing thresholds.

SSC Administration Console displays thresholds in percentage for processes associated with configured resources.

Configuring Thresholds

This section describes the procedure to configure thresholds.

To configure thresholds:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **C** to access resource monitor option.

Step 5 Press **C** to configure thresholds.

Step 6 Specify thresholds in percentage for process associated with configured resources.

Important: The SSC installation process, sets the default threshold values for resources while configuring the data base.

Viewing System Status

This section describes the procedure to view system status.

To view system status:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **C** to access resource monitor option.

Step 5 Press **S** to view system status.

SSC administration Console displays the system status. it displays percentage of active processes associated with the host name.

Important: System status includes information such as active processes and Sh sessions associated with the host (or blade) name. This includes processes such as Logd. SysMgr, ShCtrl as well as processes associated with CPU and swap. The status also displays items in input queue for the AppMgr process.

Monitoring Threshold Policies

This section describes the procedures to monitor threshold policies.

Threshold policies can be used for monitoring the service usage of the subscribers. You can also use policies for administering some parameters of SSC.

Monitoring threshold policies involves following tasks:

- Viewing Threshold Policies
- Configuring Threshold Policies

Viewing Threshold Policies

This section describes the procedure to view threshold policies.

To view threshold policies:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **d** to access threshold policy option.

Step 5 Press **V** to view existing threshold policies.

SSC administration Console displays a list of configured threshold policies.

Important: Depending upon services that are being offered and your threshold configuration strategy, threshold policies can be categorized as, threshold breach policies or maximum active Sh session breach policies.

Configuring Threshold Policies

This section describes the procedure to configure threshold policies.

To configure threshold policies:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access performance options.

Step 4 Press **C** to access resource monitor option.

Step 5 Press **P** to configure a threshold policy.

Step 6 Specify whether you want to reject the new session when the threshold is breached.

SSC Administration Console configures the threshold breach policy and displays appropriate message.

Administering Profile

This section describes the procedures to administer the subscriber profile.

Important: The profile administration option is available only when you log in to SSC Administration Console as policy administrator or as a user whose credentials include the policy administration credentials. If you have logged in using default policy administrator credentials then profile administration option can be accessed by pressing **1** otherwise it can be accessed by pressing **6** or associated option number. For more information refer *User Administration* section.

Each subscriber account is identified by its unique International Mobile Subscriber Identity (IMSI) or Mobile Subscriber ISDN Number (MSISDN). A subscriber profile links plans and subscription tires to an account. Thus a subscriber profile facilitates service customization for a specific subscriber account.

A subscriber profile identifies various usage, data or service plans and add-on, associated with a subscriber, along with privileges and entitlements that can be availed by the profile holder.

Depending upon the services that are being provided, a subscriber profile may have following attributes:

- Mobile Subscriber ISDN Number (MSISDN).
- International Mobile Subscriber Identity (IMSI).
- Enable e-mail flag.
- Enable SMS flag.
- Subscription Status.
- Flag Name.
- Flag value.
- Billing start date.

Important: Attributes of the subscriber profile can also be provisioned using SPR APIs such as *createSubscriber*, *updateSubscriber* and *deleteSubscriber*. Refer *Cisco SPR Provisioning Guide* for more information.

Important: SSC provides a facility to bulk load the subscriber profile data, refer *Bulk Load Provisioning* feature in *Overview* chapter and the procedure to bulk load the subscriber profile in *Before You Begin* section of *SSC Administration* chapter.

Profile administration includes tasks related to provisioning of subscriber profiles as well as plans. Provisioning tasks can be categorized as:

- Creating new subscriber profiles or plans.
- Associating plans with subscriber profile.
- Modifying existing subscriber profiles.
- Modifying plans for top-up facility.
- Viewing individual subscriber profile or plan.
- View all configured subscriber profiles or plans.

This section includes following sub-sections:

- Viewing Subscriber Profile and Usage
- Administering Subscriber Profile

Viewing Subscriber Profile and Usage

This section describes the procedures to view subscriber's profile and service usage.

Viewing subscriber profile and associated usage of services involves following tasks:

- Viewing Existing Subscriber Profile
- Viewing Service Usage

Viewing Existing Subscriber Profile

This section describes the procedure to view existing subscriber profile.

To view existing profile:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **a** to access view profile option.

Step 5 Specify International Mobile Subscriber Identity (IMSI) or Mobile Subscriber ISDN Number (MSISDN) or NAI associated with the subscriber whose profile you want to view.

SSC Administration Console displays the subscriber record.

Viewing Service Usage

This section describes the procedure to view existing usage of a subscriber profile.

To view usage:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **b** to access view usage option.

Step 5 Specify International Mobile Subscriber Identity (IMSI) or Mobile Subscriber ISDN Number (MSISDN) or NAI associated with the subscriber, whose usage you want to view.

Step 6 Specify do you want to view usage for a specific data plan.

Step 7 Provide the plan id, if you have answered as yes in the previous step.

Step 8 Specify plan name, if you have answered as yes in step 6.

SSC Administration Console displays the subscriber usage or appropriate error message.

Administering Subscriber Profile

This section describes the procedures to administer a subscriber profile.

Subscriber profile administration involves following tasks:

- Adding Subscriber Profile
- Deleting Subscriber Profile
- Modifying Subscriber Profile

Important: Enhanced SSC architecture supports multiple values for subscriber profile attributes. If a given attribute such as **description** supports multiple values, then while maintaining the subscriber profile, SSC Administration Console keeps on displaying this field till you enter a blank for it.

Adding Subscriber Profile

This section describes the procedure to add a subscriber profile.

To add a subscriber profile:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **b** to access add subscriber option.

Step 5 SSC Administration Console displays a message for providing subscriber credentials.

Important: For steps 6 to 8, press enter key if you do not want to change the existing value.

Step 6 Specify either IMSI, MSISDN or NAI as an id for this subscriber.

Step 7 Specify subscriber name and description.

Step 8 Specify Billing Date in format DD/MM/YYYY.

Step 9 Specify subscription tire.

Step 10 Specify whether you want to send SMS notifications to this subscriber.

Step 11 Specify e-mail address for sending the notifications through mail.

Step 12 Specify whether you want to give profile attribute to this subscriber.

SSC Administration Console communicates this information to the back-end database and displays appropriate message.

Deleting Subscriber Profile

This section describes the procedure to delete a subscriber profile.

To delete a subscriber profile:

Step 6 Login to the SSC node with administrative privileges.

Step 7 Access the SSC Administration Console by executing the script `./sscadm`.

Step 8 Press **1** to access profile administration option.

Step 9 Press **c** to access delete subscriber option.

Step 10 Specify either IMSI, MSISDN or NAI as an id for this subscriber whose record you want to delete from the database.

SSC Administration Console deletes the record and displays appropriate message. Or it displays an error message indicating that such record is not available.

Modifying Subscriber Profile

This section describes the procedure to modify a subscriber profile.

To modify a subscriber profile:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **d** to access modify subscriber option.

Step 5 Specify either IMSI, MSISDN or NAI as an id for this subscriber, whose record you want to modify in the database.

Important: For steps 6 to 8, press enter key if you do not want to change the existing value.

Step 6 Specify subscriber name and description.

Step 7 Specify Billing Date in format DD/MM/YYYY.

Step 8 Specify subscription tire.

Step 9 Specify whether you want to send SMS notifications to this subscriber.

Step 10 Specify e-mail address for sending the notifications through mail.

Step 11 Specify whether you want to give profile attribute to this subscriber.

SSC Administration Console communicates this information to the back-end database and displays appropriate message.

Administering Plans

This section describes the procedures to administer service and data plans for the subscriber.

Administering service and data plans for a subscriber profile involves following tasks:

- Associating Plan
- Toping -up Quota
- Updating Plan
- Resetting Usage
- Recharging Plan
- Disassociating Plan

Associating Plan

This section describes the procedure to associate a usage or data plan with the subscriber profile.

To associate a plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **f** to access associate plan option.

Step 5 Specify subscriber profile details.

Step 6 Specify details for the data plan such as Plan Name, Subscription order, start date and end date in the format DD/MM/YYYY.

Step 7 Specify whether you want to generate the notifications for this subscriber.

Step 8 Specify whether you want to associate more plans for this subscriber.

Step 9 If you have selected **y** in the previous step, then continue to provide the details for additional data plans.

SSC Administration Console associates the specified data plans with this subscriber. If such plans are not available in the database, then it displays appropriate error message.

Important: While specifying subscriber profile details, you can use either IMSI/MSIDN or NAI of this subscriber as well as its subscriber id.

Toping -up Quota

This section describes the procedure to update the usage limit or to top-up the quota for subscriber.

To top-up quota:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **g** to access top-up quota option.

Step 5 Specify subscriber profile details. While specifying subscriber profile details, you can use either IMSI/MSIDN or NAI of this subscriber as well as its subscriber id.

Step 6 If you are specifying the top-up quota for a data plan, then specify plan name or plan Id.

Step 7 If you are specifying the top-up quota for the service plan, then specify plan name along with parent plan name or plan Id.

Step 8 Specify volume quota in bytes.

Step 9 Specify time quota in seconds.

SSC Administration Console updates the values in the data base and displays appropriate message.

Updating Plan

This section describes the procedure to update a usage or data plan.

To update plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **i** to access update plan option.

Step 5 Specify subscriber credentials. You can use either IMSI/MSIDN or NAI of this subscriber as well as its subscriber id, for specifying the credentials. SSC Administration Console will update the subscription details for this subscriber.

Step 6 Specify plan name.

Step 7 Specify subscription order.

Step 8 Specify start date.

Step 9 Specify end date.

Step 10 Specify the subscription status details such as **1**- disabled, **2** – Forever, **3**- Enabled, **4**- For current billing cycle. You can specify the required status by entering associated number.

Step 11 Specify whether you want to generate the notification.

Step 12 Specify whether you want to update more plans. If you select **yes**, then provide the information.

SSC Administration Console updates the plan in the database.

Resetting Usage

This section describes the procedure to re-set a subscriber's service usage.

To re-set usage:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **j** to access reset usage option.

Step 5 Specify the subscriber profile key such as subscriber id, of the subscriber whose usage you want to reset

Step 6 Specify the id or name of the plan that you want to reset.

> ***Important:*** For re-setting a service plan you need to specify the id of the parent plan as well.

Step 7 SSC Administration Console re-sets the subscriber usage that is associated with the selected service plan or displays appropriate error message.

Recharging Plan

This section describes the procedure to re-charge a data or service plan associated with the subscriber.

To re-charge plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **k** to access recharge plan option.

Step 5 Specify the subscriber profile key such as subscriber id, of the subscriber whose plan you want to recharge.

Step 6 Specify the id or name of the plan that you want to recharge.

> ***Important:*** For re-charging a service plan you need to specify the id of the parent plan as well.

Step 7 SSC Administration Console recharges the selected plan associated with this subscriber or displays associated error message.

Disassociating Plan

This section describes the procedure to dis-associate a usage or data plan.

To disassociate a plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **1** to access profile administration option.

Step 4 Press **l** to access disassociate plan option.

Step 5 Specify subscriber credentials. You can use either IMSI/MSIDN or NAI of this subscriber as well as its subscriber id, for specifying the credentials.

Step 6 Specify the id or name of the plan that you want to disassociate from this subscriber.

SSC Administration Console disassociates this plan from subscriber or displays appropriate error message.

Administering Group Accounts

This section describes the procedures to administer group accounts.

Important: The group administration option is available only when you log in to SSC Administration Console as policy administrator or as a user whose credentials include the policy administration credentials. If you have logged in using default policy administrator credentials then group administration option can be accessed by pressing **2** otherwise it can be accessed by pressing **7** or associated option number. For more information refer *User Administration* section.

A group account is a subscription that is being availed by multiple subscribers simultaneously where one of the subscribers is designated as head of the group and can have special administrative privileges for all other members of this group. Multiple data plans may be associated with a group account. Such an account can be used to:

- Allow multiple subscribers to share an account.
- Provide differential treatment to head of the group as compare to other members.
- Configure thresholds on group account usage.
- Generate notifications upon reaching such thresholds.

Important: A group account is mostly associated with family plans.

Group administration includes following provisioning tasks:

- Creating group accounts and associating members with such accounts.
- Modifying group account by adding or deleting its members.
- Viewing existing group profile.
- Associating plan with group profile.

This section includes following sub-sections:

- Manage Group
- Manage Members
- Manage Subscriptions

Manage Group

This section describes the procedure to view, add and delete group accounts.

Managing group profile involves following tasks:

- Viewing Existing Group Profile
- Adding Group Account
- Deleting Group Account

Viewing Existing Group Profile

This section describes the procedure to view an existing group profile.

To view existing group profile:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access group administration option.

Step 4 Press **a** to access view option.

This option allows you to view existing group accounts and plans.

Step 5 Press **V** to access view details option.

Step 6 Specify the group name whose details you want to view.

SSC Administration Console displays the group profile details such as its name, MSISDN, subscription tire, billing date, short description of the group, its status and e-mail as well as SMS notification status.

Adding Group Account

This section describes the procedure to add a group account.

To add a group account:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access group administration option.

Step 4 Press **a** to access manage group option.

Step 5 Press **o** to configure a new subscriber group account.

Step 6 Specify the group account name.

Step 7 Specify the description of this group account.

Step 8 Specify the subscription tire associated with this group.

Step 9 Specify SMS notification preference. If you select, **yes**, then notifications will be sent as SMS.

Step 10 Specify MSISDN.

Step 11 Specify e-mail notification preference. If you select **yes**, then notifications will be sent as an e-mail.

Step 12 If you select **yes** in the previous step, then specify the e-mail address.

Step 13 Specify billing date in dd/mm/yyyy format.

Deleting Group Account

This section describes the procedure to delete a group account.

To delete a group account:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access group administration option.

Step 4 Press **a** to access manage group option.

Step 5 Press **t** to delete an existing group account.

SSC Administration Console deletes the group account and displays appropriate message.

Manage Members

This section describes the procedures to add a member to and delete a member from group account.

Managing members of a group account involves following tasks:

- Adding Member to Group Account
- Deleting Member from Group Account

Adding Member to Group Account

This section describes the procedure to add a member to a group account.

To add a member to group account:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access group administration option.

Step 4 Press **b** to access manage member option.

Step 5 Press **M** to add a member to an existing group account.

Step 6 Specify name of the group to which you want to add this member.

Step 7 Specify subscriber credentials. You can use either IMSI/MSIDN or NAI of this subscriber as well as its subscriber id, and add this subscriber to the group.

Step 8 Specify whether you want to add this subscriber as group administrator

SSC Administration Console adds the member to the group and displays appropriate message.

Deleting Member from Group Account

This section describes the procedure to delete a member from a group account.

To delete a member from group account:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access group administration option.

Step 4 Press **b** to access manage member option.

Step 5 Press **t** to delete a member from an existing group account.

Step 6 Specify name of the group account from which you want to delete this member.

Step 7 Specify whether you want to delete this subscriber from the associated group account.
SSC Administration Console adds the member to the group and displays appropriate message.

Manage Subscriptions

This section describes the procedure to associate a plan with the group profile.

Managing subscriptions for a group account involves following tasks:

- Associating Plan with Group Profile

Associating Plan with Group Profile

This section describes the procedure to associate a plan with group profile.

To associate a plan with group profile:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **2** to access group administration option.

Step 4 Press **c** to access manage subscription option.

Step 5 Press **f** to associate a plan with an existing group account.

Step 6 Specify the group account name.

Step 7 Specify subscription order.

Step 8 Specify start date and end date in DD/MM/YYYY format.

Step 9 Specify whether you want to generate the notifications.

Step 10 Specify whether you want to associate more plans with this group.

Step 11 If you select **yes** in previous step, then provide the information for additional plans.
SSC Administration Console associates the plan with the group account and displays appropriate message.

Administering Plans

This section describes the procedures to administer the service and data plans.

Important: The plan administration option is available only when you log in to SSC Administration Console as policy administrator or as a user whose credentials include the policy administration credentials. If you have logged in using default policy administrator credentials then plan administration option can be accessed by pressing **3** otherwise it can be accessed by pressing **8** or associated option number. For more information refer *User Administration* section.

Depending upon services that are being provided as per the business model, following parameters constitute a plan:

- Unique name and Id.
- Payment type such as pre-paid or post-paid.
- Subscription validity such as start and end time.
- Frequency of re-charge period such as weekly, monthly, six monthly.
- Category of the service or subscriber as defined by service provider.
- Priority of service or subscriber as defined by service provider.
- Grace period, and number of days allowed, if the period is enabled.
- QoS parameters.
- Usage limits for volume or time consumption.
- Thresholds for volume or time consumption.

A plan defines the services that are being rendered to the subscriber. Depending upon their payment method such as pre-paid or post-paid, different categories of plans can be associated with them. Following are various plan categories:

- **Data Plan**: This is the basic category that has an independent existence. A subscriber can be associated with single or multiple data plans.
- **Service Plan**: A service plan is always associated with a data plan. A service plan cannot have an independent existence from its parent data plan.
- **Service Pack**: This is a service plan that needs to be explicitly subscribed by the subscriber.

Data plan, service plan and service pack define the basic services that can be rendered by the subscriber.

Add – on is always associated with the data or service plans or packs. Add on is used to render customized services by enhancing the attributes of existing plans. Following are the add-on categories:

- **Service Add-on**: Used to enable tethering.
- **Allowance Add-on**: Used to increment volume or time usage.
- **Validity Add-on**: Used to increment subscription validity.

This section includes following sub-sections:

- View Plans
- Administer Plans

View Plans

This section describes the procedures to view a specific plan or all plans.

Viewing plans involves following tasks:

- Viewing a Specific Plan
- Viewing All Plans

Viewing a Specific Plan

This section describes the procedure to view a specific usage or data plan.

To view a specific plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access plan administration option.

Step 4 Press **a** to access view option.

Step 5 Specify the **name** of the plan whose details you want to view.

SSC Administration Console displays the plan details such as plan id, name, type, associated volume as well as time usage limits along with validity, monitoring level and start as well as end date.

Viewing All Plans

This section describes the procedure to view all existing usage as well as data plans.

To view all plans:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access plan administration option.

Step 4 Press **e** to access view all plans option.

SSC Administration Console displays a list of all existing usage as well as data plans.

Administer Plans

This section describers the procedures to administer plans.

Administering plans involves following tasks:

- Adding New Plan
- Deleting Plan
- Modifying Plan

Adding New Plan

This section describes the procedure to add a new usage or data plan.

To add a new plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access plan administration option.

Step 4 Press **b** to add a new plan.

Step 5 Specify the name and short description for a new plan.

Step 6 Specify base usage limits, such as volume limit in bytes and time usage limits in seconds.

Step 7 Specify the validity period for this plan in days.

Step 8 Specify the start date for this plan in YYYY –MM- DD format and the start time in HH:MM:SS format.

Step 9 Specify end date and end time in same format as of start date and start time.

Step 10 Specify the roaming details, use values **1** for home, **2** for roaming and **3** for both.

Step 11 Enter quota limit type, use values **1** for hard limit and **2** for soft limit.

Step 12 Specify **y** if you want to add another threshold for this plan.

Important: While configuring a new plan, if you select the threshold category as time or any, then you need to specify absolute and percentage value for such threshold category.

Step 13 Specify the quota or usage type, use values **1** for volume, **2** for any and **3** for time based usage of the service.

Step 14 If you have selected volume as a quota or usage type then specify absolute volume.

Step 15 Specify **y** if you want to generate a notification, when the threshold mentioned in previous steps is crossed

Step 16 Specify whether you want to configure additional usage limits (service plans) for this plan. If you select **yes**, then specify the name for the usage limit (service plan).

Step 17 Specify the volume usage limits in bytes and time usage limits in seconds.

Step 18 Specify the validity period.Select value **1** for hard limit and **2** for soft limit.

Step 19 Specify whether you want to add additional threshold. If you select **no**, then specify whether you want to configure additional usage limits (service plans).

Once you have configured all the data plans and corresponding usage limits (service plans), then SSC Administration Console displays the message that the plan is added successfully to the database.

Deleting Plan

This section describes the procedure to delete an existing plan.

To delete a plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access plan administration option.

Step 4 Press **c** to access delete plan option.

Step 5 SSC Administration Console displays a list of existing plans. Select the plan that you want to delete.

SSC Administration Console deletes the selected plan.

Modifying Plan

This section describes the procedure to modify an existing plan.

To modify a plan:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **3** to access plan administration option.

Step 4 Press **d** to access modify plan option.

Step 5 Specify name of the plan that you want to modify.

Step 6 Specify following values as per the category of modifications that you want to perform on the existing plan.Select **1** for changing plan details, **2** for changing existing usage limits, **3** for adding new usage limits to the plan, **4** for deleting existing usage limits from the plan.

Step 7 If you select option **1** in previous step, then specify the description for the plan.

Step 8 Specify updated volume and time usage limits.

Step 9 Specify new validity period.

Step 10 Specify new start and end date as well as time.

Step 11 Specify the changed roaming status for the plan, the valid options are **1** for home, **2** for roaming and **3** for both.

Step 12 Specify changed quota limits, the valid options are 1 – for hard limit, 2 – for soft limit.

Step 13 Select **y**, if you want to change any other threshold for this plan.

Step 14 Specify updated quota type. Valid values are **1** for volume, **2** for any and **3** for time quota.

Step 15 Specify your choice for modified quota or usage and provide new absolute as well as percentage values.

Step 16 Specify whether you want to generate a notification when this threshold is crossed.

Step 17 Specify the template name, if you want to store this plan as a template.

Step 18 Specify whether you want to change any threshold for this plan.

Step 19 Specify whether you want to change volume, time or any other category of quota associated with this plan.

SSC Administration Console updates the plan details in the database.

Administering Data Store

This section describes the procedures to administer the subscriber data store.

Important: The data store administration option is available only when you log in to SSC Administration Console as policy administrator or as a user whose credentials include the policy administration credentials. If you have logged in using default policy administrator credentials then data store administration option can be accessed by pressing **5** otherwise it can be accessed by pressing **9** or associated option number. For more information refer *User Administration* section.

This section includes following sub-sections:

- Administering Subscriber Tires
- Administering Notification Templates
- Administering Auto provisioning Templates

In a Policy Charging and Control (PCC) solution SSC acts as a data store for Subscriber Profile Registry (SPR). As per your PCC implementation and the services that are being offered, SSC stores following information in a database:

- Subscriber Tire.
- Profile Attribute.
- Notification Template.
- Auto provisioning Template

Important: It is recommended that SSC Administration Console should not be used for subscriber provisioning, the provisioning should carried out using bulk upload script and CSV file.

Administering Subscriber Tires

This section describes the procedures to administer the data related to subscriber tire.

Subscribers can be categorized into different tires such as gold, silver or bronze based on the kind of services consumed and corresponding charges paid by them. A subscription or subscriber tire can be used to provide appropriate policy as well as charging treatment to the subscriber, when they are accessing the network. Depending on the business model, it is possible to create consumer or corporate subscription tires with which appropriate service plans can be associated.

Administering subscriber tire involves following tasks:

- Adding New Subscriber Tire
- Viewing All Subscriber Tires
- Viewing a Specific Subscriber Tire
- Deleting Specific Subscriber Tire

Adding New Subscriber Tire

This section describes the procedure to add a new subscriber tire.

To add a new subscriber tire:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **a** to access subscriber tire option.

Step 5 Press **N** to add a new tire.

Step 6 specify tire name.

Step 7 Specify description for this tire.
SSC Administration Console adds the subscriber tire and displays appropriate message.

Viewing All Subscriber Tires

This section describes the procedure to view all existing subscriber tires.

To view all existing subscriber tires:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **a** to access subscriber tire option.

Step 5 Press **V** to view all existing subscriber tires.
SSC Administration Console displays names of all available subscriber tires.

Viewing a Specific Subscriber Tire

This section describes the procedure to view details of a specific subscriber tire.

To view a specific subscriber tire:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **a** to access subscriber tire option.

Step 5 Press **w** to view a specific subscriber tire.

Step 6 Specify the name of subscriber tire, whose details you want to view.
SSC Administration Console displays tire id, its name and description.

Deleting Specific Subscriber Tire

This section describes the procedure to delete a specific subscriber tire.

To delete a subscriber tire:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **a** to access subscriber tire option.

Step 5 Press **l** to access delete a subscriber tire option.

Step 6 Specify the name of subscriber tire, that you want to delete.

SSC Administration Console deletes the subscriber tire and displays appropriate message.

Administering Notification Templates

This section describes the procedures to administer the data related to notification templates.

Notification templates are used to convey policy changes as well as status or usage related updates to the subscribers. SSC can send notifications as e-mail or SMS messages using the mail servers and SMSCs. SSC console can also be used to create and maintain notification templates.

Important: Refer *Event Notification Management* feature, from *Features and Functionality* section of the *Overview*chapter.

Administering notification templates involves following tasks:

- Adding New Notification Template
- Viewing Notification Template
- Viewing all Notification Templates
- Deleting Notification Template
- Updating Notification Template

Adding New Notification Template

This section describes the procedure to add a new notification template.

To add new notification template:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **c** to access notification template option.

Step 5 Press **N** to add a new template.

Step 6 specify template name.

Step 7 Specify event type associated with this notification template.

Event type indicates occurrence of some event or status change related to the service usage of the subscriber.For example you can create an event type as say Quota80%Full, which indicates that the subscriber has utilized 80% of his or her quota.

Step 8 Specify the SMS message that you want to associate with this template or press enter to skip this option.

Important: Notification template can have maximum 2000 characters.

Step 9 Specify the e-mail message that you want to associate with this template or press enter to skip this option.

SSC Administration Console adds the notification template to the database.

Viewing Notification Template

This section describes the procedure to view an existing notification template.

To view a notification template:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **c** to access notification template option.

Step 5 Press **V** to view an existing notification template.

Step 6 Specify the name of template that you want to view.

SSC Administration Console displays the template id, name, type of associated event along with SMS and e-mail message.

Viewing all Notification Templates

This section describes the procedure to view all available notification templates.

To view all notification templates:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **c** to access notification template option.

Step 5 Press **w** to view all configured notification templates.

SSC Administration Console displays the list of all available notification templates.

Deleting Notification Template

This section describes the procedure to delete a notification template.

To delete a notification template:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **c** to access notification template option.

Step 5 Press **t** to delete an existing notification template.

Step 6 Specify name of the notification template that you want to delete.

SSC Administration Console deletes this notification template and displays appropriate message.

Updating Notification Template

This section describes the procedure to update a notification template.

To update a notification template:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **c** to access notification template option.

Step 5 Press **U** to update a notification template.

Step 6 Specify name of the notification template that you want to update.

Step 7 Specify the event type associated with this notification template.

Event type indicates occurrence of some event or status change related to the service usage of the subscriber.For example you can create an event type as say Quota80%Full, which indicates that the subscriber has utilized 80% of his or her quota.

Step 8 Specify updated notification message that you want to send through SMS or press enter key to keep this field blank.

Step 9 Specify the updated notification message that you want to send through e-mail or press enter key to keep this field blank.

SSC Administration Console updates the notification template and displays appropriate message.

Administering Auto provisioning Templates

This section describes the procedures to administer auto provisioning templates.

Auto provisioning template can be used to create a subscriber profile in SSC on the fly. Such scenario may arise if a subscriber is requesting for higher QoS through Online Charging System (OCS) node when their profile is not available with SSC, as SSC is still being integrated in the system. The auto provisioning template can have mandatory as well as default attributes. Mandatory attributes will have hard coded default values. These values will be over written by the user input. Hence user input is mandatory for such attributes. Optional attributes will have zero as the default value,

Important: Subscriber auto provisioning template can be configured using SSC administration console as well as by policy provisioning method.

Administering auto provisioning templates involves following tasks:

- Creating Auto provisioning Template
- Viewing Auto provisioning Template

Creating Auto provisioning Template

This section describes the procedure to create an auto provisioning template.

To create an auto provisioning template:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **d** to access auto provisioning option.

Step 5 Press **T** to access auto provisioning option.

Important: Press # to remove existing value and <enter > to keep existing default value

Step 6 Specify subscriber name.

Step 7 Specify brief description for this subscriber

Step 8 Specify subscription tire that is to be associated with this subscriber.

Step 9 Specify billing start date in DD/MM/YYYY format.

Step 10 Enter y or n to enable or disable SMS notification.

Step 11 Enter y or n to enable or disable e-mail notification.

Step 12 If e-mail notification is enabled then specify e-mail address.

Step 13 Specify whether you want to set profile attributes for this subscriber.

Important: SSC Administration Console displays the name and expected values for the profile attributes. Select appropriate value or press <enter> to ignore this profile attribute.

Step 14 Specify whether you want to associate a plan with this subscriber.

Step 15 If you select y in previous step, then specify plan details such as plan name.

Step 16 SSC Administration Console configures the auto provisioning template or displays appropriate error message.

Viewing Auto provisioning Template

This section describes the procedure to view an existing auto provisioning template.

To view an existing auto provisioning template:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **5** to access data store administration option.

Step 4 Press **d** to access auto provisioning option.

Step 5 Press **v** to view existing templates.

SSC Administration Console displays parameters or flags of auto provisioning template such as Enable e-mail, Enable SMS, Notification preference and Subscription Order along with their default values.

Monitoring SSC Security Using Console

This section describes the procedures to monitor the security of SSC.

Important: The number to access security option from SSC Administration Console varies as per your access credentials. If you log-in with policy administrative credentials then security option can be accessed by pressing **9** otherwise it can be access by pressing **7**. For more information refer *User Administration* section.

This section includes following sub-sections:

- Changing Password
- Monitoring Security Using System Audit
- Managing Session

Changing Password

This section describes how to change the system password.

Changing Password

This section describes the procedure to change system password.

To change password:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **7** to access security option.

Step 4 Press **a** to access change password option.

Step 5 Specify old and new password.

Step 6 Confirm new password.

SSC Administration Console changes the password and displays appropriate message.

Monitoring Security Using System Audit

This section describes audit records and lists procedures to use audit logs to monitor security of SSC node.

Various provisioning operations and events associated with the SSC deployment are recorded or audited. Such records are known as audit records. These records are categorized as system log, SPR log and event log. Audit records can be used for security, monitoring as well as troubleshooting purpose.

An audit record contains:

- **Audit Id** A unique identifier for each record. The audit id is generated by the SSC.

- **Event Id** It represents a category of event associated with the SSC deployment. For example adding a subscriber is an event associated with SSC it will have an identifier, sending a notification through SMS is another event associated with SSC so it will have a different identifier.
- **Module Id** It represents the SSC module that has recorded or audited this information. For example provisioning events will be recorded by profile manager.
- **Client Context** It represent the type of client associated with this event. For example, the client can be SSC Console, a SOAP or XML API used for SSC provisioning or a PPT client.
- **Subscriber Id** It represents the subscriber associated with this event. For example when a subscriber is created or deleted then corresponding subscriber id will be stored in the audit record.
- **Plan Id** It represents a data, service or group plan associated with the event. For example if a plan is created or recharged then corresponding plan id will be stored in audit record.
- **Audit Date** It represents the date when this audit record is generated.
- **Request Data** It represents the data requested by the SSC operation. It is available in XML format.
- **Response Data** It represents the response received by the SSC operation. It is available in XML format.

Important: Audit record stores only successful transactions. Unsuccessful transactions that do not affect SSC deployment are not stored.

Depending upon your access privilege you can monitor and maintain security of the SSC instance by accessing following audit records:

- System Audit
- SPR Audit
- Event Log Audit

Important: The SPR and Event Log audit options are available only when you log in to SSC Administration Console as policy administrator or as a user whose credentials include the policy administration credentials.

System audit records events related to configuration of:

- Sh server and peer.
- EN controller and manager.
- Log demon.
- Process log
- Bulk statistics.
- Bulk statistics FTP.
- SNMP alarm.
- RSMon.
- Ud client and attribute.

SPR Audit records events related to creation and deletion of:

- Subscription tire.
- Profile attribute.
- Subscriber profile.

- Notification template.
- Data plan.
- Group account.

SPR Audit also records event related to updates to:

- Subscriber profile.
- Profile attribute.
- Notification templates.

Event logs records event related to:

- Sending an SMS to SMPP server.
- Sending an e-mail to SMTP server.

Refer to sections *SSC Logs Administration* and *Monitoring System Logs* for more information.

System as well as SPR or event audit involves following tasks:

- Viewing Logs
- Viewing Log Records

Viewing Logs

This section describes the procedure to view system audit logs.

To view logs:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **7** to access security option.

Step 4 Press **b** to access system audit option.

Step 5 Press **V** to access view logs option.

Step 6 Specify the start date and start time of the period for which you want to view the logs. In DD- MM-YYY HH:MM format.

Step 7 Specify the end date and end time in the format mentioned in the previous step.

Step 8 Select the filter that is to be used to access the SPR or event audit logs, by specifying **y** or **n**. You can select module id, event id or subscriber details as the filter.

SSC Administration Console displays the logs.

Viewing Log Records

This section describes the procedure to view records of system audit log.

To view log records:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **7** to access security option.

Step 4 Press **b** to access system audit option.

Step 5 Press **L** to access view log record option.

Step 6 Specify the record Id of the log record that you want to view.

SSC Administration Console displays the log record.

Managing Session

This section describes how to manage system sessions.

Viewing Existing Session

This section describes the procedure to view existing system session.

To view existing session:

Step 1 Login to the SSC node with administrative privileges.

Step 2 Access the SSC Administration Console by executing the script `./sscadm`.

Step 3 Press **7** to access security option.

Step 4 Press **c** to access manage session option.

Step 5 Press **V** to view information regarding existing session.

SSC Administration Console displays User Name, Role, Log on Time, time and date of Last Activity, for all the active sessions.

Chapter 4
Troubleshooting the SSC

This chapter briefly describes troubleshooting and monitoring information, known issues and their work around if available.

You may face issues while working with a Subscriber Service Controller (SSC) deployment, as well as while installing or un-installing an SSC instance. For troubleshooting such issues SSC deployment provides following categories of support data:

- System logs that record deployment infrastructure information such as web servers and active sessions.
- Audit or event logs that record events related to subscriber profile and service usage.
- Scripts that can be used to generate system verification information, such as generating eth and host IPs as well as generating their IP maps.
- Current status of processes associated with any SSC component.
- Scripts that can be used to dump database.
- Scripts that can be used to view grid status and re-attach a grid if it is detached.
- Scripts to view network connectivity status.

Important: You can access system statistics for monitoring and troubleshooting the SSC instance, refer section *Monitoring System Statistics* in *SSC Administration* chapter as well as schema statistics appendices.

Following log files can be used for troubleshooting purpose:

- **/var/log/message**: This log file records all the installation related errors and alert messages.
- **/localhome/ssc/log/sn_SSC.log**: This log file records, alarms, application errors as well as database query failure issues related to the SSC instance.
- **/localhome/ssc/log/startup.log**: This log file records the segmentation errors received by any SSC related process along with start-up and incremental log.
- **/localhome/ssc/log/SscHaTool_yyymmdd_hh:mm:ss.log** : This log file records information related to High Availability (HA) activities. This file is created only if the HA feature is enabled for the deployment.

Following scripts can be used for troubleshooting purpose:

- **maintenacemode.sh**: By default after performing the installation and upgrade procedures SSC deployment is in the maintenance mode. Cron job execution is halted when the maintenance mode is enabled. Use **Maintenacemode.sh** script from */localhome/ssc/tools* directory to enable or disable the maintenance mode or to view its status.
- **./hbtool**: Execute this script, from */localhome/ssc* directory, with SSC administrator privileges. It displays list of all active processes except profile manager process. For each process it displays PID, facility, instance, start time and total restarts. This tool also displays the restart count for the specific process that has died and restarted.
- **./createCronjobForDumpingmonitoringInfo.sh**: Execute this script, with privileges of a root user, from *localhome/ssc/tools/MonitoringCron* directory. This cron job is executed after every fifteen minutes. It logs

parameters such as, disk, memory and CPU usage as well as outputs of sscadm status, imdb status and imdb check commands. It also logs semaphore details and ping results for host names. These details are stored in **monitoring.log** file.

- **./removeCronjobForDumpingmonitoringInfo.sh**: Execute this script with privileges of a root user, from *localhome/ssc/tools/monitoringCron* directory. This command removes the cron job created by the command *./createCronJobForDumpingMonitoringInfo.sh* .
- **./dumpMonitoringInfo.sh**: Execute this script, with privileges of a root user, from *localhome/ssc/tools/monitoringCron* directory. This command logs the parameters described in command ./**createCronjobForDumpingMonitoringInfo.sh.** These parameters are logged in **monitoring.log** file, instead of creating a cron job.
- **./sscdbstatus**: Execute this script from */localhome/ssc/install/spr_install/tools* directory with database user privileges.This script lists the status of database and IMDB application.
- **./sscdb_shutdown**: Execute this script from */localhome/ssc/install/spr_install/tools* directory. This script shuts down the SSC database.
- **./sscdb_backup**: Execute this script from */localhome/ssc/install/spr_install/tools* directory. This script creates a back-up of SSC database. Before executing this script, ensure that the status of SSC application, database and IMDB is not active.
- **./sscdb_startup**: Execute this script from */localhome/ssc/install/spr_install/tools* directory. This script start ups down the SSC database.

Following scripts can be used for troubleshooting the IMDB or database grid issues:

- **checkGridAttach.sh**: Execute this script with privileges of a root user, from l*localhome/ssc/install/spr_install/tools/DbMonitorCron* directory. It displays current status of the IMDB grid.
- **checkT10Health.sh**: Execute this script with privileges of a root user, from *localhome/ssc/install/spr_install/tools/GridAttachCron* directory. It displays current status of the IMDB application.

Following scripts can be used for verifying IP addresses and host names with respect to the IP map of the deployment:

- common.sh
- compare_eth_ip.sh
- compare_host_ip.sh
- generate_eth_ip_map.sh
- generate-host_ip_map.sh
- ping_all_hosts_from_all_machines.sh
- ping_hostnames.sh
- system_verification.sh

Important: These scripts are located in /localhome/ssc/tools/System Verification directory.

Following trouble shooting sections provide information about possible cause and work around if available for such issues. The issues are categorized as:

- Issues Pertaining to SSC Installation
- Issues Pertaining to SSC Startup
- Issues Pertaining to SSC Database

- Issues Pertaining to In Memory Database (IMDB) Application

Issues Pertaining to SSC Installation

This section includes the issues that you may face during single host as well as cluster installation for your SSC deployment.

Problem:	RDBMS database creation fails.
Possible Cause(s):	Installer is not able to create the database schema.
Action(s):	• Log-in as root user. • Access the installation log by issuing following command `tailf /var/log/messages` • The log file should contain following entries.: Result of installing post install steps for *database* 0 and SSC installation is done. • Absence of the above mentioned entries in log suggests that display issues may be interrupting execution of database utilities. • As a root user issue following command: `su -database- c "/localhome/install/database/runInstaller -silent -noconfig -responseFile /localhome/install/database/ssc_database_sw_install.rsp"` • This command will update log file in `../var/log/messages` directory. • Un-install SSC on this blade. • Again install SSC on this blade.

Problem:	Installer hangs while installing database.
Possible Cause(s):	This may be due to some issue related to X11 forwarding.
Action(s):	• Log-in as root user. • Access `.. /var/log/message` directory. • Ensure that this directory contains a message - Host created for searching xauth list is datablade2/unix:10. • Ensure that this directory does not contain any message stating – Searching xauth list using key. • Delete .Xauthority file from `home/root` directory. • Issue following command: `mv /var/.com.zerog.registry.xml var/.com.zerog.registry.xml.` • Start the installation process again.

Problem:	During installation process lost connectivity to installer.
Possible Cause(s):	You may lose connectivity to installer if you try to configure management interface using the GUI based installer.

Action(s):	• Exit installation process. • Delete.. `/tmp/ssc` folder. • Re-install SSC without configuring management interface.

Issues Pertaining to SSC Startup

This section includes the issues that you may face during initiating the SSC using the administrative scripts, provided during installation.

Problem:	Neither SSC starts nor does it gives any specific error message.
Possible Cause(s):	SSC is not able to display the cause for not starting.
Action(s):	• Log in as SSC admin user. • Access the logs in file `logs/startup.log` directory. • Read the messages and fix the issues mentioned in the log file. • Re-start SSC.

Problem:	SSC does not start while giving apache error message.
Possible Cause(s):	SSC is not able to start and displays following message `Error: Syntax error on line 40 of /localhome/ssc/3rdparty/apache/conf/httpd.conf`
Action(s):	• Log in as SSC admin user. • Access the `etc/hosts` file, and get the ip address of the blade where SSC is not starting. • Edit the file `localhome/ssc/3rdparty/apache/conf/httpd.conf` and add this IP address before the port as follows: `Listen 192.168.10.2:8080` where 192.168.10.2 is the host IP address. • Stop SSC using command `sscadmin stop.` • Start SSC using command `sscadmin start.` • Configure the profile config using system administration option of SSC Administration Console to prevent the reoccurrence of this error.

Problem:	After installation Sh controller is not coming up.
Possible Cause(s):	Sh controllers do not start until you bind these controllers using SSC administration console.
Action(s):	• Log-in to console is an SSC administrator. • Use the Interface Management option to bind Sh controllers. • Refer to Managing Interfaces section, in SSC administration chapter of the SSC Installation & Administration guide.

Problem:	SSC does not stop properly.
Possible Cause(s):	Heart beat daemon is not able to kill all the processes related to application and database of this SSC instance.

Action(s):	• Stop SSC instance using script `./sscadm stop`. • List all the SSC processes that are still active by using command `ps -e | grep sn_*`. • Kill each of this SSC related process. • Re-start SSC using script `./sscadm start`.

Problem:	File size of Start-up log file keeps on increasing.
Possible Cause(s):	The start-up log file may keep on increasing in size due to increased number of debug or error log entries.
Action(s):	Ensure that following script and system parameter are added to a cron job: • `purgefile.sh`script is available which rotates the start-up log file when the file size exceeds 1 Gb. • In the `system.cfg`file a parameters `MaxSscStartupLogFileCount` is added, this parameter controls the number of start-up log files the can be present on a system. Following are the locations of these scripts: • create cron job – scripts/LogFilesPurgeCron/createCronJobForPurgingLogFiles.sh • remove cron job - scripts/LogFilesPurgeCron/removeCronJobForPurgingLogFiles.sh

Problem:	In a two blade cluster HA deployment, after restoring back-up, system may not be able to bind the profile controller interface.
Possible Cause(s):	Some parameter settings in the cluster configuration file may cause this issue.
Action(s):	• Login as SSC administrator. • Stop SSC application on both the blades using script `./sscadm stop`. • Access */etc/cluster/ cluster.config* file on both the blades. • Ensure that parameter **<cman expected_vosts>** has value **1**. • Ensure that the parameter **two_node** has value **1**. • Ensure that parameter **broadcast** has value **yes**. You may need to add this parameter.

Issues Pertaining to SSC Database

This section includes the issues that you may face when SSC is trying to access the subscriber or subscription information from database.

Problem:	Not able to start `database` listener.
Possible Cause(s):	`database` listener process is not running.
Action(s):	• From the location *$database_HOME/bin* execute **lsnrctl**. • At *lsncrtl* prompt enter **start** to initiate the *listnerl* process. • Enter **quit**.

Problem:	12519:*database*-12519:TNS: no appropriate service handler found – error listed in `log/sn_SSCn.log` file.
Possible Cause(s):	Listener process may not have been registered for the database.
Action(s):	• Ensure that the listener has started. • Login as *database*super user, by issuing command: `su -database`. • Access the directory `../localhome/ssc/install/spr_install .` • Check the database status by issuing following command:`./sscdbstatus.sh SSC .` • If database status shows errors, then check whether the listener process is owned by *database*. • If *database*no longer owns the listener process, and this process is owned by daemon, then kill listener process, as a root user and using kill -9 <pid> command. • Login as *database* administrator and start listener, by issuing command:`lsnrctl start .` • Now, again check the status of database, by accessing `../ssc/install/spr_install` directory and by issuing command: `./sscdbstatus.sh SSC .`

Problem:	Oracle database creation hangs.
Possible Cause(s):	This issue may be observed for some deployments, when executing SSC installer using Xming from Windows 7.
Action(s):	• Exit SSC installer. • Delete */var/.com.*xml* file • Restart SSC installer.

Problem:	Oracle database creation fails.
Possible Cause(s):	For some deployments display issue may prevent the execution of the database utilities.

Action(s):	• Access *var/log/messages* file. • In this file search for the statement *Result of installing post installation steps for oracle is 0* If this statement is not appearing in the log then it indicates that the database creation failure is due to display issue. • Log in with root administrative privileges and execute following command `su-l oracle -c "/localhome/install/oracle/runInstaller -responseFile /localhome/install/oracle/ssc_oracle_sw_install.rsp -nowelcome –silent .` • Above mentioned command creates a log file that logs the failure messages along with suggested work around. • After fixing the errors using work around, un-install SSC. • Install SSC on the same blade again.

Issues Pertaining to In Memory Database (IMDB) Application

This section includes the issues that you may face when SSC is trying to access the subscriber or subscription information from database using the IMDB application.

Problem:	Grid creation fails.
Possible Cause(s):	Installer is not able to create the *IMDB_App* grid.
Action(s):	• Login as a root user. • Access the following file on the blade where database is configured: `/localhome/`*`database`*`/app/`*`database`*`/product/11.2.0/dbhome_1/network/admin/tnsnames.ora`. • Check the SSC entry in this file that contains following fields `(DESCRIPTION =, (ADDRESS_LIST = (ADDRESS= PROTOCOL = TCP) (HOST = datablade1) (PORT = 1521)) CONNECT_ DATA = (SID =SSC))).` • Ensure that you can log-in to database as `sqlplus spradm/spr_adm@SSC .`

Appendix A
ENAPP Schema Statistics

The Event Notification Application (ENAPP) schema provides the following type of statistics:

- **Counter**: A counter records incremental data cumulatively and rolls over when the counter limit is reached. The limit depends upon the counter data type.
- **Gauge**: A gauge statistics indicates a single value representative of a single instance. This type is often used to track particular events in time.
- **Fixed Value String**: A string statistics indicates the name of a service instance or a node.

Important: The format string syntax is described by *Schema Format String Syntax* in the *Bulk Statistics Overview* chapter.

Important: Unless otherwise indicated all statistics are of proprietary type based on 3GPP standard.

Important: Unless otherwise indicated, all statistics are counters. For statistics with the Int32 data type, the roll-over to zero limit is 4,294,967,295. For statistics with the Int64 data type, the roll-over to zero limit is 18,446,744,073,709,551,615. All statistics are cumulative and reset only by one of the following methods: roll-over (as described above), after a system restart, or after a clear command is performed. All statistics are considered standards-based unless otherwise noted.

The following variables are supported:

Table 4. ENAPP Schema Statistics

Statistic	Description	Data Type
in_events	Indicates total number of incoming events. Trigger: When an event from IPCF or SSC is received at event notification manager. Availability: Available across event notification application.	Gauge/Int64
out_events	Indicates total number of out going events. Trigger: When an event is sent out by event notification manager. Availability: Available across event notification application.	Gauge/ Int64
in_sms_events	Indicates total number of incoming SMS events. Trigger: When an event from IPCF or SSC is received at event notification manager with SMS as notification method. Availability: Available across event notification application.	Gauge/ Int64
out_sms_events	Indicates total number of out going SMS events. Trigger: When SMS is sent for an event. Availability: Available across event notification application.	Gauge/ Int64

Statistic	Description	Data Type
in_email_events	Indicates total number of incoming e-mail events. Trigger: When an event from IPCF or SSC is received at event notification manager with an e-mail as notification method. Availability: Available across event notification application.	Gauge/ Int64
out_email_events	Indicates total number of out going e-mail events. Trigger: When an e-mail is sent out for an event. Availability: Available across event notification application.	Gauge/ Int64
out_email_rate	Indicates rate per second for out going e-mails. Trigger: When an e-mail is sent out for an event. Availability: Available across event notification application.	Gauge/ Int64
out_sms_rate	Indicates rate per second for out going SMSs. Trigger: When an SMS is sent out for an event. Availability: Available across event notification application.	Gauge/ Int64
in_sms_rate	Indicates rate per second for in coming SMSs. Trigger: When an event from IPCF or SSC is received at event notification manager with an SMS as notification method. Availability: Available across event notification application.	Gauge/ Int64
in_email_rate	Indicates rate per second for in coming e-mails. Trigger: When an event from IPCF or SSC is received at event notification manager with an e-mail as notification method. Availability: Available across event notification application.	Gauge/ Int64
sms_failed	Indicates total number of failed SMS. Trigger: When SMS send operation fails. Availability: Available across event notification application.	Gauge/ Int64
email_failed	Indicates total number of failed e-mails. Trigger: When an e-mail send operation fails. Availability: Available across event notification application.	Gauge/ Int64

Important: For information on statistics that are common to all schema see the *Statistics and Counters Overview* chapter.

Appendix B
PROFAPP Schema Statistics

The Profile Application (PROFPP) schema provides the following types of statistics:

- **Counter**: A counter records incremental data cumulatively and rolls over when the counter limit is reached. The limit depends upon the counter data type.
- **Gauge**: A gauge statistic indicates a single value representative of a single instance. This type is often used to track particular events in time.
- **Fixed Value String**: A string statistic indicates the name of a service instance or a node.

Important: The format string syntax is described by *Schema Format String Syntax* in the *Bulk Statistics Overview* chapter.

Important: Unless otherwise indicated all statistics are of proprietary type based on 3GPP standard.

Important: Unless otherwise indicated, all statistics are counters. For statistics with the Int32 data type, the roll-over to zero limit is 4,294,967,295. For statistics with the Int64 data type, the roll-over to zero limit is 18,446,744,073,709,551,615. All statistics are cumulative and reset only by one of the following methods: roll-over (as described above), after a system restart, or after a clear command is performed. All statistics are considered standards-based unless otherwise noted.

The following variables are supported:

Table 5. PROFAPP Schema Statistics

Statistic	Description	Data Type
viewPlan_requests	Indicates total number of requests to get plan record. Trigger: When profile application receives a view plan request. Availability: Available across profile application.	Gauge/ Int64
setPlan_requests	Indicates total number of requests to set (create or update) the plan information. Trigger: When profile application receives a create or update plan request. Availability: Available across profile application.	Gauge/ Int64
deletePlan_requests	Indicates total number of requests to delete plan records. Trigger: When profile application receives delete plan request. Availability: Available across profile application.	Gauge/ Int64
viewallPlans_requests	Indicates total number of requests to get all plan records. Trigger: When profile application receives a get list of plans request. Availability: Available across profile application.	Gauge/ Int64
viewSubscriber_requests	Indicates total number of requests to get (create or update) subscriber record. Trigger: When profile application receives get subscriber details request. Availability: Available across profile application.	Gauge/ Int64

Statistic	Description	Data Type
setSubscriber_requests	Indicates total number of requests to set (create or update) subscriber information. Trigger: when profile application receives create or update subscriber details request Availability: Available across profile application.	Gauge/ Int64
deleteSubscriber_requests	Indicates total number of requests to delete subscriber record. Trigger: When profile application receives delete subscriber request. Availability: Available across profile application.	Gauge/ Int64
setPlanToSubscriber_requests	Indicates total number of request to associate plan with subscriber. Trigger: When profile application receives associate or update plan to subscriber request. Availability: Available across profile application.	Gauge/ Int64
viewallTiers_requests	Indicates total number of requests to get list of all subscription tires. Trigger: When profile application receives get all tire requests. Availability: Available across profile application.	Gauge/ Int64
setTier_requests	Indicates total number of requests to crate subscription tires. Trigger: When profile application receives a new tire creation request. Availability: Available across profile application.	Gauge/ Int64
deleteTier_requests	Indicates total number of requests to delete subscription tires. Trigger: When profile application receives a delete tire request. Availability: Available across profile application.	Gauge/ Int64
viewallAttributes_requests	Indicates total number of requests to get all profile attributes. Trigger: When profile application receives view all profile attribute request. Availability: Available across profile application.	Gauge/ Int64
setAttribute_requests	Indicates total number of requests to set (create or update) profile attributes. Trigger: When a profile attribute is created or updated. Availability: Available across profile application.	Gauge/ Int64
deleteAttribute_requests	Indicates total number of requests to delete profile attributes. Trigger: When a profile attribute is deleted. Availability: Available across profile application.	Gauge/ Int64
viewtiers_requests	Indicates total number of requests to view subscription tires. Trigger: When profile application receives get tire requests. Availability: Available across profile application.	Gauge/ Int64
prof_db_err	Indicates total number of database errors while processing profile requests. Trigger: When any database error occurs. Availability: Available across profile application.	Gauge/ Int64

Important: For information on statistics that are common to all schema see the *Statistics and Counters Overview* chapter.

Appendix C
SHAPP Schema Statistics

The Sh Application (SHAPP) schema provides the following type of statistics:

- **Counter**: A counter records incremental data cumulatively and rolls over when the counter limit is reached. The limit depends upon the counter data type.
- **Gauge**: A gauge statistic indicates a single value representative of a single instance. This type is often used to track particular events in time.
- **Fixed Value String**: A string statistic indicates the name of a service instance or a node.

Important: The format string syntax is described by *Schema Format String Syntax* in the *Bulk Statistics Overview* chapter.

Important: Unless otherwise indicated all statistics are of proprietary type based on 3GPP standard.

Important: Unless otherwise indicated, all statistics are counters. For statistics with the Int32 data type, the roll-over to zero limit is 4,294,967,295. For statistics with the Int64 data type, the roll-over to zero limit is 18,446,744,073,709,551,615. All statistics are cumulative and reset only by one of the following methods: roll-over (as described above), after a system restart, or after a clear command is performed. All statistics are considered standards-based unless otherwise noted.

The following variables are supported:

Table 6. SHAPP Schema Statistics

Statistic	Description	Data Type
sh_db_query	Indicates total number of database queries made during Sh call processing. Trigger: When DB API is called. Availability: Available across Sh application.	Gauge/ Int64
db_rid_usage	Indicates current usage count per Rating Id. Trigger: When a given rating id is used. Availability: Available across Sh application.	Gauge/ Int64
db_umon_usage	Indicates current usage count per usage monitor. Trigger: When a usage monitor is used. Availability: Available across Sh application.	Gauge/ Int64
db_sess_usage	Indicates current session usage. Trigger: Usage for a given session. Availability: Available across Sh application.	Gauge/ Int64
db_rid_upd	Indicates total number of updates per rating id. Trigger: When a given rating id is updated. Availability: Available across Sh application.	Gauge/ Int64

Statistic	Description	Data Type
db_umon_upd	Indicates total number of database usage updates, incremented for each database update, each plan in a Profile Update Request.- (PUR). Trigger: When a database usage is updated for PUR. Availability: Available across Sh application.	Gauge/ Int64
sh_db_err	Indicates total number of database errors encountered in processing of Sh calls. Trigger: When database API has returned an error. Availability: Available across Sh application.	Gauge/ Int64
sh_notif	Indicates total number of Push Notification Request (PNR) IPC messages sent by application manager to Sh controller. Trigger: When PNR is generated at application manager. Availability: Available across Sh application.	Gauge/ Int64
sh_db_profile	Indicates requested subscriber profile. Trigger: When a subscriber profile is requested. Availability: Available across Sh application.	Gauge/ Int64
snr_in	Indicates total number of Subscriber Notification Request (SNRs) messages received. Trigger: When an SNR is received. Availability: Available across Sh application.	Gauge/ Int64
sna_out	Indicates Subscriber Notification Answer (SNA) Sent. Trigger: When an SNR is sent. Availability: Available across Sh application.	Gauge/ Int64
pur_in	Indicates total number of Profile Update Request (PUR) messages received. Trigger: When a PUR is received. Availability: Available across Sh application.	Gauge/ Int64
pua_out	Indicates total number of Profile Update Answer (PUA) replies sent. Trigger: When a PUA is sent. Availability: Available across Sh application.	Gauge/ Int64
pnr_out	Indicates total number of Push Notification Request (PNR) messages sent. Trigger: When a PNR is sent. Availability: Available across Sh application.	Gauge/ Int64
pna_in	Indicates Push Notification Answer (PNA) messages received. Trigger: When a PNA is received. Availability: Available across Sh application.	Gauge/ Int64
ipc_appmgr_req	Indicates total number of IPC requests sent to application manager by Sh controller. Trigger: When an IPC request is sent to application manager by Sh controller. Availability: Available across Sh application.	Gauge/ Int64
snr_err	Indicates total number of subscriber Notification Request (SNR) error messages. When an SNR eror message is sent or received. Available across Sh application.	Gauge/ Int64
sna_err	Indicates total number of Subscriber Notification Answer (SNA) error messages. When an SNA error message is sent or received. Available across Sh application.	Gauge/ Int64
pur_err	Indicates total number of Profile Update Request (PUR) error messages. When a PUR error messages is sent or received. Available across Sh application.	Gauge/ Int64

Statistic	Description	Data Type
pua_err	Indicates total number of Profile Update Answer (PUA) error messages. When a PUR error messages is sent or received. Available across Sh application.	Gauge/ Int64
pnr_err	Indicates total number of Push Notification Request (PNR) error messages. When a PNR error messages is sent or received. Available across Sh application.	Gauge/ Int64
pna_err	Indicates total number of Push Notification Answer (PNR) error messages. When a PNA error messages is sent or received. Available across Sh application.	Gauge/ Int64

Important: For information on statistics that are common to all schema see the *Statistics and Counters Overview* chapter.