Copyright

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaimer all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.
# Contents

About This Document.............................................................................................................. v
Document Conventions ........................................................................................................... vi

## Chapter 1

### NCC System Architecture

Overview.......................................................................................................................... 1
NCC System Architecture Overview .................................................................................. 1
SMS and SLC Server Operation ......................................................................................... 4
VWS Server Operation ...................................................................................................... 5

## Chapter 2

### Service Management and Control

Overview.......................................................................................................................... 7
Service Management and Control Overview ........................................................................ 7
init Daemon Management .................................................................................................. 8
init Stop and Start Processes ............................................................................................... 9
SLEE Management ........................................................................................................... 12
Database Management ...................................................................................................... 15

## Chapter 3

### Monitoring and Managing

Overview.......................................................................................................................... 21
Monitoring and Managing Overview .................................................................................. 21
Software Version Levels ................................................................................................... 21
Running Processes ............................................................................................................ 22
SLEE Resource Usage ........................................................................................................ 27
Rolling Snoop Archives ..................................................................................................... 31
Rolling Snoop Risks .......................................................................................................... 33

## Chapter 4

### Service Logic Controller (SLC)

Overview.......................................................................................................................... 35
Service Logic Controller Overview ................................................................................... 35
Service Logic Execution Environment ................................................................................ 35
Network Connectivity Agents ............................................................................................. 38
Checking Services ............................................................................................................. 39

## Chapter 5

### Service Management System (SMS)

Overview.......................................................................................................................... 43
Service Management System Overview .............................................................................. 43
Java Screens ....................................................................................................................... 43
Replication .......................................................................................................................... 46
EDR Management .............................................................................................................. 48
Provisioning Interface (PI) .................................................................................................. 50
Business Processing Language .......................................................................................... 53
Chapter 6
Voucher and Wallet Server (VWS) ............................................. 57
   Overview .................................................................................. 57
   Voucher and Wallet Server Overview ....................................... 57
   Useful Commands and Scripts ................................................ 62

Chapter 7
Troubleshooting ........................................................................ 65
   Overview .................................................................................. 65
   Common Troubleshooting Procedures ..................................... 65

Appendix A
NCC Directory Structure and Contents .................................... 81
NCC Glossary of Terms ................................................................. 83
Index ........................................................................................... 91
About This Document

Scope

The scope of this document includes all functionality a user must know in order to effectively operate the Oracle Communications Network Charging and Control (NCC) application. It does not include detailed design of the service.

Audience

This guide is written primarily for NCC administrators. However, the overview sections of the document are useful to anyone requiring an introduction.

Prerequisites

A solid understanding of UNIX and a familiarity with IN concepts are an essential prerequisite for safely using the information contained in this technical guide. Attempting to install, remove, configure or otherwise alter the described system without the appropriate background skills, could cause damage to the system; including temporary or permanent incorrect operation, loss of service, and may render your system beyond recovery.

Although it is not a prerequisite to using this guide, familiarity with the target platform would be an advantage.

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

Related documents

The following documents are related to this document:

- NCC Installation Guide
- NCC User's Configuration Guide
Document Conventions

Typographical Conventions

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

<table>
<thead>
<tr>
<th>Formatting convention</th>
<th>Type of information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Special Bold</strong></td>
<td>Items you must select, such as names of tabs. Names of database tables and fields.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Name of a document, chapter, topic or other publication. Emphasis within text.</td>
</tr>
</tbody>
</table>
| **Button**            | The name of a button to click or a key to press. Example: To close the window, either click 
 |                       | Close, or press Esc. |
| **Key+Key**           | Key combinations for which the user must press and hold down one key and then press another. Example: Ctrl+P, or Alt+F4. |
| **Monospace**         | Examples of code or standard output. |
| **Monospace Bold**    | Text that you must enter. |
| **variable**          | Used to indicate variables or text that should be replaced. |
| **menu option > menu option >** | Used to indicate the cascading menu option to be selected, or the location path of a file. Example: Operator Functions > Report Functions Example: /IN/html/SMS/Helptext/ |
| **hypertext link**    | Used to indicate a hypertext link on an HTML page. |

Specialized terms and acronyms are defined in the Glossary at the end of this guide.
Overview

Introduction

This chapter introduces the Oracle Communications Network Charging and Control (NCC) system architecture.

In this chapter

This chapter contains the following topics.

NCC System Architecture Overview 1
SMS and SLC Server Operation 4
VWS Server Operation 5

NCC System Architecture Overview

Architecture diagram

This diagram depicts the NCC system from a network architecture perspective:

System components

The architect diagram, from the bottom layer up, we see:

- A number of disparate telecommunications services (for example, mobile, fixed, IP) showing the ability of the NCC system to handle convergence.
- Secondly, the network control aspect is handled using services templates (for example, fixed, mobile, data and TV).
Finally the on-line charging layer handles the service rating, subscriber balance management (and voucher/promotion management if appropriate).

Two optional additional products are also depicted in this diagram, Messaging Manager and Number Services Manager, which are out of the scope of this document.

Server components diagram

This diagram shows how the three main server components of the NCC system combine to form the system architecture.

Server descriptions

The server components are as follows:

- The Service Logic Controller (SLC) is the main interface to the network and handles all service processing (voice/SMS/data content).
  Service processing is handled through the Service Logic Execution Environment (SLEE), with the various network connectivity agents (for example, diameter, radius, MAP, SIP and the ACS control plan logic, defining the service logic for all enabled services.
- The Service Management System (SMS) provides the base system management functionality, including:
  - The Java administration UI
  - Centralized data storage
  - Replication functionality
- The Voucher and Wallet Server (VWS) is essentially the billing component of the system (this could also be provided by a third-party billing system, such as Oracle Communications Billing and Revenue Management (BRM).
  Billing provides:
  - Prepaid Rating
  - Balance Management
  - Voucher Management
  - Promotion Tracking facilities
Multiple servers configuration diagram

The system architecture can support multiple server configurations as shown in this diagram:

Note: The configuration of the VWS in a redundant pair set-up and the SLC running in an N+1 configuration. Here the SMS is set up in a redundant cluster configuration using Oracle RAC for the database component.
Chapter 1

SMS and SLC Server Operation

Operation diagram

This diagram shows the main components and operation of the SMS and SLC servers:

SLC component list

This table describes the main components for the Service Logic Controller.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charging Control Services (CCS)</td>
<td>Provides the charging control logic and tools.</td>
</tr>
<tr>
<td>Advanced Control Services (ACS)</td>
<td>Provides the real time engine for control plan execution, effectively the call processing engine.</td>
</tr>
<tr>
<td>Billing Engine Client</td>
<td>Provides the interface which processes requests from the call processing engine to the Voucher and Wallet servers.</td>
</tr>
<tr>
<td>Service Logic Execution Environment (SLEE)</td>
<td>Routes calls to the ACS and to other machines through the SLEE interfaces (TCAP and Billing Engine Client).</td>
</tr>
</tbody>
</table>

SMS component list

This list describes the main components for the Service Management System

- Centralized storage of logs, alarms, statistics.
- In-built CRM system which can be provisioned directly or externally via the provisioning interface.
- Replication method used to transfer relevant data from the main database on the SMS to the VWS and SLC servers, including:
  - Subscriber and account wallet data
  - Tariff and rate tables, for example.
VWS Server Operation

Operation diagram

This diagram shows the main components and operation of the Voucher and Wallet (VWS) server:

VWS component list

This list describes the main components for the Voucher and Wallet Server.

- The BE Synch component, which runs on each VWS, synchronizes the subscriber wallet data between the databases on the two servers, here depicted running in a redundant pair set-up.
- The BE Server component, which runs on each VWS, handles all incoming requests from the SMS and SLC client processes, and can be extended using plug-ins.
Overview

Introduction

This chapter explains the management and control of the NCC product.

In this chapter

This chapter contains the following topics.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Management and Control Overview</td>
<td>7</td>
</tr>
<tr>
<td>init Daemon Management</td>
<td>8</td>
</tr>
<tr>
<td>init Stop and Start Processes</td>
<td>9</td>
</tr>
<tr>
<td>SLEE Management</td>
<td>12</td>
</tr>
<tr>
<td>Database Management</td>
<td>15</td>
</tr>
</tbody>
</table>

Service Management and Control Overview

Introduction

The NCC solution is a group of programs, or applications, that run on Oracle's Solaris architecture (UNIX based operating system), Sun server and database.

A familiarity with UNIX and Oracle database concepts and commands is necessary to fully understand the management and control of the applications that make up the whole solution.

NCC concepts

A concept to think about when considering service management is solution redundancy.

The NCC solution uses both the $N+1$ and $2N$ concepts to increase service reliability and greatly reducing the chances of a complete Service outage. These redundancy approaches are used in the following ways:

SLC usage

The SLC (an SCP in signaling terms) nodes handle network traffic in an $N+1$ configuration.

All nodes independently handle traffic at the same time. In the case of node failure, or service interruption, the remaining node(s), have the extra capacity to handle the increased load of the unavailable node (up to the projected peak traffic load).

VWS usage

The VWS nodes work in the more traditional $2N$, or hot standby, configuration. This consists of a logical pair of servers running in a primary and secondary node configuration that are constantly updating and synchronizing themselves.

In the case of node failure or service interruption to the primary node, the secondary node provides instant and uninterrupted backup until the primary node is back in service.
SMS usage
The SMS (an SMF in signaling terms) is the exception, though Oracle can provide a redundant solution in the form of Oracle Solaris Cluster software, there is no redundancy at this time, this is outside the scope of this document.

In general though, if the SMS is not being used in a real-time, mission critical capacity, then a small amount of downtime is seen as acceptable.

Management and control methods
There are two main methods of service management and control of NCC components:

1. init daemon managed applications
   The init (short for "initialization") daemon is a core UNIX process (PID=1) that spawns all other processes. The /etc/inittab file controls the init daemon and can be used to manage running applications.

2. SLEE managed applications
   SLEE is a computing term and stands for Service Logic Execution Environment. The NCC SLEE manages a group of applications that can communicate with each other while efficiently sharing resources.

Note:
- All the NCC servers have some components that are managed by the init daemon.
- Only the SLC and VWS servers have components that are managed by the SLEE.

init Daemon Management

init daemon process
The init daemon process "is the default primordial user process" on a UNIX system (see $ man init information).

In Solaris, init initiates the core components of the Solaris service management facility (see $ man pages for svc.configd and svc.startd), and will restart these components if they fail.

Backwards compatibility
For backwards compatibility, init also starts and restarts general processes according to rules specified in the /etc/inittab file and the start/stop scripts defined in the legacy /etc/init.d and /etc/rc?.d directories (see $ man page for inittab and init.d).

inittab file
NCC uses the inittab file to manage and control a number of its daemon processes. All NCC init managed processes are configured during the installation process to be run when the server is in runlevel 3 or 4 (rstate).

$ man inittab
...skipped...
The inittab file is composed of entries that are position dependent and have the following format:
  id:rstate:action:process
NCC process identification

The easiest way to identify the NCC process which are managed by init is to search (grep command) for the "IN" string in the /etc/inittab file, which will list the process startup scripts.

$ grep "IN" /etc/inittab

Tip: The general naming convention format of the process startup scripts is the name of the running process with "Startu" on the end:

Format: process_nameStartup.sh
Example: smsAlarmRelayStartup.sh

Process running checking

To check if the process is running you use the UNIX ps command (process status – see $ man ps information) and search for the process name.

$ ps -ef | grep smsAlarmRelay

It is worthwhile becoming familiar with the NCC processes managed by init.

init Stop and Start Processes

inittab file configuration

The following are general rules you can use to control (stop and start) NCC processes configured to run in the /etc/inittab file.

- To stop a process, you edit the /etc/inittab file and for the relevant line you either; comment out (# character at start of line), or change the action field (3) from respawn to off
- To start a process, you edit the /etc/inittab file and for the relevant line you either; un-comment (remove # character at start of line), or change the action field (3) from off to respawn.
- Issuing the init q command forces an immediate reread of the inittab file.
- You must be the super-user (root) to edit the /etc/inittab file and issue the init q command.
- When a process needs to be restarted, for example after a configuration change, then the UNIX kill command can be used to terminate the running process, whereby init will detect the failed process and restart it.

Changing the run level

At times it may be necessary to stop all the NCC init managed processes at once. You can manually edit the inittab file and comment out all the NCC processes but this can be fiddly, takes time and can be prone to error.

The quickest and easiest way to stop all the processes is to simply lower the run-level of the server to state 2 (multi-user). This instructs the init daemon to stop any of it's managed processes, specified in the inittab file, that are not configured to run in this level (the rstate field).
The start and stop scripts in the `/etc/rc/state.d` directories will also run.

As mentioned earlier the NCC processes are configured to run in either states 3 or 4 so that when the `init 2` command is run (instructs the init daemon to move into run-level 2), then init will automatically terminate all its managed processes that are not configured to run in this new level.

To automatically restart these stopped processes again, you move back into run-level 3 with the `init 3` command.

You must be super-user to change the server run-level.

Generally speaking you would only ever want to do use this method during platform maintenance, be it either; application, database, or server related interventions.

**Example - updateLoader**

Follow these steps to stop and start the updateLoader process.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1    | Become the root user, enter:  
       $ su - root  
       Password: *******  
       Sourcing `/etc/profile.ORAN` |
| 2    | Check the updateLoader process is running, enter:  
       `ps -ef | grep update`  
       `smf_oper: 850  1  0  Oct 04 0:22  
       /IN/service_packages/SMS/bin/updateLoader -nodeid 301  
       root 19354 19349 0 22:34:08 pts/1 0:00 grep update` |
| 3    | Edit (use your preferred text editor) the `/etc/inittab` file and comment out (add the `#` character to beginning of line) the `updateLoaderStartup.sh` entry and save the change.  
       `vi /etc/inittab`  
       `...skipped...`  
       `#scp5:34:respawn:su - smf_oper -c "exec  
       /IN/service_packages/SMS/bin/updateLoaderStartup.sh >>  
       /IN/service_packages/SMS/tmp/updateLoader.log 2>&1" > /dev/null 2>&1  
       0<&1`  
       `[Esc]`  
       `:wq`  
       `"/etc/inittab" 36 lines, 3045 characters` |
| 4    | Tell init to reread the inittab file:  
       `init q` |
| 5    | Check the updateLoader process has stopped:  
       `ps -ef | grep update`  
       `root 19431 19349 0 22:40:06 pts/1 0:00 grep update` |
| 6    | Edit the `/etc/inittab` file and remove the `#` from the `updateLoaderStartup.sh` entry and save the change:  
       `vi /etc/inittab`  
       `...skipped...`  
       `scp5:34:respawn:smf_oper -c "exec  
       /IN/service_packages/SMS/bin/updateLoaderStartup.sh >>  
       /IN/service_packages/SMS/tmp/updateLoader.log 2>&1" > /dev/null 2>&1  
       0<&1`  
       `[Esc]`  
       `:wq`  
       `"/etc/inittab" 36 lines, 3045 characters` |
| 7    | Tell init to reread the inittab file:  
       `init q` |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 8    | Check the updateLoader process has started and is running again:  
  
  ```bash
  ps -ef | grep update
  smf_oper 19475 1 0 22:42:43 ? 0:00
  /IN/service_packages/SMS/bin/updateLoader -nodeid 301
  root 19566 19349 0 22:42:45 pts/1 0:00 grep update
  ```  |

  **Example - smsMaster**

  Follow these steps to restart the smsMaster process.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1    | Check the smsMaster process are running:  
  
  ```bash
  $ ps -ef | grep smsMaster
  smf_oper 978 1 0 Oct 04 ? 9:28
  /IN/service_packages/SMS/bin/smsMaster -c
  smf_oper 1299 978 1 Oct 04 ? 653:19
  /IN/service_packages/SMS/bin/smsMaster -c
  smf_oper 6138 3205 0 00:21:04 pts/1 0:00 grep smsMaster
  ```  |

  **Note:** The second (Process ID or PID) and third columns (Parent PID or PPID) of the output. The PPID of 1, on the first line, denotes it as the init process and the smsMaster process is a child process. The second smsMaster listed is child process of the first one as its PPID matches the first lines PID.

| 2    | As the smsMaster process owner (smf_oper) terminate the process with the kill command (signal the process to stop running, or exit):  
  
  ```bash
  $ kill 978
  ```  |

  **Note:**  
  As PID 978 is the parent process, the child process will inherit the SIGTERM signal (kill command's default signal (either; -TERM, or -15 switch)) from its parent. It would be okay to specify both PIDS. Using the SIGTERM signal is best practice as it allows the child and parent processes to cleanup and close files before terminating itself.  
  
  The super-user root has global ownership permissions allowing it to send signal to any process.

| 3    | Check that the init daemon has instantly restarted the smsMaster process:  
  
  ```bash
  $ ps -ef | grep smsMaster
  smf_oper 6173 1 0 00:23:06 ? 0:01
  /IN/service_packages/SMS/bin/smsMaster -c
  smf_oper 6188 6173 1 00:23:06 ? 0:24
  /IN/service_packages/SMS/bin/smsMaster -c
  smf_oper 6800 3205 0 00:41:09 pts/1 0:00 grep smsMaster
  ```  |

  **Tip:** If either of the previous smsMaster processes are still listed then this may indicate that the process is hung or stuck and may need a more forceful shutdown signal. If this is the case then the SIGKILL signal (either; -KILL or -9 switch) is recommended.  
  
  ```bash
  $ kill -9 978 1299
  ```
SLEE Management

Introduction

The SLC and VWS servers have components that are managed by the NCC SLEE. Even though the services run on both these platforms are completely different, the concepts for how they are controlled are exactly the same.

In a nutshell, the SLEE provides a common environment for multiple different service logic applications to run in and simultaneously manage and communicate events between themselves in an orderly way, while interfacing with multiple external networks and/or applications.

SLEE control

Control of the SLEE is managed by a utility called SLEE Control and the command to use it is `slee-ctrl`.

The `slee-ctrl` tool provides the ability to stop, start, or restart the SLEE and, among other things, will verify that all SLEE processes were started, or have actually been stopped.

Basically it is a wrapper script that provides the user with extra checks and protection from causing issues. It still calls the SLEE start and stop scripts, all the while avoiding the pitfalls that inexperienced operators may have.

`slee-ctrl` simplifies SLEE control:

- Only one command name to remember.
- No need to remember which UNIX user you must be (it will remind you if it's wrong).
- One valid SLEE_USER must be configured and only this user or super-user root can run the start, stop, or restart commands.
- Do not need to remember the location or names of the SLEE start and stop scripts.
- Do not have to be in the `/IN/service_packages/SLEE/bin` directory to run the command.
- Verifies that all SLEE instance processes are terminated when the stop command issued.
- Verifies that no other SLEE instance processes are running when the start command issued.
- List the current process status of SLEE applications.
- Access to the SLEE check command which displays internal SLEE resource usage.
- Provides an audit trail by logging a history of when `slee-ctrl` commands were run.

`slee-ctrl` modes of operation

The `slee-ctrl` tool has two modes of use:

- Command line
- Interactive session mode

Documentation for `slee-ctrl` is in the form of a manual page. It is recommended that you read this to understand the full capabilities of the tool (enter `man slee-ctrl`). Also try entering `slee-ctrl help` on the command line for a full list of valid commands.

Example VWS start up

To start the VWS SLEE on the command line, enter:

```
$ su - ebe_oper
Password: 
$ slee-ctrl start
```

SLEE Control: v,1.0.11: script v,1.21: functions v,1.48: pslst v,1.118
Example SLC stop

To stop the SLC SLEE in session mode, enter:

```
$ su -.acs_oper
Password:
$ slee-ctrl
```

SLEE Control: v,1.0.11: script v,1.21: functions v,1.48: pslist v,1.118

User acs_oper; session [16893]; terminal pts/2; started Wed Oct 27 03:41:57 GMT 2010

The following variables are set and will be used to run the SLEE.

- SLEE_USER: acs_oper
- SLEE_SCRIPT: /IN/service_packages/SLEE/bin/slee.sh
- SLEE_CONFIG: /IN/service_packages/SLEE/etc/SLEE.cfg
- SLEE_LOG: /IN/service_packages/SLEE/tmp/SLEE.log

Type help at prompt for valid commands.

```
[acs_oper] slee-ctrl> stop
```

Type "yes" if you are sure: yes

```
Info: slee_ctrl_lock_file: lock file created for "stop" command.
Info: slee_ctrl_stop: 20101027-03:42:40 GMT: Running SLEE stop.sh...
Oct 27 03:42:40 stop(17106) SleeRoot::shutdown()=9 sleeRoot.cc@883: SLEE Shutdown
SLEE: Using shared memory offset: 0xc0000000
SleeRoot: Shutting Down...
SleeRoot: SIGUSR1 Watchdog (PID 14290).
SleeRoot: Disable all services...
SleeRoot: ...done
SleeRoot: Send management end to all interfaces...
SleeRoot: ...done
SleeRoot: Send management end to all applications...
SleeRoot: ...done
SleeRoot: Wait to allow service/application completion...
SleeRoot: ...done
SleeRoot: Kill all interfaces...
SleeRoot: SIGKILL Interface (PID 14262).
...skipped...
SleeRoot: SIGKILL Interface (PID 14289).
SleeRoot: ...done
SleeRoot: Kill all applications...
SleeRoot: SIGKILL Application (PID 14251).
...skipped...
SleeRoot: SIGKILL Application (PID 14261).
SleeRoot: ...done
SleeRoot: Delete semaphore manager.
```
SleeRoot: Delete shared memory.
SleeRoot: All Done.
Info: slee_ctrl_clean: cleaning SLEE shared memory and semaphores...
Info: slee_verify_stop: Verifying all SLEE process(es) have stopped...
Info: slee_verify_stop: No running SLEE processes found.
Info: slee_verify_stop: /IN/service_packages/ACS/.slee_file deleted.
Info: slee_ctrl_lock_file: lock file deleted for "stop" command.

Note: In session mode you are prompted to type in yes if you want to stop or restart the SLEE. This safety check is not enforced when run from the command line.

Example VWS smf_oper restart

To restart the VWS SLEE as the smf_oper user, enter:

$ slee-ctrl restart

SLEE Control: v,1.0.11: script v,1.21: functions v,1.48: pslist v,1.18

Example stopped processes check

To check the status of the SLEE stopped processes, enter:

[acs_oper] slee-ctrl> status

Note: The vssp process has not be found in this example indicating that it is not running. A further manual check for the vssp process could be made using the UNIX ps command to verify the output.

$ ps -ef | grep vssp
acs_oper 19976  1586   0 03:59:29 pts/2 0:00 grep vssp

Example monitor SLEE resources

To monitor the internal SLEE resource usage with check, enter:

[acs_oper] slee-ctrl> check 1 5
Chapter 2, Service Management and Control

SLEE: Using shared memory offset: 0xc0000000

<table>
<thead>
<tr>
<th>Time</th>
<th>Dialogs</th>
<th>Apps</th>
<th>AppIns</th>
<th>Servs</th>
<th>Events</th>
<th>Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>04:16:29</td>
<td>70000</td>
<td>24</td>
<td>240</td>
<td>16</td>
<td>207051</td>
<td>25000</td>
</tr>
<tr>
<td>04:16:30</td>
<td>70000</td>
<td>24</td>
<td>240</td>
<td>16</td>
<td>207051</td>
<td>25000</td>
</tr>
<tr>
<td>04:16:31</td>
<td>70000</td>
<td>24</td>
<td>240</td>
<td>16</td>
<td>207051</td>
<td>25000</td>
</tr>
<tr>
<td>04:16:32</td>
<td>70000</td>
<td>24</td>
<td>240</td>
<td>16</td>
<td>207051</td>
<td>25000</td>
</tr>
<tr>
<td>04:16:33</td>
<td>70000</td>
<td>24</td>
<td>240</td>
<td>16</td>
<td>207051</td>
<td>25000</td>
</tr>
</tbody>
</table>

[acs_oper] slee-ctrl>

Note: The check command is a separate SLEE utility located in /IN/service_packages/SLEE/bin directory. Use check -h to see a brief description of usage. For more detail on the check utility refer to the SLEE Technical Guide.

Corrupt memory symptom

If the SLEE's shared memory becomes corrupted, for whatever reason, you may find, when you try stopping the SLEE, it will hang.

As a rule of thumb, if it takes longer than 15 seconds to stop the SLEE, it is quite likely to have hung. You need to press Ctrl C to return to the command line prompt.

If you come across this scenario, use the slee-ctrl stop abort command. This will send a terminate signal (kill -TERM) to any running SLEE processes, wait 3 seconds, then send a kill signal (kill -KILL) to any remaining SLEE processes still running (if any). For example:

[ebe_oper] slee-ctrl> stop abort

Always try the stop command first before trying the stop abort command.

Run levels

The servers that have the SLEE component installed are configured with an /etc/rc3.d start script and /etc/rc1.d stop script.

This means that on boot up the server should come up and automatically move to a state where it can handle traffic without operator intervention. You may notice that unlike the init managed processes the SLEE will not be stopped in run-level 2. This is done to prevent any unnecessary stopping of the SLEE that could cause interruption to live traffic.

If system administrators want to change this behavior then find the rc scripts as follows:

```bash
# find /etc/init.d /etc/rc?.d -name \"slee
/etc/init.d/slee
/etc/rc1.d/K01slee
/etc/rc3.d/S99slee
#
```

Warning: If reconfiguring these rc scripts then you must follow this rule:

The SLEE must be started after the database and must be stopped before the database.

If the SLEE is not stopped before the database then the database shutdown will hang due to SLEE processes having open shadow connections.

Database Management

Introduction

The database is an integral part of the NCC solution and the majority of the NCC applications have a dependency on it being available before they are able to start.
The solution design has the SMS database as the master data store. The SLC and VWS databases are replicated nodes containing the same data, or in some cases subset of data, that the master SMS node contains.

Currently this is a NCC specific application and is often simply referred to as replication.

Note: The VWS database also has its own set of special tables (BE_% tables) that are not part of the replicated set of SMS tables. The VWS BE_% tables contain a near real-time persistent store of billing data.

Oracle System IDs

This table shows the unique instance names or Oracle System IDs (ORACLE_SID) of each server database.

<table>
<thead>
<tr>
<th>Server</th>
<th>Oracle SID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>SMF</td>
</tr>
<tr>
<td>SLC</td>
<td>SCP</td>
</tr>
<tr>
<td>VWS</td>
<td>E2BE</td>
</tr>
</tbody>
</table>

Database verification

The simple way to verify the database is okay and that the NCC processes can connect to it is to start an sqlplus session, enter:

```
$ su – smf_oper
Password: 
$ sqlplus /
```

SQL*Plus: Release 11.2.0.3.0 - Production on Wed Oct 27 21:00:41 2010
Copyright (c) 1982, 2007, Oracle. All Rights Reserved.

Connected to:  
Oracle Database 11g Release 11.2.0.3.0 - 64bit Production

SQL> quit
Disconnected from Oracle Database 10g Release 11.2.0.3.0 - 64bit Production
$

The database on each server component is configured to start at boot time by the init daemon when the Server passes through run-level 2 using the /etc/rc2.d/S99oracle script.

Note: As discussed earlier, the NCC processes are configured to start in run-level 3. This ensures that the database is available before the NCC processes start. It also has the added advantage that going to run-level 2 stops the NCC processes but does not shut down the database.

Shadow connections

If the database needs to be shut down for maintenance, before this can happen, all connections to the database (often referred to as shadow connections) must be disconnected first.

This means that all the NCC processes (init and SLEE managed) must be shut down.

An easy way to check for shadow connections to the database (without connecting to the database) is using the UNIX ps command. Enter:

```
$ ps -ef | grep oracle.*LOCAL
```

<table>
<thead>
<tr>
<th>User</th>
<th>PPID</th>
<th>PID</th>
<th>Username</th>
<th>Group</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle</td>
<td>1116</td>
<td>1</td>
<td>oracle</td>
<td>oracle</td>
<td>0:00 oracleSCP (LOCAL=NO)</td>
</tr>
<tr>
<td>oracle</td>
<td>1106</td>
<td>1</td>
<td>oracle</td>
<td>oracle</td>
<td>0:29 oracleSCP (LOCAL=NO)</td>
</tr>
<tr>
<td>oracle</td>
<td>19564</td>
<td>1</td>
<td>oracle</td>
<td>oracle</td>
<td>0:00 oracleSCP (LOCAL=NO)</td>
</tr>
</tbody>
</table>
Note: The Parent PID (PPID) are always 1 for shadow connections and in this example the process name, oracleSCP, shows the SID of the database indicating it is a SLC server.

Database shutdown

Follow these steps to shut down the database (and listeners) on an NCC server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1    | Stop the SLEE on SLC or VWS servers only.  
Start at step 2 for the SMS servers:  
$ slee-ctrl stop  
SLEE Control: v,1.0.11: script v,1.21: functions v,1.48: pslist v,1.118  
[acs_oper] slee-ctrl> stop  
...skipped... |
| 2    | Stop the all NCC init managed processes by putting the server into run-level 2 (root user):  
$ su -  
Password:  
Sourcing /etc/profile.GRA  
$ init 2 |
| 3    | Verify that all NCC processes have stopped using the pslist command:  
$ pslist  
C APP USER PID PPID STIME COMMAND  
0 ACS Did not match regex: /acs_oper.*"/IN\service_packages\ACS\bin\acsStatsMaster( \$)+/  
0 ACS Did not match regex: /acs_oper.*"/IN\service_packages\ACS\bin\cmnPushFiles( \$)+/  
0 SLEE Did not match regex: /_oper.*"/IN\service_packages\ACSUSC\bin\slee_acs( \$)+/  
0 SLEE Did not match regex: /_oper.*"/IN\service_packages\ACSUSC\bin\slee_acsLocalSLEE( \$)+/  
0 SLEE Did not match regex: /_oper.*"/IN\service_packages\E2BE\bin\BeClient( \$)+/  
0 SLEE Did not match regex: /_oper.*"/IN\service_packages\LCP\bin\locApp( \$)+/  
0 SLEE Did not match regex: /_oper.*"/IN\service_packages\OSD\bin\osdInterface( \$)+/  
.  
.  
.  
0 UIS Did not match regex: /uis_oper.*"/IN\service_packages\UIS\bin\cmnPushFiles( \$)+/  
0 XMS Did not match regex: /smf_oper.*"/IN\service_packages\XMS\bin\oraPStoreCleaner( \$)+/  
total processes found = 0 [ 31 expected, 31 not found ]  
================================= run-level 2 =====================

...skipped...
Chapter 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Verify no shadow connections exist:</td>
</tr>
<tr>
<td></td>
<td>$ ps -ef</td>
</tr>
<tr>
<td></td>
<td>root 29128 29059   0 22:07:40 pts/2       0:00 grep oracle.*LOCAL</td>
</tr>
<tr>
<td></td>
<td>#</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you do find any shadow connections but no NCC processes are running then someone, or something else has got an open connection to the database. It might just be an sqlplus session someone has open. Finding out who, or what, is outside the scope of this procedure but the shadow connection will have to be disconnected before running database shutdown.</td>
</tr>
<tr>
<td>5a</td>
<td>Shut down the database (method 1):</td>
</tr>
<tr>
<td></td>
<td>$ /etc/init.d/oracle stop</td>
</tr>
<tr>
<td></td>
<td>Stopping Oracle:</td>
</tr>
<tr>
<td></td>
<td>Sourcing /etc/profile.ORA</td>
</tr>
<tr>
<td></td>
<td>LSNRCTL for Solaris: Version 10.2.0.4.0 - Production on 27-OCT-2010 23:09:39</td>
</tr>
<tr>
<td></td>
<td>Copyright (c) 1991, 2007, Oracle. All rights reserved.</td>
</tr>
<tr>
<td></td>
<td>Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(PORT=1521)))</td>
</tr>
<tr>
<td></td>
<td>The command completed successfully</td>
</tr>
<tr>
<td></td>
<td>Sourcing /etc/profile.ORA</td>
</tr>
<tr>
<td></td>
<td>Processing Database instance &quot;SCF&quot;: log file /u01/app/oracle/product/10.2/shutdown.log</td>
</tr>
<tr>
<td></td>
<td>#</td>
</tr>
<tr>
<td>5b</td>
<td>Shut down the database (method 2) - changing to the oracle user and running the dbshut command, as follows:</td>
</tr>
<tr>
<td></td>
<td>$ su - oracle</td>
</tr>
<tr>
<td></td>
<td>$ dbshut</td>
</tr>
<tr>
<td></td>
<td><strong>as above...</strong></td>
</tr>
<tr>
<td>6</td>
<td>Verify the oracle database processes are not running:</td>
</tr>
<tr>
<td></td>
<td>$ ps -ef</td>
</tr>
<tr>
<td></td>
<td>root 29587 29059   0 22:59:00 pts/2       0:00 grep ora_</td>
</tr>
<tr>
<td></td>
<td>#</td>
</tr>
</tbody>
</table>
Database startup

Follow these steps to start the database (and listeners) and NCC components. This is simply a reverse of the database shutdown procedure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>Start the database (method 1): &lt;br&gt; $ su -&lt;br&gt; Password:&lt;br&gt; $ /etc/init.d/oracle start&lt;br&gt; Starting Oracle:&lt;br&gt; Sourcing /etc/profile.ORA&lt;br&gt; LSNRCTL for Solaris: Version 11.2.0.3.0 - Production on 27-OCT-2010 23:13:59&lt;br&gt; Copyright (c) 1991, 2007, Oracle. All rights reserved.&lt;br&gt; Starting /u01/app/oracle/product/11.2/bin/tnslsnr: please wait...&lt;br&gt; TNSLSNR for Solaris: Version 11.2.0.3.0 - Production System parameter file is /u01/app/oracle/product/11.2/network/admin/listener.ora Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=testslc)(PORT=1521))) Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=testslc)(PORT=1521))) STATUS of the LISTENER ------------------------ Alias LISTENER Version TNSLSNR for Solaris: Version 11.2.0.3.0 - Production Start Date 27-OCT-2010 23:13:59 Uptime 0 days 0 hr. 0 min. 0 sec Trace Level off Security ON: Local OS Authentication SNMP OFF Listener Parameter File /u01/app/oracle/product/11.2/network/admin/listener.ora Listening Endpoints Summary... (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=testslc)(PORT=1521))) Services Summary... Service &quot;SCP&quot; has 1 instance(s). Instance &quot;SCP&quot;, status UNKNOWN, has 1 handler(s) for this service... The command completed successfully Sourcing /etc/profile.ORA Processing Database instance &quot;SCP&quot;: log file /u01/app/oracle/product/11.2/startup.log * Note: another valid db startup method is</td>
</tr>
<tr>
<td>1b</td>
<td>Start the database (method 2) - changing to the oracle user and running the dbstart command, as follows: &lt;br&gt; $ su - oracle&lt;br&gt; $ dbstart&lt;br&gt; as above...</td>
</tr>
</tbody>
</table>
| 2    | You would expect to see the following running database processes: <br> $ ps -ef | grep ora_<br> oracle 33 1 0 23:21:18 ? 0:01 ora_pmon SCP<br> oracle 43 1 0 23:21:18 ? 0:01 ora_cckptSCP<br> oracle 49 1 0 23:21:18 ? 0:01 ora_mmon SCP<br> root 117 29059 0 23:34:47 pts/2 0:00 grep ora_<br> oracle 56 1 0 23:21:31 ? 0:02 ora_cjq0 SCP<br> oracle 35 1 0 23:21:18 ? 0:00 ora_psp0 SCP<br> oracle 51 1 0 23:21:18 ? 0:00 ora_mmn1 SCP<br> oracle 47 1 0 23:21:18 ? 0:00 ora_reco SCP<br> oracle 39 1 0 23:21:18 ? 0:00 ora_dbw0 SCP<br> oracle 45 1 0 23:21:18 ? 0:01 ora_smn SCP<br> oracle 37 1 0 23:21:18 ? 0:01 ora_mman SCP<br> oracle 41 1 0 23:21:18 ? 0:00 ora_lgwr SCP
You may verify the database instance is accepting connections:

```
$ su - smf_oper -c "echo exit |sqlplus /"
```

Sourcing /etc/profile.ORA


Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Connected to:
Oracle Database 11g Release 11.2.0.3.0 - 64bit Production

SQL> Disconnected from Oracle Database 11g Release 11.2.0.3.0 - 64bit Production

Starting the remaining NCC components should occur (dependent on SLEE rc?.d script rules) by putting the server back into run level 3.

$ init 3

Shutting down the Sun Server

The procedure to shut down a Sun server is not be discussed in great detail here as System Administrators generally have their own procedures that they like to follow to do this.

What is suggested is a method that may be followed.

It is recommended that the system administrators who maintain the NCC servers create and test a detailed server shutdown procedure that meets their needs.

The general steps include:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shut down the NCC applications and database (as previously described).</td>
</tr>
<tr>
<td>2</td>
<td>Make a connection to the Sun server console (specific to the Server and network setup).</td>
</tr>
<tr>
<td>3</td>
<td>Issue a server shutdown command to stop the operating system (for example init 0).</td>
</tr>
<tr>
<td>4</td>
<td>Power server off (refer to Sun Server documentation).</td>
</tr>
</tbody>
</table>

Starting the Sun Server

The procedure to start a Sun server can be dependent on the setup of the server and the procedures that system administrators may like to use for the servers they maintain.

Standard practice for the NCC servers would be for the Solaris operating system to boot up when the server is powered on.

It will be configured to bring the system up to run-level 3 with a running database and NCC components, as per the Solaris service management facility, including the legacy /etc/inittab, /etc/rc?.d scripts.
Overview

Introduction
This chapter gives some hints and tips for system administrators to manage the NCC product.

In this chapter

This chapter contains the following topics.

- Monitoring and Managing Overview
- Software Version Levels
- Running Processes
- SLEE Resource Usage
- Rolling Snoop Archives
- Rolling Snoop Risks

Monitoring and Managing Overview

Overview

For system administrators new to the NCC solution, the monitoring and managing of the solution can seem a little daunting due to the large number of different processes and potentially complex interactions with different network types and services.

Like anything though, the more you use it and the more familiar it becomes and the easier it gets.

The aim of this chapter is to introduce some common tools and aids to help administrators become more comfortable in monitoring the solution without getting involved with the technical detail of each component and its operation.

Software Version Levels

Base components

The NCC base components, or applications, and NCC application patches are installed on the system using the pkgadd command; the Solaris software package management facility utility.

The way to display information about the installed software packages is with the pkginfo command.

Basic pkginfo command

When the pkginfo command is used by itself, it will list every software package currently installed on the system.

You can filter this software list, so that only the NCC packages will be listed, by specifying the -a (architecture) switch along with the string sun4u.
It is useful to also specify the -x (version) switch to see the version number of the base applications as this is not listed in the pkginfo output by default.

Example output
The following example output displays the NCC software levels as generated on a VWS. Enter:

$ pkginfo -xa sun4u
Response:

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLEE</td>
<td>Oracle SLEE Installation</td>
<td>(sun4u) 3.2.0.24</td>
</tr>
<tr>
<td>acsBe</td>
<td>ACS Installation</td>
<td>(sun4u) 2.4.3.4</td>
</tr>
<tr>
<td>beBe</td>
<td>BE (for BE) Installation</td>
<td>(sun4u) 2.4.0.24</td>
</tr>
<tr>
<td>ccsBe</td>
<td>CCS (for BE) Installation</td>
<td>(sun4u) 3.1.8.3</td>
</tr>
<tr>
<td>dapExtras</td>
<td>Oracle dapExtras</td>
<td>(sun4u) 2.1.0.4</td>
</tr>
<tr>
<td>slee-ctrl</td>
<td>Oracle SLEE Control Tool</td>
<td>(sun4u) 2.0.0.0</td>
</tr>
<tr>
<td>smsExtras</td>
<td>SMS Installation</td>
<td>(sun4u) 3.1.2.8</td>
</tr>
<tr>
<td>supportBe</td>
<td>Oracle Support Tools</td>
<td>(sun4u) 2.0.0.0</td>
</tr>
</tbody>
</table>

Running Processes

Overview
In the UNIX world a running application, or program, is referred to as a process.

Basically a process is the active instance of the running program that the operating system is allocating system resources to, allowing it to execute instructions.

In the UNIX environment the ps command (see man ps) is used to generate a snapshot report of the current status of process(es) and hence how you can tell that an application is running.

Complex environments
In a complex environment, where multiple running processes making up an application suite, the trick is knowing which processes to identify.

To do this you would need to distinguish each NCC daemon that is configured to run in the /etc/inittab file and the SLEE configuration file (SLEE.cfg).

The use of start-up scripts can further complicate this task, requiring each script to be checked for the executable binary file name.

To simplify this task the NCC support tools package provides a utility called pslist that, among other things, will identify and quickly verify the status of the NCC processes running on the platform.

pslist command
The pslist command uses a process list configuration (.plc) file containing regular expressions of the relevant NCC processes that are matched against the ps -ef command output. Enter:

$ pslist
Response:

---------- Tue Nov 23 01:03:46 GMT 2010 ----------
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Time</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACS</td>
<td>acs_oper</td>
<td>1004</td>
<td>04-Oct /IN/service_packages/ACS/bin/acsCompilerDaemon</td>
</tr>
<tr>
<td>ACS</td>
<td>acs_oper</td>
<td>1008</td>
<td>04-Oct IN/service_packages/ACS/bin/acsProfileCompiler</td>
</tr>
<tr>
<td>ACS</td>
<td>acs_oper</td>
<td>7553</td>
<td>28-Oct rvice_packages/ACS/bin/acsStatisticsDBInserter</td>
</tr>
<tr>
<td>CSD</td>
<td>ccs_oper</td>
<td>1047</td>
<td>04-Oct IN/service_packages/OSD/bin/ccsCDRReplayer</td>
</tr>
<tr>
<td>CCS</td>
<td>ccs_oper</td>
<td>1011</td>
<td>04-Oct /IN/service_packages/CCS/bin/ccsCDRFileGenerator</td>
</tr>
<tr>
<td>CCS</td>
<td>ccs_oper</td>
<td>1033</td>
<td>04-Oct N/service_packages/CCS/bin/ccsCDRFileGenerator</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>1406</td>
<td>104-Oct /IN/service_packages/CCS/bin/ccsProfileDaemon</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>943</td>
<td>04-Oct IN/service_packages/CCS/bin/ccsChangeDaemon</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>946</td>
<td>04-Oct IN/service_packages/SMS/bin/smsAlarmManager</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>947</td>
<td>04-Oct IN/service_packages/SMS/bin/smsAlarmDaemon</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>948</td>
<td>04-Oct IN/service_packages/SMS/bin/smsStatsThreshold</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>949</td>
<td>04-Oct IN/service_packages/SMS/bin/smsTaskAgent</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>969</td>
<td>04-Oct IN/service_packages/SMS/bin/smsTrigDaemon</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>979</td>
<td>04-Oct IN/service_packages/SMS/bin/smsConfigDaemon</td>
</tr>
<tr>
<td>SMS</td>
<td>smf_oper</td>
<td>980</td>
<td>04-Oct IN/service_packages/SMS/bin/smsStatsDaemonRep</td>
</tr>
</tbody>
</table>

Note: The listed output is from a SMS platform and is grouped by user and application components.

### Default plc file

When a UNIX user first runs the pslist command without command line options it will automatically generate a default .plc file by scanning the `/etc/inittab` and `/IN/service_packages/SLEE/etc/SLEE.cfg` file, if existing.

The user’s default .plc file can be viewed with the pslist `-v` command line option. Enter:

```
$ pslist -v
```

Response:

```
[[/[IN/service_packages/ACS/tmp/ps_processes.telco-p-slc01.plc]

# pslist: default process list configuration (plc) file used to match and 
# display running processes.
# File creation time: Tue Nov 23 01:58:39 GMT 2010
# Lines beginning with a hash (#) character are ignored.
# $1="grouped-apps name (max 5-char)" $2="regex of process" [$3+=comments] 

#******************************************************************************
ACS acs_oper.*/IN/service_packages/ACS/bin/acsStatsMaster inittab
ACS acs_oper.*/IN/service_packages/ACS/bin/acsStatsLocalSLEE inittab
ACS acs_oper.*/IN/service_packages/ACS/bin/acsStatsReplayer inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsMaster inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsNamingServer inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsReportsDaemon inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsReportScheduler inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsStatsAgent inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsStatsDaemon inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsStatsDaemonRep inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsTrigDaemon inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsTrigDaemon inittab
SMS smf_oper.*/IN/service_packages/SMS/bin/smsTrigDaemon inittab
sms smf_oper.*/IN/service_packages/SMS/bin/smsUpdateLoader inittab
UIS uis_oper.*/IN/service_packages/UIS/bin/UssdMfileD inittab
UIS uis_oper.*/IN/service_packages/UIS/bin/UssdMfileD inittab
XMS smf_oper.*/IN/service_packages/XMS/bin/oraPStoreCleaner inittab
SLEE .*_oper.*/IN/service_packages/ACS/bin/acsStatsLocalSLEE
SLEE .*_oper.*/IN/service_packages/ACS/bin/acsStatsReplayer
SLEE .*_oper.*/IN/service_packages/ACS/bin/acsStatsTracker
SLEE .*_oper.*/IN/service_packages/SLEE/bin/watchdog
SLEE .*_oper.*/IN/service_packages/SLEE/bin/alarmIF
SLEE .*_oper.*/IN/service_packages/SLEE/bin/replicationIF
SLEE .*_oper.*/IN/service_packages/SLEE/bin/timerIF
SLEE .*_oper.*/IN/service_packages/SLEE/bin/xmlTcapInterface
```

ps_processes.telco-p-slc01.plc: END

[Press space to continue, q to quit, h for help]
SLEE against init

There is an important distinction to make for the processes that are managed by either the init daemon or SLEE.

Each of the init managed processes is an independent daemon and can easily be turned on and off by editing the `/etc/inittab` file.

When started, the SLEE creates a common backbone that ties a group of applications together.

The main point is that you can individually configure init managed processes to run, but for SLEE managed processes, they are either all or none running.

pslist SLEE only example

The following pslist example is taken on a VWS and shows running SLEE processes, but no running init managed processes. Enter:

```
$ pslist
```

Response:

```
------------------------ Tue Nov 23 02:48:46 GMT 2010 ------------------------
C APP USER PID PPID STIME COMMAND
 1 SLEE ebe_oper 16139  1 02:23:25 /IN/service_packages/SLEE/bin/timerIF
 1 SLEE ebe_oper 16143  1 02:23:25 /IN/service_packages/E2BE/bin/beVWARS
 1 SLEE ebe_oper 16156  1 02:23:25 /IN/service_packages/E2BE/bin/beSync
 1 SLEE ebe_oper 16157  1 02:23:25 /IN/service_packages/E2BE/bin/beServer
 4 SLEE ebe_oper 16166  1 02:23:25 /IN/service_packages/E2BE/bin/beGroveller
 1 SLEE ebe_oper 16178  1 02:23:26 /IN/service_packages/SLEE/bin/replicationIF
 1 SLEE ebe_oper 16179  1 02:23:26 /IN/service_packages/DAP/bin/dapIF
 1 SLEE ebe_oper 16182  1 02:23:26 /service_packages/E2BE/bin/beEventStorageIF
 1 SLEE ebe_oper 16183  1 02:23:26 /service_packages/E2BE/bin/beServiceTrigger
 1 SLEE ebe_oper 16184  1 02:23:26 /service_packages/E2BE/bin/beEventStorageIF
 1 SLEE ebe_oper 16185  1 02:23:26 /IN/service_packages/SLEE/bin/watchdog
 0 CCS Did not match regex: /ccs_oper.*.bin\/*updateLoader\( |$\)+/
 0 CCS Did not match regex: /ccs_oper.*.bin\/*updateLoader\( |$\)+/
 0 CCS Did not match regex: /ccs_oper.*.bin\/*ccsMFileCompiler\( |$\)+/
 0 CCS Did not match regex: /ccs_oper.*.bin\/*ccsMFileCompiler\( |$\)+/
 0 E2BE Did not match regex: /be_oper.*.bin\/*beCDRMover\( |$\)+/
 0 E2BE Did not match regex: /be_oper.*.bin\/*beCDRMover\( |$\)+/
 0 SMS Did not match regex: /sms_oper.*.bin\/*smsAlarmDaemon\( |$\)+/
 0 SMS Did not match regex: /sms_oper.*.bin\/*smsAlarmDaemon\( |$\)+/
 0 SMS Did not match regex: /sms_oper.*.bin\/*smsStatsDaemon\( |$\)+/
 0 SMS Did not match regex: /sms_oper.*.bin\/*smsStatsDaemon\( |$\)+/
total processes found = 29 [ 38 expected, 9 not found ]
```

Note: The count column (C) is 0 for the processes that were not matched and the total processes found output highlights that the expected number of processes were not matched. In this case there is a clue on the bottom line as to why the init managed processes are not running.

Expected against Not Found processes

It is worthwhile noting that the expected and not found counts are only an estimate of the number of processes missing.

Some processes may spawn multiple child processes that may have the same process name (for example, PI processes on the SMS) making it impossible to accurately predict how many processes are expected or not found.

Recreate default plc file

If changes are made to the platform and the running services then it may be necessary to re-create the default plc file.

You can do this using the pslist -d option.
Warning: Only processes that are configured to run will be added to the default .plc file. For example, if a /etc/inittab process is commented out, or set to off, then when the pslist-d command is run the commented entry will not be added to the list.

Another option is to become root user and run pslist -xy to delete all user’s default .plc file. The next time a user runs the pslist command, it will automatically re-create a default .plc file.

pslist syntax

To see a full list of supported command line options, with a brief description, use pslist -h (help) option or man pslist for full documentation on pslist usage.

Syntax:

pslist -[acCehiqrRstvxyz] [-d (esg|slee|init)] [-S SLEE config] [-f .plc file] [-u user] [-k (1|9|15)] [-l (1|2)] [regex (app-name|process name)]

pslist parameters

This table gives a brief description of the supported options.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -d        | Creates the default process list configuration [~user/tmp/ps_processes.hostname.plc] file. Valid hostname arguments are:   
  • esg scan both the inittab and SLEE config files (default)   
  • slee scan the defined SLEE configuration file   
  • init[tab] scan the /etc/inittab file |
| -r        | Displays system resource use information (for example. %cpu, %memory). |
| -s        | Scans the SLEE config file and prints the status of the matched process(es). |
| -i        | Scans /etc/inittab file for start-up scripts and prints the status of the matched process(es). |
| -e        | Scans both the defined SLEE config file and the /etc/inittab file and prints the status of the matched process(es). |
| -c        | Clustered SMS option that creates a temporary .plc file to list cluster managed processes (requires scstat command). |
| -f        | Specify a process list configuration (.plc) file different to the default one. [~user/tmp/ps_processes.hostname.plc]. |
| -S        | Specify a different SLEE config file. |
| -u        | Specify a different user as the process owner (can be regex). |
| -C        | The output in the COMMAND column is not trimmed so the full command line is displayed. |
| -a        | Displays the command line arguments of matched process(es) (SunOS only). |
| -q        | No output in quiet mode. The exit value is the count of the matched processes (up to a maximum of 99). |
| -t        | Displays a process tree of PPID and COMMAND (SunOS only). |
| -v        | View the process list configuration (.plc) file. |
| -x        | Ask to remove any default process list configuration files (ps_processes.hostname.plc) found in the /tmp, ~user/tmp, and ~<*_oper>/tmp directories. |
### Parameter Description

- **-k**  Ask if one of the following kill signals should be sent to all matched processes.  
  Valid arguments are:  
  1  SIGHUP  
  9  SIGKILL  
  15  SIGTERM

- **-y**  Specify yes.  Use with -x to confirm remove, or -k option to confirm kill.

- **-l**  Adds an entry to the system log with the expected and actual process count info.

- **-z**  Creates a softlink for the shorter "pslist" command in directory /usr/local/bin.  
  **Note:** Users must have that directory set in their PATH environment variable for it to work.

- **-R**  Displays pslist revision info.

- **-h**  Displays the above usage text.

### Creating own plc file

As can be seen, there are multiple command line options and the more experienced administrator may like to make their own .plc file (-f option) with an alias command to list other important processes.

For example, you could create a command to list the Oracle database processes on the VWS.

```bash
$ cat <<EOF >ora.plc
ORA ora_.*E2BE   core db processes
ORA oracleE2BE   shadow process
EOF
$ alias psdb='pslist -f ora.plc $*'
# note: add this line to your user ~/.profile.
$ psdb -r
```

---

<table>
<thead>
<tr>
<th>APP USER</th>
<th>PID</th>
<th>PPID</th>
<th>S</th>
<th>%CPU</th>
<th>%MEM</th>
<th>VSZ</th>
<th>RSS</th>
<th>TIME</th>
<th>ELAPSED</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA oracle 744</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.3</td>
<td>4319336</td>
<td>4091784</td>
<td>30:40</td>
<td>50-07:34:48</td>
<td>ora_pmon_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 746</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.2</td>
<td>4317864</td>
<td>4090304</td>
<td>02:13</td>
<td>50-07:34:48</td>
<td>ora_psp0_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 748</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.2</td>
<td>4317864</td>
<td>4090528</td>
<td>02:41</td>
<td>50-07:34:48</td>
<td>ora_mman_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 750</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.3</td>
<td>4323928</td>
<td>4095976</td>
<td>05:02</td>
<td>50-07:34:48</td>
<td>ora_dbw0_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 752</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.2</td>
<td>4330840</td>
<td>4091264</td>
<td>03:47</td>
<td>50-07:34:48</td>
<td>ora_lgwr_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 754</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.2</td>
<td>4319928</td>
<td>4091472</td>
<td>45:09</td>
<td>50-07:34:48</td>
<td>ora_ckpt_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 756</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.3</td>
<td>4318952</td>
<td>4092184</td>
<td>04:40</td>
<td>50-07:34:48</td>
<td>ora_smon_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 758</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.2</td>
<td>4319720</td>
<td>4090904</td>
<td>00:00</td>
<td>50-07:34:48</td>
<td>ora_reco_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 760</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.3</td>
<td>4319720</td>
<td>4092048</td>
<td>04:59</td>
<td>50-07:34:48</td>
<td>ora_mmon_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 762</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>51.2</td>
<td>4323928</td>
<td>4090744</td>
<td>02:32</td>
<td>50-07:34:48</td>
<td>ora_mml1_E2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16159</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16161</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16163</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16168</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16170</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16172</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16175</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16177</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16181</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16189</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16191</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16193</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16195</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16197</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:33</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16199</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681704</td>
<td>00:00</td>
<td>19:05:31</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16201</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681704</td>
<td>00:00</td>
<td>19:05:31</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16203</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317984</td>
<td>3681832</td>
<td>00:00</td>
<td>19:05:31</td>
<td>oracleE2BE</td>
<td></td>
</tr>
<tr>
<td>ORA oracle 16205</td>
<td>1</td>
<td>S</td>
<td>0.0</td>
<td>46.1</td>
<td>4317920</td>
<td>3681768</td>
<td>00:00</td>
<td>19:05:31</td>
<td>oracleE2BE</td>
<td></td>
</tr>
</tbody>
</table>
General comment

Generally speaking, pslist is the only command you need to remember when checking for the NCC processes configured to run on any platform and it is a good place to start when investigating or troubleshooting issues.

Note: The slee-ctrl status and resource commands respectively call the pslist-s and pslist-src commands to generate output.

SLEE Resource Usage

Introduction

SLEE resources are created at run time and are used during service control for passing information between SLEE interfaces and applications.

These are internal values that have no specific meaning to the rest of the network and are entirely local to the running SLEE.

The NCC SLEE provides an application called check that can monitor and report on current SLEE resource usage. See SLEE Technical Guide for more information on this utility.

SLEE resources

There are three main types of internal SLEE resources;

- Dialogs - exist for the duration of the call.
- Events - these are transient and are deleted upon delivery to the relevant SLEE entity.
- Calls

If you have a networking background then you may notice a similarity to the SS7 model here. In fact, at a high level, the SLC SLEE considers everything that hits the platform as a Call instance, be it a voice or data call, SMS, or some sort of business process logic.

Like the SS7 model, a call instance has a source and destination address for a communication channel or dialog to pass data or events back and forth.

For example, a new service request hits a SLEE interface generating a new call instance.

The SLEE Interface will create a dialog to the relevant SLEE application and the call context data is put into an event and sent (through the dialog) to the SLEE application for processing.

The SLEE application can create new dialogs to other SLEE interfaces or applications for the call instance.

Resource snapshot

The following is an example of typical SLEE resource usage snapshots taken on a SLC at one second intervals.
Chapter 3

/IN/service_packages/SLEE/bin$ check 1 5

<table>
<thead>
<tr>
<th>Time</th>
<th>Dialogs</th>
<th>Apps</th>
<th>AppIns</th>
<th>Servs</th>
<th>Events</th>
<th>Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>22:24:02</td>
<td>61753</td>
<td>9</td>
<td>90</td>
<td>0</td>
<td>196170</td>
<td>21874</td>
</tr>
<tr>
<td>22:24:03</td>
<td>61797</td>
<td>9</td>
<td>90</td>
<td>0</td>
<td>196164</td>
<td>21892</td>
</tr>
<tr>
<td>22:24:04</td>
<td>61845</td>
<td>9</td>
<td>90</td>
<td>0</td>
<td>196164</td>
<td>21900</td>
</tr>
<tr>
<td>22:24:05</td>
<td>61841</td>
<td>9</td>
<td>90</td>
<td>0</td>
<td>196170</td>
<td>21900</td>
</tr>
<tr>
<td>22:24:06</td>
<td>61886</td>
<td>9</td>
<td>90</td>
<td>0</td>
<td>196192</td>
<td>21909</td>
</tr>
</tbody>
</table>

Notes:
- The dialog, events, and calls values changing.
- The output values, in square brackets, on the second row, indicates the maximum SLEE resource values allocated on SLEE start-up.
- You should note that the events value appears to be lower than the first output value. This is a known issue due to the fact Events can be configured to pre-allocated sizes with different values (SLEE.cfg) causing the check output value to be miscalculated. This issue can safely be ignored.

SLEE health

The SLC SLEE resource usage in a healthy, well functioning, network will fluctuate up and down during the course of a day as the call rates and call mix changes.

During high or peak call volume, more SLEE resources are used (that is, lower SLEE resource values), but will return back towards their maximum values at low call volume times, such as early morning.

The configured amount of SLEE resource is a lot higher than necessary for normal operation to allow the SLC to cope for a period of time with abnormal network behavior and/or software bugs which can prevent the SLEE resources from being freed up correctly (this situation is often referred to as a call leak).

Normal check output

So what is normal for the SLC check output?

There is no simple answer as every network is different. What is normal for your network can only be found by monitoring the SLC SLEE resource usage over a period of time, taking regular SLEE resource snapshots to create a normal historical trend.

Once a normal pattern of SLEE resource usage has been established, over weeks and months, then anything outside of this normal trend may indicate an issue with either; the NCC software, or, more often than not, the connecting SS7 network itself.

Experience has shown that this usually occurs due to routing failure and/or congestion within the SS7 network elements. The NCC term we use for leaked voice calls is an AWOL (absent without leave) call.

AWOL calls

An AWOL voice call usually occurs when the SLC does not receive an applyChargingReport (ACR) from the SS7 network and therefore does not know whether the call has ended or not. This will tie up the SLEE resource because, as far as the SLC is concerned, the call never ends.

The CAP (CAMEL Application Part) signaling standard does not cover the scenario of stale calls on the SLC where the SLC does not receive a response from the SS7 network for an in progress call.

It can be argued that when a response from the Network does not arrive, after a certain amount of time since the last response, that the SLC could assume it will never receive any more responses and should therefore abort the call, thereby freeing up the SLEE resource.

Another consideration is that most billing reservations have a defined length of validity and call flow transactions within the SS7 network need to be within this time limit also.
As a defense mechanism to this type of stale call scenario, the NCC solution has an optional AWOL setting that allows the SLC to clear out stale calls once they pass a configurable period of time. This allows the finite SLEE resources on the SLC to be freed up, if abnormal SS7 network behavior occurs.

**Note:** The timeout parameters in the MAP (Mobile Application Part) signaling protocol, used for Short Message Service (SMS), allows the SLC to clear out stale transactions.

### Scarcie SLEE resources

As a rule of thumb, the following values should indicate a problem condition that may require urgent investigation:

- **Serious** - should be investigated:
  - SLEE dialogs or calls are less then 25% of their maximum value.
- **Critical** - must be urgently investigated:
  - SLEE dialogs or calls are less then 10% of their maximum value.
  - SLEE events are around 50% of their maximum value.

**Note:** New calls can still be made if there are available dialog and calls resources that are greater than 0. The only time new calls cannot be made is when the free dialogs and/or calls are completely exhausted. At this stage the best cause of action is a quick SLEE restart, to reset the SLEE resources, allowing new calls to be made.

### Warning messages

The NCC SLEE will generate one warning event, in the `/var/adm/messages` log file, for each SLEE resource that breaks a threshold of 80% of its maximum value, similar to this example:

```
Sep 12 01:36:37 telco-p-slc01 watchdog: [ID 953149 user.warning] watchdog(18965)
WARNING: 20006 Call Instances Locked breaches 80% of total available instances (25000)
```

If SLEE resources should become exhausted then the `/var/adm/messages` log file will start spewing out entries, similar to the following notice message, for each failed call attempt:

```
Sep 17 03:22:59 telco-p-slc01 xmsTrigger: [ID 167701 user.notice] xmsTrigger(18957)
NOTICE SleeInterfaceAPI=8006 sleeInterfaceAPI.cc@248: Overload: SLEE is out of call instances
```

### Resource leak

If a SLEE resource leak is caught early then it will be the rate of the call leak that determines the true severity of the issue.

A slow leak of days, weeks, or months may be acceptable with general platform maintenance clearing leak calls during SLEE restarts.

A rapid SLEE resource loss over hours, minutes or seconds (depending on current call rates) requires instant action and investigation.

Good call tracing in the signaling network is vital in tracking down where in the network the issue is originating.

### Monitoring SLEE resources

The NCC Support Tools package provides the `check-SLEE.sh` script that, among other things, can be used for generating a timestamped log file of SLEE resource usage.

It is designed to run from the SLC `acs_oper` user's `crontab` file. If the following entry does not exist, add it with the `crontab` command, as below:

```
acs_oper@telco-p-slc01$ crontab -e
...skipped...
# the following entry is logging internal SLEE resource usage
```
* * * * * (. /IN/service_packages/ACS/.profile ;
/IN/service_packages/SUPPORT/bin/check-SLEE.sh ) >>
/IN/service_packages/SUPPORT/tmp/check-SLEE.log 2>&1

Tip: One minute snapshot intervals are recommended (as highlighted).

**check-SLEE.sh output**

This example output is generally what you will see on a well functioning healthy network with SLEE resources adjusting up and down by small margins over the course of a minute.

The output of the check-SLEE.sh script is written to the check-Time_Dialogs_Events_Calls_CAPS.log file in the /IN/service_packages/SUPPORT/tmp directory. You can view this log with ckslee command as follows:

```
$ ckslee
```

<table>
<thead>
<tr>
<th>Date-Time</th>
<th>Diags</th>
<th>Events</th>
<th>Calls</th>
<th>[Change]</th>
<th>CAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>20101125-03:43:00</td>
<td>86889</td>
<td>253630</td>
<td>43287</td>
<td>[+0.04%]</td>
<td>5</td>
</tr>
<tr>
<td>20101125-03:44:01</td>
<td>86904</td>
<td>253630</td>
<td>43300</td>
<td>[+0.05%]</td>
<td>5</td>
</tr>
<tr>
<td>20101125-03:45:00</td>
<td>86905</td>
<td>253631</td>
<td>43283</td>
<td>[-0.07%]</td>
<td>5</td>
</tr>
<tr>
<td>20101125-03:46:00</td>
<td>86911</td>
<td>253627</td>
<td>43297</td>
<td>[+0.06%]</td>
<td>6</td>
</tr>
<tr>
<td>20101125-03:47:00</td>
<td>86924</td>
<td>253632</td>
<td>43296</td>
<td>[-0.00%]</td>
<td>5</td>
</tr>
<tr>
<td>20101125-03:48:00</td>
<td>86870</td>
<td>253629</td>
<td>43264</td>
<td>[-0.13%]</td>
<td>5</td>
</tr>
<tr>
<td>20101125-03:49:00</td>
<td>86926</td>
<td>253631</td>
<td>43296</td>
<td>[+0.13%]</td>
<td>5</td>
</tr>
<tr>
<td>20101125-03:50:00</td>
<td>86945</td>
<td>253630</td>
<td>43306</td>
<td>[+0.04%]</td>
<td>4</td>
</tr>
<tr>
<td>20101125-03:51:00</td>
<td>86908</td>
<td>253627</td>
<td>43293</td>
<td>[-0.05%]</td>
<td>4</td>
</tr>
<tr>
<td>20101125-03:52:00</td>
<td>86938</td>
<td>253628</td>
<td>43302</td>
<td>[+0.04%]</td>
<td>5</td>
</tr>
</tbody>
</table>

**Notes:**

The [Change] value is a measure percentage difference between the previous Calls value and is useful in highlighting a sudden change resource usage.

The CAPS (Call attempts per second) column is an extra, but requires the SIGTRAN stack(s) to be configured to output their average CAPS rate. If they are not configured, this column will show N/A. See NCC SIGTRAN Technical Guide and the monitorperiod, rejectlevel, reportperiod, and displaymonitors parameters to enable CAPS reporting.

**check-SLEE.sh archiving**

Problems with SLEE resources will usually be found when the solution is first installed, or when the underlying signaling network has changes made to it.

This is when having a historical log of SLEE resource usage over time is a great tool in determining the trend, or a trigger point to an issue occurring.

To archive the check-Time_Dialogs_Events_Calls_CAPS.log file, add the following line to the /IN/service_packages/ACS/etc/logjob.conf file.

```
log /IN/service_packages/SUPPORT/tmp/check-Time_Dialogs_Events_Calls_CAPS.log age 240 size 1M arcdir /IN/service_packages/SUPPORT/tmp/archive
```

**check-SLEE.sh usage**

The head of the check-SLEE.sh script is extensively commented and explains some other ways the check-SLEE.sh script can be used, such as automatic SLEERestarts if SLEE resources go below a defined threshold.

**VWS SLEE resources**

As all the VWS processes are SLEE Interfaces, the SLEEResource usage pattern is different to the SLC.
On SLEE start-up, dialogs are created between the different SLEE interfaces for events to be passed back and forth. However the operations on the VWS are purely transactional and the concept of a call instance is not necessary. Therefore only the events value ever changes, with the dialogs and calls values remaining static as shown here:

```bash
$ slee-ctrl check 1 5
```

SLEE Control: v,1.0.10: script v,1.19: functions v,1.46: pplist v,1.118

```
[eb_pl]e ebe_oper] slee-ctrl> check 1 5
SLEE: Using shared memory offset: 0xc0000000
03:05:06        Dialogs  Apps    AppIns     Servs      Events   Calls
       [1000] [10] [100] [10] [71250] [500]
03:05:06        964       10       100        10        71252  500
03:05:07        964       10       100        10        71253  500
03:05:08        964       10       100        10        71255  500
03:05:09        964       10       100        10        71254  500
03:05:10        964       10       100        10        71255  500
```

Note: You can use the slee-ctrl command to call the check program.

Unless advised to, the monitoring of VWS SLEE resource usage is of little benefit.

**Rolling Snoop Archives**

**Introduction**

The NCC solution sits between the SS7 signaling network and LAN with Network Connectivity Agents (NCA) providing interfaces into the SLEE to interpret, convert and retransmit various network protocols, such as SIGTRAN (SS7 over IP), DIAMETER, SOAP/XML, SMPP and internal messaging protocols.

Being able to capture the reality of what is actually being sent over the wire is a vital tool when analyzing NCA related issues to help identify the source of the problem, be it local or remote.

The Solaris operating system comes with its own network packet analyzer software utility, the aptly named snoop command (see Snoop traces (on page 77)). Running the snoop utility allows you to trace and capture incoming and outgoing traffic passing through a server’s Network Interface Card (NIC) Devices.

To aid in the tracing of network devices and the retention of their snoop capture files the Support Tools package provides, what has become known as, the rolling snoop scripts.

**Scripts**

You can find the latest version of the rolling snoop scripts in the latest Support Tools package which are installed in the /IN/service_packages/SUPPORT/bin directory.

The `rolling-snoop.sh` and `start-rolling-snoop.sh` scripts are heavily commented and it is advisable to read these to get a better understanding of the scripts and their configuration.

For ease of use and convenience it is recommended that the `start-rolling-snoop.sh` and `stop-rolling-snoop.sh` wrapper scripts are used to control the rolling-snoop.sh script even though it may be run independently.

`rolling-snoop.sh`

The script that runs the snoop command.

Responsible for checking disk space, and archiving capture files before exiting.

The command line arguments allow you to specify a capture file name prefix and the ability to pass in valid snoop command line expressions to filter packets on, such as IP traffic that is either; scpt or tcp protocol, on port x or host y (use `$ man snoop` for more details of valid expressions).
Usage:

rolling-snoop.sh [capture file prefix:]network_card_interface_device_name [snoop options]

For example:

rolling-snoop.sh e1000g2
rolling-snoop.sh uas01-sig-pri:e1000g2 sctp port 14000
rolling-snoop.sh usms2-chrg-sec:nxge1 -c 1000000 tcp port 3989
rolling-snoop.sh usms01a-mgmt-pi:e1000g0 not icmp port 2999 or port 3000

Note: Must be run as root super-user.

start-rolling-snoop.sh
This is a wrapper script where you configure all the network devices you want to snoop, which are then passed as command line parameters to the rolling-snoop.sh script.

Each configured NIC will start a rolling-snoop.sh script, which in turn starts and controls the the snoop command. The example section below is where you define the network device(s) to trace.

/IN/service_packages/SUPPORT/bin$ vi start-rolling-snoop.sh
...skipped...

```bash
cat << CONFIG_END |sed '/^ *#/d; s/^ *///; s/\(.*\)\(.*\)/\1/; /^ */d' > $TEMP_FILE

### CONFIGURE NETWORK DEVICES HERE ###
# configuration examples below:
# e1000g1 # comments ignored after hash
# ${HOST}-sig-pri:e1000g1
# ${HOST}-sig-sec:nxge1 $PACK_COUNT sctp port 14000
# uas01-chrg-pri:e1000g0 -c 250000 tcp host charging-gw port 3989

CONFIG_END
...
```

stop-rolling-snoop.sh
When the stop-rolling-snoop.sh is run, all snoop processes are terminated (independently started snoop commands will also be killed), quickly followed by the termination of the rolling-snoop.sh scripts.

It is the stopping of the rolling-snoop.sh script that manages the archiving of the current capture files. So by regularly stopping and starting the rolling-snoop.sh script, we can easily create an archived repository of snooped traffic.

snoop_archiver.sh
This is a wrapper script to run the start-rolling-snoop.sh and stop-rolling-snoop.sh scripts and manage the removal of old archived capture files.

This script can be configured, as an hourly root crontab job, thereby creating an archive repository of capture files in hourly timestamped directories.

Here is an example snoop_archiver.sh script:

/IN/service_packages/SUPPORT/bin$ cat snoop_archiver.sh
#!/bin/ksh
#######################################################################
# Revision: snoop_archiver.sh,v 1.4 2010/01/05 01:55:10 gcato Exp $
# script to regularly archive rolling snoops files
# see rolling_snoop.sh KEEP_SECONDS variable to define archiving frequency
# (usually 60 minutes intervals)
# run from root crontab
# 59 * * * */IN/service_packages/SUPPORT/bin/snoop_archiver.sh >/dev/null 2>&1
# how long to keep archived snoop files before deleting

```
```
KEEP_DAYS=3

# snoops archive directory
SNOOP_DIR=/IN/service_packages/SUPPORT/snoops/archive

# snoop directory suffix (usually TZ variable value)
SUFFIX= GMT

# stop all snoops (this will automatically archive the files)
/IN/service_packages/SUPPORT/bin/stop-rolling-snoop.sh

sleep 1

# restart the rolling snoops
/IN/service_packages/SUPPORT/bin/start-rolling-snoop.sh

# delete old archived snoop dirs
find ${SNOOP_DIR} -type d -name \*${SUFFIX} -mtime +${KEEP_DAYS} |xargs rm -rf

# compress snoop files
find ${SNOOP_DIR}/${SUFFIX}/( -name \*snoop -a ! -name \*gz ) |xargs nice gzip 2>/dev/null

Default directory
The default output directory is /IN/service_packages/SUPPORT/snoops/(current|archive). The current directory contains the capture files currently being written to and archive directory contains time-stamped directories with the saved capture files.

Analyzing the Capture Files
A search of the web will provide a list of different protocol analyzer products, such as Wireshark, that can be used to view the capture file data. Please see the documentation of your protocol analyzer of choice for more information on interpreting the output.

Rolling Snoop Risks

Introduction
When running rolling snoop there are potential problems inherent with any data capture tool. This topic covers the major “look out for” issues.

Disk space
The rolling-snoop.sh script has a MAX_DISK_PERCENTAGE variable (default 75%) and will not run if the output capture file disk partition exceeds this disk space usage threshold (only checked on start-up and subsequent stop/start of snoop command).

This is to prevent the capture files from taking too much disk space and affecting the Event Data Records and process log files from being created.

Warning  Change with extreme caution.

If there is limited disk space then you can either; reduce the KEEP_DAYS variable in the snoop_archiver.sh script, or soft-link the /IN/service_packages/SUPPORT/snoops directory to a disk with spare capacity. For example:

# mkdir /volA/snoops
# rm -r /IN/service_packages/SUPPORT/snoops
# ln -s /volA/snoops /IN/service_packages/SUPPORT/snoops
Capture file size

The Solaris snoop command does not have a max duration option.

*Do not confuse the KEEP SECONDS variable in the* rolling-snoop.sh *script with how long the snoop command actually runs for.*

The MAX_PACKET_COUNT variable (default 100000 packets), also configured in the rolling-snoop.sh script, sets the limit to how big a capture file will grow to before a new capture file is started. If there is a lot of traffic on an interface, you may want to decrease this value to keep the capture file to a manageable size.

It is recommended that this is set inside the configurable section of the start-rolling-snoop.sh by defining a -c option. Further filtering options, on a per device level, can also help keep the capture file size manageable (read the script's comments for more details).

Depending on the amount of IP traffic, you may want to increase or decrease the frequency that the snoop_archiver.sh runs in the crontab.

If increasing the frequency to greater than 60 minutes then you must also increase the KEEP SECONDS variable (default 3600) in the rolling-snoop.sh script, otherwise when rolling-snoop.sh is stopped, capture files older than 60 minutes will be rolled over.

**Warning:** Not setting, or setting the MAX_PACKET_COUNT variable to a huge value, increases the potential for a snoop capture file to completely fill up the used space of the output disk partition to 100%.

Missing packets

Watch out for the routing of packets through secondary, or fail-over, NIC devices, which are configured in a multipathing group. You will need to snoop both network interfaces to capture all incoming and outgoing traffic.

```
# man ifconfig

...skipped...

MULTIPATHING GROUPS

Physical interfaces that share the same IP broadcast domain can be collected into a multipathing group using the group keyword. Interfaces assigned to the same multipathing group are treated as equivalent and outgoing traffic is spread across the interfaces on a per-IP-destination basis. In addition, individual interfaces in a multipathing group are monitored for failures; the addresses associated with failed interfaces are automatically transferred to other functioning interfaces within the group.

For more details on IP multipathing, see in.mpathd(1M) and ...

Basically, just because a packet came in on a network interface does not mean it will go out on the same interface. To find multipathed interfaces use the ifconfig -a command to find the network interfaces that are configured with the same groupname (if any).

Some monitoring and testing will usually show you which interfaces you need to monitor to catch all the traffic you want.

The crontab configured start and stop time will also have a small window of missed packets.
Overview

Introduction

This chapter explains how and why the SLC is used.

In this chapter

This chapter contains the following topics.

Service Logic Controller Overview 35
Service Logic Execution Environment 35
Network Connectivity Agents 38
Checking Services 39

Service Logic Controller Overview

Introduction

The SLC is used to handle calls using compiled control plan logic which is initially defined on the SMS and replicated to each SLC node.

All the main processing takes place inside the SLEE. On the SLC, this processing is primarily handled by slee_acs. Depending on the protocols involved on the network, a number of Network Connectivity Agent processes will also be running.

Service Logic Execution Environment

Introduction

The main process working to handle requests between the network and the SLEE is slee_acs. slee_acs is part of the Oracle Communications Network Charging and Control, and is located in

/IN/service_packages/ACS/

For more information on configuration options, refer to the appropriate product technical guide.

SLEE.cfg

Configuration for the SLEE in general is contained in /IN/service_packages/SLEE/etc/SLEE.cfg. This contains configuration for the resources allocated to the SLEE, and the applications, services and servicekeys of applications running on the SLEE.

- MAX<Parameter>: Contains the maximum resources allocated to the SLEE, such as
  - Applications
  - Services
  - Dialogs
  - Events
• Calls
  • APPLICATION: Contains the location of the application startup scripts, and how many instances to run.
  • INTERFACE: Contains the definitions for interfaces on the SLEE, their startup scripts and interface type.
  • SERVICE: Defines the applications/interfaces as a service (can be done multiple times for each application/interface).
  • SERVICEKEY: Defines the service to be triggered for received service keys.

ACS.conf

Configuration for other ACS components are contained in /IN/service_packages/ACS/etc/acs.conf. This contains general configuration options for the following processes:
  • acsStatisticsDBInserter
  • acsStatsMaster
  • acsStatsLocal
  • acsCompilerDaemon

It also contains configuration for acsChassis, which specifies:
  • Plug-ins
  • Services
  • Normalization
  • ACS EDR generation
  • Some other specific call-handling scenario configuration options

eserv.config

Remaining configuration is primarily found inside /IN/service_packages/eserv.config. Each product has a top level section, (for example “ACS {}” for ACS) and the underlying processes for each product are configured in sub-sections of eserv.config.

There are a few exceptions to this. Most notably SUA and M3UA Interface configuration, which is found in /IN/service_packages/SLEE/etc/

SLEE Watchdog

The SLEE watchdog is responsible for keeping track of all the processes running inside the SLEE. Upon SLEE startup, all the processes are registered with the watchdog. The watchdog periodically checks each process to make sure it is processing events correctly.

If not, the watchdog marks the process as suspect and sends the process a management event. During the next watchdog cycle (default 30 seconds) the watchdog will check that the event has been processed. If the event was not actioned, the process will be aborted and restarted.

Abort information
Whenever a process is aborted or restarted by the watchdog, there are appropriate records in SLEE/log/syslog, for example:

watchdog(18186) WARNING: Interface beVWARS3 does not exist at PID 18169, presuming dead.
Jul 18 00:53:16.091448 watchdog(18186) WARNING: Sending SIGABRT to interface beVWARS3, process 18169.
Jul 18 00:53:42.250416 watchdog(18186) WARNING: Interface beVWARS3 does not exist at PID 18169, presuming dead.
Jul 18 00:53:42.250844 watchdog(18186) WARNING: Restarting interface beVWARS3 (was process 18169).
Jul 18 00:53:42 watchdog(18186) SleeInterfaceInstance::start()=3 sleeInterfaceInstance.cc@156: Starting Interface beVWARS3.sh: PID: 8237

The watchdog also has built in deadlock prevention. A timer is set before beginning a check loop to ensure that it does not get deadlocked on a semaphore. If the timer expires, the watchdog believes the SLEE is having serious issues and will restart the entire SLEE.

Note: Some interactions with a process can stop it from responding to watchdog management events, one common example of this is a gcore. In this situation, the watchdog should be killed or sent a SIGUSR1 signal to stop operating.

The SLEE will need to be restarted in order for the watchdog to become operational again.

Update loader

The updateLoader process on the SLC is the client-side of IN Replication. It is responsible for receiving and applying updates from the smsMaster process on the SMS.

The updateLoader is run from initMaster, and runs in run-level 2.

While not a traffic handling application, this process is absolutely crucial to the health of the platform; non-replicated changes can cause major subscriber issues and revenue loss on a solution.

Checking replication status

On the SLC side, the updateLoader process and log file can be checked to make sure the process is up and running, and not presenting any errors.

See the SMS Replication section for information on the SQL queries required to check replication directly from the SMS database.

Full replication

In the event of a replication issue, it may be required to instruct the updateLoader to perform a full resync.

This performs a full collection of data from the SMS database. Depending on the amount of data, and what information is configured to replicate (for example, replicating subscriber data will mean information for every subscriber on the platform is replicated) replication can take a number of hours to complete.

Performing a Full Resync

To perform a full resync, open the updateLoader startup script, and add the -resync argument to the command line (highlighted), and restart the updateLoader process. Enter:

```bash
$ vi /IN/service_packages/SMS/bin/updateLoaderStartup.sh
```

Edit the result as shown:

```
. /IN/service_packages/SMS/.profile-scp
echo "'date' - Waiting for DB SCP"
pid=""
while [ -z "$pid" ] ; do
  pid=`ps -ef | grep "ora_pmon_SCP" | awk '{$8=""; $9=""; print $2}'`
  if [ -z "$pid" ] ; then
    echo "..."
    sleep 30
  fi
done
echo "'date' - DB SCP is ready"
```

```
while [ ! -f "/IN/service_packages/SMS/etc/replication.config" ] ; do
  echo "..."
  sleep 30
done
```

```
echo "'date' - Replication Cfg is ready"
exec /IN/service_packages/SMS/bin/updateLoader -nodeid 301 -resync
```

Enter:
\$ pkill updateLoader

**Result:** The updateLoader is restarted in full resync mode.

**Resync progress**
The progress of a Full Resync can be monitored through `/IN/service_packages/SMS/tmp/updateLoader.log`:

Thu Nov 11 01:09:41 GMT 2010 - Waiting for DB SCP
Thu Nov 11 01:09:41 GMT 2010 - DB SCP is ready
Thu Nov 11 01:09:41 GMT 2010 - Waiting for Replication Cfg
Thu Nov 11 01:09:41 GMT 2010 - Replication Cfg is ready

initialiseNode: Reading '/IN/service_packages/SMS/etc/replication.def'

... 

Node 301 SMS comparison/resync client ready.
Oct 11 01:09:44.966814 updateLoader(21378) NOTICE: Update Loader replication process started (node 301)

Cancelling any current client action.
Oct 11 01:09:44.979322 updateLoader(21378) NOTICE: Reached master node 1 at `<IP Address>'
RES: Thu Oct 11 01:10:08 2010: Node 301, started processing X SMS and Y SCP records.
RES: Thu Oct 11 01:10:08 2010: Node 301, resynchronisation pass 1, started processing of X SMS and Y SCP records.
Oct 11 01:10:08.291659 smsCompareResyncClient(21515) NOTICE: Beginning resynchronisation for node 301.
RES: Thu Oct 11 01:10:18 2010: Node 301, table NP_DN_RANGE, group NP_DN_RANGE_0, processed A of X SMS and B of Y SCP records.

Nov 11 01:12:05.308062 updateLoader(21378) NOTICE: Resynchronization Finished. Processing Queued Updates
Node 301 SMS comparison/resync client ready.
Nov 11 01:12:05.353114 updateLoader(21378) NOTICE: Finished Processing Queued Updates

The process will periodically report how far through the resync it is, including number of rows (out of total <node type> rows - highlighted example).

Once complete, updateLoader will return to regular operations. It is recommended to remove the -resync flag as soon as the resync has finished and restart the process.

**Network Connectivity Agents**

**Introduction**

Network connectivity agents (NCAs) exist to interface the various protocols running on the network with slee_acs and the rest of the SLEE.

For most NCAs, there is an associated process running to translate the incoming protocol to the internal protocol used by slee_acs (INAP).

**Example NCAs**

This table lists some examples of NCAs:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Package</th>
<th>Process</th>
<th>Log File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter (Northbound)</td>
<td>DCD</td>
<td>diameterBeClient</td>
<td>/IN/service_packages/DCD/tmp</td>
</tr>
<tr>
<td>Diameter (Southbound)</td>
<td>DCA</td>
<td>diameterControlAgent</td>
<td>/IN/service_packages/DCA/tmp</td>
</tr>
<tr>
<td>MAP</td>
<td>MMX</td>
<td>xmsTrigger (via adapter)</td>
<td>/IN/service_packages/XMS/tmp</td>
</tr>
<tr>
<td>SIP</td>
<td>SCA</td>
<td>sca_if</td>
<td>/IN/service_packages/SLEE/tmp</td>
</tr>
<tr>
<td>SMPP</td>
<td>MMX</td>
<td>xmsTrigger (via adapter)</td>
<td>/IN/service_packages/XMS/tmp</td>
</tr>
<tr>
<td>SIGTRAN</td>
<td>SIGTRAN</td>
<td>sua_if / m3ua_if</td>
<td>/IN/service_packages/SLEE/tmp</td>
</tr>
<tr>
<td>XML/TCAP</td>
<td>TCAP_IF</td>
<td>xmlTcpInterface</td>
<td>/IN/service_packages/SLEE/tmp</td>
</tr>
<tr>
<td>USSD</td>
<td>UIS</td>
<td>ussd_gw</td>
<td>/IN/service_packages/UIS/tmp</td>
</tr>
<tr>
<td>SOAP/XML</td>
<td>OSD</td>
<td>osdInterface</td>
<td>/IN/service_packages/OSSD/tmp</td>
</tr>
</tbody>
</table>
Information logging

Each NCA generally writes to its own log file and to the syslog. This should help identify what the program was doing right before experiencing an issue. This information is a key requirement when raising SRs with Oracle support.

Checking Services

Introduction

The SLEE service on the SLC can be checked using the interactive slee-ctrl interface. Slee-ctrl is part of the slee-ctrl package, and is generally available on all machines that run a SLEE.

Note: The Monitoring and Managing (on page 21) chapter covers checking of services in more detail.

Interactive interface

To enter the interactive interface, run slee-ctrl with no arguments. Enter:

```
$ slee-ctrl
```

Result: You are then presented with some environment information, and a slee-ctrl prompt:

```
SLEE Control: v,1.0.11: script v,1.21: functions v,1.48: pslist v,1.18

User acs_oper; session [5570]; terminal pts/3; started Thu Oct 28 03:53:48 GMT 2010

The following variables are set and will be used to run the SLEE.
SLEE_USER    acs_oper
SLEE_SCRIPT  /IN/service_packages/SLEE/bin/slee.sh
SLEE_CONFIG  /IN/service_packages/SLEE/etc/SLEE.cfg
SLEE_LOG     /IN/service_packages/SLEE/tmp/SLEE.log
```

[acs_oper] slee-ctrl>

Tip: Entering help at prompt lists the valid commands.

Example status reporting

From the prompt, you can issue a series of different commands to interact with the SLEE, or get information about resources, and other things.

Some examples are shown below:

Status

To check the current status of the SLEE, including processes, enter:

```
[acs_oper] slee-ctrl> status
```

```
---------------------------- Thu Oct 25 03:56:23 GMT 2010 -----------------------------
 C APP USER PID PPID STIME COMMAND
 6 SLEE acs_oper 1402  1 00:12:35 /IN/service_packages/ACS/bin/slee_acs
 1 SLEE acs_oper 1404  1 00:12:35 /IN/service_packages/SLEE/bin/capgw
 1 SLEE acs_oper 1405  1 00:12:35 /IN/service_packages/RAP/bin/rap
 1 SLEE acs_oper 1406  1 00:12:35 /IN/service_packages/LCP/bin/locApp
 1 SLEE acs_oper 1407  1 00:12:35 /IN/service_packages/ACSUSB/bin/slee_acs
 1 SLEE acs_oper 1408  1 00:12:35 /IN/service_packages/UIS/bin/ussdgw
 1 SLEE acs_oper 1409  1 00:12:35 /IN/service_packages/SLEE/bin/timerIF
 1 SLEE acs_oper 1410  1 00:12:35 /IN/service_packages/SLEE/bin/alarmIF
```
Resources
To check the status of SLEE resources, in particular memory/CPU usage, enter:

```
[acs_oper] slee-ctrl> resources
```

```
--- Fri Oct 29 01:28:31 GMT 2010 ---

APP USER PID PPID S %CPU %MEM VSZ RSS TIME ELAPSED COMMAND
SLEE acs_oper 10267 1 0.0 4.0 633584 314720 00:02 04:45:10 slee_acs
SLEE acs_oper 10268 1 0.0 4.0 633584 314720 00:02 04:45:10 slee_acs
SLEE acs_oper 10269 1 0.0 4.0 633584 314720 00:02 04:45:10 slee_acs
SLEE acs_oper 10270 1 0.0 4.0 633584 314720 00:02 04:45:10 slee_acs
SLEE acs_oper 10271 1 0.0 4.0 633584 314720 00:02 04:45:10 slee_acs
SLEE acs_oper 10272 1 0.0 4.0 633584 314720 00:02 04:45:10 slee_acs
SLEE acs_oper 10273 1 0.1 3.4 527728 271760 00:43 04:45:10 timerIF
SLEE acs_oper 10274 1 0.0 3.4 527760 271800 00:00 04:45:10 alarmIF
SLEE acs_oper 10275 1 0.1 3.7 552960 290896 00:53 04:45:10 acsStatsLocalSLEE
SLEE acs_oper 10276 1 0.1 3.5 539712 276120 00:44 04:45:10 replicationIF
SLEE acs_oper 10277 1 0.1 3.7 552960 290896 00:53 04:45:10 BeClient
SLEE acs_oper 10278 1 0.0 3.6 544856 281864 00:00 04:45:10 xmlTcapInterface
SLEE acs_oper 10279 1 0.1 3.4 527784 271824 01:08 04:45:10 watchdog
```

```
total processes found = 13
```

Memory: total 7.9G, used 6.1G (77.6%) + 128.0K (0.0%) /tmp, free 1.8G (22.4%) OK
Swap: total 4.4G, used 2.1G (48.9%), free 2.2G (51.1%) OK

Call resources
To check the status of SLEE call resources, in particular free calls and events, enter:

```
[acs_oper] slee-ctrl> check 1
```

```
SLEE: Using shared memory offset: 0xc0000000
01:29:03 Dialogs Apps AppIns Servs Events Calls
[70000] [30] [296] [30] [207152] [25000]
01:29:03 70000 29 290 24 207146 25000
01:29:04 70000 29 290 24 207146 25000
01:29:05 70000 29 290 24 207146 25000
01:29:06 70000 29 290 24 207146 25000
01:29:07 70000 29 290 24 207146 25000
01:29:08 70000 29 290 24 207146 25000
01:29:09 70000 29 290 24 207146 25000
```

A dwindling number of free calls indicates a call leak (this means the number of available calls that the SLC is decreasing in such a manner that eventually it will no longer be able to serve traffic). In this situation the only real solution is to restart the SLEE and reset the available resources. If the problem continues to happen, it will be prudent to investigate the type of traffic hitting the platform and attempt to determine what is triggering the leak. Slower response times from other network elements can also cause a decrease in free SLEE resources.

Stop and start
To stop, start, or restart the SLEE, enter as required at the prompt:

```
[acs_oper] slee-ctrl> stop
[acs_oper] slee-ctrl> start
[acs_oper] slee-ctrl> restart
```
Service Management System (SMS)

Overview

Introduction

This chapter explains how and why the SMS is used.

In this chapter

This chapter contains the following topics.

<table>
<thead>
<tr>
<th>Service Management System Overview</th>
<th>43</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Screens</td>
<td>43</td>
</tr>
<tr>
<td>Replication</td>
<td>46</td>
</tr>
<tr>
<td>EDR Management</td>
<td>48</td>
</tr>
<tr>
<td>Provisioning Interface (PI)</td>
<td>50</td>
</tr>
<tr>
<td>Business Processing Language</td>
<td>53</td>
</tr>
</tbody>
</table>

Service Management System Overview

Introduction

The SMS is responsible for setup and maintenance of many aspects of the platform, and contains the web-based java front-end for viewing and altering configuration.

Behind the scenes the SMS receives EDRs from the SLC and VWS, and processes them before archival, removal, or forwarding for further processing by external systems.

The SMS also runs a number of additional services, including the Provisioning Interface (PI), the alarm, statistics and replication subsystems, along with processes for billing interaction and Business Processing Logic (BPL).

Java Screens

Introduction

The front-end for configuring the NCC runs through Java on the SMS. To access, connect to http://SMS_Server_Address/sms.jnlp.

Oracle Listener

Connections to the database are handled by the Oracle Listener. If experiencing problems connecting to the Java screens, check the status of the listener using lsnrctl as the oracle user, by entering at the $ prompt:

$ lsnrctl status

LSNRCTL for Solaris: Version 10.2.0.5.0 - Production on 29-OCT-2010 02:07:51
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(PORT=1521)))

<table>
<thead>
<tr>
<th>STATUS of the LISTENER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Start Date</td>
</tr>
<tr>
<td>Uptime</td>
</tr>
<tr>
<td>Trace Level</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>SNMP</td>
</tr>
</tbody>
</table>

Listener Parameter File /u01/app/oracle/product/10.2/network/admin/listener.ora

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=testusms) (PORT=1521)))

Services Summary...
Service "SMF" has 1 instance(s).
  Instance "SMF", status UNKNOWN, has 1 handler(s) for this service...
Service "SMF.testusms.SMF" has 1 instance(s).
  Instance "SMF", status READY, has 1 handler(s) for this service...
Service "SMF_XPT.testusms.SMF" has 1 instance(s).
  Instance "SMF", status READY, has 1 handler(s) for this service...

The command completed successfully

Start and stop listener

You can stop and start the listener using lsnrctl stop and start command. Enter at the $ prompt:

$ lsnrctl stop
$ lsnrctl start

Listener configuration

Configuration for the listener is in the file $ORACLE_HOME/network/admin/listener.ora. Generally this information will not need to change, unless an aspect of the network changes, for example, hostname, or IP resolution.

Java packages

The front-end java packages are contained in /IN/html. SMS.jnlp calls SMS.sig.jar, which makes up the foundations of the screens.

Additional packages exist for the various products installed, for example. ACS (acs.sig.jar), CCS (ccs.sig.jar) and so on.

Control Plan Editor

The Control Plan Editor (CPE) is a front end for designing call handling logic. In general, every single event that triggers the NCC platform will hit a control plan at some point.

The control plan used and nodes traveled by an event triggering the platform are written to the associated ACS EDR in the CPN and TFN tags.

For each event there will be an Event Detail Record (EDR), the only real exception being when an engine error occurs and processing cannot continue. In this scenario, ACS would still write a call dump, so a record should still be available.

Tracing a Control Plan

If a problem can be traced to an ACS EDR, then the Control Plan Editor can be used to find the control plan used, and trace through each node to see exactly how the event traversed it.
Follow these steps to trace a control plan through the CPE.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main SMS menu select <strong>Services -&gt; ACS Service -&gt; Control Plans</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Select the appropriate customer from the top right-hand <strong>Customer</strong> box.</td>
</tr>
<tr>
<td>3</td>
<td>Select <strong>Open</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Select the appropriate control plan, based on the <strong>CPN</strong> tag.</td>
</tr>
<tr>
<td>5</td>
<td>Press <strong>N</strong> to show node numbers.</td>
</tr>
<tr>
<td>6</td>
<td>Using the contents of the <strong>TFN</strong> tag, follow the calls progress through the plan.</td>
</tr>
</tbody>
</table>

**Tips:**
- Clicking once on a node will highlight and indicate all connected nodes and associated exits, along with tool-tip descriptions. Note that the connection highlighting does not occur if the Control Plan is opened with the structure read-only.
- Sub-Control Plan nodes (SCPN) can be opened in a **view** mode directly from the node edit screen.
- The Start and End node IDs are not reported when a SCPN node is triggered; as a result it can sometimes be difficult to trace how a Sub-Control Plan ended.

**acsCompilerDaemon**
When a control plan is saved the dialog box shown on screen is the output of the SMS process `acsCompilerDaemon`, which validates and compiles control plans.

If there is an issue compiling a control plan, and the CPE Save dialog box does not contain enough information to go forward, consider putting the `acsCompilerDaemon` into **DEBUG** to get more information about why the compilation failed.

**Tip:** If the save dialog is completely blank - the `acsCompilerDaemon` may not be running at all.

**ccsBeOrb**
When the CCS portion of the screens need to interact with the VWSs, this is done through `ccsBeOrb.

The most common reason for the screens needing to query the VWS is when opening the Edit Subscriber screen. This displays all real-time Wallet information about a subscriber.

If both the VWSs are restarted and there is a complete billing outage, it can take a couple of minutes for `ccsBeOrb` to realize it has disconnected and reconnect. This process can be sped up by restarting `ccsBeOrb`

The error message below is indicative of this problem:

![Error Displaying Account](image)

However, if the error message remains, there is a definite problem with the connection between the SMS and the VWSs.
Replication

Introduction

The SMS is responsible for managing replication on the platform. From the front-end, configuration is handled through the Java screens in Operator Functions -> Node Management, and then:

- Replication Nodes configures the node number and address.
- Table Replication contains tables to be replicated to sub-nodes.
- Replication Node Types allows the configuration of node types with pre-determined tables replicated.

Configuration completed

When configuration is complete (or has changed) a special file called replication.config is generated and put on all replication nodes in /IN/service_packages/SMS/etc. Any processes that use the smsMaster as a means of replication use this file to decide where to send replication updates to, and what to replicate (in the case of updateLoader).

Processes include:

- Alarm subsystem (smsAlarmDaemon)
- Statistics subsystem (smsStatsDaemon)
- Data replication (updateLoader)
- Upstream replication (replicationIF)

When the SLC or VWS needs to replicate a change (usually to the SMS), this is sent upstream through replicationIF.

Checking replication status

Replication can be checked using a few queries on the database on the SMS.

There are three main tables required to check the status of replication:

1. REP_ORA_RENUMBERED
   This table contains all the information that is yet to be replicated.
2. REP_PENDING_QUEUE
   This table contains the ID of the last event replicated.
3. REP_CNF_NODE
   This table contains a list of the configured replication nodes for reference.

Viewing backlog

To view the current backlog of changes waiting to be replicated, run the following SQL query as smf_oper on the SMS. This command will show how many values are yet to be replicated down to the nodes. The larger the number, the further behind replication currently is. Enter:

SQL> select count(*), node_number from rep_ora_renumbered group by node_number;

<table>
<thead>
<tr>
<th>COUNT(*)</th>
<th>NODE_NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>162</td>
<td>301</td>
</tr>
<tr>
<td>129</td>
<td>302</td>
</tr>
<tr>
<td>122</td>
<td>351</td>
</tr>
<tr>
<td>116</td>
<td>352</td>
</tr>
<tr>
<td>6305218</td>
<td></td>
</tr>
</tbody>
</table>
Event Id checking
Another way to check the current status of replication is to use the following SQL query to list the minimum and the maximum ID. Enter:

```sql
SQL> select min(event_id), max(event_id) from rep_ora_renumbered
```

<table>
<thead>
<tr>
<th>MIN(EVENT_ID)</th>
<th>MAX(EVENT_ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>164431033</td>
<td>170738029</td>
</tr>
</tbody>
</table>

If the difference between Min and MAX is large as above, this indicates a clear problem with replication.

Problem node ID

Once you have determined that there is a problem with replication, it is important to determine if one particular node has fallen behind or if replication has completely failed. To do this, you must run the following SQL. Enter:

```sql
SQL> select * from rep_pending_queue;
```

<table>
<thead>
<tr>
<th>NODE_ID</th>
<th>ROE_EVENTID</th>
</tr>
</thead>
<tbody>
<tr>
<td>301</td>
<td>164432645</td>
</tr>
<tr>
<td>302</td>
<td>170738026</td>
</tr>
<tr>
<td>351</td>
<td>170738026</td>
</tr>
<tr>
<td>352</td>
<td>170738026</td>
</tr>
</tbody>
</table>

The ROE_EVENTID is the current event ID that the node is processing. If the event ID is close to the maximum event ID (170738029), then the node is essentially in sync, but if the ROE_EVENTID is a long way off, that node is having issues receiving updates.

Problem node name

Once it is determined which NODE_ID is behind on replication, run the following SQL command to resolve the name of the node. Enter:

```sql
SQL> select description, node_number from REP_CNF_NODE;
```

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>NODE_NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAS01</td>
<td>301</td>
</tr>
<tr>
<td>UAS02</td>
<td>302</td>
</tr>
<tr>
<td>UBE01</td>
<td>351</td>
</tr>
<tr>
<td>UBE02</td>
<td>352</td>
</tr>
</tbody>
</table>

In this example, we can see that the node_id that is behind (301) is connected to UAS01.

Problem resolution

The two most common ways to resolve a replication issue is to:

- Perform a full resync on the SLC (see *Full replication* (on page 37) for the details)
- Restart the smsMaster on the SMS.
EDR Management

Overview

The SMS is generally responsible for receiving, processing and archiving EDRs received from the other nodes on the NCC platform.

cmnPushFiles is responsible for "pushing" EDRs to the SMS, which receives them via cmnReceiveFiles. Depending on the location they are received to, they are processed by other processes or scripts, before being archived.

EDR process flow diagram

Here is an overview of the EDR process flow:

Receiving files

Incoming EDRs are received by the network service cmnReceiveFiles. The destination of the EDR is controlled by the cmnPushFiles process on the sending machine.
EDR are generally separated into different directories for different EDRs. For example, an ACS EDR would be sent to `/IN/service_packages/SMS/cdr/received`, and BE EDRs would be sent to `/IN/service_packages/CCS/logs/CDR-in`. This allows for more targeted troubleshooting when looking at EDR flow.

### Processing EDRs

The processing of EDRs depends on their location.

Processing for CCS or BE EDRs is handled by `ccsCDRLoader`, which runs from inittab as a background process.

Under normal circumstances ACS EDRs are not processed at all, and are just archived.

#### ccsCDRLoader

Billing EDRs originating from the VWSs are processed in real-time by `ccsCDRLoader`. As soon as an EDR is found in the incoming directory, it is picked up by the `ccsCDRLoader` process and run through the configured plug-ins.

**Configured plug-ins**

Configuration, such as incoming/outgoing directory, enabled plug-ins and plug-in settings are defined in `/IN/service_packages/eserv.config`. The results of the processing are dependant on the plug-ins that are running.

Plug-ins include:

- **AcsCustIdPlugin**
  
  Ensures ACS Customer ID is present, if not it will look it up in the database

- **VoucherRedeemPlugin**
  
  Ensures voucher redemption is updated in the CCS_VOUCHER_REFERENCE table in the SMS database

- **AcctHistPlugin**
  
  Ensures the CCS Account History table is updated with subscriber changes

- **CDRStoreDBPlug**
  
  Writes the EDR details to the CCS_BE_EDR table in the SMS database

- **FileWriterCDRLoaderPlugin**
  
  Writes the EDR details to file after `ccsCDRLoader` has finished processing
  
  If configured, can also alter the timezone of the date fields

With this in mind, if the CCS Subscriber screens show no EDR history for a subscriber that has made calls, the `ccsCDRLoader` would be one place to check for issues.

### Archiving

Similar to processing, the archiving of EDRs is dependant on the location of the files. After processing, billing EDRs are moved to a final location, for example, `/IN/service_packages/CCS/logs/CDR-store`.

The archival of EDRs is done by three scripts:

1. **ACS EDR**
   
   `/IN/service_packages/SMS/bin/smsCdrProcess.sh`

2. **BE EDR**
   
   `/IN/service_packages/CCS/bin/ccsCDRTrimFilesStartup.sh`

3. **Database EDR records**
ACS EDR archiving is handled by the `smsCdrProcess.sh` script which is launched from `crontab` once per day (usually midnight GMT).

It contains a number of configurable parameters, but generally it will simply call the `smsProcessCdr` binary from `/IN/service_packages/SMS/bin`, move CDRs from `SMS/cdr/received` to `SMS/cdr/processed`, and delete files older than 31 days.

The script can be altered to perform some additional tasks, e.g. placing a suffix on the final filenames, but in general it is quite rudimentary.

Billing EDR archiving is handled by the `ccsCDRTimFilesStartup.sh` script which is launched from `crontab` once per day (usually midnight GMT).

The script calls the `ccsCDRTimFiles` binary, which will remove EDR files from the specified directory that are older than the specified amount of days.

In general, this is `/IN/service_packages/CCS/logs/CDR-store`, and files older than 30 days.

Billing EDRs are also removed from the database after a set period of time.

This is controlled by the `/IN/service_packages/CCS/bin/cdrDeletionStartup.sh` script, which runs a simple cleanup script on the database once per day from `crontab` (usually 03:15 GMT).

The script itself can be found in `/IN/service_packages/CCS/bin/cdrDeletion.sql`.

In general, this will be configured to remove any EDRs older than seven days.

### Customer Specific Processing

From time to time, a customer may have some more specific requirements for EDR files, rather than just storing on the NCC SMS for a number of days before deleting.

Reasons for this include:

- ACS EDR reconciliation for billing
- BE EDR transfer to mediation server for processing to third party front-end
- More thorough archival flexibility:
  - Splitting EDR into daily files
  - Compression
  - Longer retention

If a customer specific processor or archiver is in place, this is usually indicated by some of the following:

- `smf_oper` crontab has `smsCdrProcessor` entry commented or reading/writing to a different location.
- `ccs_oper` crontab has `ccsCDRLoader` reading/writing to a different location.
- New "cdrArchiver.sh options" in the "_oper crontabs and bin directories.
- Modified directory structure in `CCS/logs` or `SMS/cdr`.
- Separate mount point for EDR, for example, `/global/EDR` or similar.

### Provisioning Interface (PI)

#### Overview

The Provisioning Interface (PI) runs as a service on the SMS.
PI is primarily responsible for handling external requests for data on the NCC platform. It will accept an external connection (supporting a number of protocols), provide authentication and respond to requests for subscriber information.

This includes simple interactions such as balance queries and performing recharges through to creating new subscribers and issuing commands that trigger through to a control plan to perform complex Business Processing Language (BPL) interactions.

**Supported protocols**

Supported protocols are:

- XML
- SOAP
- Native Oracle Syntax (plain-text)

**Processes using PI**

There are a number of processes responsible for running the PI. They are as follows:

- PIManager
  Responsible for starting and stopping PIprocess instances, and the PIbeClient.
- PIprocess
  Each listening port is run through a PIprocess
  Handles requests and executes commands
  Each port has a defined protocol it is listening for:
  - XML
  - SOAP
  - Standard.
- PIbeClient
  Interacts with the billing engine.
- smsTrigDaemon
  Used when the PI needs to trigger a control plan on the SLC, usually for a BPL command.

**Command delivery**

Each set of commands for the PI are delivered in a separate package for each product, for example, ccsPI for CCS and billing commands, ccsACS for ACS commands.

Commands are issued via the required protocol, based on the configuration shown in the SMS screens under Services > Provisioning > Administration > Ports tab. Each defined port handles one protocol type only.

**Command structure**

The basic structure of a PI command is:

\[\text{Command} = \text{Action}: \text{Parameter}_1 = \text{Value}_1, \text{Parameter}_2 = \text{Value}_2, \ldots;\]

**Tip:** The semi-colon terminates and executes the command.

Some example Command=Action combinations are:

- CCSCD1=QRY
  Subscriber query
- CCSCD1=ADD
  Add Subscriber
Chapter 5

CCSCD1=CHG
  Change Subscriber
CCSCD1=DEL
  Delete Subscriber
CCSCD3=RCH
  Recharge Account or Voucher

Note: Each action has a specific set of expected parameters. See the relevant PI commands guide for more information.

Command responses

Each request will receive either a positive or negative acknowledgment (ACK or NACK). The response will generally contain further information, although in some cases the response will just be an ACK.

Running a PI session

Use the following process to access the PI.

First, connect to the PI through telnet to a valid port, enter:

```
$ telnet server port
...
```

Tip: Escape character is `[^].`

There is no prompt, but the first interaction the PI expects is a username and password, terminated with a semi-colon:

```
user,password;
ACK;
```

This indicates the connection is successful, if not the response would be in the negative:

```
user,password;
NACK,72-INVALID LOGON - username,password;Connection to localhost closed by foreign host.
```

Once successfully connected, commands can be executed. See the relevant PI commands guide for more information on available commands.

Some example Native Oracle Syntax commands and responses are shown below:

**Subscriber Query**

This command runs a subscriber query, enter:

```
CCSCD1=QRY:MSISDN=12345;
```

Response:

```
CCSCD1=QRY:ACK:MSISDN=12345,ACCOUNT_NUMBER=1012345,PRODUCT=POSTPAID,SERVICE_PROVIDER =ORACLE,STATUS=A,CREATION_DATE=20100721044959,WALLET_EXPIRY_DATE=,BALANCE_EXPIRY_DATE=2011106040500,BALANCE=500,INITIAL_BALANCE=0,LANGUAGE=english,FREE_SWAPS_REMAINING=0,LAST_SWAP_RESET_DATE=;...
```

52  NCC System Administrator’s Guide
Balance Query - all balances
This command runs an all balance query, enter:

CCSCD1=QRY:MSISDN=12345,BALANCE_TYPE=ALL;

Response:
CCSCD1=QRY:ACK:MSISDN=12345,ACCOUNT_NUMBER=1012345,PRODUCT=POSTPAID,STATUS=A,WALLET_EXPIRY_DATE=,LANGUAGE=english,BALANCES=General Cash:500:20111106040500|Free SMS:5;20101122173422;

Balance Query - specific balance
This command runs a specific balance query, enter:

CCSCD1=QRY:MSISDN=12345,BALANCE_TYPE=Free SMS,LIST_TYPE=_BALANCE|BALANCE_EXPIRY_DATE;

Response:
CCSCD1=QRY:ACK:MSISDN=12345,ACCOUNT_NUMBER=1012345,BALANCE_EXPIRY_DATE=20101122173422,BALANCE=5;

Note: Balance types such as General Cash, or Free SMS are configurable, so the output may vary from platform to platform.

Voucher Type Recharge
This command runs a voucher type recharge request, enter:

CCSCD3=RCH:RECHARGE_TYPE=VoucherType,REFERENCE=100 Free SMS,MSISDN=12345;

Response:
CCSCD3=RCH:ACK;

Business Processing Language

Introduction
More complex and advanced commands can be run by using Business Processing Language (BPL). A BPL command is configured through the SMS UI under Services > Prepaid Charging > Task Management.

For full details on configuring BPL, see the CCS User's Guide.
Example BPL configuration

In this example Edit Business Process Logic screen, a command name, parameters and control plan are defined:

Example Disconnect Cause mappings

Mappings between Disconnect Cause and the message returned to the PI is also done through Services > Prepaid Charging > Task Management.
302 is the PI result code for a successful BPL command.

So in this example, the Control Plan exited with a Disconnect Cause of 100, which was mapped to the display message of "All actions completed OK".
Overview

Introduction

This chapter explains how and why the VWS servers are used.

In this chapter

This chapter contains the following topics.

Voucher and Wallet Server Overview
Useful Commands and Scripts

Voucher and Wallet Server Overview

Introduction

Any interactions by subscribers that require payment are processed, at some point, by the VWS. The VWS database contains important subscriber information, and all information relating to their balances, promotions and vouchers. Like the SLC, all the main processing takes place inside the SLEE; the main processes responsible for handling billing interactions are:

- beVWARS
- beServer
- beSync
- beGroveller

Some NCAs may also be configured to handle other interactions between VWS and SLC (for example, DAP, OSD). Understanding when these interactions are invoked will also aid the troubleshooting process.

Billing pairs

VWSs are configured in billing pairs, rather than the standard N+1 model that the SLCs follow. One machine acts as the primary, the other secondary, whereby the primary processes all traffic, and syncs the information to the secondary.

In the event of an outage of the primary, traffic is handed to the secondary for processing. When the primary is brought back into operation, it requests all the updates it is missing from the secondary and begins to resync. Only once the syncing process is complete, will the primary resume operation and begin to handle all the traffic again.

From a subscriber's perspective this is a completely transparent process. If an initial request is handled by the primary and it is taken out of service by the time a subsequent reservation comes in, the secondary will step in and handle the reservation. Regardless of the status of the primary, the secondary will continue to handle billing for any calls that "bounce" to it until the calls are complete.
Processes location

Billing processes are located in /IN/service_packages/E2BE/bin. Each process writes to its own log file in E2BE/tmp. Each instance of beVWARS also writes to its own log file.

General Billing Terms

Explanation of a few basic billing terms will aid understanding of how the NCC VWS works, and the information provided in the rest of the VWS section.

- Subscriber
  The end user
- Wallet
  A container for a subscriber’s buckets.
  Many-to-many relationship with a subscriber:
  - A subscriber can have one primary and one secondary wallet
  - A wallet may be shared between many subscribers
- Bucket
  A record of a balance for a subscriber inside a wallet.
  One-to-many relationship with a wallet:
  - A wallet can have many buckets
  - A bucket can only belong to one wallet
- Periodic Charge
  Stored in a regular bucket, but with additional references to the periodic charge.
  Uses Expiry as the renewal date, that is, when the bucket expires the periodic charge will renew.
  Uses Value to store the current periodic charge state:
  - 1 - Terminated
  - 2 - Unsubscribed
  - 3,4,5,6 - Active (varying states of active)
  - 7,8,9 - Grace (varying states of Grace Period)
- ACK/NACK
  Standard nomenclature for a successful (ACK) or failed (NACK) response from the VWS.

beServer process

The beServer acts as a central contact point for connecting clients to the billing engine. Essentially any interaction with beVWARS will first go through beServer.

beServer maintains a list of currently connected clients and handles new connections.

Client list

Different clients include:

- beClient (SLC)
- PIBeClient (PI on the SMS)
- ccsBeOrb (Java screens on the SMS)
- beGroveller (background process for keeping un-used wallets up to date)

Listening port

The VWS server listens on port 1500 for incoming connections, and uses the Oracle Escher protocol for communications. If troubleshooting is required for billing traffic - port 1500 will contain the conversation that happens on the wire between NCC components.
**Client ID**
Each connecting client has its own unique client ID. This is derived from a hash of the client name, specified by the configuration of the incoming client process.

Upon connection, beServer logs the client name and client id, which can be a useful reference when trying to determine the client for an EDR, for example:

Nov 23 04:36:11 ube01 beServer: [ID 839465 user.notice] beServer(21708) NOTICE: Client 'slc01_ccsBeClient' (ClientId 87783972) has connected
Nov 23 04:36:13 ube01 beServer: [ID 839465 user.notice] beServer(21708) NOTICE: Client 'PIbeClient' (ClientId 161986004) has connected

**beVWARS process**
beVWARS is the main process handling the work-load on a VWS. It is responsible for all interactions between the subscriber and their funds.

At a rudimentary level, it holds the cache that represents the most up-to-date information about a subscriber balance information, including uncommitted funds (that is, reservations).

Upon a request for a subscriber's wallet, beVWARS will load the subscriber information from the database into cache, and periodically flush and write to the database based on configuration (beVWARS.walletCache{} section in eserv.config).

**Handlers**
beVWARS is reasonably flexible, and will operate using a configured set of Message and Event Handlers.

Message Handlers define how beVWARS will handle message requests from clients (for example, how to handle a voucher recharge request).

Event Handlers (known as plugins) contain a set of instructions to be run on wallets each time an event is triggered (for example, instructions to delete an expired balance).

**Plugins example list**
Plugins will be run prior to the handlers, so that any maintenance has been run prior to call connection. Plugins include:

- `beVWARSExpiry.so`  
  Processes expired buckets, ensuring that expired funds are removed from the database

- `beVWARSMergeBuckets.so`  
  Manages the number of buckets a wallet is allowed. If the maximum is hit, the new bucket will be merged into an existing one instead

- `ccsVWARSExpiry.so`  
  Maintains CCS Wallet States, for example.
  - Moves Dormant Wallets to Active when they are used
  - Deletes Terminates Wallets after a configurable period of time

- `ccsVWARSActivation.so`  
  Activates Wallets including initial credits

- `ccsVWARSPeriodicCharge.so`  
  Handles all PeriodicCharge interactions and state changes

- `ccsNotification.so`  
  Creates real-time notifications

**Handlers example list**
Handlers include:

- `ccsVWARSReservationHandler.so`
Performs the UBE-side processing of all messages relating to chargeable call processing including calculating tariffs

- ccsVWARSNamedEventHandler.so
  Performs the UBE-side processing of messages relating to named events. This includes:
  - Returning the cost for an event class and event name combination
  - Generating named event EDRs.

- ccsVWARSRechargeHandler.so
  Handles General Wallet Recharges

- beVWARSRechargeHandler.so
  Handles EDR generation in some situations where one would not usually be generated (can be specifically requested by a BE Client)

- ccsVWARSWalletHandler.so
  Performs the UBE side processing of all messages relating directly to wallets. This includes:
  - Wallet Information (WI) - responds with wallet information
  - Wallet Create (WC) - creates new wallets
  - Wallet Update (WU) - updates wallets
  - Wallet Delete (WD) - deletes existing wallets and corresponding buckets
  - Bad PIN updates (BPIN) - updates Bad PIN balance if the wallet has one.
  
  EDRs are produced for all Wallet updates (create/modify/delete/recharge) with the details of the change.

- ccsVWARSVoucherHandler.so
  Performs the Billing Engine side processing of messages directly relating to vouchers. This includes voucher reservation/commit, alteration and deletion

**beVWARS scalability**

beVWARS is a scalable process, and runs multiple instances on the NCC platform.

As the beVWARS contains the most up to date information about a Wallet, the beServer needs to ensure that not only is the workload even, but subsequent requests for wallet information must always go to the same beVWARS instance.

**Workload spreading**

The algorithm for this is WalletID MOD Total beVWARS Instances.

The Wallet ID is essentially an identity field in the database, and will increment in a way that ensures even workload.

The number of instances created is determined by /IN/service_packages/SLEE/etc/SLEE.cfg. For example:

```
INTERFACE=beVWARS0 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS1 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS2 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS3 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS4 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS5 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS6 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS7 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS8 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS9 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS10 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS11 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS12 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS13 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS14 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beVWARS15 beVWARS.sh /IN/service_packages/E2BE/bin EVENT
```

However, it is also defined in the BE{} section of eserv.config, which saves time and complexity:

```
numVWARS = 16
```
**beSync process**

beSync is responsible for keeping the Primary and Secondary Billing Engine pair in the same state at any given time.

Each time the beVWARS performs an interaction on the database, a sync file is written to the beSync repository - usually `/IN/service_packages/E2BE/sync/<beVWARS Instance #>`.

These sync files are processed by beSync and used to write the information to the other Billing Engine in the pair. After they are completed the files are deleted. The number of files waiting to be processed can be indicative of an unsynchronized Billing Engine pair.

When only one node in a Billing Engine pair is running, all the information yet to be sent to the other node will start collecting in the beSync repository and will continue to do so until it comes back up.

beSync will also transmit information about new reservations, ensuring that both Billing Engine nodes are aware of any ongoing uncharged funds. The result is that the Primary can go down mid-call, and the subscriber will not be aware that anything has gone wrong.

**Billing Engine startup**

Upon startup, beSync will ask each local beVWARS for their last written sequence number.

beSync uses this, and the BE_VWARS_SEQ_NUM table in the database, to track what updates are yet to be synced between the machines in the pair and begin syncing immediately.

Since beServer will not accept any connections until the Billing Engine is completely up to date, it can be prudent to monitor the backlog in `E2BE/sync` to see how it is progressing.

beSync will also collect reservations from the other node, so it is completely up to date.

**beGroveller process**

beGroveller is responsible for searching the database for unused wallets, and sending them to the correct beVWARS process when requested.

During normal processing, events are triggered only when a subscriber interacts with the wallet. Some events (such as expiry and periodic charges) should be triggered regardless of whether the wallet has been used by a subscriber recently or not.

**Event processing**

In order to process these events, beGroveller collects and sends lists of wallets IDs to beVWARS for processing. This processing triggers any events which are due to occur in the same way a normal interaction would, except wallets triggered from beGroveller lists do not trigger any message handlers.

**No-processing times**

In general it is not imperative that buckets are expired in real-time, and grovelling unused wallets consumes resources that beVWARS would otherwise be using to process regular traffic.

For this reason beGroveller contains some configuration (beGroveller{} section in `eserv.config`) for running only during certain times of the day:

```plaintext
noProcessingTimes = [
  { startsAt = "06:00", endsAt = "09:30" }
]
```

During these no-processing times when the beVWARS asks for more wallets to grovel, beGroveller will report that there are none.
beGroveller scalability

Like beVWARS, beGroveller is also a scalable process, and runs multiple instances on the NCC platform. Although the beGroveller uses the same algorithm for calculating which beGroveller is going to serve a particular wallet, it does not need to run the same number of instances as beVWARS - it will often run much less.

Both beVWARS and beGroveller are able to determine the instances of the other, and will access the appropriate instance accordingly.

Workload spreading

The algorithm for this is WalletID MOD Total_beGroveller_Instances

The number of instances created is determined by /IN/service_packages/SLEE/etc/SLEE.cfg. For example:

```
INTERFACE=beGroveller0 beGroveller.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beGroveller1 beGroveller.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beGroveller2 beGroveller.sh /IN/service_packages/E2BE/bin EVENT
INTERFACE=beGroveller3 beGroveller.sh /IN/service_packages/E2BE/bin EVENT
```

However, it is also defined in the BE{} section of eserv.config - which saves time and complexity:

```
numGrovnellers = 4
```

Useful Commands and Scripts

Introduction

This topic lists a few useful scripts for investigating a billing issue.

Without access to the SMS screens (quite common when dealing with a production environment) it can be difficult to ascertain basic information about a subscriber and their wallets.

showCli.sh

This script displays the basic information about a CLI in the database. At a glance it will tell you:

- whether the number exists in the database, and
- if so, some useful information about their entry (including defined wallet IDs)

It can also be used to compare the information on the SMS database with the VWS (or SLC) database; thus allowing a quick check that replication is functioning.

All databases should always have the same information. If there are differences, there could be an issue with replication, and a full resync may be required.

Machine Type: SMS, VWS, SLC

Location: /IN/service_packages/CCS/bin/showCli.sh

Usage: ./showCli.sh CLI/MSISDN

Example Output:

```
/IN/service_packages/CCS/bin$ ./showCli.sh 12345
CLI        ACCT_REFERENCE NAME                            WALLET ACCOUNT_NUMBER
----------   ------------------------------- --------------
12345                2143                         Primary   2143           1656
```

showWallet.sh

This script displays the contents of a subscriber's wallet. At a glance it will give you information on the wallet state, and what buckets are contained within that wallet, including expiry dates and references.
It can also be used to compare the information on the Primary and Secondary Billing Engine databases - thus allowing a quick check that the Billing Engine pair is in sync. Unless one of the nodes has been down for an extended period of time, and is still being brought into sync (in which case it will not be handling traffic), the results on both Billing Engine nodes should have the same information in the database.

**Note:** beVWARS operates a cache, so the database will not necessarily reflect a subscriber’s available funds. Ongoing reservations are not written to the database until they are confirmed. A subscriber could legitimately appear to have sufficient funds for a call in the database, but have insufficient funds due to an in-progress reservation.

**Machine Type:** VWS

**Location:** /IN/service_packages/E2BE/bin/showWallet.sh

**Usage:** ./showWallet.sh WalletID

**Example Output:**

```
/IN/service_packages/E2BE/bin$ ./showWallet.sh 2143
Showing wallet 2143 on e2be_admin

<table>
<thead>
<tr>
<th>ID</th>
<th>MAX_CONCURRENT</th>
<th>S</th>
<th>NEVER_EXPIRES</th>
<th>EXPIRY</th>
<th>NEVER_ACTIVATED</th>
<th>ACTIVATION_DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2143</td>
<td>10</td>
<td>A</td>
<td>1</td>
<td>20100701022600</td>
<td>0</td>
<td>20100726035409</td>
</tr>
</tbody>
</table>

WALLET BALANCE_TYPE | NEVER_EXPIRES | MINIMUM_CREDIT |
-------------------|---------------|----------------|
2143               | 22 D          | 0              |
2143               | 27 D          | 0              |

2 rows selected.

<table>
<thead>
<tr>
<th>ID</th>
<th>WALLET</th>
<th>BALANCE_TYPE</th>
<th>NEVER_EXPIRES</th>
<th>EXPIRY</th>
<th>VALUE</th>
<th>NEVER_USED</th>
<th>LAST_USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>16734</td>
<td>2143</td>
<td>22</td>
<td>0</td>
<td>20111106040400</td>
<td>500</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>20101122043401</td>
<td>16998</td>
<td>2143</td>
<td>27</td>
<td>0</td>
<td>19700101000000</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>20101123033753</td>
<td>17078</td>
<td>2143</td>
<td>27</td>
<td>0</td>
<td>20101223041742</td>
<td>600</td>
<td>0</td>
</tr>
</tbody>
</table>

6 rows selected.

**Tip:** The output is wrapped, and generally easier to read within a terminal window.
Overview

Introduction

This chapter explains the important processes on each of the server components in the NCC, and a number of example troubleshooting methods which will help aid the troubleshooting process before raising a support ticket.

In this chapter

This chapter contains the following topics.

Common Troubleshooting Procedures

Common Troubleshooting Procedures

Introduction

To troubleshoot the product, first you must identify the system which is responsible for the service which needs troubleshooting.

As explained in the Product System Architecture section, there are three main server components in the NCC:

- **Service Logic Controller (SLC)**
  
  The SLC is responsible for most real-time service processing (for example, voice/SMS/data). Call handling issues are likely to require troubleshooting on the SLC.

- **Service Management System (SMS)**
  
  The SMS is responsible for provisioning, data warehousing and replication. Issues specific to certain subscribers, coinciding with important changes to rating, concerning EDRs or with external provisioning (via the Provisioning Interface (PI)) require troubleshooting on the SMS.

- **Voucher and Wallet Server (VWS)**
  
  The VWS is responsible for voucher redemption and call rating (this includes balance management and promotions tracking). Issues concerning subscribers' balances, top-ups and vouchers are likely to require troubleshooting on the VWS.

Important notice

Please note that NCC packages are complete versions and were tested as such.

If you have any questions or problems, please contact Oracle Communications Network Charging and Control Support Organization by submitting an SR through Metalink or by referring to the Oracle website for the support contact information in your country.

The Oracle support website is located at [http://www.oracle.com/support/contact.html](http://www.oracle.com/support/contact.html).
**General tools**

The following information is not specific to any particular type of node, and can be helpful when investigating any problem situation.

The list of processes is built from `inittab`, and will highlight any defined that are not running. If a SLEE is present, its configuration will be parsed, and SLEE processes included in the list.

**Process status**

There are a few basic checks that can be run on any of the machines, which are provided as part of the supportScp (SLC/VWS) or supportSms (SMS) packages. These give you a quick look at what processes are running.

**Example - pslist**

This example shows the `pslist` command used with no parameters.

Command:

```
$ pslist
```

Result:

```
------------------------ Thu Oct 24 04:56:53 GMT 2010 ------------------------
C APP USER PID PPID STIME COMMAND
1 ACS acs_oper 1004 1 04-Oct /service_packages/ACS/bin/acsCompilerDaemon
1 ACS acs_oper 1008 1 04-Oct /service_packages/ACS/bin/acsProfileCompiler
1 ACS acs_oper 13833 1 00:12:38 ice_packages/ACS/bin/acsStatisticsDBInserter
1 OSD acs_oper 1047 1 04-Oct /service_packages/OSD/bin/osdWsdRegenerator
1 CCS ccs_oper 1033 1 04-Oct /IN/service_packages/CCS/bin/ccsCDRFileGenerator
1 CCS ccs_oper 13833 1 00:12:38 ice_packages/ACS/bin/acsStatisticsDBInserter
2 CCS ccs_oper 1406 1043 04-Oct /IN/service_packages/CCS/bin/ccsProfileDaemon
1 CCS ccs_oper 9413 1 04-Oct /IN/service_packages/CCS/bin/ccsChangeDaemon
1 EFM smf_oper 995 1 04-Oct /IN/service_packages/EFM/bin/smsAlarmManager
1 PI smf_oper 1050 1 04-Oct /IN/service_packages/PI/bin/PImanager
6 PI smf_oper 1319 1050 04-Oct PIprocess
1 PI smf_oper 9186 1050 04-Oct PIbeClient
2 SMS smf_oper 6173 1 21-Oct /IN/service_packages/SMS/bin/smsMaster
1 SMS smf_oper 941 1 04-Oct /IN/service_packages/SMS/bin/smsAlarmRelay
1 SMS smf_oper 943 1 04-Oct /IN/service_packages/SMS/bin/smsNamingServer
1 SMS smf_oper 944 1 04-Oct /IN/service_packages/SMS/bin/smsReportsDaemon
1 SMS smf_oper 946 1 04-Oct /IN/service_packages/SMS/bin/smsReportScheduler
1 SMS smf_oper 947 1 04-Oct /IN/service_packages/SMS/bin/smsAlarmDaemon
1 SMS smf_oper 948 1 04-Oct /IN/service_packages/SMS/bin/smsStatsThreshold
1 SMS smf_oper 949 1 04-Oct /IN/service_packages/SMS/bin/smsTaskAgent
1 SMS smf_oper 969 1 04-Oct /IN/service_packages/SMS/bin/smsTrigDaemon
2 SMS smf_oper 979 1 04-Oct /IN/service_packages/SMS/bin/smsConfigDaemon
1 SMS smf_oper 980 1 04-Oct /IN/service_packages/SMS/bin/smsStatsDaemonRep
```

**Example - pslist -d**

This example shows the `pslist` command used with the `-d` parameter. From time to time, processes will be added to or removed from `inittab/SLEE`. The `-d` parameter instructs pslist to reconstruct the list.

Command:

```
$ pslist -d
```

Result:

```
Scanning input file. 
[ /etc/inittab ]
Scanning input file. 
[ /IN/service_packages/SLEE/etc/SLEE.cfg ]
Info: Did not find SLEE config file [ /IN/service_packages/SLEE/etc/SLEE.cfg ]
```

Does the SLEE application exist on this machine?
Processes also have command line arguments, which are passed in the calling shell script.

Some NCA interface configuration is also housed in a separate file; for example, for SIGTRAN interfaces (sua_if/m3ua_if) the configuration is often specified in

```
/IN/service_packages/SLEE/etc/sigtran.config
```

Configuration for NCC products and processes are made almost exclusively in the file

```
/IN/service_packages/eserv.config
```

The file is broken down into sections and subsections, grouped together by {} brackets. Each product respectively.

There are some exceptions, notably ACS and SLEE, which have some separate configuration files in

```
/IN/service_packages/ACS/etc/acs.conf and /IN/service_packages/SLEE/etc/SLEE.cfg
```

Some NCA interface configuration is also housed in a separate file; for example, for SIGTRAN interfaces (sua_if/m3ua_if) the configuration is often specified in

```
/IN/service_packages/SLEE/etc/sigtran.config or interface_service.config
```

Note: Processes also have command line arguments, which are passed in the calling shell script - normally named

```
/IN/service_packages/<Product>/bin/ProcessNameStartup.sh
```

Support audit

Oracle Support can track changes made to the platform by collecting machine configuration through

```
gatherConfig.sh
```

Delivered as part of the supportScp (SLC/VWS) or supportSms (SMS) packages, it can be scheduled to run from the root crontab, or run by hand periodically and be provided to Oracle Support for inclusion into the database.
Example gatherConfig.sh

```
/IN/service_packages/SUPPORT/bin/gatherConfig.sh /IN/service_packages/SUPPORT/audit `hostname` -date +%Y%m%d > /IN/service_packages/SUPPORT/tmp/gatherConfig.log 2>&1
```

The resulting audit, named `hostname-date.tar.gz` will be found in `/IN/service_packages/SUPPORT/audit`

cmnPushFiles/cmnnReceiveFiles

cmnPushFiles is responsible for monitoring a location on the SLC/VWS for new files, and will "push" the files to the SMS.

cmnPushFiles is called from init script, and will run in run-level 3 and generally runs multiple instances.

Each instance will monitor the EDRs of a certain product or process (for example, MM EDRs created by xmsTrigger, ACS EDRs created by slee_acs), however it can also be used to push expiry messages or notifications between machines.

In order for cmnPushFiles to successfully "push" files to the SMS, the network service cmnReceiveFiles must be configured on the SMS in `/etc/inetd.conf` and `/etc/services`

cmnPushFiles is crucial to the EDR processing chain, and if it is not running or configured incorrectly, then files will build up on the SLC/VWS indefinitely until the system runs out of disk space.

Example - PushFiles

Consider this sample output from a VWS:

```
$ ps -ef | grep Push
```

```
  ebe_oper 12479 ... cmnPushFiles -d /IN/service_packages/E2BE/logs/CDR-out -r /IN/service_packages/
  ccs_oper 12519 ... cmnPushFiles -d /IN/service_packages/CCS/logs/expiryMessage/ -r /IN/service_package
  ccs_oper 12480 ... cmnPushFiles -d /IN/service_packages/CCS/logs/wallet -r /IN/service_packages/CC
  ccs_oper 12482 ... cmnPushFiles -d /IN/service_packages/CCS/logs/ccsNotificationWrite/ -r /IN/serv
```

The command response shows there are four instances of cmnPushFiles running.

Using the arguments given to the process, what the process is responsible for can usually be determined:

```
$ pargs 12479
```

```
12479: cmnPushFiles -d /IN/service_packages/E2BE/logs/CDR-out -r /IN/service_packages/
argv[0]: cmnPushFiles
argv[1]: -d
argv[2]: /IN/service_packages/E2BE/logs/CDR-out
argv[3]: -r
argv[4]: /IN/service_packages/CCS/logs/wallet
argv[5]: -h
argv[6]: usms.CdrPush
argv[7]: -F
```

Here we see this cmnPushFiles is taking completed EDRs from CDR-out on the VWS and sending them to CDR-in on the SMS.

Space issues

If the cmnPushFiles log file (`/IN/service_packages/E2BE/tmp/cmnPushFiles`), or the syslog is reporting insufficient space, checking available space in CDR-out on the VWS and CDR-in on the SMS will be the first step to diagnosing the problem.

Core files

When monitoring a platform, or investigating issues, it is important to check for core files.

Processes running from init script will be automatically restarted by Solaris, and processes running inside the SLEE will be restarted by the watchdog if they stop running.

If a process cores due to a recurring traffic scenario, it will be restarted and continue to core until the mount point runs out of disk space.
Core file location
The location of core files differs depending on configuration, and how the process was started.

The first thing to check is the output of coreadm, which specifies how the operating system will handle core files.

Multiple core locations
In this example, core files will write to the directory they were called from (in the case of SLEE processes, this will be `/IN/service_packages/SLEE/bin`), and will be named simply `core`. In this situation, the majority of `/IN/service_packages` will need to be checked for core files.

```
$ coreadm
  global core file pattern: core
  global core dumps: disabled
  per-process core dumps: enabled
  global setid core dumps: disabled
  per-process setid core dumps: disabled
  global core dump logging: disabled
```

Single core location
However, if configured as in this example, all core files will be written to one central location (often on a separate mount point). In this situation, only one directory/mount needs to be checked.

This can also reduce the risk of an important mount point getting filled up with core files.

```
$ coreadm
  global core file pattern: /var/crash/core-%n-%p-%f
  global core file content: default
  init core file pattern: core
  init core file content: default
  global core dumps: enabled
  per-process core dumps: disabled
  global setid core dumps: enabled
  per-process setid core dumps: disabled
  global core dump logging: enabled
```

Diagnostic information
Processes that core can be a risk to the platform for many reasons, and should be dealt with as quickly as possible.

In general they indicate a software fault that will require investigation by Oracle Engineering, so it is important to collect the following diagnostic information:

**Gdb backtrace**
In order for Oracle Engineering to investigate a core file, the most important piece of information (apart from the core itself) is the gdb backtrace.

Follow these steps to collect the backtrace.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>If not possible from the filename itself, determine what process created the core, using the file command.</td>
</tr>
</tbody>
</table>

```
$ file core
  core.: ELF 32-bit MSB core file SPARC Version 1, from 'slee_acs'
```
Step | Action
--- | ---
2 | Open the core using gdb, with the original binary and the core file as arguments.  

**Note:** The exact binaries and libraries that generated the core file are required. If the product version has changed, it is unlikely gdb will be able to interpret the core correctly.

```bash
$ gdb /IN/service_packages/ACS/bin/slee_acs core
```

GNU gdb 6.6  
Copyright (C) 2006 Free Software Foundation, Inc.  
GDB is free software, covered by the GNU General Public License, and you are welcome to change it and/or distribute copies of it under certain conditions.  
Type "show copying" to see the conditions.  
There is absolutely no warranty for GDB. Type "show warranty" for details.  
This GDB was configured as "sparc-sun-solaris2.10"...

warning: core file may not match specified executable file.
Reading symbols from /usr/lib/libumem.so.1...done.
Loaded symbols for /usr/lib/libumem.so.1
Reading symbols from /IN/service_packages/ACS/lib/libacsDummy.so...done.
Loaded symbols for /IN/service_packages/ACS/lib/libacsDummy.so
…snip…
Reading symbols from /IN/service_packages/RIMS/lib/librimsMacroNodes.so...done.
Loaded symbols for /IN/service_packages/RIMS/lib/librimsMacroNodes.so
Reading symbols from /IN/service_packages/LCP/lib/liblcpmacronodes.so...done.
Loaded symbols for /IN/service_packages/LCP/lib/liblcpmacronodes.so
Reading symbols from /lib/ld.so.1...done.
Loaded symbols for /lib/ld.so.1
Core was generated by `/IN/service_packages/ACS/bin/slee_acs'

Result: Eventually you will be presented with the most recent frame of the core, the signal which ended the process, and a (gdb) prompt.

Program terminated with signal 10, Bus error.  
#0 0xfe2d6328 in _smalloc () from /lib/libc.so.1
(gdb)

3 | To view all frames in the core, initiate a summary backtrace by typing `bt` at the prompt, see **Example summary backtrace** (on page 70).

(gdb) bt

4 | To view all frames and all their information in the core, initiate a full backtrace by typing `bt full` at the prompt, see **Example full backtrace** (on page 71).

(gdb) bt full

**Note:** This information will need to be provided to Oracle Support for further investigation.

**Example summary backtrace**  
Initiate a summary backtrace by typing `bt` at the prompt, all frames in the core will be shown:

```
(gdb) bt
#0 0xfe2d6328 in _smalloc () from /lib/libc.so.1
#1 0xfe2d659c in malloc () from /lib/libc.so.1
#2 0xfe6f3540 in operator new (sz=4) at new_op.cc:48
#3 0xfd318fa4 in cmn::escher::Array::push_back (this=0x18c1ce8, val=@0xffbfd030) at cmnEscherEntry.hh:229
#4 0xfd55248 in ccs::Message::CDR::appendFromString (this=0xffbfd0d8, fields=  
  [static npos = 4294967295, _M_dataplus = {<allocator<char>> = {<No data fields>}, _M_p = 0x18c08c4 "CLI=64225750736|ACS_CUST_ID=12|PC_AC=1|PC_PRC=1|TZ=NZ|PC_SCD=D07"}, static  
  _S_empty_rep_storage = {0, 0, 0, 0}) at /volB/DEV_BASE/AB7_2DEG_HILLARY/ndonebug/CCS/include/ccsMessage.hh:1581
#5 0xfd030ac in fox::ExtendedWalletUpdate::doAction (this=0x1a13cb0, request=@0x1,  
  responseRequired=0xfffebfe40, actionResponse=0x29c00,  
  context=0xffb0d0e0, serviceContext=0x19eb4b8, parms=0xffb0d2b0) at /opt/gcc-  
  3.2.3/include/c++/3.2.3/bits/stl_alloc.h:664
```
Example full backtrace

Initiate a full backtrace by typing `bt full` at the prompt; all frames and all information contained in them will be shown. This can sometimes be many pages, and can sometimes result in endless junk information - collect as much as appears useful. The example below causes gdb to crash after the 5th frame:

(gdb) bt full
#0 0xfe2d6328 in _smalloc () from /lib/libc.so.1
No symbol table info available.
#1 0xfe2d639c in malloc () from /lib/libc.so.1
No symbol table info available.
#2 0xfed35248 in ccs::Message::CDR::appendFromString (this=0xffbfd0d8, fields=
{static npos = 4294967295, _M_dataplus = {<allocator<char>> = {<No data fields>}, _M_p = 0x18c08c4 "CLI=64225750736|ACS_CUST_ID=12|PC_AC=1|PC_PRC=1|TZ=NZ|PC_SCD=D07"}, static _S_empty_rep_storage = {0, 0, 0, 0}}) at
/volB/DEV_BASE/AB7_2DEG_HILLARY/nondebug/CCS/include/ccsMessage.hh:1581
field = {pimpl = {rep = 0x1a25af0}}
val = {static npos = 4294967295, _M_dataplus = {<allocator<char>> = {<No data fields>}, _M_p = 0x18a0f94 "PC_SCD"}, static _S_empty_rep_storage = {0, 0, 0, 0})
cdrEntry = {static npos = 4294967295, _M_dataplus = {<allocator<char>> = {<No data fields>}, _M_p = 0x1800e00 "PC_SCD=D07"}, static _S_empty_rep_storage = {0, 0, 0, 0}}
equals = 4290760752
start = 4290760768
end = 64
#5 0xfed350ac in fox::ExtendedWalletUpdate::doAction (this=0x1a13cb0, request=0xffbefeb40, responseRequired=0xffbfdfb0, actionResponse=0x1a8c80, context=0x1a8e828, serviceContext=0x1a8e808, parms=0x1a8e8b0) at /opt/gcc-3.2.3/include/c++/3.2.3/bits/stl_alloc.h:664
cdr = {<Array> = (pimpl = {rep = 0x1a28d40}), <No data fields>}
parms = (acsChassisActionParms &) 0x1: <error reading variable>
eurw = {class ExtendedWalletUpdateRequest * 0xffbeeb40
balanceInfoArray = {<Array> = {<No data fields>}, <error reading variable>}
addBalanceInfoArray = true
sbbia = (class SmallBalanceBucketInfoArray
Segmentation Fault (core dumped)
Memory leaks

While monitoring the platform, it may be determined that a certain process is constantly increasing in memory, indicating a memory leak. Oracle Solaris has built in tools to diagnose these further - all of which is useful to the investigations of Oracle Engineering.

Memory leaks can be a great risk to the platform, as other processes will struggle to run if the machine does not have a sufficient amount of free memory. In low memory situations the OS will start paging information in and out of memory, causing a performance impact, and system instability.

A slow leak may pose little danger to the platform; however it is prudent to investigate sooner rather than later. In general leaks indicate a software fault that will require investigation by Oracle Engineering, so it is important to collect the following diagnostic information as soon as possible:

Libumem

Oracle Solaris comes with libumem memory diagnostic libraries, which are run by setting environment variables prior to running a binary. This is usually achieved by changing the startup shell script for each process causing issues. After running the binary long enough for the leak to present, the process can then be instructed to core. The resulting core contains information that helps tell a developer exactly where in the code the un-released memory was allocated. The information will need to be provided to NCC Support for further investigation.

Follow these steps to collect this information:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1    | Locate the startup script for the problem process.  
For SLEEE processes, this is located on the APPLICATION or INTERFACE line of /IN/service_packages/SLEE/etc/SLEE.cfg  
For example, xmsTrigger.  
INTERFACE=xmsIf xmsTrigger.sh /IN/service_packages/XMS/bin 
EVENT  
The startup script is therefore /IN/service_packages/XMS/bin/xmsTrigger.sh  
For INIT processes, this is located in /etc/inittab  
For example, updateLoader  
scp5:34:respawn:su - smf_oper -c "exec /IN/service_packages/SMS/bin/updateLoaderStartup.sh >> /IN/service_packages/SMS/tmp/updateLoader.log 2>&1" > /dev/null 2>&1 0<&1  
The startup script is therefore /IN/service_packages/SMS/bin/updateLoaderStartup.sh  
See NCC process identification (on page 9) and SLEE.config (on page 35) for more information.  
Note: In this example, we will use the Messaging Manager binary xmsTrigger |
| 2    | Open the startup script for editing, and add lines to enable libumem. Type the command:  
$ vi /IN/service_packages/XMS/bin/xmsTrigger.sh  
Result: The following is displayed.  
#!/usr/bin/ksh  
exec /IN/service_packages/XMS/bin/xmsTrigger "uas01" >> /IN/service_packages/XMS/tmp/xmsTrigger.log 2>&1 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 3    | Type the following lines before the exec command to enable libumem:  
  # libumem options  
  UMEM_DEBUG=default  
  UMEM_LOGGING=transaction  
  LD_PRELOAD_32=/usr/lib/libumem.so.1  
  export UMEM_DEBUG UMEM_LOGGING LD_PRELOAD_32 |
| 4    | Restart the process, either by issuing a `kill` command, or for this example by restarting the SLEE. Type the command:  
  `$ slee-ctrl restart` |
| 5    | Generate enough traffic, or wait enough time for the leak to present itself. One way to check for this is by using the output of `pmap PID | grep heap`. If the heap is constantly increasing in size, it is likely the result of leaked memory. For example:  
  `$ pmap 10645 | grep heap`  
  $00282000 1528K rwx-- [ heap ]  
  ...  
  `$ pmap 10645 | grep heap`  
  $00282000 3056K rwx-- [ heap ] |
| 6    | Be sure to double-check the process is running the appropriate libumem library. For example:  
  `$ pldd 10645| grep umem`  
  /lib/libumem.so.1 |
| 7    | Tell the process to create a core file using gcore. For example:  
  `$ gcore 10645`  
  gcore: core.10645 dumped |

**Note:** Depending on the size of the process memory footprint, this may take some time. If the process is a SLEE process, consider first killing the SLEE watchdog, so that the process is not perceived as unresponsive and restarted automatically by the watchdog.
### Chapter 7

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 8    | Open the core with mdb. When presented with a > prompt, enable symbol demangling and try to find the leaks using ::findleaks.  
In the example below, there are a number of entries which have leaked just 1 - these are usually fine. Anything higher than 1 is potentially a legitimate leak that needs addressing.  
Type the command:  
```bash  
mdb core.10645  
```  
Loading modules: [ libumem.so.1 libc.so.1 ld.so.1 ]  
At the > prompt, type:  
```bash  
> $G  
C++ symbol demangling enabled  
> ::findleaks  
```
| Result: The list of leaked entries is shown.  
<table>
<thead>
<tr>
<th>CACHE</th>
<th>LEAKED</th>
<th>BUFCTL</th>
<th>CALLER</th>
</tr>
</thead>
<tbody>
<tr>
<td>0035408</td>
<td>1</td>
<td>003828e8</td>
<td>libc.so.1`strdup+0xc</td>
</tr>
<tr>
<td>0035208</td>
<td>1</td>
<td>003e5950</td>
<td>libcintlsh.so.9.0`nlfinit+0x78</td>
</tr>
<tr>
<td>0034de08</td>
<td>1</td>
<td>003dd0e0</td>
<td>libcintlsh.so.9.0`nlthnew+4</td>
</tr>
<tr>
<td>0035e08</td>
<td>1</td>
<td>005248</td>
<td>libcintlsh.so.9.0`nlhtns1+4</td>
</tr>
<tr>
<td>0035408</td>
<td>1</td>
<td>0038a250</td>
<td>libcintlsh.so.9.0`nlpains+0x48</td>
</tr>
<tr>
<td>0034da08</td>
<td>1</td>
<td>00383068</td>
<td>libstdc++.so.5.0.3`_Znwj+0x1c</td>
</tr>
<tr>
<td>0035608</td>
<td>1</td>
<td>00368e88</td>
<td>libstdc++.so.5.0.3`_Znwj+0x1c</td>
</tr>
<tr>
<td>0035408</td>
<td>1</td>
<td>00382a50</td>
<td>libclntsh.so.9.0`nlhtnsl+4</td>
</tr>
<tr>
<td>0034da08</td>
<td>1</td>
<td>003830e0</td>
<td>libclntsh.so.9.0`nlpains+0x48</td>
</tr>
<tr>
<td>0035608</td>
<td>1</td>
<td>00360078</td>
<td>libstdc++.so.5.0.3`_Znwj+0x1c</td>
</tr>
<tr>
<td>0035408</td>
<td>1</td>
<td>00383008</td>
<td>libstdc++.so.5.0.3`_Znwj+0x1c</td>
</tr>
<tr>
<td>0035408</td>
<td>1</td>
<td>003830d0</td>
<td>libstdc++.so.5.0.3`_Znwj+0x1c</td>
</tr>
<tr>
<td>0035608</td>
<td>1</td>
<td>003600f0</td>
<td>libstdc++.so.5.0.3`_Znwj+0x1c</td>
</tr>
<tr>
<td>0034dc08</td>
<td>1</td>
<td>003de168</td>
<td>mmxiSMPP.so`default_malloc_ex+0xc</td>
</tr>
<tr>
<td>Total</td>
<td>18 buffers, 10264 bytes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9 To view more information about trouble entries (for example 003da168 - 3 leaks), use the bufctl_audit command with the address of the leak.  
For example, type:  
```bash  
> 003da168$<bufctl_audit  
```
| Result: The leak information is displayed (see at end of procedure.  
| Note: Alternatively run ::findleaks -d, which will automatically display the bufctl_audit for all of the reported buffers.  

#### 003da168 leak report  
<table>
<thead>
<tr>
<th>ADDR</th>
<th>BUFADDR</th>
<th>TIMESTAMP</th>
<th>THREAD</th>
<th>CACHE</th>
<th>LASTLOG</th>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>3da168</td>
<td>3d9868</td>
<td>32bc1722f96e</td>
<td>1</td>
<td>3da168</td>
<td>33f324</td>
<td></td>
</tr>
<tr>
<td></td>
<td>34de08</td>
<td>33f324</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libumem.so.1`umem_cache_alloc+0x13c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libumem.so.1`umem_alloc+0x60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libumem.so.1`malloc+0x28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`default_malloc_ex+0xc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`CRYPTO_malloc+0x4c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`BN_new+0x10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`xms::smpp::ProtocolHandler::convertBNDec1dToHex+0x358</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`xms::smpp::ProtocolHandler::isMatchMessageId+0x2a8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`xms::smpp::ProtocolHandler::updateSMPPRequest+0xdef0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mmxiSMPP.so`xms::smpp::ProtocolHandler::makeSMPPRequest+0x75c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Log files

All NCC processes write to their own log file, usually /IN/service_packages/<Product>/tmp/Process.log.

They will also write errors to the syslog, which generally has a longer retention period than log files. Log files are maintained by smsLogCleaner, which runs from each user's crontab using configuration in /IN/service_packages/Product/etc/logjob.conf usually once per hour.

Logs are archived to /IN/service_packages/Product/tmp/archive/ and usually kept for seven days (configurable on the command line).

When a process is put in debug, this extra information is written to the log file only.

Note: Files archived by smsLogCleaner can have their names changed.

Debug

All NCC processes contain debug flags, which can be used to collect useful diagnostic information in the event of issues.

This is done in two main ways:

1. by specifying debug flags in the startup script - which results in debug for all processing as long as the process is up.
2. by setting tracing parameters inside configuration files.

The first is available to all NCC processes, the second to a select few traffic handling applications which require more targeted debugging.

Startup flags

After locating the process startup script, debug flags can be specified via environment variable (debug statement highlighted):

    $ vi slee_acs.sh
    #!/usr/bin/ksh
    DEBUG=all,-COMMON_escher,-COMMON_escher_detail,-COMMON_PD,-COMMON_Utils,-slee_api
    export DEBUG
    exec /IN/service_packages/ACS/bin/slee_acs  >>
    /IN/service_packages/ACS/tmp/slee_acs.log 2>&1

The flags available differ by process, and generally Oracle Support will advise the flags required. DEBUG=all covers all debug defined in the process, but will be quite verbose so should be limited.

Flags can be subtracted from "all" or individual flags specified.

Available flags

To find out all the options available to a specific process, use the strings command along with grep.

For example type:

    $ strings slee_acs.sh | grep cmnDebug_FLAG

Result: All the flags available are listed.

    cmnDebug_FLAG_Engine
    cmnDebug_FLAG_Chassis
    cmnDebug_FLAG_ACS_Chassis_CdrWrite
    cmnDebug_FLAG_slee_acs
cmnDebug_FLAG_misc
cmnDebug_FLAG_COMMON_Utils
cmnDebug_FLAG_COMMON_Utils_cmnUnit
cmnDebug_FLAG_acsChassisSLEE
cmnDebug_FLAG_acsNOA
cmnDebug_FLAG_acsAWOL
cmnDebug_FLAG_acsCommon
cmnDebug_FLAG_acsCdr
cmnDebug_FLAG_Config
cmnDebug_FLAG_ConfigFileImpl
cmnDebug_FLAG_cmnPrefixTree
cmnDebug_FLAG_COMMON_cmnTime
cmnDebug_FLAG_cmnAssert
cmnDebug_FLAG_ACS_NotifIF

Note: The cmnDebug_FLAG_ prefix part is assumed by debug so can be left off when configuring the Debug command.

Flags to avoid
The following flags are used by the majority of processes, and result in a lot of debug.
They are recommended to be removed unless otherwise requested.

- COMMON_escher[_detail]
- COMMON_FD
- COMMON_Utils
- slee_api

Selective tracing
Selective debug is available to some of the more important real-time traffic handling processes. These include:

- slee_acs
- beVWARS
- xmsTrigger

In each case, a configurable tracing section contains a list of criteria for tracing (A-party and B-party for slee_acs, walletid for beVWARS), and will temporarily switch to debug for the duration of the triggering event.

Configuration can be made in eserv.config in the tracing{} section of the process, which is explained in full detail in the technical guides.

Once set, the process can be sent a SIGHUP signal to re-read its configuration, including the tracing section.

Tracing example
For example, here is an ACS tracing{} section for slee_acs:

```plaintext
tracing = {
    # Is tracing enabled? (default false)
    enabled = true

    # Originating Addresses that we want to trace
    origAddress = ["12345"]

    # Destination Addresses that we want to trace
    destAddress = ["12345"]
}
```
# What debug level should the tracing be at?
traceDebugLevel = "all"

xmsTrigger tracing
xmsTrigger tracing is set in the same fashion; however the resulting information goes to a separate file xmsTrigger.trc, does not contain debug, but does capture all the major decision points in a transaction.

Trace points are defined as:

**Input**

1. Message received from network With which addresses?
2. Message decoding information
   - Do we allow alternate delivery?
   - Which protocol version is this?
   - What was the message text (if showPrivate)?
3. Message passed to Messaging Manager
   - Result from ParentContext::handleSMSubmit?
4. Response received from MM
5. Response sent to network

**Output**

1. SMSubmit received from Messaging Manager
   - Is the delivery type SME or MC?
   - Do we need to consult a third party (for example, HLR) for any reason?
   - What are the addresses involved?
2. Outgoing encoding information
   - Which protocol version are we using?
3. Message sent to network
4. Response received from network
5. Response sent to Messaging Manager

**Snoop traces**

When dealing with issues related to real-time traffic handling, it is imperative to have reference snoop traces to observe the behavior of the NCC software at the network/signaling level.

This information allows analysis of incoming messages, the responses sent back and the timing. Each standard is thoroughly documented and must conform to the appropriate specifications.

Snoop traces allow there to be no uncertainty about the conversation between the NCC platform and external components.

**Running a snoop trace**

Snoops are initiated as the root user. Command line arguments give the user a fair amount of control over what gets collected; from the interface to the port and transport protocol.

At a rudimentary level, snoop can be instructed to display all incoming traffic for an interface. However, it is more useful to first determine what traffic is required (the more detail the better) and save to a file for analysis in a trace interpreter.

To see a list of all the snoop command line parameters, type:
$ man snoop

This gives a full list, with definitions.

**Snoop example**

In this example, diameterControlAgent has a handle on the local address 172.21.153.142 on port 3868. Using ifconfig, this is shown to be on interface e1000g1.

**Note:** Network Connectivity Agents (NCAs) commonly use more than one interface for receiving/sending information. There are failover and loadsharing scenarios where this is required. The groupname specified will sometimes indicate the type of traffic, for example, "SIG-A" and "SIG-B" shows that more than one interface is used for SIGTRAN.

First, determine the interface the target process is attached to. This can be achieved by checking the output of ifconfig, inspecting the process with pfiles and cross-checking the results as highlighted:

```
$ ps -ef | grep diameterControlAgent
acs_oper 160 1 0 Oct 20 ? 251:34 diameterControlAgent
$ pfiles 160 | grep sock
  socketname: AF_UNIX /tmp/dcaIf-0.0.112.20101020123758
  socketname: AF_INET 0.0.0.0 port: 3868
  socketname: AF_INET 172.21.153.142 port: 3868
  socketname: AF_INET 172.21.153.142 port: 3868
$ ifconfig -a
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
e1000g0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.21.153.82 netmask fffffffc0 broadcast 172.21.153.127
    groupname mgmt
    inet 172.21.153.142 netmask ffffffff00 broadcast 172.21.153.159
    groupname chr
    inet 172.21.153.140 netmask ffffffff00 broadcast 172.21.153.159
    groupname sig
    inet 172.21.153.100 netmask ffffffff00 broadcast 172.21.153.255
    groupname sig
    inet 172.21.153.104 netmask ffffffff00 broadcast 172.21.153.255
    groupname chrg
    inet 172.21.153.205.27 netmask ffffffff00 broadcast 172.21.205.255
nxge0: flags=2001000849<UP,BROADCAST,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 6
    inet 172.21.153.81 netmask ffffffff00 broadcast 172.21.153.127
    groupname mgmt
    inet 172.21.153.141 netmask ffffffff00 broadcast 172.21.153.159
    groupname chrg
    inet 172.21.153.101 netmask ffffffff00 broadcast 172.21.153.255
    groupname sig
```

Information level of detail

To collect all information on the example interface, we can use the `-d` argument along with `-o` to get an output snoop file for our interpreter to use:

```
$ snoop -d e1000g1 -o diameterControlAgent.snoop
```

However, to target the snoop even more, we can also restrict to port 3868 using the `-c` argument.

```
$ snoop -d e1000g1 -c tcp port 3868 -o diameterControlAgent.snoop
```
Note: tcp is assumed as Diameter is a tcp protocol.

To run a snoop for an extended period of time, it can be called with nohup or suffixed with & to have it run in the background. In this situation it is recommended to also use the --q argument, which suppresses the packet count.

Snoop interpreter

Once a snoop has been collected, an interpreter can be used to view the packets in a graphical interface.

Wireshark (www.wireshark.org) is one such widely used protocol analyzer, and contains plugins for decoding many telephony protocols, including:

- INAP
- Camel
- MAP
- Diameter.

Wireshark contains many useful features, which are outside of the scope of this document. In general, it will work quite well out of the box, automatically recognizing and decoding protocols without need for special configuration. For more information, see the Wireshark website - www.wireshark.org.

Process failure

You can check whether a process is restarting using the SMS Alarms subsystem.

Processes raise alarms when they are stopped or started. The alarms include:

- Their name
- The time the alarm was logged
- Some other information about why the event may have occurred

Further information about the specific alarm can be found in the application's alarms guide.

Alarms can be accessed from the:

- Syslog on the local machine and the SMS(s). For more information, see SMS Technical Guide.
- Alarms tab in the SMS Alarms Management screen. For more information, see SMS User's Guide.

Checking installed packages

To check the details of an installed package, use the pkginfo command.

Example command: pkginfo -l smsSms

Example output: This is an example of the output of the example command above.

```
PKGINST:  smsSms
NAME:  Oracle smsSms
CATEGORY:  application
ARCH:  sun4u
VERSION:  3.1.0
VENDOR:  Oracle
PSTAMP:  smsNode20041020104925
INSTDATE:  Oct 20 2004 13:15
EMAIL:  support@oracle.com
STATUS:  completely installed
FILES:      348 installed pathnames
            39 directories
            89 executables
            152448 blocks used (approx)
```
For more information about the pkginfo utility, see the system documentation.

**Checking Oracle**

A number of services and functions rely on access to the Oracle database. To check that Oracle is available to a service, check the following:

1. Use sqlplus to check that you can log into Oracle with the username and password the service is using to connect (these can usually be found in the service’s configuration file).
   
   **Example command:** `sqlplus smf/smf`

2. Where the tables required for a service are known, use SQL queries to check that:
   - the tables exist, and
   - they have appropriate content.

For more information about SQL queries, see the Oracle documentation.

**Checking network connectivity**

Network connectivity will affect any process which requires communication between two different network addresses.

Network connectivity should support ssh sessions between the two machines experiencing the problem.

If you can open an ssh session between the two machines, check the following before contacting Level 1 support with details:

- If the address of either of the machines specified in the Node Management screens is a hostname, check that the hostnames used in the ssh sessions are the hostnames specified in the Node Management screen.

If you cannot ssh, check the following before contacting Level 1 support with details:

- Check that the hostname is resolving correctly in the DNS.
- Check that the physical network connection is working correctly.
- Check that the inetd and sshd are running.
- Check that sshd is listening on the expected port.
- Check that the smf_oper and acs_oper accounts are not locked, and that the username and password combinations being used are correct.

**Replication**

Replication may be failing for the following reasons:

- ssh keys have not been correctly set up between origin and destination machines.
- The destination node has been incorrectly set up in the Node Management screens of the SMS Java screens.
- Oracle is not running correctly.
- A new replication.cfg file has not been created after a change.
- replication.cfg may not be successfully copying to the destination machine (an error should display when the **Create Config File** button on the Node Management screens is clicked).
- The partition on the destination machine where the data is being replicated to may be full.
- The updateLoader on the destination machine may be running incorrectly.
- The destination database may be substantially out of sync with the SMF. Run a resync.
Appendix A

NCC Directory Structure and Contents

Component directory structure and contents

This table lists the product directory structure for each component product. The default installation directory for each product is:

/IN/service_packages/product_home/

Each component product is installed in this directory, for example, /IN/service_packages/ACS/ is the product home directory for the ACS product.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/IN/service_packages/product_home/</td>
<td>Product Home directory.</td>
</tr>
<tr>
<td>/IN/service_packages/product_home/bin</td>
<td>Product Binary executables and .sh files.</td>
</tr>
<tr>
<td>/IN/service_packages/product_home/tmp</td>
<td>Product log files.</td>
</tr>
<tr>
<td>/IN/service_packages/product_home/etc</td>
<td>Product configuration files.</td>
</tr>
<tr>
<td>/IN/service_packages/product_home/lib</td>
<td>Product library executable files.</td>
</tr>
<tr>
<td>/IN/service_packages/product_home/db</td>
<td>Product database installation scripts.</td>
</tr>
<tr>
<td>/IN/service_packages/product_home/cdr</td>
<td>Product EDR files.</td>
</tr>
</tbody>
</table>

Component Product Directories and Description

This table lists the set of component (product home) directories installed as part of an NCC install and which conform to the product directory structure as described in the Component directory structure and contents.

Notes:
- Not all component products exist on each NCC server.
- Not all sub-directories will exist for each component product.
- The component list will depend on the specific NCC installation and will most likely be a sub-set of all NCC components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSD</td>
<td>Open Services Development</td>
</tr>
<tr>
<td>PI</td>
<td>Provisioning Interface</td>
</tr>
<tr>
<td>DAP</td>
<td>Data Access Pack</td>
</tr>
<tr>
<td>ACS</td>
<td>Advanced Control Services</td>
</tr>
<tr>
<td>SMCB</td>
<td>Short Message Charging</td>
</tr>
<tr>
<td>USSD</td>
<td>USSD Roaming Application</td>
</tr>
<tr>
<td>RAP</td>
<td>Roaming Application Part (Camel Roaming)</td>
</tr>
<tr>
<td>VSSP</td>
<td>Virtual SSP</td>
</tr>
<tr>
<td>SMSC</td>
<td>SMS Interface</td>
</tr>
<tr>
<td>SCA</td>
<td>Session Control Agent</td>
</tr>
<tr>
<td>IS41</td>
<td>U-CA-IS41 (CDMA)</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>DCA</td>
<td>Diameter Control Agent</td>
</tr>
<tr>
<td>DCD</td>
<td>Diameter Control Driver</td>
</tr>
<tr>
<td>SLEE</td>
<td>Service Logic Execution Environment</td>
</tr>
<tr>
<td>CCS</td>
<td>Charging Control Services</td>
</tr>
<tr>
<td>XMS</td>
<td>Messaging Manager application</td>
</tr>
<tr>
<td>SMS</td>
<td>Service Management System</td>
</tr>
<tr>
<td>E2BE</td>
<td>Voucher &amp; Wallet Server</td>
</tr>
<tr>
<td>RIMS</td>
<td>Routing Information for Mobile Services</td>
</tr>
<tr>
<td>LCP</td>
<td>Location Capabilities Pack</td>
</tr>
</tbody>
</table>
NCC Glossary of Terms

AAA

ACS
Advanced Control Services configuration platform.

ANI
Automatic Number Identification - Term used in the USA by long-distance carriers for CLI.

BE
Billing Engine

C7
See SS7.

CAMEL
Customized Applications for Mobile network Enhanced Logic
This is a 3GPP (Third Generation Partnership Project) initiative to extend traditional IN services found in fixed networks into mobile networks. The architecture is similar to that of traditional IN, in that the control functions and switching functions are remote. Unlike the fixed IN environment, in mobile networks the subscriber may roam into another PLMN (Public Land Mobile Network), consequently the controlling function must interact with a switching function in a foreign network. CAMEL specifies the agreed information flows that may be passed between these networks.

CAP
CAMEL Application Part

CCS
1) Charging Control Services (or Prepaid Charging) component.
2) Common Channel Signalling. A signalling system used in telephone networks that separates signalling information from user data.

CDMA
Code Division Multiple Access is a method for describing physical radio channels. Data intended for a specific channel is modulated with that channel's code. These are typically pseudo-random in nature, and possess favourable correlation properties to ensure physical channels are not confused with one another.

CDR
Call Data Record
Note: The industry standard for CDR is EDR (Event Detail Record). Over time EDR will replace CDR in the Oracle documentation.
CLI
Calling Line Identification - the telephone number of the caller. Also referred to as ANI.

Connection
Transport level link between two peers, providing for multiple sessions.

CPE
Control Plan Editor (previously Call Plan Editor) - software used to define the logic and data associated with a call - for example, “if the subscriber calls 0800 nnnnnn from a phone at location xxx then put the call through to bb bbb bbbb”.

CPU
Central Processing Unit

cron
Unix utility for scheduling tasks.

crontab
File used by cron.

DAP
Data Access Pack. An extension module for ACS which allows control plans to make asynchronous requests to external systems over various protocols including XML and LDAP.

Diameter
A feature rich AAA protocol. Utilises SCTP and TCP transports.

DP
Detection Point

DTMF
Dual Tone Multi-Frequency - system used by touch tone telephones where one high and one low frequency, or tone, is assigned to each touch tone button on the phone.

E2BE
Code used to designate some components and path locations used by the UBE.

EDR
Event Detail Record

Note: Previously CDR. The industry standard for CDR is EDR (Event Detail Record). Over time EDR will replace CDR in the NCC documentation.
**GPRS**

General Packet Radio Service - employed to connect mobile cellular users to PDN (Public Data Network- for example the Internet).

**GSM**

Global System for Mobile communication.

It is a second generation cellular telecommunication system. Unlike first generation systems, GSM is digital and thus introduced greater enhancements such as security, capacity, quality and the ability to support integrated services.

**GUI**

Graphical User Interface

**HLR**

The Home Location Register is a database within the HPLMN (Home Public Land Mobile Network). It provides routing information for MT calls and SMS. It is also responsible for the maintenance of user subscription information. This is distributed to the relevant VLR, or SGSN (Serving GPRS Support Node) through the attach process and mobility management procedures such as Location Area and Routing Area updates.

**HPLMN**

Home PLMN

**HTML**

HyperText Markup Language, a small application of SGML used on the World Wide Web.

It defines a very simple class of report-style documents, with section headings, paragraphs, lists, tables, and illustrations, with a few informational and presentational items, and some hypertext and multimedia.

**IN**

Intelligent Network

**INAP**

Intelligent Network Application Part - a protocol offering real time communication between IN elements.

**IP**

1) Internet Protocol
2) Intelligent Peripheral - This is a node in an Intelligent Network containing a Specialized Resource Function (SRF).

**ISDN**

Integrated Services Digital Network - set of protocols for connecting ISDN stations.

**ISUP**

ISDN User Part - part of the SS7 protocol layer and used in the setting up, management, and release of trunks that carry voice and data between calling and called parties.
LCP
Location Capabilities Pack - set of software components used by other applications to look up the location of mobile devices.

M3UA
MTP3 User Adaptation. The equivalent of MTP in the SIGTRAN suite.

MAP
Mobile Application Part - a protocol which enables real time communication between nodes in a mobile cellular network. A typical usage of the protocol would be for the transfer of location information from the VLR to the HLR.

MC
Message Centre. Also known as SMSC.

Messaging Manager
The Messaging Manager service and the Short Message Service components of Oracle Communications Network Charging and Control product. Component acronym is MM (formerly MMX).

MM
Messaging Manager. Formerly MMX, see also XMS (on page 89) and Messaging Manager (on page 86).

MT
Mobile Terminated

MTP
Message Transfer Part (part of the SS7 protocol stack).

MTP3
Message Transfer Part - Level 3.

NP
Number Portability

Oracle
Oracle Corporation

Peer
Remote machine, which for our purposes is capable of acting as a Diameter agent.

PI
Provisioning Interface - used for bulk database updates/configuration instead of GUI based configuration.
PIN
Personal Identification Number

PLMN
Public Land Mobile Network

RIMS
Routing Information for Mobile Services. Used to cache HLR lookup information.
Note: Now known as "Messaging Manager Navigator".

SCA
1) Service Centre Address
2) Session Control Agent for Session Initiation Protocol (SIP)

SCCP
Signalling Connection Control Part (part of the SS7 protocol stack).

SCP
Service Control Point. Also known as SLC.

SCTP
Stream Control Transmission Protocol. A transport-layer protocol analogous to the TCP or User Datagram Protocol (UDP). SCTP provides some similar services as TCP (reliable, in-sequence transport of messages with congestion control) but adds high availability.

Session
Diameter exchange relating to a particular user or subscriber access to a provided service (for example, a telephone call).

SGML

SGSN
Serving GPRS Support Node

SIP
Session Initiation Protocol - a signaling protocol for Internet conferencing, telephony, event notification and instant messaging. (IETF)

SLC
Service Logic Controller (formerly UAS).
SLEE
Service Logic Execution Environment

SME
Short Message Entity - an entity which may send or receive Short Messages. It may be located in a fixed network, a mobile, or an SMSC.

SMPP
Short Message Peer-to-Peer protocol

SMS
Depending on context, can be:
- Short Message Service
- Service Management System platform
- NCC Service Management System application

SMSC
Short Message Service Centre - stores and forwards a short message to the indicated destination subscriber number.

SOAP

SQL
Structured Query Language - a database query language.

SRF
Specialized Resource Function - This is a node on an IN which can connect to both the SSP and the SLC and delivers additional special resources into the call, mostly related to voice data, for example play voice announcements or collect DTMF tones from the user. Can be present on an SSP or an Intelligent Peripheral (IP).

SS7
A Common Channel Signalling system used in many modern telecoms networks that provides a suite of protocols which enables circuit and non circuit related information to be routed about and between networks. The main protocols include MTP, SCCP and ISUP.

SSP
Service Switching Point

SUA
Signalling Connection Control Part User Adaptation Layer
Switching Point
Anything that can send and receive C7 messages.

System Administrator
The person(s) responsible for the overall set-up and maintenance of the IN.

TCAP
Transaction Capabilities Application Part – layer in protocol stack, message protocol.

TCP
Transmission Control Protocol. This is a reliable octet streaming protocol used by the majority of applications on the Internet. It provides a connection-oriented, full-duplex, point to point service between hosts.

UCAI
Universal Call Agent ISUP (formerly VSSP)

UIS
USSD Interactive Services

USSD
Unstructured Supplementary Service Data - a feature in the GSM MAP protocol that can be used to provide subscriber functions such as Balance Query and Friends and Family Access.

VLR
Visitor Location Register - contains all subscriber data required for call handling and mobility management for mobile subscribers currently located in the area controlled by the VLR.

VSSP
Virtual SSP - old name for UCAI

VWS
Oracle Voucher and Wallet Server (formerly UBE).

XML
eXtensible Markup Language. It is designed to improve the functionality of the Web by providing more flexible and adaptable information identification.

It is called extensible because it is not a fixed format like HTML. XML is a 'metalanguage' — a language for describing other languages—which lets you design your own customized markup languages for limitless different types of documents. XML can do this because it's written in SGML.

XMS
Three letter code used to designate some components and path locations used by the Oracle Communications Network Charging and Control Messaging Manager (on page 86) service and the Short Message Service. The published code is MM (on page 86) (formerly MMX).
Index

0

003da168 leak report • 76

A

AAA • 85
Abort information • 38
About This Document • v
ACS • 85
ACS.conf • 38
acsCompilerDaemon • 47
Analyzing the Capture Files • 35
ANI • 85
Architecture diagram • 1
Archiving • 51
Audience • v
Available flags • 77
AWOL calls • 30

B

Backwards compatibility • 8
Balance Query - all balances • 54
Balance Query - specific balance • 54
Base components • 23
Basic pkginfo command • 23
BE • 85
beGroveller process • 63
beGroveller scalability • 64
beServer process • 60
beSync process • 63
beVWARS process • 61
beVWARS scalability • 62
Billing Engine startup • 63
Billing pairs • 59
Business Processing Language • 55

C

C7 • 85
Call resources • 42
CAMEL • 85
CAP • 85
Capture file size • 36
CCS • 85
ccsBeOrb • 47
ccsCDRLoader • 51
ccsCDRRTrimFilesStartup.sh • 52
CDMA • 85
CDR • 85
cdrDeletionStartup.sh • 52
Changing the run level • 9
Checking installed packages • 81
Checking network connectivity • 82
Checking Oracle • 82
Checking replication status • 39, 48
Checking Services • 41
check-SLEE.sh output • 32
check-SLEE.sh archiving • 32
check-SLEE.sh usage • 32
CLI • 86
Client ID • 61
Client list • 60
cmnPushFiles/cmnReceiveFiles • 70
Command delivery • 53
Command responses • 54
Command structure • 53
Common Troubleshooting Procedures • 67
Complex environments • 24
Component directory structure and contents • 83
Component Product Directories and Description • 83
Configuration completed • 48
Configured plug-ins • 51
Connection • 86
Control Plan Editor • 46
Copyright • ii
Core file location • 71
Core files • 70
Corrupt memory symptom • 15
CPE • 86
CPU • 86
Creating own plc file • 28
cron • 86
crontab • 86
Customer Specific Processing • 52

D

DAP • 86
Database Management • 15
Database shutdown • 17
Database startup • 19
Database verification • 16
Debug • 77
Default directory • 35
Default plc file • 25
Diagnostic information • 71
Diameter • 86
Disk space • 35
Document Conventions • vi
DP • 86
DTMF • 86

E

E2BE • 86
EDR • 86
EDR Management • 49
EDR process flow diagram • 50
eserv.config • 38
Event Id checking • 49
Event processing • 63
Example - pslist • 68