BEA WebLogic Network Gatekeeper™

User's Guide

Version 1.0
Document Revised: March 14, 2005

Copyright

Restricted Rights Legend

Trademarks or Service Marks

Contents

1. Introduction and Roadmap

2. Installation

3. Network Gatekeeper Management Tool

4. Application Connection - Web Services

5. Service Provider and Application Administration

6. Network SLA Administration

7. OSA Gateway Connection

8. SLEE and SLEE Service Operation

9. User Administration

10.Statistics Handling

11.Charging Data Export

12.Alarm and Event Administration

13.Mailbox Administration

14.Routing Administration

15.User Interaction Announcement Administration

16.Whitelist Administration

17.Recommended Periodic Maintenance

18.Service Extension

19.System Scaling

20.System Backup and Restoration

B. List of Configuration Parameters

C. User Certificates and Private Keys

D. Writing Service Level Agreements

E. Writing Network SLA Files

F. Writing OAM Batch Files

G. References

Introduction and Roadmap

The following sections describe the audience for and organization of this document:

- "Document Scope and Audience" on page 1-2
- "Guide to this Document" on page 1-2
- "Terminology" on page 1-3
- "Related Documentation" on page 1-6

Document Scope and Audience

The purpose of the document is to describe the operation and maintenance related to BEA WebLogic Network Gatekeeper, including the following:

- start up and configuration
- operation
- maintenance
- application connection
- alarm handling

Intended audience is support engineers and system administrators working with BEA WebLogic Network Gatekeeper.

Guide to this Document

The document contains the following chapters:

- This chapter, Introduction and Roadmap, describes the structure and contents of this document, the used writing conventions, and related documentation.
- Installation describes how to install and perform basic configuration of WebLogic Network Gatekeeper.
- Network Gatekeeper Management Tool describes the WebLogic Network Gatekeeper management application, the Network Gatekeeper management tool, used for most of the WebLogic Network Gatekeeper OAM tasks.
- Application Connection - Web Services describes the measures to take before an application using the Extended APIs can set up the communication with BEA WebLogic Network Gatekeeper
- Service Provider and Application Administration describes how to register and maintain applications and user accounts in BEA WebLogic Network Gatekeeper.
- OSA Gateway Connection describes how to set up the initial connection with an OSA/Parlay gateway.
- SLEE and SLEE Service Operation describes how to change and supervise the state of the SLEEs and the individual SLEE services. It also describes how to view the resource

utilization of the individual SLEEs and the versions of the SLEE services installed in the SLEEs.

- User Administration describes how to administer the administrative system users and user groups.
- Statistics Handling describes how to create and print reports of the number of service transactions handled by the system.
- Charging Data Export describes how to export charging data to a file.
- Alarm and Event Administration describes how to view and interpret the entries in the alarm list and event log.
- Mailbox Administration describes how to administrate mailboxes and message translations (mailbox short codes and message keywords).
- Routing Administration describes how to set up the routing towards the networks.
- User Interaction Announcement Administration describes how to connect the applications' announcement IDs with the actual announcements installed in the network.
- Whitelist Administration describes how to administrate the whitelists specifying which destination addresses are allowed for a service provider's applications.
- Recommended Periodic Maintenance provides a list of the recommended maintenance procedures.
- Service Extension describes the general principles on how to extend the system with new service functionality and how to connect new networks to BEA WebLogic Network Gatekeeper.
- System Scaling describes how to scale BEA WebLogic Network Gatekeeper in different levels.
- System Backup and Restoration describes how to perform system backups and restorations.
- System Upgrade describes how system upgrades and patches are handled.
- Alarm and Fault Handling describes the actions to take when an alarm has appeared in the alarm list.

Terminology

The following terms and acronyms are used this document:

- API —Application Programming Interface
- Application —A telecom enabled computer application accessed either from a telephony terminal or a computer.
- Application Developer —An organization or individual developing applications.
- Service Provider —An organization offering services provided by one or more applications to end users.
- AS —Application Server
- ATE —Application Test Environment
- CORBA —Common Object Request Broker Architecture
- End User —Person that uses an application. An end user can be identical to a subscriber, for instance in a prepaid service. The end user can also be a non-subscriber, for instance in an automated mail-ordering application where the subscriber is the mail-order company and the end user is a customer to this company.
- Enterprise Operator —See *Service Provider.*
- ESPA —Extended web services APIs and Service Capanilties.
- GMLC —Gateway Mobile Location Centre
- GMSC —Gateway Mobile Switching Centre
- GUI —Graphical User Interface
- HA —High Availability
- HTML —Hypertext Markup Language
- IDL —Interface Definition Language
- IIOP —Internet Inter-ORB Protocol
- INAP —Intelligent Network Application Part
- IOR —Interoperable Object Reference
- IP —Internet Protocol
- MAP —Mobile Application Part
- MMS —Multimedia Message Service

- MPC —Mobile Positioning Centre
- MPP —Mobile Positioning Protocol
- MTP —L3 Message Transfer Part Layer 3
- Network Plug-in —A network plug-in the Betwork gatekeeper to a network based service node or SCSes through a specific protocol.
- Network Service —See Service
- NS —Name Service or Network Simulator
- OAM —Operation, Administration, and Maintenance
- Operator —The owner of the Ntwork Gatekeeper
- ORB —Object Request Broker
- OSA —Open Service Access
- OSS —Operation Support System
- SCCP —Signalling Connection Control Part
- SCF —Service Control Function
- SCS —Service Capability Server
- SCS Plug-in —A network plug-in used to connect SCSes to the WebLogic Network Gatekeeper.
- Service —A network provided service capability.
- Service Capability —See Service
- SLA —Service Level Agreement
- SLEE —Service Logic Execution Environment
- SLEE —Service A software module that is designed to execute in the SLEE.
- SMPP —Short Message Peer-to-Peer Protocol
- SMS —Short Message Service
- SOAP —Simple Object Access Protocol

- SPA —Service Provider APIs
- SPC —Signalling Point Code
- SQL —Structured Query Language
- SRF —Service Resource Function
- SS7 —Signalling System 7
- SSF —Service Switching Function
- SSN —Sub System Number
- Subscriber —A person or organization that subscribes for an application. The subscriber is charged for the service usage. Also eee End User.
- TCAP —Transaction Capability Application Part
- TCP —Transmission Control Protocol
- UDDI —Universal Description, Discovery and Integration
- URL —Universal Resource Locator
- User —A person working with OAM through the WebLogic Network Gatekeeper Mangement Tool that has an administrative user name and password. An application accessing services through one or more APIs and has a user name and a password.
- VAS —Value Added Service
- VLAN Virtual Local Area Network
- VPN —Virtual Private Network
- WSDL —Web Services Definition Language
- XML —Extended Markup Language

Related Documentation

This user's guide is a part of BEA WebLogic Network Gatekeeper documentation set. The following documents contain other types of BEA WebLogic Network Gatekeeper information:

- *BEA WebLogic Network Gatekeeper Product Description* describes BEA WebLogic Network Gatekeeper functions and system characteristics.

- *Developer's Guide for Parlay X* describes how to design and implement applications on the Extended and Parlay X Web Services APIs.
- *Developer's Guide for Extended Web Services* describes how to design and implement applications on the extended Web Services APIs.
- *Application Test Environment User's Guide* describes how to use BEA WebLogic Network Gatekeer Application Test Environment when it comes to application test.
- *API Description for Parlay X* describes the open APIs available for developers and applications.
- *API Description for Extended Web Services* describes APIs available for developers and applications.

Other documentation

The third party documentation needed to operate and maintain BEA WebLogic Network Gatekeeper system is listed in "References" on page G-1.

Installation

This chapter describes the installation of a WebLogic Network Gatekeeper in a clustered environment. For a complete and successful installation, all sections and steps below have to be performed in the order they are presented.

Before you start the installation it is recommended that you learn the basics about the Network Gatekeeper by reading the *BEA WebLogic Network Gatekeeper Product Description*.

The installation instruction covers installation on RedHat Linux Advanced Server 3 and HP-UX Itanium v11.23.

The instructions below describes the steps to be taken for each server in the cluster building up the WebLogic Network Gatekeeper.

The paths to the installation files are described in "Installation CD" on page A-2 and the directory structure for an installed system is described in "Installed system" on page A-3.

Individual files are referred to as `filename<version>.type`. For example, a file referred to as `jrockit-j2sdk<version>.bin.gz` could have the full name `jrockit-j2sdk1.4.2_05-linux-ia32.bin.gz`.

The following sections provide installation instructions:

- "Installation on Linux" on page 2-2
- "Installation on HP-UX" on page 2-4
- "Installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" on page 2-7

Installation on Linux

Login

1. Log in to the target server as **root**. All commands described in this section assumes that you log in as **root** user

2. Verify that the correct OS patches are installed. Refer to the release notes for a description of necessary patches.

Extract the binaries for Linux

3. Copy from the CD or the download directory, the file `wng_linux.zip` to the local file system.

4. Extract the installation binaries by issuing the command:
   `unzip wng_linux.zip`

5. Enter the password obtained from the BEA eLicense system.

6. The installation files are extracted to the local file system in the subdirectory `./linux`

Install the JRockit SDK

7. Change directory to `<path to installation files>/linux`

8. Decompress the files by issuing the command:

   ```
   gunzip jrockit-j2sdk<version>.bin.gz
   ```

9. Make the file properties binary and executable by issuing the command:

   ```
   chmod u+x jrockit-j2sdk<version>.bin
   ```

10. Install the JDK by issuing the command:

    ```
    ./jrockit-j2sdk<version>.bin
    ```

11. Follow the commands as prompted.

Configure the JVM

12. Define the environment variable JAVA_HOME to the newly installed JDK:

    ```
    JAVA_HOME=<Java installation path>/j2sdk<version>
    ```

13. Append JAVA_HOME first in the path:

    ```
    PATH=$JAVA_HOME/bin:$PATH
    ```

14. Make sure the correct JVM is used. Issue the command:

    ```
    java -version
    ```

    The output should be (may differ slightly depending on version):

    ```
    Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_05-b04)
    ```

    ```
    BEA WebLogic JRockit(TM) 1.4.2_05 JVM R24.4.0-1 (build
    ari-38120-20041118-1131-linux-ia32, Native Threads, GC strategy:
    parallel)
    ```

Install database

Follow the instructions below to install MySQL. MySQL should only be installed on two servers in the cluster building up the WebLogic Network Gatekeeper. Normally the servers resides in the Network Layer of the cluster.

15. Change directory to `/usr/local/`

16. Unpack the installation files for MySQL by issuing the command:

    ```
    gunzip -c <path to installation files>/linux/mysql-<version>.tar.gz | tar
    xvf -
    ```

17. Follow the MySQL installation instruction. The instructions are found in

    ```
    /usr/local/mysql-<version>/INSTALL-BINARY
    ```

    Below is an summary of commands to install MySQL, refer to the actual installation instructions for a description of each command.

    ```
    groupadd mysql
    ```

```
useradd -g mysql mysql
cd /usr/local
ln -s /usr/local/mysql-standard-<version> mysql
cd mysql
scripts/mysql_install_db --user=mysql
chown -R root.
chown -R mysql data
chgrp -R mysql.
bin/mysqld_safe --user=mysql &
```

Unpack WebLogic Network Gatekeeper software

18. Change directory to `/usr/local`
19. Unpack the software by issuing the command:

```
gunzip -c <path to installation files>/linux/wng_linux_i386.tar.gz | tar
xvf -
```

20. Continue with "Installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" on page 2-7.

Installation on HP-UX

Login

1. Log in to the target server as **root**. All commands described in this section assumes that you log in as **root** user
2. Verify that the correct OS patches are installed. Refer to the release notes for a description of necessary patches.

Extract the binaries for HP-UX

3. Copy from the CD or the download directory, the file `wng_linux.zip` to the local file system.
4. Extract the installation binaries by issuing the command:

```
crypt < wng_hpux.tar.crypt | tar xvf -
```

5. Enter the password obtained from the BEA eLicense system..
6. The installation files are extracted to the local file system in the subdirectory `./hpux`

Install patches

7. Use swinstall to install Java-out-of the-box. The depot file is named `<path to installation files>/wng/hpux/joob_<version>.depot`
8. Untar the OS patches in the file `<path to installation files>/wng/hpux/patches/hpux_<version>.tar`
9. Create depots from the files in the previously un-tared files by executing the script`./create_depot_hp-ux_11`
10. Use `swinstall` to install the created depot.

Install the Java SDK

11. Install the JDK by issuing the command:

```
swinstall -s <path to installation files>/wng/hpux/sdk<version>.depot\*
```

Configure the JVM

12. Define the environment variable:

```
JAVA_HOME=/opt/java1.4
```

```
13.Append JAVAHOME first in the PATH
```

```
PATH=$JAVA_HOME/bin:$PATH
```

14. Make sure the correct JVM is used. Issue the command:

```
java -version
```

The output should be (may differ slightly depending on version):

```
Java(TM) 2 Runtime Environment, Standard Edition (build
1.4.2.03-040401-16:07)
```

```
Java HotSpot(TM) Server VM (build 1.4.2 noubar:06.01.04-17:39 PA2.0
(aCC_AP), mixed mode)
```

Install database

Follow the instructions below to install MySQL. MySQL should only be installed on two servers in the cluster building up the WebLogic Network Gatekeeper. Normally the servers resides in the Network Layer of the cluster.

15. Change directory to `/usr/local`
16. Unpack the installation files for MySQL by issuing the command:

    ```
    tar xvf <installation file directory>/wng/hpux/mysql-<version>
    ```

17. Follow the MySQL installation instruction. The instructions are found in

    ```
    /usr/local/mysql-<version>/INSTALL-BINARY
    ```

    Below is an summary of commands to install MySQL, refer to the actual installation instructions for a description of each command.

    ```
    groupadd mysql
    useradd -g mysql mysql
    cd /usr/local
    ln -s /usr/local/mysql-<version> mysql
    cd mysql
    scripts/mysql_install_db --user=mysql
    chown -R root.
    chown -R mysql data
    chgrp -R mysql.
    bin/mysqld_safe --user=mysql &
    ```

Unpack WebLogic Network Gatekeeper software

18. Change directory to `/usr/local`
19. Unpack the software by issuing the command:

    ```
    tar xvf <path to installation files>/wng/hpux/wng_hpux_ia64.tar
    ```

Installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files

Due to import control restrictions for some countries, the Java Cryptography Extension (JCE) policy files shipped with the Java 2 SDK, Standard Edition and the Java 2 Runtime Environment allow strong but limited cryptography to be used.

An unlimited strength version of these files indicating no restrictions on cryptographic strengths is available on the Java 2 SDK web site for those living in eligible countries.

20. Download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. The files can be found at the download page for the J2SE used under the heading **Other Downloads**.

    Note: The version of the JCE Policy files must be correlated with the Java version installed.

21. Replace the `local_policy.jar` and `US_export_policy.jar` files in the directory:

    Linux: `<path to JRockit>/j2sdk<version>/jre/lib/security`

    HP-UX: `/opt/java1.4<version>/jre/lib/security`

    with the files included in the downloaded zip file.

Configure WebLogic Network Gatekeeper software

22. Edit the file `<installation path>/bin/slee_properties.xml`

    Modify in the `<SLEE_PROPERTIES>` tag:

    – `name` to a descriptive name for the SLEE

    Modify in the `<SLEE_HOST>` tag:

    – `address` to the IP-address of the server.

    Modify in the `<SLEE_PATH>` tag:

    – `slee_install_path` to the path of the SLEE, normally `/usr/local/slee`

    – `database_install` to the path of the MySQL installation. Ignore if MySQL is not installed on this server.

    Modify in the `<SLEE_DB_1>` tag:

    – `address` IP-address of the server running the first database.

    – `port` port number for the database on this server.

Modify in the `<SLEE_DB_2>` tag:

- `address` IP-address of the server running the second database.
- `port` port number for the database on this server.

Modify in the `<BACKUP>` tag:

- `directory` to the directory to store the back-up.

Note: All servers in a cluster shall have identical values in `<SLEE_DB_1>`, `<SLEE_DB_2>` and `<BACKUP>`

There are other configuration options for memory sizes, garbage collections sizes, and CORBA configuration used to tune the system. These parameters are deployment specific and depends on type of server, CPU type and son on. The default values can be used.

23. Change directory to the installation directory of the WebLogic Network Gatekeeper: `/usr/local/slee/bin`
24. Make sure all scripts are executable by issuing the command:

```
chmod u+x *.sh
```

25. Create start-up scripts by issuing the command:

```
./SLEEConfig.sh
```

26. Finalize the configuration by issuing the command:

```
./postconfig.sh
```

This command sets up database tables etc.

Delete unused services

Depending on the type of server being installed delete the service not relevant for the one being set up.

27. See "SLEE Services" on page 2-10 for all list of services and delete the unused accordingly.

Start the WebLogic Network Gatekeeper supervision process

28. Change directory to the installation directory: `/usr/local/slee/bin`

29. .Start the WebLogic Network Gatekeeper supervision process by issuing the command:

```
./runAgent.sh &
```

Start Network Gatekeeper Management Tool

30. Follow the instructions in "Starting an Network Gatekeeper Management Tool and adding a SLEE" on page 3-10 to start to configure the individual SLEEs in the WebLogic Network Gatekeeper.

Configure the WebLogic Network Gatekeeper

31. It is recommended to autostart MySQL at reboot. Refer to the instructions for MySQL and the operating system.

32. It is recommended to autostart the WebLogic Network Gatekeeper at reboot. Refer to the instructions for the operating system. The script to be autostarted is `/usr/local/slee/bin/runAgent.sh`

    Note: MySQL must be started before the WebLogic Network Gatekeeper is started.

33. Setup backup procedures as described in "System Backup and Restoration" on page 20-1.

34. Create administrative accounts as described in "User Administration" on page 9-1.

35. Configure relevant network protocol plug-in as described in "Network plug-ins" on page B-24.

36. Configure Web Services ports as described in "Application Connection - Web Services" on page 4-1.

37. Create service provider and application accounts as described in "Service Provider and Application Administration" on page 5-1.

38. Create service provider and application SLAs as described in "Writing Service Level Agreements" on page D-1.
39. Create network SLAs as described in "Writing Network SLA Files" on page E-1.

Test the installation

When all servers in the cluster have been installed and configured, the complete installation must be verified using test applications.

SLEE Services

This sections describes all the different SLEE services in the installation directory structure.

It explains which files that can be removed, depending on the type of server being installed.

The following notation is used in this section:

- AL —Access Layer server
- NL —Network Layer server
- M —Mandatory
- O —Optional
- R —Remove

Directory _autoslee

The following files are included as default in the directory `/usr/local/slee/bin/_autoslee`

a_slee_trace.jar (M)

b_event_channel.jar (M)

b_slee_alarm.jar (M)

c_slee_event.jar (M)

c_slee_snmp.jar (O. Keep for SNMP support)

d_slee_backup.jar (O. Keep on server running DB)

d_slee_charging.jar (M)

e_slee_global_counter.jar (NL - M, AL - R) e_slee_list_matcher.jar (NL - M, AL - R)

e_slee_time.jar (O. Used for time synchronization if not done on OS level.)

f_policy.jar (NL - M, AL - R)

g_slee_resource.jar (NL - M, AL - R)

h_slee_statistics.jar (NL - M, AL - R)

i_slee_common_loader.jar (M)

i_slee_scsmgr.jar (NL - M, AL - R)

x_embedded_tomcat.jar (NL - O. Keep if local web service is used, for example MM7, AL - M)

Directory autosrv

The following files are included as default in the directory `/usr/local/slee/bin/autosrv`

b_charging_resource.jar (NL - O, AL - R)

b_cimd_gms_resource.jar (NL - O, AL - R)

b_db_sp_resource.jar (NL - O, AL - R)

b_eaif_mms_resource.jar (NL - O, AL - R)

b_mlp_ul_resource.jar (NL - O, AL - R)

b_mm7_gms_resource.jar (NL - O, AL - R)

b_mps_ul_resource.jar (NL - O, AL - R)

b_mps_us_resource.jar (NL - O, AL - R)

b_smpp_gms_resource.jar (NL - O, AL - R)

b_smpp_gms_resource_ussd.jar (NL - O, AL - R)

cert_builder.jar (NL - O, AL - R)

c_osa_nichs.jar (NL - O. Keep if call control is supported, AL - R)

d_resource_osa_access.jar (NL - O, AL - R)

e_resource_osa_ul.jar (NL - O, AL - R)

resource_osa_callui.jar (NL - O, AL - R)

resource_osa_cs.jar (NL - O, AL - R)

resource_osa_gcc.jar (NL - O, AL - R)

resource_osa_gui.jar (NL - O, AL - R)

resource_osa_messaging.jar (NL - O, AL - R)

resource_osa_mms.jar (NL - O, AL - R)

resource_osa_mpcc.jar (NL - O, AL - R)

resource_osa_sp.jar (NL - O, AL - R)

resource_osa_us.jar (NL - O, AL - R)

subscription_handler.jar (NL - O, AL - R)

x_espa_access.jar (NL - M, AL - R)

x_espa_call_control.jar (NL - O, AL - R)

x_espa_call_ui.jar (NL - O, AL - R)

x_espa_charging.jar (NL - O, AL - R)

x_espa_messaging.jar (NL - O, AL - R)

x_espa_messaging_ui.jar (NL - O, AL - R)

x_espa_subscriberprofile.jar (NL - O, AL - R)

x_espa_userlocation.jar (NL - O, AL - R)

x_espa_userstatus.jar (NL - O, AL - R)

x_sespa_access.jar (NL - R, AL - M)

x_sespa_callcontrol.jar (NL - R, AL - O)

x_sespa_callui.jar (NL - R, AL - O)

x_sespa_charging.jar (NL - R, AL - O)

x_sespa_messaging.jar (NL - R, AL - O)

x_sespa_messaging_ui.jar (NL - R, AL - O)

x_sespa_subscriberprofile.jar (NL - R, AL - O)

x_sespa_userlocation.jar (NL - R, AL - O)

x_sespa_userstatus.jar (NL - R, AL - O)

Directory autowar

The following files are included as default in the directory `/usr/local/slee//bin/autowar`

mm7_vasp.war (AL - R, NL -Keep if MM7 plug-in is used)

parlayx.war (AL - Keep if Parlay X interface is used, NL -R)

wespa.war (AL - Keep if Extended Web Services interface is used, NL -R)

CHAPTER 3

Network Gatekeeper Management Tool

The following sections describe the Network Gatekeeper Management Tool:

About the Network Gatekeeper Management Tool

The SLEEs and the SLEE services are managed through the Network Gatekeeper Management Tool. It provides a graphical and a text based interface.

Both the graphical and the text based interface tool can access the SLEEs through a CORBA connection and support execution of OAM batch files (scripts). The text based management tool may also be used through a remote connection such as telnet.

Graphical Network Gatekeeper Management Tool interface

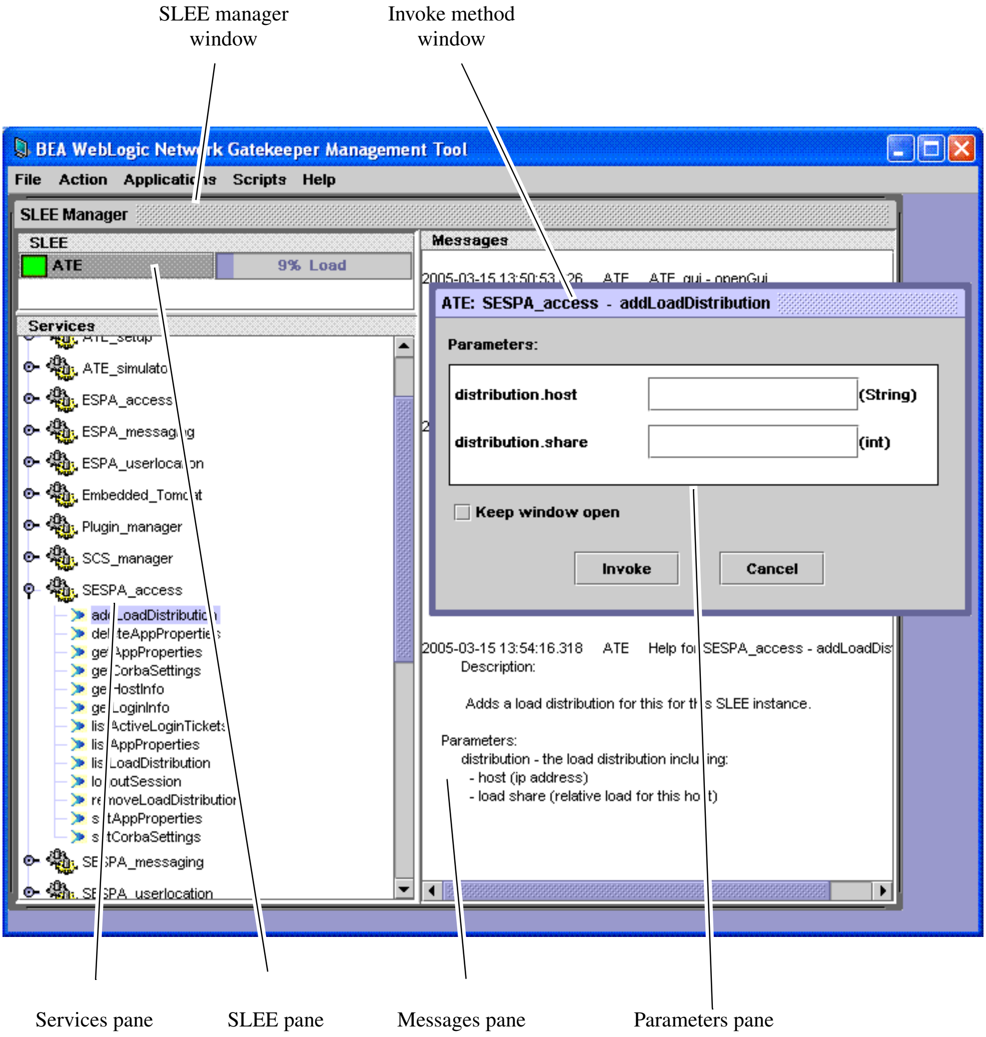
The SLEE services are displayed in the Network Gatekeeper Management Tool. When selecting one of the SLEE services, the administrative methods available for that service are displayed. Depending on the logged in user's authority level and service group belonging, different sets of SLEE services and methods are displayed. A user has one of the following authority levels:

- Read only user
- Standard read and write user
- Administrator user

The authority and service group concepts are further described in the chapter "User Administration" on page 9-1.

Main window

All management can be performed through the Network Gatekeeper Management Tool's main window. The window and its components are shown in Figure 3-1, "Network Gatekeeper Management Tool Main window," on page 3-3.



distribution.host		(String)
distribution.share		(int)

☐ Keep window open

```
2005-03-15 13:50:53.?26    ATE    ATE.gui - openGui

2005-03-15 13:54:16.318    ATE    Help for SESPA_access - addLoadDis
      Description:

       Adds a load distribution for this for this SLEE instance.

    Parameters:
      distribution - the load distribution including:
        - host (ip address)
        - load share (relative load for this host)
```

Figure 3-1 Network Gatekeeper Management Tool Main window

From the menu bar in the Main window you can initiate a number of actions related to the Network Gatekeeper Management Tool itself and to connecting and disconnecting SLEEs to the SLEE manager.

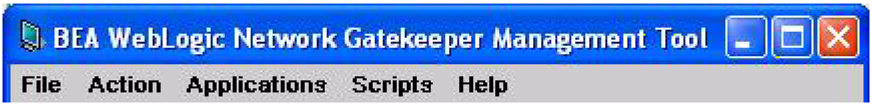


Figure 3-2 Network Gatekeeper Management Tool menu bar

File menu

File - Auto saving configurations
If the check box is selected, the SLEEs you have added to the management tool window and the installed management plug-ins will automatically appear in the Network Gatekeeper Management Tool the next time you log on.

File - Exit
Exits and logs off the Network Gatekeeper Management Tool.

Actions menu

Actions - Add SLEE...
Opens a dialog box where you can add a SLEE to the SLEEs pane.

Actions - Remove SLEE...
Opens a dialog box where you can remove a SLEE from the SLEEs pane.

Actions - Reload SLEE...
Opens a dialog box where you can reload a SLEE’s services and methods.

Actions - Add as alarm listener
Adds the Network Gatekeeper Management Tool as an alarm listener for the SLEEs in the SLEE pane. The alarms will be displayed in the Messages pane.

Actions - Remove as alarm listener
Removes the Network Gatekeeper Management Tool as an alarm listener for the SLEEs in the SLEE pane. The alarms will no longer be displayed in the Messages pane.

Actions - Set alarm severity...
Opens a dialog box where you can set the lowest severity of the alarms to be displayed.

Applications menu

Applications - Start Certificate Builder
Starts the Certificate Builder where you can generate your own user certificates and private keys.

Applications - Start Rule Development Tool
Starts the Rule Development Tool if installed.

Applications - SLEE manager - View SLEE manager
Clear the check box if you do not want to view the SLEE manager window.

Applications - SLEE manager - Logout
Logs off a user without exiting the Network Gatekeeper Management Tool.

Applications - Plug-in - Add plug-in...
Opens a dialog box where you can add a management plug-in. Added plug-ins appear in the menu.

Applications - Plug-in - Remove plug-in...
Opens a dialog box where you can remove a management plug-in.

Scripts menu

Scripts - Run script...
Opens a dialog box where you can select and run an OAM batch file. The file could be a recorded OAM session or written from scratch. The result is presented in a separate window in the Network Gatekeeper Management Tool.

Scripts - Recording a test case - Set file name...
Opens a dialog box where you can specify a file name for file where the recorded OAM session will stored.

Scripts - Recording a test case - Start recording
Starts recording the OAM activities performed through the Network Gatekeeper Management Tool. The output file can be run as an OAM batch file.

Scripts - Recording a test case - Stop recording
Stops recording the OAM activities performed through the Network Gatekeeper Management Tool.

Help menu

Help - User's Guide...
Opens a user's guide describing the Network Gatekeeper Management Tool and the tasks you can perform with it.

Help - About...
Opens the About dialog box.

Network Gatekeeper SLEE manager window

SLEE pane

This pane contains a list displaying the status, name and load of the SLEEs connected to the Network Gatekeeper Management Tool. Clicking on a SLEE displays the SLEE's services in the Services pane.

Right-clicking on a SLEE in the list displays a menu where the SLEE's process can be started or stopped, and the SLEE's state can be changed. You can also select to view a SLEE's load by right-clicking on a SLEE.

A SLEE's status is indicated by an icon, see Table 3-1, "SLEE status icons," on page 3-7.

Table 3-1 SLEE status icons

Icon	SLEE Status
🟩 (green)	SLEE state **Running**
🟨 (yellow)	SLEE state **Shutdown**
☒ (red)	The SLEE process is not responding
■ (black)	The SLEE process and the SLEE agent process are not responding
□ (white)	The SLEE user is not logged in

During SLEE status change, for example from **Shutdown** to **Running**, the change is indicated by adding a little dot with the color reflecting the "status-to-be" in the icon’s upper right corner.

Services pane

When a SLEE is selected in the SLEEs pane, this pane contains a list of all the SLEE’s services. Double-clicking on a service displays all administrative methods related to the service.

Double-clicking on a methods displays the method and its parameters in the invoke method window.

Right-clicking on a method displays a menu where you can select Help to display a short help text in the Messages pane. The help text describes the purpose of the method and the parameters used by the method.

Messages pane

This pane displays the results of method invocations and the alarms raised from the SLEE. Also, the Messages pane is used for displaying the method help texts.

Invoke method window

All methods are invoked from the invoke method window. For the methods that uses parameters, the parameter values are set in this window before the method is invoked.

Installing an Network Gatekeeper Management Tool (Unix)

The following instruction tells you how to install an Network Gatekeeper Management Tool on a Unix workstation. That is, how to install an Network Gatekeeper Management Tool on a machine that is not a BEA WebLogic Network Gatekeeper.

Install Java Runtime Environment

1. Download Java 2 runtime environment, standard edition version 1.4.2.
2. Run the installation script.

   Follow the instructions provided by the installation script. It is recommended to use the default settings.

   Install Network Gatekeeper Management Tool

3. The Network Gatekeeper Management Tool software is contained in the software bundle for WebLogic Network Gatekeeper. Copy the file `wng_manager.zip` to the local file system. The file is found in the directory where you extracted the binaries, see “Extract the binaries for Linux” on page 2-2 or “Extract the binaries for HP-UX” on page 2-4.
4. Extract the installation binaries by issuing the command:

   ```
   unzip wng_manager.zip
   ```
5. The installation files are extracted to the local file system in the subdirectory `./manager`
6. Change directory to `<path to installation files>/wng_manager`
7. Run the installation script. Enter command:

   ```
   ./install.sh
   ```

   Follow the instructions provided by the installation script. It is recommended to use the default settings.

Installing an Network Gatekeeper Management Tool (Windows 2000/XP)

The following instruction tells you how to install an Network Gatekeeper Management Tool on a Windows PC. That is, how to install a Network Gatekeeper Management Tool on a machine that is not a BEA WebLogic Network Gatekeepers.

Install Java Runtime Environment

1. Download Java 2 runtime environment, standard edition version 1.4.2 from:

   `http://java.sun.com/j2se`

2. Run the installation wizard. The file name might differ depending on the current version available for download.

   Follow the instructions provided by the installation wizard. It is recommended to use the default settings.

   Set system variables

3. Right-click on the **My Computer** icon and select **Properties** in the menu.
4. Click the **Advanced** tab
5. Click **Environment Variables...**

   Note: Be careful when working with path variables, your computer may not work properly if existing variables are removed or altered.

6. In the **System variables** table, select the **Path** variable.
7. Click **Edit...**
8. In the **Variable Value** field, enter the full search path to Java.
9. Click **OK**.
10. In the **System variables** table, select the **JAVA_HOME** variable.
11. Click **Edit...**

    If the **JAVA_HOME** variable does not exist, click **New...** to create it.

12. In the **Variable Value** field, enter the full search path to Java. Click **OK**.

    Install Network Gatekeeper Management Tool

13. The Network Gatekeeper Management Tool software is contained in the software bundle for WebLogic Network Gatekeeper. Copy the file `wng_manager.zip` to the local file system. The file is found in the directory where you extracted the binaries, see "Extract the binaries for Linux" on page 2-2 or "Extract the binaries for HP-UX" on page 2-4.

14. Extract the file `wng_manager.zip`

15. The installation files are extracted to the local file system in the subdirectory `wng_manager`

16. Change directory to `<path to installation files>\manager`

17. Run the Network Gatekeeper Management Tool set-up wizard. Double click on the file `install.bat` and follow the instructions in the wizard.

Starting an Network Gatekeeper Management Tool and adding a SLEE

The following instructions tells you how to start an Network Gatekeeper Management Tool and connect it to a SLEE.

Starting the Network Gatekeeper Management Tool

1. Start the Network Gatekeeper Management Tool. Depending if you are using a Unix workstation or Windows PC, do one of the following:

   On a Unix workstation:

   a. Open a command window.

2. Go to the `/usr/local/manager/bin` directory.

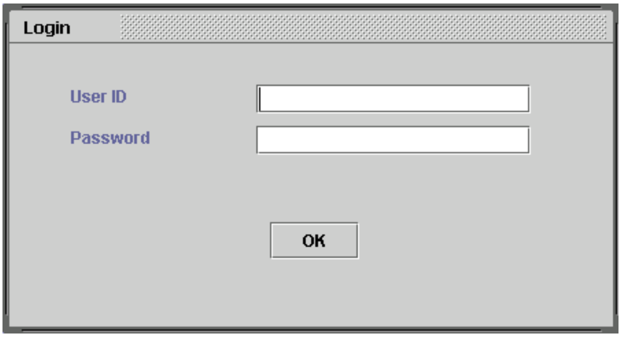
3. Enter command: `./runSleeManager.sh`

   On a Windows PC:

   b. Open the **Start** menu and select **Programs - BEA WebLogic Network Gatekeeper 1.0-Management Tool**

   On a PC, you can also start the Network Gatekeeper Management Tool by double-clicking on the `runSleeManager.bat` file in the installation directory. But, if you start the Network Gatekeeper Management Tool through the `runSleeManager.bat` file you will have to add the SLEEs to the Network Gatekeeper Management Tool every time you log in. If you start through the start menu, the SLEEs you have added will automatically be displayed at log in.

   This displays the Network Gatekeeper Management Tool's **Login** window.



4. In the **User ID** field, enter your user ID.

5. In the **Password** field, enter your password.

6. Click **OK**.

   You are now logged on to the Network Gatekeeper Management Tool. The SLEEs connected to the SLEE manger are displayed in the **SLEEs** pane. If there are no SLEE in the SLEEs pane or if you want to add more SLEEs to the management tool, continue with Step 7. below.

   Adding a SLEE to the Network Gatekeeper Management Tool

7. In the **SLEEs** pane, right-click on the background and select **Add SLEE...** from menu, or open the **Actions** menu and select **Add SLEE...**

   This displays the **Add SLEE** dialog box.

8. Enter data according to the table below:

   Note: For the SLEE name parameter, it is recommended use the SLEE name as defined when the SLEE was installed.

Parameter	Description
SLEE Name	The SLEE name you want to appear in the SLEE pane.
User ID	Your administrative (SLEE) user ID.
Password	Your administrative (SLEE) password.

9. Select if the SLEE connection shall be made using IP address and port numbers, or name service and object references files.

   Note: If bi-directional CORBA is used on BEA WebLogic Network Gatekeeper the SLEE belongs to, the connection has to be made using name service and object reference files.

10. Enter IP address and port number, *or* name service references file data according to the table below:

Parameter	Description
IP Address	The SLEE host's management resource sharing context's IP address.
NS Port	The SLEE management resource sharing context's name service port number. Default is 10007.
Agent Port	The SLEE agent's port number. Default is 6214.
SLEE reference file	The path to the SLEE management resource sharing context's name service reference file (oam_nameservice.ref).
Agent reference file	The path to the SLEE agent's object reference file (slee_agent.ref).

11. Click **OK**.

    This displays the SLEE in the **SLEEs** pane.

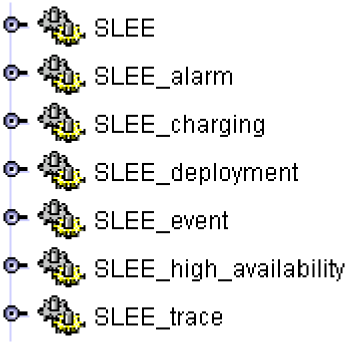
Working with the Network Gatekeeper Management Tool

The following instruction describes a general workflow on how to work with SLEE Services.

1. Start an Network Gatekeeper Management Tool, see "Starting an Network Gatekeeper Management Tool and adding a SLEE" on page 3-10.

2. Select the SLEE you want to work with. Click on the desired SLEE in the **SLEEs** pane.

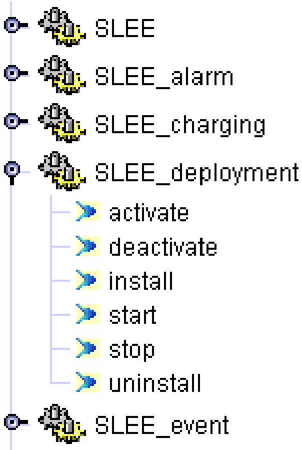
   This displays all services available in the SLEE in the **Services** pane.



If the SLEE you wan to work with is not displayed in the SLEEs pane, right-click in the background of the SLEEs pane and select **Add SLEE...** in the displayed menu.

3. Select the service you want to work with. Double-click on the desired service in the **Services** pane.

   This displays all administrative methods related to the service below the service.



   If you want a short description of what the method does, right-click on the method and select **Help** in the menu.

4. Display the parameters related to the method. Double-click on the method.

   This opens the **Invoke Method** window and displays the method's parameters in it.

5. Enter the parameters values, if any, in the input fields and click **Invoke**.

The result of the invocation is displayed in the **Messages** pane.

Text based Network Gatekeeper Management Tool

The text based Network Gatekeeper Management Tool is a command line management interface providing the same basic functions as the graphical Network Gatekeeper Management Tool. The two main benefits with the text based management tool are that you use it to manage a SLEE over a remote connection, such as Telnet, and that it can execute batch files containing SLEE commands. For more information about writing and executing batch files, see "Writing OAM Batch Files" on page F-1.

Besides the method descriptions the text based Network Gatekeeper Management Tool also provides help on the tool itself

Installing a text based Network Gatekeeper Management Tool

The text based Network Gatekeeper Management Tool uses the same software package as the GUI based Network Gatekeeper Management Tool. That is, the text based Network Gatekeeper Management Tool is installed together with the GUI based using the procedures "Installing an Network Gatekeeper Management Tool (Unix)" on page 3-8 and "Installing an Network Gatekeeper Management Tool (Windows 2000/XP)" on page 3-9.

Using the text based Network Gatekeeper Management Tool

Follow the instruction below to start and execute commands using the text based Network Gatekeeper Management Tool.

Note: It is not possible to start and stop the SLEE process through the text based Network Gatekeeper Management Tool. To start and stop a SLEE, login to the host where the SLEE executes and use the `startSlee` and `stopSlee` scripts located as described below.

Host running the SLEE	OS	Full Path
BEA WebLogic Network Gatekeeper	HP-UX Linux	`/usr/local/slee/bin/startSlee.sh` `/usr/local/slee/bin/stopSlee.sh`

1. Open a command line interface.

2. Login to the host where the SLEE executes.

   On a computer where the Network Gatekeeper Management Tool is installed. Depending if you are on a Unix workstation or Windows PC, do one of the following:

   On a Unix workstation:

   c. Go to the `/usr/local/manager/bin` directory.

3. Enter command: `./runSleeTextManager.sh`

   On a Windows PC:

   d. Go to the `C:\bea\wng\manager10\bin` directory

4. Enter command: `runSleeTextManager.bat`

   This starts up the text based Network Gatekeeper Management Tool.

5. Enter command

   ```
   addslee
   ```

   This prompts you for SLEE connection parameters. The connection can be made using IP-address and port or through the name service and object reference files.

   Note: If bi-directional CORBA is used on BEA WebLogic Network Gatekeeper the SLEE belongs to, the connection has to be made using name service and object reference files.

6. Enter connection parameters according to the table below:

Parameter	Description
IP Address	The SLEE host’s management resource sharing context’s IP address.

Parameter	Description
NS Port	The SLEE management resource sharing context's name service port number. Default is 10007.
Agent Port	The SLEE agent's port number. Default is 6214.
SLEE reference file	The path to the SLEE management resource sharing context's name service reference file (oam_nameservice.ref).
Agent reference file	The path to the SLEE agent's object reference file (slee_agent.ref).

7. Enter a descriptive name, or alias for the SLEE.

   The alias will be used in the commands written in the text based management tool and in the OAM batch files.

8. If you want to list the available commands and their usage, enter command:

   ```
   help
   ```

   This displays the following list:

```
[help]
    Displays this general help text.

[addslee]
    Adds a SLEE. User will be prompted for necessary parameters.

[slee <sleealias>]
    Selects a specific SLEE. SLEE aliases can contain spaces and
    must be typed using ""

[service <servicename>]
    Selects a specific service.

[method <methodname>]
    Selects a specific method.

[<sleealias>:<servicename:<methodname> <param1> <param2> <paramN>]
    Invokes a method directly.
    (e.g. "SLEE 1":MyService:addPerson "John" 45)
    Note that string parameters always must be typed with
    surrounding "".

[<servicename>:<methodname> <param1> <param2> <paramN>]
    Invokes a method directly. (e.g. MyService:addPerson "John" 45)
    Note that string parameters always must be typed with
    surrounding "".

[<methodname> <param1> <param2> <paramN>]
    Invokes a method when a service is selected.
    (e.g. addPerson "John" 45)

[<param1> <param2> <paramN>]
    Invokes the method which is currently selected. (e.g. "John" 45)

[back]
    Steps back. (i.e. unselect service or method)

[exec <filename>]
    Executes a file as batch. This file can contain any
    command that can be typed at the prompt.

[help <servicename>:<methodname>]
    Shows the help(description) associated with a method.

[help <methodname>]
    Shows the help(description) associated with a method of the
    currently selected service.

[info]
    Shows a list of what services or methods are available.
    If a method is selected, the method parameters and
    description will appear.

[reg_al]
```

```
        Register the management tool as alarm listener for
        the selected SLEE.

    [unreg_al]
        Register the management tool as alarm listener for the
        selected SLEE.

    [wait(millisec)]
        Wait the specified number of milliseconds. Useful when
        running scripts.

    [exit]
        Exits
```

Use the above commands according to the provided descriptions.

CHAPTER 4

Application Connection - Web Services

The following sections describe connecting to BEA WebLogic Network Gatekeeper through Web Services:

About Web Services applications

For an application to connect to BEA WebLogic Network Gatekeeper through Web Services, the application must have access to the Extended API or Parlay X WSDL files deployed in BEA WebLogic Network Gatekeeper's web server. Both the Extended API and Parlay X WSDL consist of one file for each service and the file's are deployed in BEA WebLogic Network Gatekeeper's web server at BEA WebLogic Network Gatekeeper installation.

If the application have been implemented using WSDL files with the same version but from another source than BEA WebLogic Network Gatekeeper to connect to, the application developer has to re-generate the Java (or other programming language) interface with WSDL files from BEA WebLogic Network Gatekeeper the application will connect to.

Distributing the WSDL files

The Parlay X WSDL files, can be downloaded from :

```
http:/<IP-address>/parlayx/servlet/AxisServlet
```

The Extended Web Services WSDL files can be downloaded from:

```
http:/<IP-address>/wespa/servlet/AxisServlet
```

The Parlay X WSDL files for the notification interfaces can be downloaded from:

```
http:/<IP-address>/parlayX/wsdl
```

The Extended APIs Web Services WSDL files for the notification interfaces can be downloaded from:

```
http:/<IP-address>/wespa/wsdl
```

Where `<IP-address>` is the IP address of BEA WebLogic Network Gatekeeper host where the axis servlet engine executes. The files are named `<serviceName>Listener.wsdl` and `parlayx_<serviceName>.wsdl`.

Registering service providers and applications

See "Service Provider and Application Administration" on page 5-1.

Enabling a secure SSL connection to an application

The connection between BEA WebLogic Network Gatekeeper and an application can be encrypted using SSL.

Two variants are supported:

- One-way authenticated connections
- Two-way authenticated connections

Both variants use X.509 certificates, with a private key and a public certificate.

One-way authenticated connections

When an application uses a Web Service provided by BEA WebLogic Network Gatekeeper, the WebLogic Network Gatekeeper must import it's own private key and the application needs the WebLogic Network Gatekeeper's public certificate.

When an application provides a Web Service, the application's public certificate must be imported to the WebLogic Network Gatekeeper and the application needs it's own private key.

The WebLogic Network Gatekeeper acts as a...	WebLogic Network Gatekeeper must import	An Application needs
Server (provides a Web Service)	WebLogic Network Gatekeeper's private key	WebLogic Network Gatekeeper's public certificate
Client (uses a Web Service)	Application's public certificate	Application's private key

Table 4-1 Certificate exchange for one-way authenticated sessions

Two-way authenticated connections

In addition to the setup necessary for one-way authenticated sessions, the following must also be configured for two-way authenticated sessions.

When an application uses a Web Service provided by BEA WebLogic Network Gatekeeper, the WebLogic Network Gatekeeper must import the application's certificate and the application needs it's own private key.

When an application provides a Web Service, the WebLogic Network Gatekeeper's private key must be imported to the WebLogic Network Gatekeeper and the application needs the WebLogic Network Gatekeeper's public certificate.

The WebLogic Network Gatekeeper acts as a...	WebLogic Network Gatekeeper must import	An Application needs
Server (provides a Web Service)	WebLogic Network Gatekeeper's private key Application's public certificate	WebLogic Network Gatekeeper's public certificate Application's private key
Client (uses a Web Service)	WebLogic Network Gatekeeper's private key Application's public certificate	Application's private key Application's public certificate

Table 4-2 Certificate exchange for two-way authenticated sessions

About the certificate builder

The certificate builder is a tool for generating user certificates and private keys. It can be used stand alone and through an Network Gatekeeper Management Tool. The same functions are provided in both cases. The stand alone version of the certificate builder is shown in Figure 4-1.

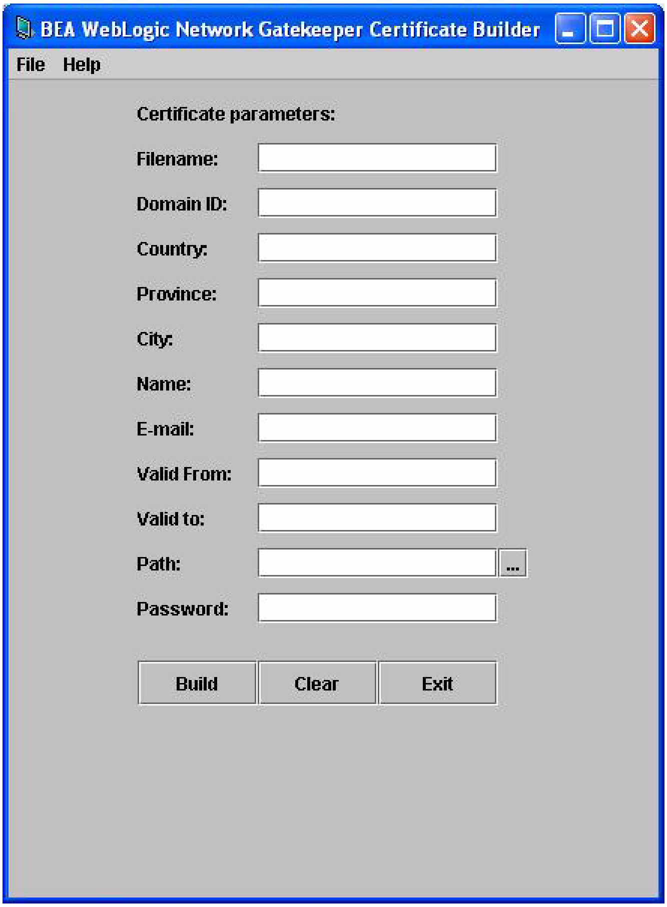


Figure 4-1 Stand alone Certificate Builder

Some fields in the certificate builder are used differently depending on what function the user certificate and private key is generated for. The specific usage of all fields are described in Table 4-3.

Table 4-3 Description of the Fields in the Certificate Builder

Field	Description
Filename	Specifies the file names of the generated user certificate and private key pair. **Example:** If `Filename` is set to `myApplication`, your files will be named: • `myApplication.key` (the private key) • `myApplication.der` (the user certificate).
Domain ID	A descriptive name.
Country	The country BEA WebLogic Network Gatekeeper is located in.
Province	The province or state BEA WebLogic Network Gatekeeper is located in.
City	The city BEA WebLogic Network Gatekeeper is located in.
Name	Contact person at your organization.
E-mail	The contact person's e-mail address.
Start date	The first date (YYYY-MM-DD) the certificate will be valid.
End date	The last date (YYYY-MM-DD) the certificate will be valid.
Path	The path to the directory where the user certificate and private key will be stored. Only existing directories can be specified. When importing a private key from a directory there must be only two files in the directory. That is, the private key and its user certificate. Therefore, it is recommended that you create a new directory for each pair of private key and user certificate you create.
Password	Defines a password that will be needed when importing the private key. Keep a note of the password, you will need it later. Note that this is the private key's password. When you import the private key in the keystore, you will also need the keystore's password. The keystore's password is defined the first time you import a private key or user certificate in the keystore.

Using the certificate builder stand alone

Follow the instruction below to generate a user certificate and private key pair.

If you perform the task through an Network Gatekeeper Management Tool, remember that the user certificate and private key will be stored on the server the Network Gatekeeper Management Tool is connected to. That is, where the SLEE runs.

1. Start the certificate builder.

   e. Open a command window.

2. Go to the `/usr/local/slee/bin/` directory.
3. Start the certificate builder. Enter command: `./runCertBuilder.sh`
4. Enter the user certificate and private key data according to Table 4-3, “Description of the Fields in the Certificate Builder,” on page 4-6.
5. Generate the user certificate and private key. Click the **Build** button.

   The user certificate and private key files are stored in the specified directory.

Using the certificate builder through an Network Gatekeeper Management Tool

Follow the instruction below to generate a user certificate and private key pair.

If you perform the task through an Network Gatekeeper Management Tool, remember that the user certificate and private key will be stored on the server the Network Gatekeeper Management Tool is connected to. That is, where the SLEE runs.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **cert_builder** service.
4. Double-click the **buildCertificate** method.
5. Enter the user certificate and private key data according to Table 4-3, “Description of the Fields in the Certificate Builder,” on page 4-6.
6. Click **Invoke**.

The user certificate and private key files are stored in the specified directory.

Configuring the WebLogic Network Gatekeeper for SSL connections

Follow the instruction below to configure the WebLogic Network Gatekeeper for SSL. The task includes generating certificates an private keys.

Create certificates

1. Follow the instructions given in "Using the certificate builder through an Network Gatekeeper Management Tool" on page 4-7 or "Using the certificate builder stand alone" on page 4-7.

Import the private key of the WebLogic Network Gatekeeper

2. Double-click the **Embedded_Tomcat** service.
3. Double-click the **importServerKey** method.
4. Enter the password for the key, as defined when it was generated, in the **keyPassword** field.
5. Enter the path to where the private key is located in the **directory** field.
6. Click **Invoke**.

Now the WebLogic Network Gatekeeper's private key is imported to the WebLogic Network Gatekeeper's keystore and the WebLogic Network Gatekeeper is configured for SSL. In order setup an SSL connection for an individual application, continue with "Setting up a one-way authenticated SSL connection" on page 4-8 or "Setting up a two-way authenticated SSL connection" on page 4-10, depending on the type of connection to use.

Setting up a one-way authenticated SSL connection

Follow the instruction below to setup a one-way authenticated secure SSL connection between an application and BEA WebLogic Network Gatekeeper. The task includes generating certificates an private keys, exchanging necessary certificates and to setup a HTTPS connection.

Configure the SSL connection when the WebLogic Network Gatekeeper acts as a server

This step is only necessary if the WebLogic Network Gatekeeper acts a server (provider of a a Web service). This is done for each application that shall use SSL connections.

Distribute certificates

1. Distribute the WebLogic Network Gatekeeper's public certificate to the service provider hosting the application.

   Add an HTTPS connector

2. Double-click the **Embedded_Tomcat** service.
3. Double-click the **addHTTPSConnector** method.
4. Enter parameters according to the table below.

Field	Type	Explanation
port	int	Port number for the HTPPS connection. Default port for HTTPS is 443.
acceptCount	int	Maximum number of connections to accept.
minThreads	int	Minimum number of threads to assign to Embedded Tomcat. Recommended value is 20.
maxThreads	int	Maximum number of threads to assign to Embedded Tomcat. Recommended value is 50.
sslClientAuth	boolean	If the SSLclient should be authenticated. In the case of one-way authentication use FALSE. In the case of two-way authentication use TRUE.

5. Click **Invoke**.

Configure the SSL connection when the WebLogic Network Gatekeeper acts as a client

This step is only necessary if the WebLogic Network Gatekeeper acts a client (user of a a Web service). This is done for each application that shall use SSL connections.

Retieve certificates from the application

1. Retrieve the application's public certificate.

   Note: The Certificate Builder can be used to generate the applications private key and public certificate.

Import the application's certificate

2. Start an Network Gatekeeper Management Tool and log in.
3. Select any SLEE.
4. Double-click the **Embedded_Tomcat** service.
5. Double-click the **importSingleUserCertificate** method.
6. Enter the path to where the application's public certificate is located in the **directory** field.

   Note: The directory must contain only the certificate.

7. Enter the alias for the application's public certificate in the **alias** field. The alias must be unique.
8. Click **Invoke**.

Register HTTPS endpoints (Parlay X only)

9. If using Parlay X, make sure that the URLs of the endpoints are registered as HTTPS addresses. The endpoints are registered in the SESPA layer of the respective service capability.
   Refer to section "Optional - Enable network initiated call notifications for Parlay X" on page 5-34 and "Optional - Enable incoming message notification for Parlay X SMS and MMS" on page 5-37.

Setting up a two-way authenticated SSL connection

This is done for each application that shall use two-way authenticated SSL connectons.

Enable one-way authentication

1. As a first step, set up a one-way authenticated SSL connection as described in "Configure the SSL connection when the WebLogic Network Gatekeeper acts as a server" on page 4-8.

   Retrieve the application's certificate

2. Retrieve the file with the application's public certificate and store it in a directory that the WebLogic Network Gatekeeper has access to.

   Import the application's certificate

3. Start an Network Gatekeeper Management Tool and log in.
4. Select any SLEE.
5. Double-click the **Embedded_Tomcat** service.
6. Double-click the **importSingleUserCertificate** method.
7. Enter the path to where the application's public certificate is located in the **directory** field.

   Note: The directory must contain only the certificate.

8. Enter the alias for the application's public certificate in the **alias** field. The alias must be unique.
9. Click **Invoke**.

Note: Make sure that the application import it's own private key.

CHAPTER 5

Service Provider and Application Administration

The following sections describe hot to administer service providers and applications:

About service provider and application administration

Administration model

BEA WebLogic Network Gatekeeper handles service providers and their applications (client applications). The service providers are registered as service provider accounts. The service providers' applications are registered as application accounts. An application account is always tied to specific service provider account. The administration model is shown in Figure 5-1, "Service provider and application administration model.," on page 5-4.

For each application account, one or more application instance groups have to be created. All application users log in to BEA WebLogic Network Gatekeeper through an application instance group. That is, the application instance group and a password identify the users origin. The application instance groups can be used for separating users from different organizations using the same application (but different instances) to access BEA WebLogic Network Gatekeeper.

An example of this is office type applications where each user has its own installation. Using application instance groups, it is possible to separate the different locations/organizations where the application is used and to regulate how many concurrent users are allowed on each location/organization.

If the application is a network initiated application, the normal case is to have one application instance group for all users.

To simplify the administration, it is possible to group service providers and applications with similar usage and charging characteristics. This is achieved through creating service provider and application groups. A group contains a Service Level Agreement (SLA) that is used by all service providers or applications in the group.

Changes in a group SLA affects all service provider accounts or application accounts in the group. It is also possible to move an account from one group to another and there by change the SLA to be used for the service provider or application.

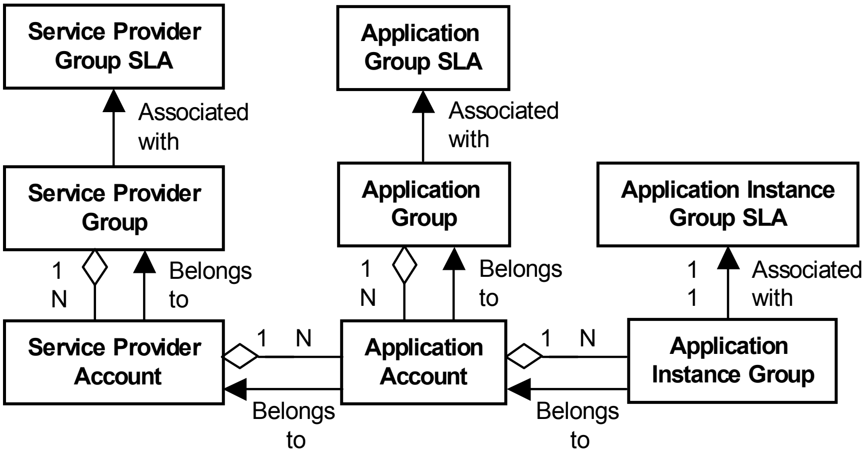


Figure 5-1 Service provider and application administration model.

Overall workflow

The main workflow when creating a service provider account with a number of application accounts is outlined below:

1. Create the service provider group with SLA (optional, only if a suitable service provider group has not already been created)
2. Create service provider account
3. Create application groups with SLAs (optional, only if suitable application groups have not already been created)
4. Create application accounts and application instance groups with SLAs

Creating a service provider group

Follow the instruction below to create a service provider group. The service provider group contains a SLA that can be used by one or more service provider accounts.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA access service is installed.

3. Double-click the **ESPA_access** service.

   Decide a suitable service provider group ID

4. Decide a suitable (descriptive) ID for the service provider group according to your naming conventions.

   Verify that the ID is not used

5. Double-click the **getNumberOfServiceProviderGroups** method.

6. Click **Invoke**.

   The total number of service provider groups in the system is displayed.

7. Double-click the **listServiceProviderGroups** method.

8. List a reasonable number of service provider group IDs. Enter the range.

9. Click **Invoke**.

   The selected number of service provider group IDs are displayed in alphabetic order. If the ID you want to use does not fit within the range, select a new range. When the correct range is displayed, verify that the ID you want to use is not in the list.

   Create service provider group SLA

10. See "Writing Service Level Agreements" on page D-1.

    Create service provider group

11. Double-click the **addServiceProviderGroupWithSLAUrl** method.

12. Enter the ID selected for the service provider group and, in the **slaContents** field, the URL for the SLA file.

    Note: Do not enter any OAM properties. OAM properties can only be set from an integrated PRM/CRM system.

13. Click **Invoke**.

    The service provider group is now created. To add service provider accounts to the service provider group, see "Creating a service provider account" on page 5-8.

Identifying a service provider group

Follow the instruction below to identify a service provider group ID.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA access service is installed.
3. Double-click the **ESPA_access** service.
4. Double-click the **getNumberOfServiceProviderGroups** method.
5. Click **Invoke**.

   The number of service provider groups in the system is displayed.
6. Double-click the **listServiceProviderGroups** method.
7. List a reasonable number of service provider group IDs. Enter the range.
8. Click **Invoke**.

   The selected number of service provider group IDs are displayed in alphabetic order. If the desired ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the service provider group.

Viewing information about a service provider group

Follow the instruction below to view information about a service provider group. The following types of information can be viewed independently of each other:

- service provider group data (SLA and other properties, if any)
- service provider group SLA
- related service provider account

  Identify the service provider group ID

1. See "Identifying a service provider group" on page 5-5.

   View data
2. Double-click the **getServiceProviderGroup** method.
3. Enter the service provider group ID.
4. Click **Invoke**.

   The service provider group's SLA and OAM properties, if any, are displayed.

   View SLA

Note, it is also possible to view the original XML SLA file.

5. Double-click the **getSLAForServiceProviderGroup** method.

6. Enter the service provider group ID.

7. Click **Invoke**.

   The service provider group's SLA is displayed.

   List related service provider accounts

8. Double-click the **getNumberOfServiceProvidersInGroup** method.

9. Enter the service provider group ID.

10. Click **Invoke**.

    The number of service provider accounts related to the service provider group is displayed.

11. Double-click the **listServiceProvidersInGroup** method.

12. List a reasonable number of service provider account IDs. Enter the service provider group ID and the range.

13. Click **Invoke**.

    The selected number of service provider group IDs are displayed in alphabetic order.

Updating the SLA for a service provider group

Follow the instruction below to update the SLA for a service provider group.

Identify the service provider group

1. See "Identifying a service provider group" on page 5-5.

   View current SLA

   Note, it is also possible to view the original XML SLA file.

2. Double-click the **getServiceProviderGroup** method.

3. Enter the service provider group ID.

4. Click **Invoke**.

   The service provider group's SLA is displayed.

   Update SLA

5. Update the SLA, see "Writing Service Level Agreements" on page D-1.
6. Double-click the **updateServiceProviderGroupSLAUrl** method.
7. Enter the service provider group ID and, in the **slaContents** field, the URL for the SLA file.

   Note: Do not enter any OAM properties. OAM properties can only be set from an integrated PRM/CRM system.

8. Click **Invoke**.

   The service provider group's SLA is now updated and in use.

Deleting a service provider group

Follow the instruction below to delete a service provider group.

Note: When deleting the service provider group, all related service provider accounts, application accounts and application instance groups will also be deleted.

Identify the service provider group

1. See "Identifying a service provider group" on page 5-5.

Delete service provider group

2. Double-click the **deleteServiceProviderGroup** method.
3. Enter the service provider group ID.
4. Click **Invoke**.

   The service provider group is now deleted.

Creating a service provider account

Follow the instruction below to create a service provider account. Note, the service provider group the service provider account shall be connected to must have been created before the service provider account is created.

Identify the service provider group

1. See "Identifying a service provider group" on page 5-5.

Decide a suitable service provider account ID

2. Decide a suitable (descriptive) ID for the service provider account according to your naming conventions.

Verify that the ID is not used

3. Double-click the **getNumberOfServiceProvidersInGroup** method.
4. Enter the service provider group ID.
5. Click **Invoke**.

   The number of service provider accounts connected to the service provider group is displayed.

6. Double-click the **listServiceProvidersInGroup** method.
7. List a reasonable number of service provider account IDs. Enter the service provider group ID and the range.
8. Click **Invoke**.

   The selected number of service provider account IDs are displayed in alphabetic order. If the ID you want to use does not fit within the range, select a new range. When the correct range is displayed, verify that the ID you want to use is not in the list.

   Create service provider account

9. Double-click the **addServiceProviderAccount** method.
10. Enter the service provider group ID and the selected service provider account ID.
11. Click **Invoke**.

    The service provider account is now created. To add application accounts to the service provider account. See "Creating an application account" on page 5-19.

    The service provider account has to be activated before the service provider's applications can access any services in the network. See "Activating a service provider account" on page 5-10.

Identifying a service provider account ID

Follow the instruction below to identify a service provider account ID.... through the service provider group

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA access service is installed.
3. Double-click the **ESPA_access** service.

Identify the service provider group

4. Double-click the **getNumberOfServiceProviderGroups** method.
5. Click **Invoke**.

   The total number of service provider groups in the system is displayed.
6. Double-click the **listServiceProviderGroups** method.
7. List a reasonable number of service provider group IDs. Enter the range.
8. Click **Invoke**.

   The selected number of service provider group IDs are displayed in alphabetic order. If the desired ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the service provider group.

   Identify the service provider account
9. Double-click the **getNumberOfServiceProvidersInGroup** method.
10. Enter the service provider group ID.
11. Click **Invoke**.

    The number of service provider accounts related to the service provider group is displayed.
12. Double-click the **listServiceProvidersInGroup** method.
13. List a reasonable number of service provider account IDs. Enter the service provider group ID and the range.
14. Click **Invoke**.

    The selected number of service provider account IDs are displayed in alphabetic order. If the desired ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the service provider account.

Activating a service provider account

Follow the instruction below to activate a service provider account. The service provider account has to be activated before any of its applications can start accessing services in the network.

Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

View current state

2. Double-click the **getStateForServiceProviderAccount** method.
3. Enter the service provider account ID.
4. Click **Invoke**.

   The service provider account's current state is displayed.

   Activate service provider account

5. Double-click the **activateServiceProviderAccount** method.
6. Enter the service provider account ID.
7. Click **Invoke**.

   The service provider account's state is changed to activated.

Viewing information about a service provider account

Follow the instruction below to view information about a service provider account. The following types of information can be viewed independently of each other:

- service provider account data (related service provider group and OAM properties, if any)
- service provider account state
- SLA related to the service provider account
- application accounts related to the service provider account

  Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

   View data

2. Double-click the **getServiceProviderAccount** method.
3. Enter the service provider account ID.
4. Click **Invoke**.

   The related service provider group's ID and the account's OAM properties, if any, are displayed.

   View state

5. Double-click the **getStateForServiceProviderAccount** method.
6. Enter the service provider account ID.
7. Click **Invoke**.

   The service provider account's current state is displayed.

   View SLA

   The SLA is related to the service provider group. To view the SLA, the service provider group ID is needed. See "View data" on page 5-11.

   Note, it is also possible to view the original XML SLA file.

8. Double-click the **getSLAForServiceProviderGroup** method.
9. Enter the service provider group ID.
10. Click **Invoke**.

    The SLA is displayed.

    List related application accounts

11. Double-click the **getNumberOfApplicationsInServiceProvider** method.
12. Enter the service provider account ID.
13. Click **Invoke**.

    The number of application accounts connected to the service provider account is displayed.

14. Double-click the **listApplicationAccountsForServiceProvider** method.
15. List a reasonable number of application account IDs. Enter the service provider account ID and the range.
16. Click **Invoke**.

    The selected number of application account IDs are displayed in alphabetic order.

Changing data (SLA) for a service provider account

Follow the instruction below to change the service provider group for a service provider account. That is, by changing the service provider group the SLA used for the service provider account is changed.

Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

   View current service provider account data

2. Double-click the **getServiceProviderAccount** method.

3. Enter the service provider account ID.

4. Click **Invoke**.

   The related service provider group's ID and the account's OAM properties, if any, are displayed.

   Change service provider account data (SLA)

5. Double-click the **updateServiceProviderAccount** method.

6. Enter the service provider account ID and a new service provider group ID.

7. Click **Invoke**.

   The related service provider group (SLA) is changed.

Logging out a service provider account

Follow the instruction below to log out a service provider account. That is, to log out all application instance group users related to the service provider account.

To log out all application instance group users related to an application account or an application instance group, see "Logging out an application account" on page 5-28 and "Logging out an application instance group" on page 5-42 respectively.

   Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

   Log out service provider account

2. Double-click the **logoutServiceProviderAccount** method.

3. Enter the service provider account ID.

4. Click **Invoke**.

   All application instance group users related to the service provider account are logged out.

Deactivating a service provider account

Follow the instruction below to deactivate a service provider account. That is, to temporarily stop the traffic to/from the service provider's applications.

Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

   View current state

2. Double-click the **getStateForServiceProviderAccount** method.
3. Enter the service provider account ID.
4. Click **Invoke**.

   The service provider account's current state is displayed.

   Deactivate service provider account

5. Double-click the **deactivateServiceProviderAccount** method.
6. Enter the service provider account ID.
7. Click **Invoke**.

   The service provider account's state is changed to deactivated.

Deleting a service provider account

Follow the instruction below to delete a service provider account.

Note: When deleting the service provider account, all related application accounts and application instance groups will also be deleted.

Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

   Delete service provider account

2. Double-click the **deleteServiceProviderAccount** method.
3. Enter the service provider account ID.
4. Click **Invoke**.

The service provider account and all related application accounts and application instance groups are deleted.

Creating an application group

Follow the instruction below to create an application group. The application group contains a SLA that can be used by one or more application accounts.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA access service is installed.
3. Double-click the **ESPA_access** service.

   Decide a suitable application group ID

4. Decide a suitable (descriptive) ID for the application group according to your naming conventions.

   Verify that the ID is not used

5. Double-click the **getNumberOfApplicationGroups** method.
6. Click **Invoke**.

   The number of application groups in the system is displayed.

7. Double-click the **listApplicationGroups** method.
8. List a reasonable number of application group IDs. Enter the range.
9. Click **Invoke**.

   The selected number of application group IDs are displayed in alphabetic order. If the ID you want to use does not fit within the range, select a new range. When the correct range is displayed, verify that the ID you want to use is not in the list.

   Create application group SLA

10. See "Writing Service Level Agreements" on page D-1.

    Create application group

11. Double-click the **addApplicationGroupWithSLAUrl** method.
12. Enter the ID selected for the application group and, in the **slaContents** field, the URL for the SLA file.

Note: Do not enter any OAM properties. OAM properties can only be set from an integrated PRM/CRM system.

13. Click **Invoke**.

    The application group is now created. To add application accounts to the application group, see “Creating an application account” on page 5-19.

Identifying an application group

Follow the instruction below to identify an application group ID.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA access service is installed.
3. Double-click the **ESPA_access** service.
4. Double-click the **getNumberOfApplicationGroups** method.
5. Click **Invoke**.

   The number of application groups in the system is displayed.
6. Double-click the **listApplicationGroups** method.
7. List a reasonable number of application group IDs. Enter the range.
8. Click **Invoke**.

   The selected number of application group IDs are displayed in alphabetic order. If the desired ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the application group.

Viewing information about an application group

Follow the instruction below to view information about an application group. The following types of information can be viewed independently of each other:

- application group data (SLA and OAM properties, if any)
- application group SLA
- related application accounts

Identify the application group ID

1. See "Identifying an application group" on page 5-16.

   View data

2. Double-click the **getApplicationGroup** method.
3. Enter the application group ID.
4. Click **Invoke**.

   The application group's SLA and OAM properties, if any, are displayed.

   View SLA

   Note, it is also possible to view the original XML SLA file.

5. Double-click the **getSLAForApplicationGroup** method.
6. Enter the application group ID.
7. Click **Invoke**.

   The application group's SLA is displayed.

   List related application accounts

8. Double-click the **getNumberOfApplicationsInApplicationGroup** method.
9. Click **Invoke**.

   The number of application accounts related to the application group is displayed.

10. Double-click the **listApplicationAccountsInGroup** method.
11. List a reasonable number of application account IDs. Enter the application group ID and the range.
12. Click **Invoke**.

    The selected number of application account IDs are displayed in alphabetic order.

Updating SLA for an application group

Follow the instruction below to update the SLA for a application group.

Identify the application group ID

1. See "Identifying an application group" on page 5-16.

   View current SLA

Note, it is also possible to view the original XML SLA file.

2. Double-click the **getApplicationGroup** method.

3. Enter the application group ID.

4. Click **Invoke**.

   The application group’s SLA is displayed.

   Update SLA

5. Update the SLA, see “Writing Service Level Agreements” on page D-1.

6. Double-click the **updateApplicationGroupSLAUrl** method.

7. Enter the application group ID and, in the **slaContents** field, the URL for the SLA file.

   Note: Do not enter any OAM properties. OAM properties can only be set from an integrated PRM/CRM system.

8. Click **Invoke**.

   The application group’s SLA is now updated and in use.

Deleting an application group

Follow the instruction below to delete an application group.

Note: When deleting the application group, all related application accounts and application instance groups will also be deleted.

Identify the application group

9. See “Identifying an application group” on page 5-16.

   Delete application group

10. Double-click the **deleteApplicationGroup** method.

11. Enter the application group ID.

12. Click **Invoke**.

    The application group and the related application accounts and application instance groups are now deleted.

Creating an application account

Follow the instruction below to create an application account. Note, the service provider account and application group the application account shall be connected to must have been created before the application account is created.

In addition you also have to set up the connection with the application, see "Application Connection - ESPA Java" on page 3-1 and "Application Connection - Web Services" on page 4-1 respectively.

Identify the service provider account

1. Identify the ID of the service provider account you want to connect the application account to. See "Identifying a service provider account ID" on page 5-9.

   Identify the application group

2. Identify the ID of the application group containing the SLA you want to use for the application account. See "Identifying an application group" on page 5-16.

   Decide a suitable application account ID

3. Decide a suitable (descriptive) ID for the application account according to your naming conventions.

   Verify that the ID is not used

4. Double-click the **getNumberOfApplicationsInServiceProvider** method.
5. Enter the service provider account ID.
6. Click **Invoke**.

   The number of application accounts connected to the service provider account is displayed.

7. Double-click the **listApplicationAccountsForServiceProvider** method.
8. List a reasonable number of application account IDs. Enter the service provider account ID and the range.
9. Click **Invoke**.

   The selected number of application account IDs are displayed in alphabetic order. If the ID you want to use does not fit within the range, select a new range. When the correct range is displayed, verify that the ID you want to use is not in the list.

   Create application account

10. Double-click the **addApplicationAccount** method.
11. Enter the service provider account ID, the selected application account ID, and the application group ID.
12. Click **Invoke**.

    The application account is now created. To add application instance groups to the application account. See "Creating an application instance group" on page 5-30.

    The application account has to be activated before the application account's application instance group users can access any services in the network. See "Activating an application account" on page 5-25.

Parameter	Description
keyStorePassword	The OSA/Parlay keystore password.
directory	The path to the directory where the application's user certificate is stored Note, only one certificate can be stored in the directory
alias	An alias to use for the certificate in the keystore. For example the application ID

Note: If the application shall access services in the network through an OSA/Parlay gateway, the application account has to be connected to the OSA/Parlay gateway. See "Connecting an application (account) to an OSA/Parlay gateway" on page 5-20.

Connecting an application (account) to an OSA/Parlay gateway

Follow the instruction below to connect an application (account) to an OSA/Parlay gateway. The application account has to be manually connected to the OSA/Parlay gateway before it can start using network services through the OSA/Parlay gateway.

The OSA/Parlay gateway operator has to provide the following information/data:

- **entOpId** (Enterprise operator ID) - Depending on how the OSA/Parlay operator administrates the applications (OSA/Parlay clients) the entOpId can be used for:
  - all applications in the WebLogic Network Gatekeeper
  - all applications connected to a service provider account

  - a single application account

- **appId** (Application ID) to be used for the application account (clientAppId=entOpId\appId)

- **service type(s)** for the OSA/Parlay SCS(es) used by the application

- OSA/Parlay **service types** for the OSA/Parlay SCSes the application shall be mapped with

- **encryption method**

- **signing algorithm**

Note: The WebLogic Network Gatekeeper must have been connected to the OSA/Parlay gateway before any applications can be connected. See "OSA Gateway Connection" on page 7-1.

Generate user certificate and private key

1. Create a new directory in the folder where you keep your applications' user certificates and private key. Give the directory a name identifying the application.

2. Generate a user certificate and private key for the application. See "Generating certificates and private keys" on page C-5.

   Use the **appId** (application account ID) and **entOpId** (service provider account ID) provided by the OSA/Parlay gateway operator.

   Set **Path** to the directory you created in Step 1.. The application's private key and user certificate will be stored in this directory.

Create OSA/Parlay client

1. Start an Network Gatekeeper Management Tool and log in.

2. Select a SLEE where the OSA access service is installed.

3. Double-click the **OSA_access** service.

4. Double-click the **addClient** method.

5. Enter the following application domain data:

Parameter	Description
osaClientAppId	The application's clientAppId (and alias in the keystore). Entered as Domain ID when generating the user certificate and private key.
clientKeyFile	The directory path (including file name) for the private key.
clientCertFile	The directory path (including file name) for the user certificate.
clientKeyPwd	The client's private key password as defined when the private key was generated.
keystorePwd	The keystore's password as defined in when configuring the WebLogic Network Gatekeeper system.

6. Click **Invoke**.

   The OSA/Parlay client is created.

   Map application account with OSA/Parlay client

   Note: One mapping has to be created for each OSA/Parlay SCS (network service) the application wants to use in the OSA/Parlay gateway.

7. Double-click the **addMapping** method.

8. Enter the following mapping data:

Parameter	Description
serviceProviderID	The service provider's service provider account ID.
applicationID	The application's application account ID.
serviceType	The service type of the OSA/Parlay SCS the application shall be mapped with.
osaClientAppId	The application's clientAppID.

Parameter	Description
properties	OSA/Parlay service properties to be used in the look up (service discovery) phase when requesting a service (OSA/Parlay SCS) from the OSA/Parlay gateway. The properties are specified as a space separated list in the following way: <propname1> <propval1> <propname2> <propval2>
encryptionMethod	The method used for encryption. Defined according to OSA/Parlay standard. If not specified, enter P_RSA_1024.
signingAlgorithm	The signing algorithm. Defined according to OSA/Parlay standard. If not specified, enter P_MD5_RSA_1024.
gatewayId	The OSA/Parlay gateway's ID. As defined when the OSA/Parlay gateway was connected. See "OSA Gateway Connection" on page 7-1.
initConnection	Indicates (TRUE/FALSE) if the connection to OSA/Parlay gateway should be initialized immediately. That is, authentication performed when the **addClient** method is invoked.

Distribute application (account) user certificate to OSA/Parlay operator

9. Copy the application's user certificates from its directory, see Step 1. on page 21, and send it to the OSA/Parlay gateway operator. Use the application account's clientAppID (entOpId\appId) as a reference.

   Note: There are two files in the directory, a user certificate (.der) and a private key (.key). Only the user certificate shall be sent to the OSA/Parlay gateway operator.

Optional - Order user interaction announcement recording and installation

10. If the application uses (is mapped to) the user interaction OSA/Parlay SCS, recording and installation of announcements have to be ordered from the OSA/Parlay gateway operator.

Identifying an application account

It is possible to identify a service provider account ID in two ways:

- Through listing application accounts for a service provider account

- Through listing application accounts related to a specific application group

Both methods are described below.

…through the service provider account

Follow the instruction below to identify an application account ID through the service provider account.

Identify the service provider account

1. See "Identifying a service provider account ID" on page 5-9.

   Identify the application account

2. Double-click the **getNumberOfApplicationsInServiceProvider** method.
3. Enter the service provider account ID.
4. Click **Invoke**.

   The number of application accounts connected to the service provider account is displayed.

5. Double-click the **listApplicationAccountsForServiceProvider** method.
6. List a reasonable number of application account IDs. Enter the service provider account ID and the range.
7. Click **Invoke**.

   The selected number of application account IDs are displayed in alphabetic order. If the application account ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the application account.

…through the application group

Follow the instruction below to identify a application account ID through the application group.

Identify the application group

1. See "Identifying an application group" on page 5-16.

   Identify the application account ID

2. Double-click the **getNumberOfApplicationsInApplicationGroup** method.
3. Enter the application group ID.

4. Click **Invoke**.

   The number of application accounts related to the application group is displayed.

5. Double-click the **listApplicationAccountsInGroup** method.

6. List a reasonable number of application account IDs. Enter the application group ID and the range.

7. Click **Invoke**.

   The selected number of application account IDs are displayed in alphabetic order. If the application account ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the application account.

Activating an application account

Follow the instruction below to activate an application account. The application account has to be activated before the application can start accessing services in the network.

Identify the application account

1. See "Identifying an application account" on page 5-23.

   View current state

2. Double-click the **getStateForApplicationAccount** method.

3. Enter the service provider account ID and application account ID.

4. Click **Invoke**.

   The application account's current state is displayed.

   Activate application account

5. Double-click the **activateApplicationAccount** method.

6. Enter the service provider account ID and application account ID.

7. Click **Invoke**.

   The application account's state is changed to activated.

Viewing information about an application account

Follow the instruction below to view information about an application account. The following types of information can be viewed independently of each other:

- application account data (related application group, OAM properties)
- application account state
- SLA related to the application account
- application instance groups related to the application account
- logged in application groups related to the application account

Identify the application account

1. See “Identifying an application account” on page 5-23.

   View application account data

2. Double-click the **getApplicationAccount** method.
3. Enter the service provider account ID and application account ID.
4. Click **Invoke**.

   The related application group’s ID and the account’s OAM properties, if any, are displayed.

   View state

5. Double-click the **getStateForApplicationAccount** method.
6. Enter the service provider account ID and application account ID.
7. Click **Invoke**.

   The application account’s current state is displayed.

   View SLA

   The SLA is related to the application group. To view the SLA, the application group ID is needed. See Step 2. *View application account data*.

8. Double-click the **getSLAForApplicationGroup** method.

9. Enter the application group ID.
10. Click **Invoke**.

    The SLA is displayed.

    List application instance groups

11. Double-click the **getNumberOfApplicationInstanceGroupsInApplications** method.
12. Enter the service provider account ID and application account ID.
13. Click **Invoke**.

    The number of application instance groups related to the application account is displayed.

14. Double-click the **listApplicationInstanceGroups** method.
15. List a reasonable number of application instance group IDs. Enter the service provider account ID, application account ID and the range.
16. Click **Invoke**.

    The selected number of application instance group IDs are displayed in alphabetic order.

    List logged in application instance groups

17. Double-click the **getNumberOfLoggedInApplicationInstanceGroups** method.
18. Enter the service provider account ID and application account ID.
19. Click **Invoke**.

    The number of logged in application instance groups related to the application account is displayed.

20. Double-click the **listLoggedInApplicationInstanceGroups** method.
21. List a reasonable number of logged in application instance group IDs. Enter the service provider account ID, application account ID and the range.
22. Click **Invoke**.

    The selected number of logged in application instance group IDs are displayed in alphabetic order.

Changing data (SLA) for an application account

Follow the instruction below to change the application group for an application account. That is, by changing the application group the SLA used for the application account is changed.

Identify the application account

1. See “Identifying an application account” on page 5-23.

   View current application account data

2. Double-click the **getApplicationAccount** method.
3. Enter the service provider account ID and application account ID.
4. Click **Invoke**.

   The related application group’s ID and the account’s OAM properties, if any, are displayed.

   Change application account data (SLA)

5. Double-click the **updateApplicationAccount** method.
6. Enter the service provider account ID and application account ID and a new application group.
7. Click **Invoke**.

   The related application group (SLA) is changed.

Logging out an application account

Follow the instruction below to log out an application account. That is, to log out all application instance group users related to the application account.

To log out all application instance group users related to an application instance group, see “Logging out an application instance group” on page 5-42.

Identify the application account

1. See “Identifying an application account” on page 5-23.

   Log out application account

2. Double-click the **logoutApplicationAccount** method.
3. Enter the service provider account ID and application account ID.

4. Click **Invoke**.

   All application instance group users related to the application account are logged out.

Deactivating an application account

Follow the instruction below to deactivate an application account. That is, to temporarily stop the traffic to/from the application.

Identify the application account

1. See "Identifying an application account" on page 5-23.

   View current state

2. Double-click the **getStateForApplicationAccount** method.
3. Enter the service provider account ID and application account ID.
4. Click **Invoke**.

   The application account's current state is displayed.

   Deactivate application account

5. Double-click the **deactivateApplicationAccount** method.
6. Enter the service provider account ID and application account ID.
7. Click **Invoke**.

   The application account's state is changed to deactivated.

Deleting an application account

Follow the instruction below to delete an application account.

Note: When deleting the application account, all related application instance groups will also be deleted.

Identify the application account

1. See "Identifying an application account" on page 5-23.

   Delete application account

2. Double-click the **deleteApplicationAccount** method.

3. Enter the service provider account ID and application account ID.
4. Click **Invoke**.

   The application account and all related application instance groups are deleted.

Creating an application instance group

Follow the instruction below to create an application instance group. The group contains a SLA specifying how many current users are allowed within the group.

Depending on the type of network services used by the application related to the application instance group, if the application accesses the WebLogic Network Gatekeeper through the Parlay X Web Services interfaces, and if the network access is through an OSA/Parlay gateway some of the following tasks may also have to be performed:

- Create mailboxes in the WebLogic Network Gatekeeper
- Order corresponding mailboxes from the OSA/Parlay gateway operator
- Create charging accounts in the WebLogic Network Gatekeeper
- Order corresponding charging accounts from the OSA/Parlay gateway operator
- Set Parlay X properties
- Enable network initiated call notifications for Parlay X
- Enable incoming message notification for Parlay X SMS and MMS

Identify the application account

1. See "Identifying an application account" on page 5-23. Select the option *...through the service provider account*.

   Decide a suitable application instance group ID

2. Decide a suitable (descriptive) ID for the application instance group according to your naming conventions.

   Verify that the ID is not used

3. Double-click the **getNumberOfApplicationInstanceGroupsInApplications** method.
4. Enter the service provider account ID and application account ID.

5. Click **Invoke**.

   The number of application instance groups related to the application account is displayed.

6. Double-click the **listApplicationInstanceGroups** method.

7. List a reasonable number of application instance group IDs. Enter the service provider account ID, application account ID and the range.

8. Click **Invoke**.

   The selected number of application instance group IDs are displayed in alphabetic order. If the ID you want to use does not fit within the range, select a new range. When the correct range is displayed, verify that the ID you want to use is not in the list.

   Create application instance group

9. Double-click the **addApplicationInstanceGroupSLAString** method.

10. Enter the following data:

Parameter	Description
serviceProviderAccountID	The service provider's service provider account ID.
applicationAccountID	The application's application account ID.
applicationInstance GroupID	The application instance group ID.
slaContents	The number of allowed concurrent users in the application instance group.
properties	Note, OAM properties can only be set from an integrated PRM/CRM system.
password	The password to be used by the application instance group users when logging in.

11. Click **Invoke**.

    The application instance group is created. Depending on the type of network services used by the application related to the application instance group and/or the application accesses BEA WebLogic Network Gatekeeper through the Parlay X Web Services interfaces, some of the following below tasks may also have to be performed.

Optional - Create mailbox(es)

12. If the application uses messaging, mailbox(es) have to created for the application. See "Mailbox Administration" on page 13-1.
13. Distribute the mailbox addresses and password to the service provider.

    Optional - Order creation of mailbox(es) in OSA gateway

14. If the ESPA messaging service is used by the application related to the application instance group, mailboxes have to be ordered from the OSA/Parlay gateway operator.

    Optional - Create charging account(s)

15. If the application related to the application group uses the ESPA charging service you also have to create accounts in your accounts database. This is not covered in this User's Guide.

    Optional - Order creation of charging account(s) in OSA gateway

16. If the application related to the application group uses the ESPA charging service AND is connected to a OSA/Parlay charging SCS in an OSA/Parlay gateway, charging accounts have to be ordered from the OSA/Parlay gateway operator.

    Optional - Set application (instance group) properties for Parlay X

    Application properties only have to be set if the application accesses the WebLogic Network Gatekeeper through the Parlay X Web Service interfaces.

17. Select a SLEE where the SESPA access service is installed.
18. Double-click the **SESPA_access** service.
19. Double-click the **setAppProperties** method.
20. Enter the following data:

Parameter	Description
serviceProviderID	The service provider account ID.
applicationID	The application account ID.
applicationInstanceGroupID	The application instance group ID.
appPassword	Password for the application instance group.

Parameter	Description
mailbox	The mailbox ID to be used for the application instance group. **Optional**, only used when the application uses the SMS or Multimedia Message Parlay X services.
mailboxPassword	Password associated with the Parlay mailbox. **Optional**, only used when the application uses the SMS or Multimedia Message Parlay X services.
merchantId	The merchant ID for the application instance group. **Optional**, only used when the application uses the Payment Parlay X service.
accountId	Account ID for the application instance group, to be used in payment/charging sessions. **Optional**, only used when the application uses the Payment Parlay X service.
currency	Currency to be used for amount charging in payment/charging sessions. **Optional**, only used when the application uses the Payment Parlay X service.
chargeVolumeType	The unit to be used for volume charging in payment/charging sessions. A unit is defined as one of the following: 0 - undefined 1 - number of times or events 2 - octets 3 - seconds 4 - minutes 5 - hours 6 - days **Optional**, only used when the application related to the application instance group uses the Payment Parlay X service.

21. Click **Invoke**.

    The Parlay X properties are set for the application instance group.

    Optional - Enable network initiated call notifications for Parlay X

    Follow the instruction below to enable notifications on network triggered calls to an application instance group related to an application using Parlay X third party call.

    The application subscribes for notifications related to an originating number and a destination number, either one of them or a combination of both. This means notifications can be subscribed for either when:

    – An A-party calls a certain B-party.

    – An A-party calls any B-party.

    – Any A-party calls a certain B-party.

    – An A-party goes off hook.

    One registration is needed for each notification to subscribe to.

22. Select a SLEE where the SESPA call control service is installed.

23. Double-click the **SESPA_call_control** service.

24. Double-click the **addParlayXNetworkCallListener** method.

25. Enter the following data.

Parameter	**Description**
endPoint	URL to the end point of the callback/notification web service implementation for network triggered calls. For example, `http://<mywebserver>/<mylistener>.wsdl`
serviceProviderID	The service provider account ID.
applicationID	The application account ID.
applicationInstanceGroup ID	The application instance group ID.

Parameter	Description
aPartyAddressExpression	A-party address (originating number) expression. For example, 46*. The format of the address expressions is explained below the table. Note, the application subscribes for notifications related to an originating number and a destination number, either one of them or a combination of both.

Parameter	Description
bPartyAddressExpression	B-party address (destination number) expression. The format of the address expression is similar to that for the A-party. Note, the application subscribes for notifications related to an originating number and a destination number, either one of them or a combination of both.
callEventCriteria	Call event criteria to trigger, or invoke, the web service. Define one of the following criterias by entering the corresponding number. 3 An originating call attempt has been made. 6 The called user was busy. 7 The called user did not answer. 8 The call failed for some reason. 10 A participant was disconnected from the call. 11 All of the above events. The call event criteria are always triggered in mode INTERRUPT allowing the application to control the call processing. If there is one or more listeners registered for the identical criteria as this one, and those listeners are registered from the same application domain as this one, the listener will be added to a High Availability and Load Balancing list. This means that the network initiated calls matching this criteria will be distributed using a round robin algorithm between the listeners with identical criteria. If the above is false, and there already is a listener registered for an address that overlaps this listener, an exception is raised. The application must implement the method corresponding to the CallEventCriteria. If not, the processing of the call is halted.
serviceCode	A string identifying the service (application) issuing the request. The information may be used for calculating charging related information. The format is unspecified.

Parameter	Description
requesterID	An ID for the requester of this service, could be a token received during log-in or the full address for the requester. If it's a full address the format shall adhere to the format as specified for the EndUserIdentifier. In other cases the format is unspecified. If the requester is unknown/unspecified an empty string shall be used.

The following rules apply to the addressExpressions:
Two wildcards are allowed: * which matches zero or more characters and ? which matches exactly one character. For E.164 addresses, * which matches zero or more characters and ? are allowed at the beginning or end.

Some valid examples for E.164 addresses:

– "123" matches specific number.

– "123*" matches all numbers starting with 123 (including 123 itself).

– "123??*" matches all numbers starting with 123 and at least 5 digits long.

– "123???" matches all numbers starting with 123 and exactly 6 digits long.

The following address ranges are illegal:

– "1?3"

– "1*3"

– "?123*"

_ "*"

_ ""

Legal occurrences of the '*' and '?' characters in AddrString should be escaped by a '\' character. To specify a '\' character '\\' must be used.

26. Click **Invoke**.

    The network call listener is registered and an ID for the listener is displayed.

27. Repeat Steps 24. to 26. for each notification to be enabled.

    Optional - Enable incoming message notification for Parlay X SMS and MMS

Follow the instruction below to enable notifications on incoming SMSes and multimedia messages to a Parlay X application. Notifications have to be enabled for each mailbox registered for the application instance group.

28. Select a SLEE where the SESPA messaging service is installed.
29. Double-click the **SESPA_messaging** service.
30. Double-click the **enableMessageNotification** method.
31. Enter the following data.

Parameter	Description
mailbox	The mailbox for which to enable notifications on incoming messages. Format: `tel:<mailbox>` For example: `tel:12345`
mailboxPassword	The password related to the mailbox
smsEndPoint	URL to the end point of the callback/notification web service implementation for incoming SMSes. For example: `http://<mywebserver>/<listener>.wsdl`
mmsEndPoint	URL to the end point of the callback/notification web service implementation for incoming MMSes. For example: `http://<mywebserver>/<listener>.wsdl`
serviceProviderID	The service provider account ID.

Parameter	Description
applicationID	The application account ID.
applicationInstanceGroup ID	The application instance group ID.
serviceCode	A string identifying the service (application) issuing the request. The information may be used for calculating charging related information. The format is unspecified.
requesterID	An ID for the requester of this service, could be a token received during log-in or the full address for the requester. If it's a full address the format shall adhere to the format as specified for the EndUserIdentifier. In other cases the format is unspecified. If the requester is unknown/unspecified an empty string shall be used.

32. Click **Invoke**.

    The listener is registered and an ID for the listener is displayed.

Identifying an application instance group

Follow the procedure below to identify an application instance group.

Identify the application instance group

1. See "Identifying an application account" on page 5-23. Select the option *...through the service provider account*.

   Identify the application instance group ID

2. Double-click the **getNumberOfApplicationInstanceGroupsInApplications** method.
3. Enter the service provider account ID and application account ID.
4. Click **Invoke**.

   The number of application instance groups connected to the application account is displayed.

5. Double-click the **listApplicationInstanceGroups** method.

6. List a reasonable number of application instance group IDs. Enter the service provider account ID, application account ID and the range.

7. Click **Invoke**.

   The selected number of application instance group IDs are displayed in alphabetic order. If the application instance group ID is not within the range, select a new range. When the correct range is displayed, verify the ID of the application instance group.

Activating an application instance group

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   View current state

2. Double-click the **getStateForApplicationInstanceGroup** method.

3. Enter the service provider account ID, application ID and application instance group ID.

4. Click **Invoke**.

   The application instance group's current state is displayed.

   Activate application instance group

5. Double-click the **activateApplicationInstanceGroup** method.

6. Enter the service provider account ID, application ID and application instance group ID.

7. Click **Invoke**.

   The application instance group's state is changed to activated.

Viewing information about an application instance group

Follow the instruction below to view information about an application account. The following types of information can be viewed independently of each other:

- application account data (related application group, OAM properties)
- application account state
- SLA related to the application account
- application instance groups related to the application account

- logged in application groups related to the application account

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   View application instance group data

2. Double-click the **getApplicationInstanceGroup** method.
3. Enter the service provider account ID, application ID and application instance group ID.
4. Click **Invoke**.

   The group's OAM properties, if any, are displayed.

   View state

5. Double-click the **getStateForApplicationInstanceGroup** method.
6. Enter the service provider account ID, application ID and application instance group ID.
7. Click **Invoke**.

   The application instance group's current state is displayed.

   View SLA

8. Double-click the **getSLAForApplicationInstanceGroup** method.
9. Enter the service provider account ID, application ID and application instance group ID.
10. Click **Invoke**.

    The SLA (number of allowed concurrent users) is displayed.

Updating the SLA for an application instance group

Follow the instruction below to update the SLA (change the number of allowed concurrent users) for an application instance group.

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   View SLA

2. Double-click the **getSLAForApplicationInstanceGroup** method.

3. Enter the service provider account ID, application ID and application instance group ID.
4. Click **Invoke**.

   The SLA (number of allowed concurrent users) is displayed.

   Update SLA
5. Double-click the **updateApplicationInstanceGroupSLAString** method.
6. Enter the service provider account ID, application ID and application instance group ID.
7. Click **Invoke**.

   The application instance group's SLA is now updated and in use.

Logging out an application instance group

Follow the instruction below to log out all users related to the application instance group.

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   Log out application instance group
2. Double-click the **logoutApplicationInstanceGroup** method.
3. Enter the service provider account ID, application ID and application instance group ID.
4. Click **Invoke**.

   All logged in users in the application instance group are logged out.

Unlocking an application instance group

Follow the instruction below to unlock an application instance group that has been locked due to too many failed log in attempts. When unlocking an application instance group, it's state is changed to activated.

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   View current state
2. Double-click the **getStateForApplicationInstanceGroup** method.

3. Enter the service provider account ID, application ID and application instance group ID.
4. Click **Invoke**.

   The application instance group's current state is displayed.

   Unlock application instance group
5. Double-click the **unlockApplicationInstanceGroup** method.
6. Enter the service provider account ID, application ID and application instance group ID.
7. Click **Invoke**.

   The application instance group is unlocked. That is, the state is changed to activated.

Changing password for an application instance group

Follow the instruction below to change password for an application instance group.

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   Change password
2. Double-click the **setPasswordForApplicationInstanceGroup** method.
3. Enter the service provider account ID, application ID, application instance group ID and new password.
4. Click **Invoke**.

   The application instance group's password is changed.

Deactivating an application instance group

Follow the instruction below to deactivate an application instance group. That is, to temporarily stop the application instance group's traffic to/from the application.

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   View current state
2. Double-click the **getStateForApplicationInstanceGroup** method.

3. Enter the service provider account ID, application ID and application instance group ID.
4. Click **Invoke**.

   The application instance group's current state is displayed.

   Deactivate application account

5. Double-click the **deactivateApplicationInstanceGroup** method.
6. Enter the service provider account ID, application ID and application instance group ID.
7. Click **Invoke**.

   The application instance group's state is changed to deactivated.

Deleting an application instance group

Follow the instruction below to deactivate an application instance group. That is, to temporarily stop the application instance group's traffic to/from the application.

Identify the application instance group

1. See "Identifying an application instance group" on page 5-39.

   Delete application instance group

2. Double-click the **deleteApplicationInstanceGroup** method.
3. Enter the service provider account ID, application ID and application instance group ID.
4. Click **Invoke**.

   The application instance group is now deleted.

   Note: If any mailboxes, charging accounts and Parlay X settings have been created for the application instance group (see "Creating an application instance group" on page 5-30), these have to be removed separately. Refer to the OAM methods available for the associated SLEE services.

Network SLA Administration

The following sections describe how to administer network SLAs:

- "About network SLA administration" on page 6-2
- "Defining request rate warning levels" on page 6-7

About network SLA administration

A network SLA specifies how much traffic can be sent to the individual network nodes connected to WebLogic Network Gatekeeper. There are two levels of network SLAs:

- A total traffic SLA, that specifies the total amount of traffic can be sent from WebLogic Network Gatekeeper to each of the underlying network nodes. The SLA is specified in an XML SLA file.
- Service provider traffic SLAs, that specify how much traffic can be sent from each service provider within a service provider group to each of the underlying network nodes. The service provider traffic SLAs are defined on service provider group level and all service providers within a group are assigned the same SLA data. There is one XML SLA file for each service provider group.

In addition, the network SLAs can specify under which load conditions the network nodes can be used. This requires that the network nodes can report their load level to WebLogic Network Gatekeeper.

The total traffic SLA file must be updated when a new network node is connected to WebLogic Network Gatekeeper's plug-in manager. A service provider traffic SLA file must be updated if the new network node shall be accessed by any of the service providers connected to the service provider group the SLA file is valid for.

In addition, a new service provider traffic SLA file has to be created and loaded every time a new service provider group is created. If no SLA file is loaded for the service provider group, there will be no traffic limits on service provider level for the service providers in that service provider group.

If no total traffic SLA is loaded, it is not possible to send any requests at all from WebLogic Network Gatekeeper to the underlying network nodes.

For more information about the service provider administration model, see "Service Provider and Application Administration" on page 5-1.

If the service provider group and account administration is handled through the WebLogic Network Gatekeeper Partner Management Tools, the network SLA administration may be integrated through theese. This is however deployment specific.

Adding a service provider traffic SLA

Follow the instruction below to add a service provider traffic SLA. The SLA specifies the amount of traffic that can be sent from a service provider to each of the underlying network nodes.

The SLA file is created on service provider group level and will be valid for all service providers within the group.

Identify the service provider group

1. See “Identifying a service provider group” on page 5-5.

   Create SLA file

2. See “Writing Network SLA Files” on page E-1.

   Add SLA

3. Select a SLEE where the ESPA Access service is installed.
4. Double-click the **ESPA_access** service.
5. Double-click the **setServiceProviderGroupNodeSlaUrl** method.
6. Enter the service provider group ID and the URL (including file name) for the SLA file.
7. Click **Invoke**.

   The service provider traffic SLA is added and valid for all service providers within the specified service provider group.

Updating a service provider traffic SLA

Follow the instruction below to update a service provider traffic SLA.

The SLA file has to be updated when a new network node has been added to WebLogic Network Gatekeeper and the service providers in the service provider group shall access the new network node.

Also, the SLA file needs to be updated if the allowed amount of traffic to an underlying network node has been changed.

Identify the service provider group

1. See “Identifying a service provider group” on page 5-5.

   View current network SLA data

Note: It is also possible to view the original XML SLA file.

2. Select a SLEE where the ESPA Access service is installed.
3. Double-click the **ESPA_access** service.

4. Double-click the **listServiceProviderGroupNodeSla** method.

5. Enter the service provider group ID.

6. Click **Invoke**.

   The service provider traffic SLA is displayed.

   Edit SLA file

7. Edit the original XML SLA file, see “Service Provider and Application Administration” on page 5-1. Add a new network node or update data related to an existing node.

   Update SLA

8. Select a SLEE where the ESPA Access service is installed.

9. Double-click the **ESPA_access** service.

10. Double-click the **updateServiceProviderGroupNodeSlaUrl** method.

11. Enter the service provider group ID and the URL (including file name) for the edited XML SLA file.

12. Click **Invoke**.

    The service provider traffic SLA is updated and valid for all service providers within the specified service provider group.

Removing a service provider traffic SLA

Follow the instruction below to remove the traffic SLA for a service provider group. When the SLA is removed, the service providers within the to the group have free access to the network nodes as long as the total traffic does not exceed the limits specified in the WebLogic Network Gatekeeper total traffic level traffic SLA.

Identify the service provider group

1. See “Identifying a service provider group” on page 5-5.

   Delete SLA

2. Select a SLEE where the ESPA Access service is installed.

3. Double-click the **ESPA_access** service.

4. Double-click the **deleteServiceProviderGroupNodeSlaUrl** method.

5. Enter the service provider group ID.
6. Click **Invoke**.

   The service provider group's traffic SLA is deleted.

Adding the total traffic SLA

Follow the instruction below to add the total traffic SLA. The SLA specifies the total amount of traffic that can be sent from WebLogic Network Gatekeeper to each of the underlying network nodes.

Create SLA file

1. See "Service Provider and Application Administration" on page 5-1.

   Add SLA

2. Start an WebLogic Network Gatekeeper Management Tool and log in.
3. Select a SLEE where the plug-in manager service is installed.
4. Double-click the **Plugin_manager** service.
5. Double-click the **setNodeSlaUrl** method.
6. Enter the URL (including file name) for the SLA file.
7. Click **Invoke**.

   The total traffic SLA is added.

Updating the total traffic SLA

Follow the instruction below to update the total traffic SLA for the WebLogic Network Gatekeeper.

The SLA has to be updated when a new network node has been added to WebLogic Network Gatekeeper's plug-in manager.

Also, the SLA needs to be updated if the allowed total amount of traffic to an underlying node has be changed.

View current network SLA data

Note: It is also possbile to view the original XML SLA file.

1. Start WebLogic Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the plug-in manager service is installed.
3. Double-click the **Plugin_manager** service.
4. Double-click the **listNodeSla** method.
5. Click **Invoke**.

   The total traffic SLA is displayed.

   Edit SLA file

6. Edit the original XML SLA file, see "Service Provider and Application Administration" on page 5-1.

   Update SLA

7. Double-click the **setNodeSlaUrl** method.
8. Enter the URL (including file name) for the edited SLA file.
9. Click **Invoke**.

   The total traffic SLA is updated.

Removing the total traffic SLA

Follow the instruction below to remove the total network SLA.

Note: If the network SLA is removed, it is not possible for WebLogic Network Gatekeeper to access any of the underlying network nodes.

1. Start WebLogic Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the plug-in manager service is installed.
3. Double-click the **Plugin_manager** service.
4. Double-click the **deleteNodeSla** method.
5. Click **Invoke**.
6. The total traffic SLA is removed and no traffic is allowed towards the network.

Defining request rate warning levels

The request rate warning level is set to 80% of the maximum allowed request rate as default. This value is used for all service types and for both total traffic and service provider level request limits. To change the warning level for one or more service types, the individual rules used for those service types has to be edited. Follow the instruction below to change the request rate warning level for a service type.

Edit existing rule file

1. Open an existing rule file.

   The default rule files are stored in the following directory :

   `/usr/local/slee/bin/policy/rules/node`

   Any of the default rule files can be used as a template.

2. Edit the file.

   To change the warning level for the *total traffic request limit*, do the following:

   a. Search for: `if( ?globalRequestRates[i] == (int)`

   b. Change the decimal value that follows `(int)` to the new warning level.

   c. Change the percentage in the “`action`” statement following the above “`if`” statement accordingly. The percentage value is used in the alarm printout.

   To change the warning level for the *service provider traffic request limit*, do the following:

   a. Search for: `if( ?spRequestRates[i] == (int)`

   b. Change the decimal value that follows `(int)` to the new warning level.

   c. Change the percentage in the “`action`” statement following the above “`if`” statement accordingly. The percentage value is used in the alarm printout.

3. Save the rule file under a new name in the same directory as the other rule files.

   Load new rule file

4. Start an Network Gatekeeper Management Tool and log in.

5. Select a SLEE where the Policy service is installed.

6. Double-click the **Policy** service.

7. Double-click the **loadNodeRules** method.
8. Enter the URL (including file name) for the rule file and the service type it is valid for.

   The valid service types can be listed through the **getTypeList** OAM method in the **Plugin_manager** service.
9. Click **Invoke**.

   The specified request rate warning level is changed.

CHAPTER 7

OSA Gateway Connection

The following sections describe how to use the OSA Gateway Connection:

About OSA/Parlay gateway connections

The WebLogic Network Gatekeeper has to have a connection with an OSA/Parlay gateway to make it possible for applications to us network services through the OSA/Parlay SCSes in the gateway. In addition the applications using OSA/Parlay SCSes has to be individually connected to the OSA/parlay gateway, see "Connecting an application (account) to an OSA/Parlay gateway" on page 5-20.

Connecting an OSA/Parlay gateway

Follow the instruction below to connect the WebLogic Network Gatekeeper to an OSA/Parlay gateway. The following has to be provided by the OSA/Parlay operator before the task can be started:

- OSA/Parlay gateway user certificate
- Either OSA/Parlay gateway name service reference file and the name of the initial object or only name service initial reference file.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the OSA access service is installed.
3. Double-click the **OSA_access** service.

   Register OSA/Parlay gateway

4. Double-click the **addGw** method.

5. Enter the following OSA/Parlay gateway data:

Parameter	Description
name	A descriptive name to be used the identification of the OSA/Parlay gateway.
osaFwCert	The directory path (including file name) for the user certificate.
reAuthWaitTime	The time in seconds to wait before re-attempting authentication and obtaining a new manager if all connections are down
keystorePwd	The password that protects the WebLogic Network Gatekeeper's keystore

6. Click **Invoke**.

   The OSA/Parlay gateway is registered and its ID is displayed. Use the ID when setting up the connection.

   Set up connection

7. Double-click the **addConnection** method.

8. Enter the following OSA/Parlay gateway data. Note, either the nsRef and nsName parameters or the initalRef parameter only can be used.

Parameter	Description
gwID	The ID created when registering the OSA/Parlay gateway.
nsRef	The directory path (including file name) for the file containing the name service IOR. Leave blank if initialRef is specified.
nsName	The name of initial object in the name service, for example: parlay_initial. Use path syntax (for example: /parlay/fw/parlay_inital) to specify recursive naming contexts. Leave blank if initialRef is specified.
initialRef	The directory path (including file name) for the file containing the IOR to the Parlay intial object. Leave blank if nsRef and nsName is specified.

9. Click **Invoke**.

   The connection with the OSA/Parlay gateway is set up its connection ID is displayed.

Listing registered OSA/Parlay gateways

Follow the instruction below to list registered OSA/Parlay gateways IDs and descriptive names.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the OSA access service is installed.
3. Double-click the **OSA_access** service.

   List OSA/Parlay gateway

4. Double-click the **listGw** method.
5. Click **Invoke**.

   The IDs and names of the registered OSA/Parlay gateways are displayed.

Disconnecting an OSA/Parlay gateway

Follow the instruction below to disconnect an OSA/Parlay gateway and delete registration data.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the OSA access service is installed.
3. Double-click the **OSA_access** service.

   Disconnect OSA/Parlay gateway
4. Double-click the **removeConnection** method.
5. Enter the gateway ID and the connection ID:
6. Click **Invoke**.

   The OSA/Parlay gateway is disconnected.

   Remove registration
7. Double-click the **removeGw** method.
8. Enter the gateway ID.
9. Click **Invoke**.

   The OSA/Parlay gateway registration is removed.

SLEE and SLEE Service Operation

The following sections describe SLEE and SLEE service operation:

About the SLEE and SLEE services

SLEE

BEA WebLogic Network Gatekeeper is built with a modular software architecture where most functions run as services in a Service Logic Execution Environment (SLEE). When a SLEE process is started, the SLEE is put in the state SHUTDOWN, see Figure 8-1.

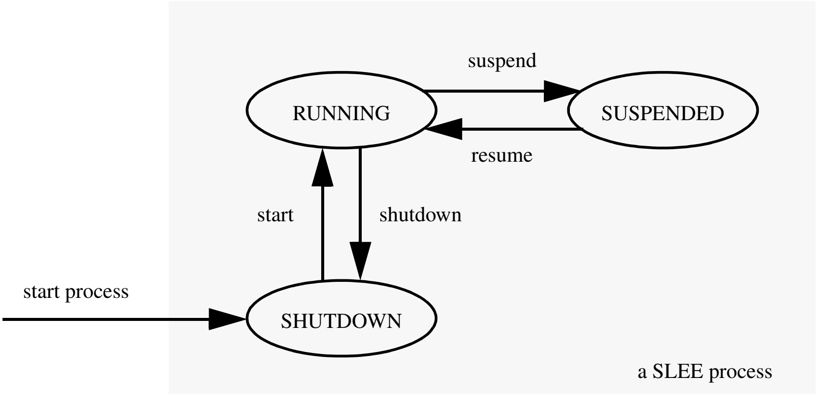


Figure 8-1 Relation between SLEE states within a SLEE process

Before the SLEE can start executing services, its state has to be changed to RUNNING. That is, to its normal executing state. When changing the state from SHUTDOWN to RUNNING, all autostarted services installed in the SLEE will be automatically started and activated.

If the SLEE state is changed from RUNNING to SHUTDOWN, all services executing in the SLEE will be stopped.

The state SUSPENDED is used when you temporarily want to stop all request sent to and from the SLEE without stopping the started or activated SLEE services.

SLEE services

All software modules installed and run in the SLEE are regarded as SLEE services. An installed SLEE service can have one of the following states (see also Figure 8-2):

- Installed

  The service software is installed in the SLEE.

- Started

  The service is started and available in the Network Gatekeeper Management Tool but cannot send and receive CORBA requests.

- Activated

  The service is activated, that is, in its normal running state where it can send and receive CORBA requests.

- Suspended

  The service is activated but cannot receive new service requests. Used for graceful service shutdown.

- Error

  The service has raised too many critical alarms and has been taken out of service by the SLEE. The allowed number of critical alarms is configured at service installation.

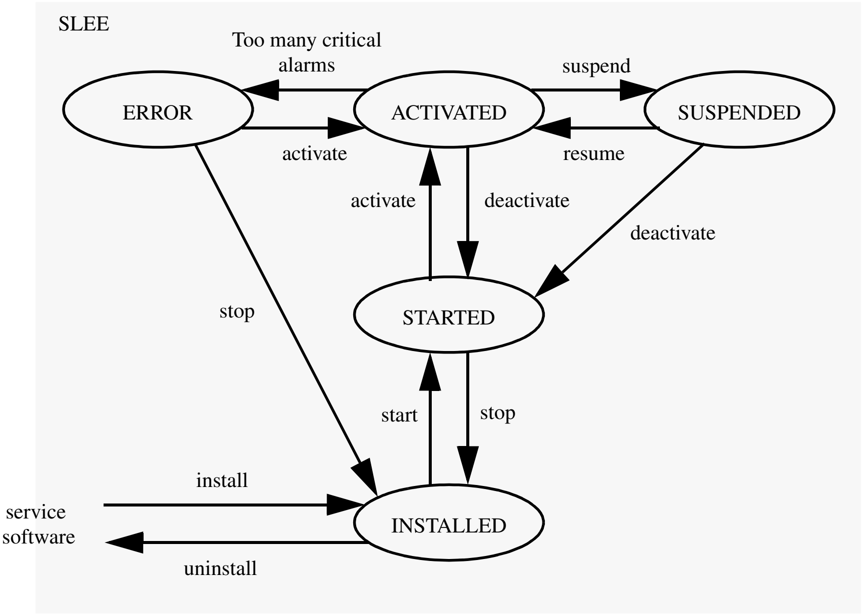


Figure 8-2 Relation between SLEE service states

In case of a SLEE restart, the services' restart order and previous operating states are retrieved from the database.

Starting a SLEE process and a SLEE agent (command window)

Follow the instruction below to start a SLEE and SLEE agent process.

1. Log in as **root** on the BEA WebLogic Network Gatekeeper server.
2. Open a command window.
3. Go to the `/usr/local/slee/bin/` directory.
4. Start the SLEE agent. Enter command:

   ```
   ./runAgent.sh&
   ```

   The SLEE agent will automatically start the SLEE process.

   In the command prompt window you can see how the SLEE agent and the SLEE processes are starting up.

   Note: Do not close the command prompt window. If you do so, the SLEE process will be terminated.

Starting a SLEE process (Network Gatekeeper Management Tool)

Follow the instruction below to start a SLEE process. To start a SLEE process through an Network Gatekeeper Management Tool, the SLEE agent process related to the SLEE must be running. That is, this instruction can only be used to start a SLEE process that has been temporary stopped through an Network Gatekeeper Management Tool as described in "Stopping a SLEE process (Network Gatekeeper Management Tool)" on page 8-6.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to work with.
3. Right-click on the selected SLEE.

   This displays a menu where you can start and stop the SLEE process and change the SLEE's state.
4. Click **Start SLEE Process** in the menu.

The icon in front of the SLEE name in the **SLEE** pane is changed to ⧅.

5. Change the SLEE state to the desired state, see “Changing SLEE state” on page 8-8.

Stopping a SLEE agent (command window)

Follow the instruction below to stop the SLEE agent, and related, processes.

Note: This instruction should only be used when stopping a SLEE process completely, for instance when performing a system upgrade. The SLEE needs to be in state SHUTDOWN to perform this operation.
To start the SLEE again, follow the instructions in “Starting a SLEE process and a SLEE agent (command window)” on page 8-5.

1. Log in as **root** on the BEA WebLogic Network Gatekeeper server.
2. Open a command window.
3. Change directory to:

```
<installation directory>/bin
```

4. Stop the processes. Enter:

```
stopAgent.sh <username> <password>
```

```
Replace <username> with a SLEE username with administrative
privileges. Replace <password> with the password.
```

Stopping a SLEE process (Network Gatekeeper Management Tool)

Follow the instruction below to stop a SLEE process.

Note: This instruction should only be used when stopping a SLEE process temporarily. If the SLEE process shall be stopped for a system upgrade, the SLEE and SLEE agent processes must be stopped, see “Stopping a SLEE agent (command window)” on page 8-6.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to work with.

3. Right-click on the selected SLEE.

   This displays a menu where you can start and stop the SLEE process and change the SLEE's state.

4. Click **StopSLEE Process** in the menu.

   The icon in front of the SLEE name in the **SLEE** pane is changed to ☒.

Viewing SLEE name

Follow the instruction below to view a SLEE's name as specified in the file `slee_properties.xml` at installation.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to view name for.
3. Double-click the **SLEE** service.
4. Double-click the **getName** method.
5. Click **Invoke**.

   The SLEE's name is displayed.

Viewing SLEE state

Follow the instruction below to view a SLEE's state. For more information about the SLEE states, see "About the SLEE and SLEE services" on page 8-3.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to view state for.
3. Double-click the **SLEE** service.
4. Double-click the **getSLEEState** method.
5. Click **Invoke**.

   The SLEE's state is displayed.

Changing SLEE state

Follow the instruction below to change a SLEE's state. For more information about the SLEE states, see "About the SLEE and SLEE services" on page 8-3.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to change state for.
3. Double-click the **SLEE** service.

   View current state

4. Double-click the **getSLEEState** method.
5. Click **Invoke**.

   The SLEE's current state is displayed.

   Set new state

6. Double-click a method according to the table below:

To change from state:	To state:	Use the following method:
SHUTDOWN	RUNNING	**start**
RUNNING	SHUTDOWN	**shutdown**
RUNNING	SUSPENDED	**suspendAccess**
SUSPENDED	RUNNING	**resumeAccess**

7. Click **Invoke**.

   The new SLEE state is displayed.

Viewing memory and disk space utilization

Follow the instruction below to view a SLEE's resource utilization.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to view resource utilization for.
3. Double-click the **SLEE** service.

4. Double-click a method according to the table below:

To view:	Use the following method:
The amount of free RAM (Mb) in the Java virtual machine the SLEE can use	**getFreeMemory**
The total amount of RAM (Mb) in the Java virtual machine where the SLEE executes	**getTotalMemory**
The available disk space (Kb) on a specific partition on the SLEE host	**getFreeDiskSpace** Use the **path** parameter to specify the partition

5. Click **Invoke**.

   The selected resource utilization data is displayed.

Viewing SLEE load and resource utilization

Follow the instruction below to view the SLEE load. It is possible to view:

- The current load
- Average load for a specified time period
- Load history for a specified time period (A list of 5 minute averages)

These load values are presented as a percentage of the maximum load.

In addition, it is possible to view a more detailed resource utilization data for the whole SLEE, the JVM and the defined load share contexts. This data includes:

- current load
- heap used
- heap total
- heap initial
- heap last GC
- And for each load share context:

- task pool size (threads)
- task pool used (threads)
- task queue size (tasks)
- task queue used (tasks)
- orb pool size (threads)
- orb pool used (threads)

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to view load for.
3. Double-click the **SLEE** service.
4. Double-click a method according to the table below:

To view:	Use the following method:
The current load.	**getLoad**
Average load.	**getAverageLoad** The time format is specified according to the system time settings. Default format is: YYYY-MM-DD hh:mm If **endTime** is left empty, the average for an hour beginning at **startTime** is displayed.
Load history	**listLoadAverages** The time format is specified according to the system time settings. Default format is: YYYY-MM-DD hh:mm If **endTime** is left empty, the average for an hour beginning at **startTime** is displayed.
Detailed SLEE load	**getLoadParameters**

5. Click **Invoke**.

   The load is displayed.

Deleting SLEE load data

Follow the instruction below to delete SLEE load data from the database. The procedure has to be performed once for each SLEE.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to delete load for.
3. Double-click the **SLEE** service.
4. Double-click the **deleteLoadAverages** method.
5. Enter end date.

   All the load data older then the entered date will be deleted. The time format is specified according to the system time settings. Default format is:
   YYYY-MM-DD hh:mm
6. Click **Invoke**.

   The load data is deleted.

Listing resource sharing contexts

Follow the instruction below to list the existing resource sharing contexts in a SLEE.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to list resource sharing contexts for.
3. Double-click the **SLEE** service.
4. Double-click the **listResourceShares** method.
5. Click **Invoke**.

   The existing resource sharing contexts are displayed.

Viewing resource utilization for a resource sharing context

Follow the instruction below to view the resource utilization for a resource sharing contexts.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to list resource sharing contexts for.

3. Double-click the **SLEE** service.

   List existing resource sharing contexts

4. Double-click the **listResourceShares** method.

5. Click **Invoke**.

   The existing resource sharing context names are displayed.

   View resource utilization

6. Double-click a method according to the table below:

To view:	Use the following method:
The SLEE task pool size.	**getResourceShareTaskPoolSize**
The number of active SLEE tasks.	**getResourceShareNoActiveTasks**
The active SLEE tasks.	**listResourceShareActiveTasks**
The SLEE task queue size.	**getResourceShareTaskQueueSize**
The number of SLEE tasks in the queue	**getResourceShareTasksInQueue**
If the SLEE task queue is stable.	**isResourceShareTaskQueueStable**
The number of active SLEE tasks.	**listNumberOfResourceShareTaskQueueSize**
The ORB thread pool size.	**getResourceShareOrbPoolSize**
The number of ORB threads used.	**getResourceShareNoCORBARequests**

7. Enter the desired resource sharing context name.

8. Click **Invoke**.

The selected resource utilization data is displayed.

Listing SLEE services in a resource sharing context

Follow the instruction below to list SLEE service in a specific resource sharing contexts. Two types of listings are possible:

- SLEE services configured to belong to a specific resource sharing context.
- Running SLEE services in a specific resource sharing context.

The difference between the two is that a SLEE service has to be started (or restarted) after it has been configured to belong to a resource sharing context to be an active part of, that is, running in the resource sharing context.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the resource sharing contexts are defined.
3. Double-click the **SLEE** service.

   List existing resource sharing contexts
4. Double-click the **listResourceShares** method.
5. Click **Invoke**.

   The existing resource sharing context names are displayed.

   List SLEE services
6. Double-click a method according to the table below:

To view:	Use the following method:
All configured SLEE service.	**listResourceShareServices**
The running SLEE service.	**listResourceShareRunningServices**

7. Enter the resource sharing context name.
8. Click **Invoke**.

   The services within the specified resource sharing contexts are displayed.

Viewing resource sharing context for a SLEE service

Follow the instruction below to view which resource sharing context a SLEE service belongs to.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the service is installed.
3. Double-click the **SLEE** service.
4. Double-click the **getServiceResourceShare** method.
5. Enter the SLEE service name.
6. Click **Invoke**.

   The resource sharing context the SLEE service belongs to is displayed.

Listing installed SLEE services

Follow the instruction below to list the SLEE services installed in a SLEE. The services can be listed on a per state basis or regardless of state.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE to list services for.
3. Double-click the **SLEE** service.
4. Double-click the **getServices** method.
5. Enter a digit according to the table below:

To list:	Enter the following digit:
All services in state UNINSTALLED	-1
All services in state INSTALLED	0
All services in state STARTED	1

To list:	Enter the following digit:
All services in state ACTIVE	2
All services in state UNKNOWN	3
All services in state SUSPENDED	4
All services in state ERROR	5

Note: You list services in a certain *state*. That is, a service in the *state* STARTED is not displayed when listing services in the *state* INSTALLED, even if a started service is, of course, installed in the SLEE.

6. Click **Invoke**.

   The names of the SLEE services fulfilling the criteria specified in the previous step are displayed.

Viewing SLEE service state

Follow the instruction below to view a specific SLEE service's state. For more information about the SLEE service states, see "About the SLEE and SLEE services" on page 8-3.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the desired service is installed.
3. Double-click the **SLEE** service.
4. Double-click the **getServiceState** method.
5. Enter the service name.

   For service names, see "Listing installed SLEE services" on page 8-14.

6. Click **Invoke**.

   The service state is now displayed.

Changing SLEE service state

Follow the instruction below to change a specific SLEE service's state. For more information about the SLEE service states, see "About the SLEE and SLEE services" on page 8-3.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the desired service is installed.

   View current state

3. Double-click the **SLEE** service.
4. Double-click the **getServiceState** method.
5. Enter the service name.

   For service names, see "Listing installed SLEE services" on page 8-14.

6. Click **Invoke**.

   The service state is now displayed.

   Set new state

7. Double-click the **SLEE_deployment** service.
8. Select one of the following methods to change the service state.

Current state:	Desired state:	Use the following method:
INSTALLED	STARTED	**start**
STARTED	INSTALLED	**stop**
STARTED	ACTIVATED	**activate**
ACTIVATED	STARTED	**deactivate**
ACTIVATED	SUSPENDED	suspend
SUSPENDED	STARTED	deactivate
SUSPENDED	ACTIVATED	resume

Note: Before going from SUSPENDED to STARTED using the **deactivate** method, the method **getServiceActivity** can be used to verify that the activity on the suspended service has ceased.

9. Enter the service name.

10. Click **Invoke**.

    The new service state is now displayed.

Viewing SLEE service version

Follow the instruction below to view a specific SLEE service's version.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the desired service is installed.
3. Double-click the **SLEE** service.
4. Double-click the **getServiceVersion** method.
5. Enter the service name.

   For service names, see "Listing installed SLEE services" on page 8-14.
6. Click **Invoke**.

   The service version is displayed.

About trace

If a SLEE service is suspected to be faulty, the trace service can be used to locate the fault in the code.

The trace information is written to file. There can be several trace files stored for one SLEE service. If the trace is currently active for the SLEE service, the active trace file is named `<service_name>.log` where `<service_name>` is the name of the SLEE service. When a trace file has reached its maximum size the file is given a time stamp telling when it was closed for writing. Closed trace files have the following format `<service_name>_YYYY-MM-DD_hh-mm-ss.log`.

The different types of trace information (trace groups) that it is possible to trace on are explained in Table 8-1 below.

Table 8-1 Trace Groups

Trace Group	Value	Description
METHOD IN	1	Writes trace information at entry of a method.
METHOD OUT	2	Writes trace information at exit of a method.
USER DEF 1	4	Writes trace information of type 1 as defined for the service.
USER DEF 2	8	Writes trace information of type 2 as defined for the service.
USER DEF 3	16	Writes trace information of type 3 as defined for the service.
USER DEF 4	32	Writes trace information of type 4 as defined for the service.
USER DEF 5	64	Writes trace information of type 5 as defined for the service.
USER DEF 6	128	Writes trace information of type 6 as defined for the service.
RAW DATA	256	Writes trace information in the form of a byte array as defined for the service.
EXCEPTIONS	512	Writes trace information at exceptions.
TRAFFIC FLOW	1024	Writes trace information when traffic related requests (both application and network initiated) are received by and sent from the service.

The usage of the USER DEF trace groups is different in different SLEE services.

The trace for a SLEE service is specified using the **setTraceFilterGroupsForService** method. The number to enter is the sum of the values representing the trace groups you want to use, see Table 8-1 on page 18. For example, if you want to use METHOD OUT (2), USER DEF 4 (32), and RAW DATA (256) you have to enter the number 290 (2+32+256=290).

Note: For performance reasons is it recommended to activate trace only for individual services and not for all services in the SLEE. Setting trace filter groups for a service to 0 does not deactivate trace for that service. Use the methods **activateTraceForService** and **deactivateTraceForService** to activate and deactivate trace for individual services. See instructions below.

Enabling trace for a SLEE

Follow the instruction below to enable trace for a SLEE. That is, make it possible for the SLEE services to write trace information to the trace file. Only SLEE services that have the trace activated will generate trace information.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE you want to enable trace for.
3. Double-click the **SLEE_trace** service.
4. Double-click the **enableTracing** method.
5. Click **Invoke**.

   Trace is enabled for the SLEE.

Specifying type of trace for a SLEE service

Follow the instruction to specify which type of trace information that shall be written to the trace file.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the desired service is installed.
3. Double-click the **SLEE** service.
4. Double-click the **setTraceFilterGroupsForService** method.
5. Enter the service name and the number representing the desired trace groups.

   For service names, see “Listing installed SLEE services” on page 8-14 and for trace groups and how to calculate the number representing the desired trace groups, see “About trace” on page 8-17.
6. Click **Invoke**.

The type of trace information to be written to the trace file is specified. Note that trace have to be activated for the service before any trace information is actually written to the trace file.

Activating trace a SLEE service

Follow the instruction below to activate trace for a single SLEE service. That is, all SLEE service will generate trace information. If trace is enabled for the SLEE, this information will also be written to file.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the desired service is installed.
3. Double-click the **SLEE** service.
4. Double-click the **activateTraceForService** method.
5. Enter the service name.

   For service names, see "Listing installed SLEE services" on page 8-14.
6. Click **Invoke**.

   Trace is activated for the specified SLEE service.

Activating trace for all services in SLEE

Follow the instruction below to activate trace for all services in a SLEE. That is, all SLEE services will generate trace information. If trace is enabled for the SLEE, this information will also be written to file.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE you want to activate trace for.
3. Double-click the **SLEE** service.
4. Double-click the **activateTraceForAllService** method.
5. Click **Invoke**.

   Trace is activated for all services in the SLEE.

Deactivating trace for a SLEE service

Follow the instruction below to deactivate trace for a single SLEE service. That is, the SLEE service will stop generating trace information.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE where the desired service is installed.
3. Double-click the **SLEE** service.
4. Double-click the **deactivateTraceForService** method.
5. Enter the service name.

   For service names, see "Listing installed SLEE services" on page 8-14.
6. Click **Invoke**.

   Trace is deactivated for all services in the SLEE.

Deactivating trace for all services in SLEE

Follow the instruction below to deactivate trace for all services in a SLEE. That is, all SLEE service in the SLEE will stop generating trace information.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE you want to deactivate trace for.
3. Double-click the **SLEE** service.
4. Double-click the **deactivateTraceForAllService** method.
5. Click **Invoke**.

   Trace is deactivated for all services in the SLEE.

Disabling trace for a SLEE

Follow the instruction below to disable trace for a SLEE. That is, SLEE services will not be able to write trace information to file.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE you want to disable trace for.

3. Double-click the **SLEE_trace** service.
4. Double-click the **disableTracing** method.
5. Click **Invoke**.

   Trace is disabled for the SLEE.

Upgrading a SLEE service

How to upgrade a SLEE service is dependant on the service and service version you upgrade to. Specific upgrading instructions are provided with new service versions.

User Administration

The following sections describe how to administer users:

About user administration

All users working with SLEE and SLEE service OAM have to be registered. Registration can be done on different levels:

- Read only
- Standard read and write
- Administrator

The level decides which administrative methods in the individual SLEE services are available for the user.

To simplify the administration of the users, service groups can be defined. These service groups consists of a number of related SLEE services. The users are then connected to the service groups. See Figure 9-1, "Users, service groups and SLEE services," on page 9-2.

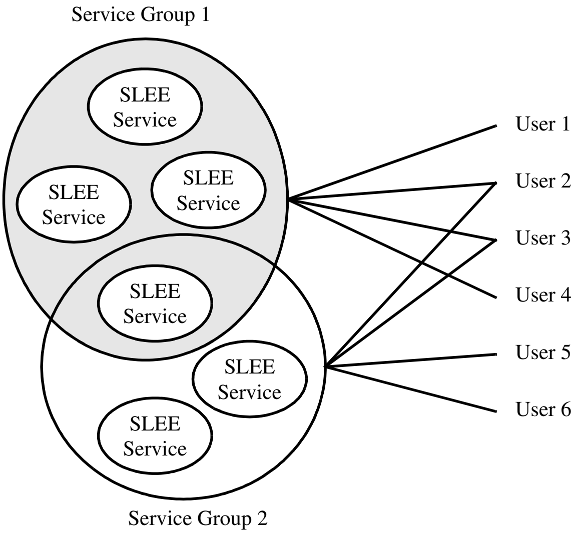


Figure 9-1 Users, service groups and SLEE services

A user can be connected to more than one service group and a SLEE service can be a member of more than one service group.

Creating a service group

Follow the instruction below to create a service group for administrative users.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **createServiceGroup** method.
5. Enter a service group name and a service group description.
6. Click **Invoke**.

   The service group is created. To add services, see "Adding a service to a service group" on page 9-3.

Adding a service to a service group

Follow the instruction below add a service to user group.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.

   List current services

4. Double-click the **listServicesInGroup** method.
5. Enter the service group name.
6. Click **Invoke**.

   The services in the specified group are displayed.

   Add new service

7. Double-click the **addServicesToGroup** method.
8. Enter the service name and service group name.

   Use a service name as displayed in the Network Gatekeeper Management Tool's **Services** pane.

9. Click **Invoke**.

   The service is added to the specified group.

Creating a user

Follow the instruction below to create an administrative user. The new user is assigned a user level which determines the types of OAM methods the user is allowed to perform.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **addUser** method.
5. Enter a user name, password and the user level. For the user level, enter a digit according to the below table:

If the user should be a:	Enter the following digit:
Read only user	1
Standard read/write user	2
Administrator user	3

6. Click **Invoke**.

   The new user is created. Before the user can start working with service administration, the user must be added to a service group, see "Adding a user to service group" on page 9-4.

Adding a user to service group

Follow the instruction below to add an administrative user to an already existing service group. A user can be added to several service groups.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.

   List available service groups

4. Double-click the **listServiceGroups** method.
5. Click **Invoke**.

   The available service group are displayed.

   Add user to service group
6. Double-click the **addUserToGroup** method.
7. Enter the service group and user name.
8. Click **Invoke**.

   The user is added to the service group.

Listing users

Follow the instruction below to list all administrative users with a specific user level.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **listUsers** method.
5. Click **Invoke**.

   The users are now displayed.

Changing password for a user

Follow the instruction below to list all administrative users with a specific user level.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **changeUserPassword** method.
5. Enter the user name, old and new password.
6. Click **Invoke**.

The password is changed.

Viewing services for a user

Follow the instruction below to list the services a specific user has access to.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.

   List service groups for user
4. Double-click the **listGroupsForUser** method.
5. Enter the user name.
6. Click **Invoke**.

   The user's service groups are displayed.

   List services in service group
7. Double-click the **listServicesInGroup** method.
8. Enter the service group name.
9. Click **Invoke**.

   The services in the specified group are displayed.
10. Repeat Steps 7. to 9. for all service groups the user belongs to.

Removing a user from a service group

Follow the instruction below to remove an administrative user from a service group.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.

   List service groups for user
4. Double-click the **listGroupsForUser** method.

5. Enter the user name.
6. Click **Invoke**.

   The user's service groups are displayed.

   Remove user from service group
7. Double-click the **removeUserFromGroup** method.
8. Enter the service group and user name.
9. Click **Invoke**.

   The user is removed from the specified service group.

Deleting a user

Follow the instruction below to delete an administrative user.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **deleteUser** method.
5. Enter the user name.
6. Click **Invoke**.

   The user is now deleted.

Viewing users in a service group

Follow the instruction below to list all administrative users in a service group.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **listUsersInGroup** method.
5. Enter the service group name.

6. Click **Invoke**.

   The users in the specified group are displayed.

Viewing services in a service group

Follow the instruction below to view all services in a service group.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.
4. Double-click the **listServicesInGroup** method.
5. Enter the service group name.
6. Click **Invoke**.

   The services in the specified group are displayed.

Removing a service from a service group

Follow the instruction below to remove a service from a service group.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.

   List current services

4. Double-click the **listServicesInGroup** method.
5. Enter the service group name.
6. Click **Invoke**.

   The services in the specified group are displayed.

   Remove service

7. Double-click the **removeServicesFromGroup** method.
8. Enter the service name and service group name.

9. Click **Invoke**.

   The new service is removed from the specified group.

Deleting a service group

Follow the instruction below to delete a service group.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE** service.

   List current groups

4. Double-click the **listServicesGroups** method.
5. Click **Invoke**.

   The services in the specified group are displayed.

   Remove group

6. Double-click the **deleteServiceGroup** method.
7. Enter the service group name.
8. Click **Invoke**.

   The service group is deleted.

Statistics Handling

The following sections describe how to work with WEbLogic Network Gatekeeper statistics:

About statistics handling

The statistics functions measures the usage of BEA WebLogic Network Gatekeeper and the network service provided by BEA WebLogic Network Gatekeeper. The usage is measured in the number of transactions handled by each service.

Statistics reports can be generated for the whole system or for individual SLEEs and/or network services. Also, the desired time period can be specified.

A pre-defined report type is the weekly report. It shows the total BEA WebLogic Network Gatekeeper usage hour by hour during a specified week. The weekly report also shows total usage for each day and the average transaction rate (transactions/second (tps)) during the busy hour of each day. A busy hour is defined as the 60 minutes during which the largest number of transactions are handled. That is, any 60 minutes (5 minute intervals are used) can be the identified as the busy hour.

Viewing statistics - system view

Following the instruction below to display statistics data in the Network Gatekeeper Management Tool. Two different report types are possible:

- Customized statistics reports where it is possible to specify SLEE, statistics type and the time period during which the statistics was generated.
- Complete system statistics for the last minute(s).

Procedure:

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE in the **SLEEs** pane.
3. Double-click the **SLEE_statistics** service in the **Services** pane.
4. To create and view a customized statistics report, double-click the **getStatistics** method and continue with Step 5..

   To view the complete system statistics for the last minute(s), double-click the **getSystemStatistics** method and enter the number of minutes in the **minutes** field. Complete the task by clicking **Invoke**.

5. Specify the one or all SLEEs using the **sleeName** field. See table below:

To view statistics data for...	Enter:
...one SLEE.	The SLEE name as specified at BEA WebLogic Network Gatekeeper installation. For information on how to display a SLEE's SLEE name, see "Viewing SLEE name" on page 8-7.
...all SLEEs	Leave field empty.

6. Specify one or all statistics types using the **statisticsType** field. See table below:

To view statistics data for...	Enter:
...a specific statistics type.	The statistics type identifier. Available statistics types can be listed using the **listStatisticsTypes** method.
...all statistics types.	`-1` (including the dash)

7. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Displays statistics data generated...
Date (In format: YYYY-MM-DD hh:mm)	Date	...within the specified time period.
Date		...after the specified from date.
	Date	...before the specified to data.
		....until now.

8. Click **Invoke**.

   The specified statistics is now displayed in the **Messages** pane.

Viewing statistics - service provider and application view

Following the instruction below to display service provider or application statistics data in the Network Gatekeeper Management Tool.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE in the **SLEEs** pane.
3. Double-click the **SLEE_statistics** service in the **Services** pane.
4. Double-click the **getStatisticsAppID** method.
5. Specify the one or all SLEEs using the **sleeName** field. See table below:

To view statistics data for...	Enter:
...all SLEEs. (the whole system)	Leave field empty.
...a specific SLEE. (only application statistics generate by the specified SLEE will be displayed)	The SLEE name as specified at BEA WebLogic Network Gatekeeper installation. For information on how to display a SLEE's SLEE name, see "Viewing SLEE name" on page 8-7.

6. Specify one or all statistics types using the **statisticsType** field. See table below:

To view statistics data for...	Enter:
...a specific statistics type.	The statistics type identifier. Available statistics types can be listed using the **listStatisticsTypes** method.
...all statistics types.	`-1` (including the dash)

7. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Displays statistics data generated...
Date (In format: YYYY-MM-DD hh:mm)	Date	...within the specified time period.
Date		...after the specified from date.
	Date	...before the specified to data.
		....until now.

8. Enter the Service Provider ID in the **entOpID** field.
9. Enter the Application ID in the **clientAppID** field.

   Use an empty string to get aggregated statistics for all applications belonging to the service provider.
10. Click **Invoke**.

    The specified statistics is now displayed in the **Messages** pane.

Printing statistics to file

Follow the instruction below to print a customized statistics data report to file.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_statistics** service.
4. Double-click the **saveStatisticsToFile** method.

5. Specify the one or all SLEEs using the **sleeName** field. See table below:

To print statistics data for...	Enter:
...one SLEE.	The SLEE name as specified at BEA WebLogic Network Gatekeeper installation. For information on how to display a SLEE's SLEE name, see "Viewing SLEE name" on page 8-7.
...all SLEEs	Leave field empty.

6. Specify a file name with or without a path in the **fileName** field.

   If no path is specified, the file is stored in the current SLEE's working directory.

7. Specify one or all statistics types using the **statisticsType** field. See table below:

To print statistics data for...	Enter:
...a specific statistics type.	The statistics type identifier. Available statistics types can be listed using the **listStatisticsTypes** method.
...all statistics types.	`-1` (including the dash)

8. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Prints statistics data generated...
Date (In format: YYYY-MM-DD hh:mm)	Date	...within the specified time period.
Date		...after the specified from date.
	Date	...before the specified to data.
		....until now.

9. Click **Invoke**.

   The specified statistics is now printed to file.

Creating a weekly system statistics report

Follow the instruction below to create a weekly system statistics report. The report shows:

- the total number of transactions during the specified week
- the number of transactions during each hour of the days in the week
- the number of transactions during each day of the week
- the transaction rate (transactions/second (tps)) during the busy hour of each day

Procedure:

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_statistics** service.
4. Double-click the **createWeeklyReport** method.
5. Specify the first day in the week using the **startDate** field.

   Use format YYYY-MM-DD.
6. Specify a file name with or without a path in the **fileName** field.

   If no path is specified, the file is stored in the current SLEE's working directory.
7. Click **Invoke**.

   The specified weekly report is now printed to file.

Deleting statistics data from the database

Follow the instruction below to delete statistics data from the database.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_statistics** service.
4. Double-click the **deleteStatistics** method.

5. Specify the one or all SLEEs using the **sleeName** field. See table below:

To delete statistics data for…	Enter:
...one SLEE.	The SLEE name as specified at BEA WebLogic Network Gatekeeper installation. For information on how to display a SLEE’s SLEE name, see “Viewing SLEE name” on page 8-7.
...all SLEEs	Leave field empty.

6. Specify one or all statistics types using the **statisticsType** field. See table below:

To delete statistics data for…	Enter:
...a specific statistics type.	The statistics type identifier. Available statistics types can be listed using the **listStatisticsTypes** method.
...all statistics types.	`-1` (including the dash)

7. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Deletes statistics data generated…
Date (In format: YYYY-MM-DD hh:mm)	Date	...within the specified time period.
Date		...after the specified from date.
	Date	...before the specified to data.
		....until now.

8. Click **Invoke**.

   The specified statistics is now deleted from the database.

Charging Data Export

The following sections describe how to export charging data:

About charging data export

Charging data can be manually exported from the database to a file, or export can be handled automatically through running a scheduled script, or through different levels of integration with billing systems. For more information about billing system integration, see Product Description - BEA WebLogic Network Gatekeeper.

The following instructions describe how export charging data manually or by using a script.

Exporting charging data (manually)

Follow the instruction below to export charging data to a file. When exporting the data from the database, you will also remove the data from the database. The task also includes checking the available disk space. A charging data table with 1.000.000 rows needs approximately 120 MB of free disk space.

Check number of database rows

1. On one of the computers where the database executes, open a command window and go to the `/usr/local/mysql/bin` directory.
2. Start MySQL command mode. Enter command:

   ```
   mysql
   ```

   This changes the prompt to `mysql>` and makes it possible to send SQL queries to the database.
3. Enter the following query:

   ```
   select count(*) from ic_slee_charging;
   ```

   The number of rows is displayed.
4. Exit MySQL command mode. Enter command:

   ```
   exit
   ```

   Verify disk space
5. Verify disk space. Enter command:

   ```
   df -k
   ```

   The available disk space (in kB) is displayed.

Note: You have to verify that there is enough disk space available on the server before exporting the charging data. A charging data table with 1.000.000 rows needs approximately 120 MB of free disk space.

Export charging data

6. Start an Network Gatekeeper Management Tool and log in.
7. Select any SLEE in the **SLEEs** pane.
8. Double-click the **SLEE_charging** service in the **Services** pane.
9. Double-click the **dumpChargingData** method.
10. Enter parameter data in the **Invoke Method** window according to the table below:

Parameter	Description
dumpfileName	The file name and path of the file that the charging data will be exported to. The file is automatically created but the directory must exist. The file is saved on a disk connected to the host where the SLEE is running. If a relative path is used, it is relative to the `bin` directory.

11. Click **Invoke**.

    The charging data is now exported to the specified file.

Exporting charging data (script)

When using the script, automatic exports of charging data can be triggered through a standard system tool such as cron.

Note: The script must not execute simultaneously on two servers. If executed simultaneously, charging data may be lost.

If the size of the charging data file is very large, a CORBA time-out error may occur in the script. The charging data will be exported to file even if this error occurs.

Before scheduling the script, it must be verified that there will be enough disk space available on the server. A charging data table with 1.000.000 rows needs approximately 120 MB of free disk space.

The script is named `db_exportCharging.sh` and located in `/usr/local/slee/bin/`.

The script takes the following arguments:

Argument	Description
`<OAM user>`	The administrator's OAM user name
`<OAM password>`	The corresponding password
`<dump file name>`	Name and location of the file to dump the charging data to.

If there already is a file with the given name, the script will terminate without exporting the charging data.

Example:

```
db_exportCharging.sh myUsername myPassword /tmp/chargingdata.txt
```

```
db_exportCharging.bat myUsername myPassword c:\tmp\
chargingdata.txt
```

Alarm and Event Administration

The following sections describe how to administer alarms and events:

About alarm and event administration

Alarm and event administration is about reconfiguring the severity level on individual alarms, viewing the alarm list and event log, and deleting old alarm and event entries from the database.

Reconfiguring alarm serverity level

Follow the instruction below to reconfigure an alarm's severity level.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_alarm** service.

   Check if already reconfigured

4. Double-click the **getReconfiguredAlarmSeverity** method.
5. Enter the alarm identifier.
6. Click **Invoke**.

   The reconfigured serverity level is displayed. If `-1` is displayed, the severity level is not reconfigured.

   Change alarm severity level

7. Double-click the **setReconfiguredAlarmSeverity** method.
8. Enter the alarm identifier and the new severity level.
9. Click **Invoke**.

   The serverity level for the specified alarm is changed.

Listing alarms with reconfigured serverity levels

Follow the instruction below to list all alarms with a reconfigured alarm severity level. The alarm identifiers and the reconfigured severity levels are displayed.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_alarm** service.

4. Double-click the **listReconfiguredAlarmSeverities** method.
5. Click **Invoke**.

   All alarms with reconfigured serverity levels are displayed.

Removing alarm serverity level reconfiguration for an alarm

Follow the instruction below to remove the reconfigured severity level for an alarm and restore the alarm's default serverity level.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_alarm** service.
4. Double-click the **removeReconfiguredAlarmSeverity** method.
5. Enter the alarm identifier.
6. Click **Invoke**.

   The alarm's default serverity level is restored.

Viewing the alarm list

Follow the instruction below to view the alarm list.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_alarm** service.
4. Double-click the **listAlarms** method.

5. Specify one or all SLEE services and one or all severity levels using the **serviceName** and **serverity** fields. See table below:

Parameter	Description
serviceName	Enter a service name if you want alarms raised by a specific SLEE service. Leave empty if you want alarms for all SLEE services
severity	Enter the severity level you are interested in: 0 - all levels 1 - warning 2 - minor 3 - major 4 - critical

6. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Lists all alarms...
Date (In format: YYYY-MM-DD hh:mm)	Date	...raised within the specified time period.
Date		...raised after the specified from date.
	Date	...raised before the specified to data.
		....raised.

7. Specify a certain alarm type or all alarm types using the **identifier** field. See table below:

To view:	Enter:
All alarm types	0 (zero)
A certain alarm type	The alarm type number

8. Click **Invoke**.

The specified alarms are displayed.

Deleting alarm entries from the database

Follow the instruction below to delete alarm list entries from the database.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE in the **SLEEs** pane.
3. Double-click the **SLEE_alarm** service.
4. Double-click the **deleteAlarms** method.
5. Specify one or all SLEE services and one or all severity levels using the **serviceName** and **serverity** fields. See table below:

Parameter	Description
serviceName	Enter a service name if you want alarms raised by a specific SLEE service. Leave empty if you want alarms for all SLEE services
severity	Enter the severity level you are interested in: 0 - all levels 1 - warning 2 - minor 3 - major 4 - critical

6. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Deletes all alarms...
Date (In format: YYYY-MM-DD hh:mm)	Date	...raised within the specified time period.
Date		...raised after the specified from date.
	Date	...raised before the specified to data.
		....raised.

7. Specify a certain alarm type or all alarm types using the **identifier** field. See table below:

To delete:	Enter:
All alarm types	0 (zero)
A certain alarm type	The alarm type number

8. Click **Invoke**.

   The specified alarms are now deleted from the database.

Viewing the event log

Follow the instruction below to view the event log.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_event** service.
4. Double-click the **listEvents** method.

5. Specify one or all SLEE services and one or all importance levels using the **serviceName** and **level** fields. See table below:

Parameter	Description
serviceName	Enter a service name if you want events raised by a specific SLEE service. Leave empty if you want alarms for all SLEE services
level	Enter the importance level you are interested in: 0 - all levels 1 - low 2 - medium 3 - high

6. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Lists all events...
Date (In format: YYYY-MM-DD hh:mm)	Date	...recorded within the specified time period.
Date		...recorded after the specified from date.
	Date	...recorded before the specified to data.
		....recorded.

7. Specify a certain event type or all event types using the **identifier** field. See table below:

To view:	Enter:
All event types	0 (zero)
A certain event type	The event type number

8. Click **Invoke**.

   The specified events are displayed.

Deleting event entries from the database

Follow the instruction below to delete event log entries from the database.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_event** service.
4. Double-click the **deleteEvents** method.
5. Specify one or all SLEE services and one or all importance levels using the **serviceName** and **level** fields. See table below:

Parameter	Description
serviceName	Enter a service name if you want events raised by a specific SLEE service. Leave empty if you want alarms for all SLEE services
level	Enter the importance level you are interested in: 0 - all levels 1 - low 2 - medium 3 - high

6. Specify a time period using the **fromDate** and **toDate** fields. See table below:

fromDate	toDate	Deletes all events...
Date (In format: YYYY-MM-DD hh:mm)	Date	...recorded within the specified time period.
Date		...recorded after the specified from date.
	Date	...recorded before the specified to data.
		....recorded.

7. Specify a certain event type or all event types using the **identifier** field. See table below:

To delete:	Enter:
All event types	0 (zero)
A certain event type	The event type number

8. Click **Invoke**.

   The specified events are now deleted.

Adding an alarm listener

Follow the instruction below to add an alarm listener. Applications acting as alarm listeners must be re-registered if they are restarted.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_alarm** service.
4. Double-click the **addAlarmListener** method.
5. Enter the following data:

Parameter	Description
listenerIOR	The stringified IOR to an object implementing the alarm listener interface.
registerInAllInstances	If set to TRUE the listener will be registered with all alarm service instances in the system. If set to FALSE the alarm listener will only be registered with this instance. That is, only alarms raised by services in this SLEE will be provided.

6. Click **Invoke**.

   The specified alarm listener is now registered.

Removing an alarm listener

Follow the instruction below to remove an alarm listener.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_alarm** service.
4. Double-click the **removeAlarmListener** method.
5. Enter the following data:

Parameter	Description
listenerIOR	The stringified IOR to an object implementing the alarm listener interface.
removeFromAllInstances	If set to TRUE the listener will be removed from all alarm service instances in the system. If set to FALSE the alarm listener will only be removed from this instance.

6. Click **Invoke**.

   The specified alarm listener is now removed.

Adding an event listener

Follow the instruction below to add an event listener. Applications acting as event listeners must be re-registered if they are restarted.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_event** service.
4. Double-click the **addEventListener** method.

5. Enter the following data:

Parameter	Description
listenerIOR	The stringified IOR to an object implementing the event listener interface.
registerInAllInstances	If set to TRUE the listener will be registered with all event service instances in the system. If set to FALSE the event listener will only be registered with this instance. That is, only event raised by services in this SLEE will be provided.

6. Click **Invoke**.

   The specified event listener is now registered.

Removing an event listener

Follow the instruction below to remove an event listener.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_event** service.
4. Double-click the **removeEventListener** method.
5. Enter the following data:

Parameter	Description
listenerIOR	The stringified IOR to an object implementing the event listener interface.
removeFromAllInstances	If set to TRUE the listener will be removed from all event service instances in the system. If set to FALSE the event listener will only be removed from this instance.

6. Click **Invoke**.

The specified event listener is now removed.

CHAPTER 13

Mailbox Administration

The following sections describe how to administer mailboxes:

About Mailbox administration

All messages arriving to BEA WebLogic Network Gatekeeper are stored in a mailbox’s inbox before retrieved by the application owning the mailbox. An application can have one or more mailboxes. The application can subscribe to get a notification each time a message arrives in one of its mailboxes. To make this work, one or more mailboxes have to be created for each application using the messaging service. The subscription of notifications is handled by the application.

Mailbox translation

In addition, destination address short codes and message prefixes can be connected to a mailbox. The combination of a mailbox address, destination address short code and message prefix is called a mailbox translation.

A destination address short code is a number that is used by the end user instead of the real mailbox address. The same destination address short code can be used for several mailboxes if it is combined with a message prefix. The message prefix is a string entered by the end user as the first part of the message.

For example, a service provider can have a destination address short code that is used to access all the service provider’s messaging based applications. For example 12345. The messages are distributed among the service provider’s mailboxes through the use of message prefixes. In this case, each application has its own mailbox. Let’s say that the service provider has two applications aimed for a radio show, one for greetings and one for requesting songs. The message prefix for to use can be defined as GREET and SONG.

That is, if an end user wants to request a song, he or she enters 12345 as destination address and starts the actual message with SONG.

In addition, if the service provider wants a general mailbox that is not connected to a specific task, it is possible to define a default mailbox using the same destination address short code (12345). When specifying a default mailbox, no message prefix is specified. This means that all messages sent to 12345 that does not start with GREET or SONG is delivered to the default mailbox.

Creating mailboxes

Follow the instruction below to create one or more mailboxes for an application account.

Note: The number of mailboxes created on BEA WebLogic Network Gatekeeper may become very large and thereby may limit the searching possibilities. Therefore it is recommended to keep track of which mailbox address ranges and mailbox passwords are used for each application in a separate file, for example an Excel file.

1. Identify a free address range to be used for the mailboxes. See the file mentioned in the note above.
2. Start an Network Gatekeeper Management Tool and log in.
3. Select a SLEE where the ESPA messaging service is installed.
4. Double-click the **ESPA_messaging** service.
5. Verify that the address range is free, double-click the **listMailboxes** method.
6. Enter the first and the last address in the **fromAddress** and **toAddress** fields.
7. Click the **Invoke** button.

   If the address range is free, no mailboxes will be displayed.
8. Double-click the **createMailboxRange** method.

   If only one mailbox should be created, use the **createMailbox** method instead.
9. Enter the following mailbox data.

Parameter	Description
startAddr	The first address in a range of free internal mailbox addresses in BEA WebLogic Network Gatekeeper. That is, you do not have to enter the service centre address part of the mailbox address. Integer (leading zeroes might have to be added to the internal mailbox address. This depends on the address format used).
endAddr	The last address in a range of free internal mailbox addresses. Must be greater than the address in startAddr.
applicationID	The application account ID of the application using the mailbox.
serviceProviderID	The service provider account ID.
pwd	A password to be used by the application when accessing the mailboxes.

10. Click **Invoke**.

    The mailboxes are now created.

11. Distribute the mailbox addresses and password to the service provider.

Deleting mailboxes by address

Follow the instruction below to delete one or more mailboxes based on address. Mailboxes can be deleted for individual addresses or by address range.

1. Identify the mailbox address or address range in the separate file created to keep track of the used mailbox addresses.
2. Start an Network Gatekeeper Management Tool and log in.
3. Select a SLEE where the ESPA messaging service is installed.
4. Double-click the **ESPA_messaging** service.
5. Verify that the address or address range you want to delete exists and that the desired service provider is the owner of all mailboxes to delete. Double-click the **listMailboxes** method.
6. Enter the first and the last address in the **fromAddress** and **toAddress** fields.
7. Click the **Invoke** button.

   Verify the addresses in the displayed address range.

8. Double-click the **removeMailboxRange** method.

   If only one mailbox shall be deleted, use the **removeMailbox** method instead.

9. Enter the first address and the last address in the range in the **startAddr** and **endAddr** fields.

   If only one mailbox shall be deleted, its address is entered in the **addr** field.

10. Click **Invoke**.

    The mailbox(es) are now deleted.

Deleting mailboxes by owner (application)

Follow the instruction below to delete all mailboxes owned by a specific application.

1. Identify the mailbox address or addresses in the separate file created to keep track of the used mailbox addresses.
2. Start an Network Gatekeeper Management Tool and log in.
3. Select a SLEE where the ESPA messaging service is installed.
4. Double-click the **ESPA_messaging** service.
5. Verify that the address or address range you want to delete. Double-click the **listMailboxesByOwner** method.
6. Enter the application account ID and service provider account ID in the **applicationId** and **serviceProviderId** fields.
7. Click the **Invoke** button.

   Verify the addresses.
8. Double-click the **removeMailboxByOwner** method.
9. Enter the application account ID and service provider account ID in the **applicationId** and **serviceProviderId** fields.
10. Click **Invoke**.

    The application's mailbox(es) are now deleted.

Adding a message translation

Follow the instruction below to specify a destination address short code and message prefix for a mailbox.

Note: The routing for the destination address short code towards BEA WebLogic Network Gatekeeper must be defined in the network. This is network specific and not covered in this User's Guide.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA messaging service is installed.
3. Double-click the **ESPA_messaging** service.

   Verify mailbox
4. Verify the mailbox address you want to add the message translation for. Double-click the **listMailboxes** method.

5. Enter the mailbox address in the **fromAddress** and **toAddress** fields.
6. Click the **Invoke** button.

   Verify the displayed address.

   List current translations
7. List the current translations. Double-click the **listMailboxTranslationsForAddress** method.
8. Enter the mailbox address.
9. Click the **Invoke** button.

   The current translation are displayed.

   Add translation
10. Double-click the **addMailboxTranslation** method.
11. Enter the following mailbox data.

Parameter	Description
destAddr	The destination address short code to be used instead of the real mailbox address.
msgPrefix	The keyword to be entered in the beginning of the message. The message prefix is case sensitive. If left empty, this mailbox will be the default mailbox for the destination address short code. That is, it will be used for messages that does not start with a valid message prefix.
mailbox	The mailbox address as verified above.

12. Click the **Invoke** button.

    The message translation is added.

Deleting a message translation

Follow the instruction below to delete a message translation for a mailbox.

1. Start an Network Gatekeeper Management Tool and log in.

2. Select a SLEE where the ESPA messaging service is installed.
3. Double-click the **ESPA_messaging** service.

   List current translations
4. List the current translations. Double-click the **listMailboxTranslationsForAddress** method.
5. Enter the mailbox address.
6. Click the **Invoke** button.

   The current translation are displayed.

   Delete translation
7. Double-click the **deleteMailboxTranslation** method.
8. Enter the following translation data.

Parameter	Description
destAddr	The destination address short code used instead of the real mailbox address.
msgPrefix	The keyword to be entered in the beginning of the message. The message prefix is case sensitive. If left empty, all message translations related to the destination address short code will be deleted.

9. Click the **Invoke** button.

   The message translation is deleted.

   Note: The actual mailboxes have to be deleted separately, see "Deleting mailboxes by address" on page 13-4 or "Deleting mailboxes by owner (application)" on page 13-4.

Setting maximum message burst size

Follow the instruction below to define the maximum number of notifications on new unread messages that shall be distributed to an application in one burst. The reason for defining this is to prevent applications from being overloaded with notifications on new messages. This setting applies to all mailboxes in the WebLogic Network Gatekeeper.

1. Start an Network Gatekeeper Management Tool and log in.

2. Select a SLEE where the ESPA messaging service is installed.
3. Double-click the **ESPA_messaging** service.
4. Double-click the **setSelectUnreadMessagesSqlSize** method.
5. Enter the maximum number of messages to be distributed in one burst in the **messages** field.
6. Click the **Invoke** button.

Routing Administration

The following sections describe how to administer the routing function:

About routing

The routing function in BEA WebLogic Network Gatekeeper allows for routing service request from the service capability modules to specific network and SCS plug-ins. See¨Figure 14-1, “Routing between service capability modules and network plug-ins,” on page 14-2.

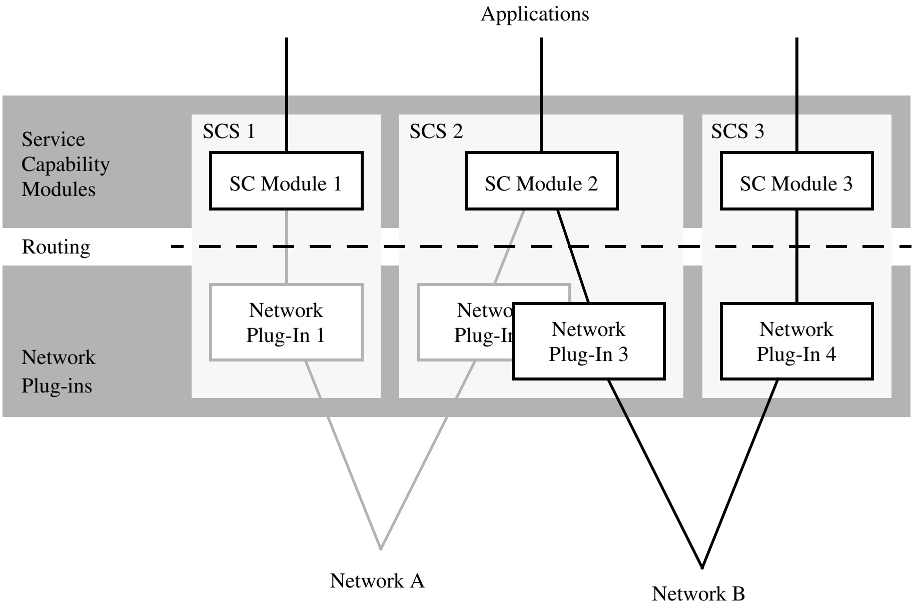


Figure 14-1 Routing between service capability modules and network plug-ins

Since the plug-ins implement the service capability modules plug-in interfaces, a network or SCS plug-in is dedicated to a certain type of service capability module. For example, a user location service capability module needs a user location plug-in.

When a plug-in is installed, it registers itself in the plug-in manager. At registration, the plug-in provides the plug-in manager with information about its type and the address plan it supports. The plug-in manager provides the plug-in with an ID. This ID is used when defining routes for the plug-in.

The routes are specified using regular expressions that match the addresses that should be routed to the plug-in.

This chapter only covers administration of routes for already installed plug-ins, how to install new plug-ins is described in "Service Extension" on page 18-1.

Route specification examples

Below follows a number of example routes specified using regular expressions:

Route expression	Description
^.*	Specifies a route that matches all addresses.
^[0-5].*	Specifies a route matching address strings starting with 0, 1, 2, 3, 4, or 5.
^[6-9].*$	Specifies a route matching address strings starting with 6, 7, 8, or 9.
^46.*$	Specifies a route matching address string starting with 46.
^46.{8}$	Specifies a route matching address strings starting with 46 containing exactly 10 digits.
^.*@.*\.com$	Specifies a route matching mail addresses in the com domain. Note that the dot in .com has to be written "\.".

In the examples:

- "^" indicates the beginning of the string.
- "." matches anything except a newline. That is, "a.b" matches any three-character string which begins with a and ends with b.
- "*" is a suffix which means the preceding regular expression is to be repeated as many times as possible. That is, in the expression "^46.*" the "." is repeated until the whole string is matched.

Adding a route

Follow the instruction below to add a new route for an already installed plug-in. If load balancing shall be achieved between two plug-in of the same type, the same routes have to be added to both plug-ins.

1. Start an Network Gatekeeper Management Tool and log in.

2. Select a SLEE where the plug-in manager is installed.
3. Double-click the **Plugin_manager** service.

   Get plug-in ID

4. Double-click the **getIdList** method.
5. Click **Invoke**.

   All current plug-ins are displayed. List current routes

6. Double-click the **getRouteList** method.
7. Click **Invoke**.

   All current routes are displayed.

   Add route

8. Double-click the **addRoute** method.
9. Enter the plug-in ID and a regular expression matching the route (address plan and set of addresses). See "Route specification examples" on page 14-3 for exmples on how to specify a route using regular expressions.
10. Click **Invoke**.

    The route is added for the plug-in.

11. If load balancing shall be achieved, repeat Steps 8. to 10. for the other plug-in of the same type.

Viewing routes

Follow the instruction below to list the routes defined for BEA WebLogic Network Gatekeeper plug-ins.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the plug-in manager is installed.
3. Double-click the **Plugin_manager** service.

   Get plug-in ID

4. Double-click the **getIdList** method.

5. Click **Invoke**.

   All current plug-ins are displayed. The IDs are in the first column.

   List current routes

6. Double-click the **getRouteList** method.

7. Click **Invoke**.

   All current routes are displayed.

Changing a route

Routes are changed by adding a new route and deleting the old, see "Adding a route" on page 14-3 and "Deleting a route" on page 14-5.

Deleting a route

Follow the instruction below to delete a route for a BEA WebLogic Network Gatekeeper plug-in.

1. Start an Network Gatekeeper Management Tool and log in.

2. Select a SLEE where the plug-in manager is installed.

3. Double-click the **Plugin_manager** service.

   Get plug-in ID

4. Double-click the **getIdList** method.

5. Click **Invoke**.

   All current plug-ins are displayed. The IDs are in the first column.

   List current routes

6. Double-click the **getRouteList** method.

7. Click **Invoke**.

   All current routes are displayed.

   Delete old route

8. Double-click the **removeRoute** method.

9. Enter the plug-in ID and the regular expression matching the route.

10. Click **Invoke**.

    All specified route is deleted.

User Interaction Announcement Administration

The following sections describe how to administer application announcements:

About user interaction announcements

When an application using a user interaction SC is connected to WebLogic Network Gatekeeper, announcements for the application have to be recorded and installed in the network. Since the announcement ID used in the network SRFs differs from the IDs used in application, a mapping between the IDs has to be performed.

The service provider has to provide lists of announcement ID used by the application.

Preparations

Before the connection can be made, the announcements have to be recorded and installed in the SRF. This is equipment dependant.

Connecting application announcement IDs to SRF IDs

Follow the instruction below to connect an announcement ID used in the application to the ID of the actual announcement installed in the SRF.

When connecting large numbers of announcements to the same SRF, it is recommended to write a batch file performing the translations. See "Writing OAM Batch Files" on page F-1.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select one of SLEEs where the user interaction service is installed.
3. Double-click the **ESPA_call_userinteraction** service.
4. Double-click the **setTranslation** method.
5. Enter data according to the table below:

Parameter	Description
infoId	Specifies the announcement ID used in the application. Should be provided by the service provider.
srfAddress	Specifies the SRF's global title.

Parameter	Description
srfAddressType	Specifies the SRF's address type: 0 - NONE 1- NUMBER 2 - GENERIC NUMBER
numberingPlan	Specifies the value of the numbering plan indicator: 1 - ISDN (E.164) 2 - data (X.121) 3 - telex (F.69) 4 - reserved, national 5 - reserved, national
addressPresentation Restricted	Specifies if address presentation is allowed or not: 0 - presentation allowed 1 - presentation restricted 2 - number not available
screeningIndicator	Specifies the value of the screening indicator: 0 - user provided, not verified 1 - user provided, verified and passed 2 - user provided, verified and failed 3 - network provided

Parameter	Description
natureOfAddress	Specifies the value of the number of address indicator: 1 - subscriber number 2 - unknown 3 - national number 4 - international number
numberQualifier	Specifies the number qualifier: 1 - additional called number 5 - additional connected number 6 - additional calling party number 7 - additional original called number 8 - additional redirecting number 9 - additional redirection number 10 - called freephone number

6. Click **Invoke**.

   The connection made.

7. Repeat Steps 4. to 6. for each connection to be made.

Deleting a connection

Follow the instruction below to delete a connection between an announcement ID used in the application and the ID of the actual announcement installed in the SRF.

When deleting large numbers of connections, it is recommended to write a batch file performing the deletion of all the connection. See "Writing OAM Batch Files" on page F-1.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select one of SLEEs where the user interaction service is installed.
3. Double-click the **ESPA_call_userinteraction** service.
4. Double-click the **deleteTranslation** method.
5. Enter the announcement ID as provided by the service provider.

6. Click **Invoke**.

   The deletion made.

CHAPTER 16

Whitelist Administration

The following sections describe how to administer whitelists:

About whitelists

Whitelists are used to allow requests from service providers and their applications through the ESPA service capabilities. There is one list for each ESPA service capabilities.

The list entries contain allowed destination addresses and references to a service provider or application. Both the service provider or application level destination addresses are checked for every request. An overview is provided in the below table.

Level	**Destination in whitelist?**			
Service Provider	Y	Y	N	N
Application	Y	N	Y	N
Total Result	allowed	not allowed	not allowed	not allowed

If no whitelist is defined on a level, all destination addresses are allowed on that level.

Destination specification examples

Below follows a number of example destinations address expressions.

Route expression	**Description**
*	Specifies a string that matches all destination addresses.
46*	Specifies a string matching all destination addresses starting with 46.
46????????	Specifies a string matching destination addresses starting with 46 containing exactly 10 digits.
@.com	Specifies a string matching mail destination addresses in the com domain.

In the examples:

* - matches any character 0 or more times.
? - matches any character exactly once.

Adding a list entry

Follow the instruction below to add a list entry to a list.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_list_matcher** service.

   List available lists
4. Double-click the **getListEntry** method.
5. Click **Invoke**.

   All current lists are displayed.

   View list description
6. Double-click the **describeList** method.
7. Enter the list name.
8. Click **Invoke**.

   A description of the lists and the valid entry formats are displayed.

   Add new entry
9. Double-click the **addListEntry** method.
10. Enter the following list entry data:

Parameter	Description
listName	The name of the list the entry is specified for.
id	The ID of service provider or application the list entry shall be valid for. Specified as: • sp_id for a service provider. For example: `sp1` • sp_idapp_id for an application. For example: `sp1app1`
expression	The destination address specified according to entry format provided in Step 8. on page 3.

11. Click **Invoke**.

    All new entry is added to the list.

Viewing list entries

Follow the instruction below to view entries in a list.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_list_matcher** service.

   List available lists

4. Double-click the **getListEntry** method.
5. Click **Invoke**.

   All current lists are displayed.

   View entries

6. Double-click the **listEntries** method.
7. Enter the following list entry data:

Parameter	**Description**
listName	The name of the list the entry is specified for.
id	The ID of service provider or application the list entry shall be valid for. Specified as: • sp_id for a service provider. For example: `sp1` • sp_idapp_id for an application. For example: `sp1app1`
expression	A search criteria according to the following: * - matches any character 0 or more times ? - matches any character exactly once
offset	The offset from the first hit to the first displayed hit.
noHits	The number of displayed hits.

8. Click **Invoke**.

   All list entries according to the search criteria, offset and desired number of displayed hits are shown.

Removing a list entry

Follow the instruction below to remove an entry from a list.

1. Identify the entry to remove. See “Viewing list entries” on page 16-4.
2. Double-click the **removeListEntry** method.
3. Enter the entry’s list name, ID and expression.
4. Click **Invoke**.

   The entry is removed from the specified list.

Removing all list entries for an ID (service provider or application)

Follow the instruction below to remove all list entries related to a list and a service provider or application.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **SLEE_list_matcher** service.
4. Double-click the **removeIDFromList** method.
5. Enter the list name and the ID. The ID is specified as:
   - sp_id for a service provider. For example: `sp1`
   - sp_idapp_id for an application. For example: `sp1app1`
6. Click **Invoke**.

   All entries related to the specified ID are removed from the list.

Recommended Periodic Maintenance

The following sections describe periodic maintenance tasks recommended with WebLogic Network Gatekeeper:

About periodic maintenance

Periodic maintenance is divided in to database cleanup and system backup tasks.

A recommended time interval is given for each task. Depending on how the system is used, the recommended time intervals may have to be adjusted.

Database cleanup

Task	How to	Recommended interval
Delete load data	See "Deleting SLEE load data" on page 8-11.	1 month
Delete usage statistics	See "Deleting statistics data from the database" on page 10-7.	1 month
Delete alarms	See "Deleting alarm entries from the database" on page 12-5.	2 months
Delete events	See "Deleting event entries from the database" on page 12-8.	1 month

System backup

Task	How to*	Recommended interval
Full system backup	See "Performing a full system backup" on page 20-3.	1 weeks
System data backup	See "Performing a system data backup" on page 20-6.	1 day
* It is recommended to use an automatic backup facility. Refer to the indicated section for information about which files and directories to backup.		

In addition, it is recommended to perform a full system backup when upgrading the system with new services.

CHAPTER 18

Service Extension

The following sections describe how to extend WebLogic Network Gatekeeper functionality:

About service extension

Service extension is about extending BEA WebLogic Network Gatekeeper's functionality to provide new Java and Web Services APIs and to support new network services and protocols.

This can be done by installing new SESPA modules, ESPA service capability modules and SCS or network plug-ins in BEA WebLogic Network Gatekeeper SLEEs. Also external protocol adapters can be connected to the Plug-in manager. For more information about system extension alternatives, see Product Description - BEA WebLogic Network Gatekeeper.

Installing a SESPA module

The following is an outline of an installation procedure to be used when adding a new SESPA service to BEA WebLogic Network Gatekeeper. SESPA services are are SLEE services, so the SLEE's standard procedure for SLEE service installation is followed.

A complete procedure, including SESPA service configuration (if any), has to be provided in the new SESPA service's documentation.

Installation can be made in run-time.

1. Install and start the SESPA service through the SLEE deployment service.
2. Configure the SESPA service through the service's own OAM methods.
3. Deploy the servlet in the Tomcat servlet engine and the web service in the Axis SOAP engine. See the new SESPA service's documentation.
4. Add the SESPA service to an existing resource sharing context or create a new resource sharing context for the SESPA service. If the SESPA service is not manually added to a resource sharing context, the "default" resource sharing context will be used for the SESPA service.
5. Activate the SESPA service through the SLEE deployment service.

Installing an ESPA service capability module

The following is an outline of an installation procedure to be used when adding a new ESPA service capability to BEA WebLogic Network Gatekeeper. ESPA service capabilities are are SLEE services, so the SLEE's standard procedure for SLEE service installation is followed.

A complete procedure, including ESPA service capability configuration (if any), has to be provided in the new ESPA service capability's documentation.

Installation can be made in run-time.

1. Install and start the ESPA service capability through the SLEE deployment service.
2. Configure the ESPA service capability through the service's own OAM methods.
3. Add the ESPA service capability to an existing resource sharing context or create a new resource sharing context for the ESPA service capability. If the ESPA service capability is not manually added to a resource sharing context, the "default" resource sharing context will be used for the ESPA service capability.
4. Activate the ESPA service capability through the SLEE deployment service.
5. Update the SLAs for the affected service provider and application groups, see "Service Provider and Application Administration" on page 5-1.

Installing a network plug-in

The following is an outline of an installation procedure to be used when adding a new network plug-in to BEA WebLogic Network Gatekeeper. Network plug-ins are SLEE services, so the SLEE's standard procedure for SLEE service installation is followed.

A complete procedure, including plug-in configuration, has to be provided in the new plug-in's documentation.

Installation can be made in run-time.

1. Install and start the plug-in through the SLEE deployment service.
2. Configure the plug-in through the plug-in's own OAM methods.
3. If the plug-in type is not one of the registered plug-in types, add the new plug-in type through the Plug-in manager service.
4. Set up the routing through the Plug-in manager, see "Routing Administration" on page 14-1.
5. Add the plug-in service to an existing resource sharing context or create a new resource sharing context for the plug-in service. If the plug-in service is not manually added to a resource sharing context, the "default" resource sharing context will be used for the plug-in service.
6. Activate the plug-in service through the SLEE deployment service.

Connecting an external protocol adapter to the plug-in manager

The following is an outline of how to connect an external protocol adapter directly to the plug-in manager. A prerequisite on the external protocol adapter is that it implements the plug-in manager's plug-in interfaces.

The connection can be made in run-time.

1. If the protocol adaptor type is not one of the registered plug-in types, add the new plug-in type through the Plug-in manager service in the Network Gatekeeper Management Tool.
2. Install and configure the protocol adaptor according to the protocol adaptor's documentation.
3. Register the protocol adaptor in the plug-in manager.

   This is dependent on how the protocol adaptor is implemented. If not handled automatically by the protocol adaptor, the protocol adaptor has to be registered manually through the through the plug-in manager service in the Network Gatekeeper Management Tool.
4. Set up the routing through the Plug-in manager, see "Routing Administration" on page 14-1.

CHAPTER 19

System Scaling

The following sections describe how to install and configure SLEEs in a domain:

About system scaling

BEA WebLogic Network Gatekeeper consists of a number of SLEEs. Each SLEE executing on a separate server. The SLEEs are assigned different types of SLEE services. A number of SLEEs that are assigned the same types of SLEE services are referred to as a SLEE domain. A large BEA WebLogic Network Gatekeeper system has the following SLEE domains:

- Application access domain
- Service execution domain
- Network plug-in domain

All SLEEs within a SLEE domain contain the same SLEE services.

Apart from the SLEE domains, there is a database domain. The databases might execute on separate servers, or the same servers as two of the SLEEs.

The number of SLEEs in each domain is depends on the load handled by each domain. When the SLEEs within a SLEE domain starts raising overloaded and severely overloaded alarms, the SLEE domain has to be expanded with another SLEE. To do this a new server is added to BEA WebLogic Network Gatekeeper system. A backup of one of the SLEEs within the SLEE domain is made, and the backup is installed on the new server. Additional registration and configuration work is then performed based on the SLEE domain.

Adding a BEA WebLogic Network Gatekeeper SLEE

The following is an outline of how to install a new SLEE in a BEA WebLogic Network Gatekeeper SLEE domain. It includes backup of an existing SLEE within the SLEE domain, software installation on the new server (OS and SLEE backup copy), and starting the SLEE process.

Backup SLEE

1. Back one of the SLEEs in the desired SLEE domain, see “Performing a full system backup” on page 20-3. If a database executes on the same server as the SLEE, do not back up the database related files.

Install OS and SLEE backup copy

2. See “Performing a full system restoration” on page 20-8, but do not start the SLEE process.

Edit SLEE properties file

3. Go to the `/usr/local/slee/bin/` directory.

4. Open the file `slee_properties.xml` in a text editor.

5. Change the `<SLEE_HOST>` parameter in the file to IP address of your new server. For more information about the individual parameters, see "SLEE start-up parameters" on page B-9.

6. Save `slee_properties.xml` and exit the editor.

   Prepare scripts for start-up

7. Enter command:

   ```
   ./SLEEConfig.sh
   ```

   The system scripts are updated with the configuration data specified in the `slee_properties.xml` file.

   Initiate system for start-up

8. Enter command:

   ```
   ./postconfig.sh
   ```

   The configuration scripts are run and the database is restarted.

   Start SLEE process

9. Start the SLEE process through the SLEE agent. Enter command:

   ```
   ./runAgent.sh&
   ```

   The SLEE agent is now starting up the SLEE process. When the process has started, the SLEE will be in the same state as the of the backed up SLEE.

   Continue with configuration of the SLEE. See the following sections.

Configuring an application access SLEE

The following is an outline of how to configure an application access SLEE.

1. Configure the SESPA services in the new SLEE instance according to the other SESPA services in the other application access SLEEs. For information about the SESPA service configuration parameters, see "SESPA" on page B-13. The parameters are presented in tables, one for each SESPA service. The ones that have to be set manually are marked **SLEE** in the **Level** column.

2. Distribute the new SESPA services' WSDL files to the application providers.

Configuring a service execution SLEE

The following is an outline of how to configure an SCS proxy SLEE.

1. Configure the ESPA service capabilities in the new SLEE instance according to the other ESPA service capabilities in the other service execution SLEEs. For information about the ESPA service capability configuration parameters, see "ESPA access and ESPA service capability modules" on page B-15. The parameters are presented in tables, one for each ESPA service capability. The ones that have to be set manually are marked **SLEE** in the **Level** column.

Configuring an network plug-in SLEE

The following is an outline of how to configure an IP network and SCS plug-in SLEE.

1. Configure the plug-ins in the new SLEE instance according to the other plug-ins in the other IP network and SCS plug-in SLEEs. For information about the plug-ins configuration parameters, see "Network plug-ins" on page B-24. The parameters are presented in tables, one for each plug-in proxy. The ones that have to be set manually are marked **SLEE** in the **Level** column.

2. Depending on plug-in type, the plug-ins' addresses may have to be registered in the network node(s) they communicate with.

System Backup and Restoration

The following sections describe how to backup and restore WebLogic Network Gatekeeper installations:

About system backup

The following sections describe two types of system backups. The first type, the full system backup, makes a backup copy of all BEA WebLogic Network Gatekeeper related software, installed applications, configuration files and database tables. A full system backup should be performed after the system has been successfully verified and after major re-configurations, upgrades and when patches have been installed in the system.

The second type, the system data backup, is a smaller backup that makes a backup copy of the configuration files, user certificates and database tables. This backup has to be performed on a regular basis and when new applications have been installed.

System backup procedures may vary for different systems and configurations, depending on system type, additional equipment connected to the system, and so on. This chapter gives a recommendation on how to perform backup and restore, and also gives information the tools to support these procedures.

Setting up backup directories

The database and system backup files generated by the backup scripts are named as follows:

- Static MySQL files are backed up to `system_<date>.zip`.
- MySQL database files are backed up to `data_<date>.zip`

Where `<date>` represents the creation date and time.

The files are zipped together and requires an unzip-utility, like jar, in order to restore them.

The backup-files are created in a directory as defined in the xml-tag `<BACKUP directory="<dir>"/>` in the file `slee_properties.xml`. Replace `<dir>` with the full path to the desired directory, preferably on a separate disk.

To apply the changes, the script SLEEConfig.sh -px must be executed. The script is located in the `bin` directory of the installation.

For example, edit the file `slee_properties.xml` and change the lines to (the given path is just an example of a path to a separate disk):

```
<BACKUP directory="/backup"/>
```

Save and close the file, and run the script SLEEConfig.sh -px to apply the changes.

Enable binary logging

To enable data backups on a single database system, make sure binary logging is enabled.

Activate binary logging

1. Open the MySQL configuration file `/usr/local/mysql/data/my.cnf`
2. Add the following rows, if they are not present:

   ```
   server-id=1
   log-bin=/usr/local/mysql/data/query-bin
   ```

   If the rows were not present, proceed with the next step. If the rows are present, binary logging is enabled and no further action is needed.

   Restart MySQL

   Since MySQL is stopped during this procedure, make sure that all SLEEs using the database are in state shutdown.

3. Open a command tool.
4. Change directory to the installation of MySQL. Enter command:

   ```
   cd /usr/local/mysql/
   ```

5. Stop MySQL. Enter command:

   ```
   ./bin/mysqladmin -u root -p shutdown
   ```

6. When asked for, enter the password for the MySQL root user.
7. Execute the restart-script. Enter command:

   ```
   ./bin/safe_mysqld &
   ```

Performing a full system backup

Follow the instruction below to perform a full system backup. The backup saves all software and data related to the BEA WebLogic Network Gatekeeper system, including third party products and database tables.In order to reduce the size of the database backup, it is recommended to dump the charging data to a text-file, see Chapter 9, “Charging Data Export” before performing the backup. It is also recommended to remove old alarms, events, and statistics from the database. See “Deleting alarm entries from the database” on page 10-4, “Deleting event entries from the database” on page 10-7, and “Deleting statistics data from the database” on page 8-7.

Copy files and directories

1. Copy the following on each server in the system to the backup directory:
   - All scripts for autostart of the database and the SLEE, as cofigured during the installation.
   - `/usr/local/slee/` (SLEE, SLEE services, and applications)

   It is recommended to use a compression utility, for example jar, in order to minimize the diskspace required for the backup.

Backup single database system

If using a single database system, follow the instructions below to perform a backup. If using a replicated database system, perform the procedure as described in "Backup replicated database system" on page 18-6.

Note: No updates can be made on the database during the full system backup, causing the system to halt during the procedure. It is strongly recommended to shutdown all SLEE instances that use the database during the full system backup.

1. Login in as administrator on the computer hosting the database and open a command window.
2. Login to the database with the MySQL client. Enter command:

   ```
   /usr/local/mysql/bin/mysql -u root -p
   ```

3. When prompted for, enter the password for the database root user.

   The prompt `mysql>` is displayed.

Caution: If the MySQL client is closed during the execution of Step 4 to Step 9, the result will be corrupt data in the backup.

4. Flush tables and obtain table locks. Enter command:

   ```
   FLUSH TABLES WITH READ LOCK;
   ```

5. Flush binary logs, that is switch current log file. Enter command:

   ```
   FLUSH LOGS;
   ```

6. List currently used binary log-file. The name of the log will be used in a later step. Enter command:

   ```
   SHOW MASTER STATUS;
   ```

A list is displayed:

```
+--------+----------+--------------+------------------+
| File   | Position | Binlog_do_db | Binlog_ignore_db |
+--------+----------+--------------+------------------+
| <file> | <pos>    |              |                  |
+--------+----------+--------------+------------------+
1 row in set (0.00 sec)
```

`<file>` is the name of the old binary log.

7. Remove old binary logs. Enter command:

```
PURGE MASTER LOGS TO '<file>'
```

`<file>` is replaced by a file name as output in Step 6 on page 5. The name is for example `query-bin.114`

8. Copy the MySQL directory `/usr/local/mysql/` to a backup directory without exiting the MySQL client.

Note: This step must be performed from another command window, or using a file manager. Do not exit the MySQL client.

9. Unlock all tables. Enter command:

```
UNLOCK TABLES;
```

10. Exit from the MySQL client. Enter command:

```
exit
```

The backup is complete and the tables are unlocked.

Backup replicated database system

follow the instructions below to perform a backup.

If using a single database configuration, see "Backup single database system" on page 18-4.

Note: The standby database will be shutdown during the backup. If the currently active database crashes during the backup, there will be no database available for BEA WebLogic Network Gatekeeper, causing it to fail.

Note: It is important to perform the procedure on both computers hosting the database in order to create a complete backup.

1. Repeat Step 2 to Step 3 on both computers hosting the database.

2. Login in as administrator and open a command window.

3. Execute the dual database system backup script. Enter command:

   ```
   /usr/local/slee/bin/db_runDualSystemBackup.sh
   ```

   If the script was run on the standby database, it will create a backup. It will also produce a message informing where to find the files. The files `system_<date>.zip` and `data_<date>.zip`, where `<date>` represents the current date and time, are created. Static MySQL files are backed up to `system_<date>.zip.` MySQL Database files are backed up to `data_<date>.zip`

   If the script was run on the currently active database only the configuration file, `my.cnf`, and MySQL static files are copied. It will also produce a message informing where to find the files.

   In both cases, the files are created in the directory as configured. See "Setting up backup directories" on page 18-1.

Performing a system data backup

Follow the instruction below to perform a system data backup. The backup saves all BEA WebLogic Network Gatekeeper system data from the database, but not BEA WebLogic Network Gatekeeper system software.

Copy files and directories

1. Copy the following directories, including subdirectories, on each server in the system.

   – `/usr/local/slee/bin/` (directories with jar files for SLEE services, auto started services and installed applications)

   – `/usr/local/slee/certificates/` (user certificates)

   It is recommended to use a compression utility, for example jar, in order to minimize the diskspace required for the backup.

Single database system

The system data backup on a single database system does not interfere with the system operation. The script can be a scheduled job to be executed periodically. The backed up files should be moved from the backup directory and saved on tape after each execution to avoid full disk.

Note: The files backed up are the ones generated since the last full system backup. In order to reduce the size of the files, and thereby shorten the time it takes to perform a restoration, it is recommended to perform a full system backup on a regular basis when using a single database system. It is important to save all system data backup files since the last full system backup.

1. Login in as administrator and open a command window on the database machine.
2. Execute the single database system data backup script. Enter command:

   ```
   /usr/local/slee/bin/db_runSingleDataBackup.sh
   ```

   When the script completes, it has created a backup. It also produces a message informing where to find the files.

   The file `data_<date>.zip`, where `<date>` represents the current date, is created. The file is created in the directory as configured. See "Setting up backup directories" on page 18-1.

Replicated database system

The script can be a scheduled job to be executed periodically. It should be scheduled to run at the same time on both database nodes, since it will only copy files on the standby database. The backed up files should be moved from the backup directory and saved on tape after each execution to avoid full disk.

1. If using a replicated database system, follow the instructions below to perform a backup.

   Note: The standby database will be shutdown during the backup. If the currently active database crashes during the backup, there will be no database available for BEA WebLogic Network Gatekeeper, causing it to fail.

   Note: It is important to perform the procedure on both computers hosting the database in order to create a complete backup.

2. Repeat Step 3 to Step 4 on both computers hosting the database.
3. Login in as administrator and open a command window.
4. Execute the dual database system backup script. Enter command:

   /usr/local/slee/bin/db_runDualDataBackup.sh

   If the script was run on the standby database, it will create a backup. The script displays a message informing where to find the backed up files.
   The file `data_<date>.zip`, where `<date>` represents the current date and time, is created. Database tables are backed up to `data_<date>.zip`

   If the script was run on the currently active database only the configuration file, no files are copied. The script displays a recommendation to run the script on the inactive database.

In both cases, the files are created in the directory as configured. See "Setting up backup directories" on page 18-1.

About system restoration

System restoration includes both restoring the full BEA WebLogic Network Gatekeeper system and restoring the system data. When restoring the full system, all BEA WebLogic Network Gatekeeper software (including third party software) and all system data is restored. In case of a system data restoration, user certificates and database tables are restored.

For a successful restoration, the backup must have been performed according to the sections "Performing a full system backup" on page 18-3 and "Performing a system data backup" on page 18-6 respectively.

Also, it is important that the same directory structure is used on the restored system as on the backed up system.

If one of the databases in the system has failed it is possible to create a snapshot of the still running database host and use that snapshot for restoring the failed database. This is called a database snapshot restoration.

Performing a full system restoration

Follow the instruction below to perform a full system restoration. The restoration requires:

- the UNIX installation package
- BEA WebLogic Network Gatekeeper CD-ROM or downloaded installation files.
- a backup copy made according to the section "Performing a full system backup" on page 18-3.
- any patches installed after the backup was made

Install OS

1. Install the UNIX operating system. See the installation instructions included in the UNIX installation package.

Install resent patches

2. Install BEA WebLogic Network Gatekeeper patches received since the backup was performed. See the instructions provided with the patches. There is no need to install the patches included prior to the latest full system backup.

Copy backup files

3. Copy the full system backup copy, as set up in "Copy files and directories" on page 20-4 to the newly installed BEA WebLogic Network Gatekeeper.

Restore the database software

1. Install the MySQL software according to the installation guide.
2. Make sure the MySQL server is shut down. Enter command:

   ```
   /usr/local/mysql/bin/mysqladmin -u root -p shutdown
   ```

3. When prompted for, enter the password for the root database user.
4. Overwrite the entire MySQL directory with the files backed up during the last full system backup. Perform the following commands:

   ```
   cd /usr/local/mysql/
   ```

   ```
   jar xf <system_backup_file>
   ```

   Where `<system_backup_file>` is the name of the back-up file.

5. Perform a system data restoration from the latest system data backup, as described in "Performing a system data restoration" on page 18-11.

Start SLEE process

6. Start the SLEE process by rebooting the server.

   When the server reboots, the SLEE agent will be automatically start up the SLEE process. When the process is started, the SLEE will be in the same state as it was at the time of the backup.

Performing a system data restoration

Caution: Follow the instruction below to perform a restoration of BEA WebLogic Network Gatekeeper system data. After the restoration, all data that has been written to the database after the latest backup will be lost.

It is necessary to run system data backups frequently to avoid to large data loss in case of a database crash

Note: The restoration requires a system data backup copy made according to the section "Performing a system data backup" on page 18-6.

The MySQL `root` user is used in all MySQL commands.

Restore files

1. Copy the directories from the backup copy to following directories:

   – `/usr/local/slee/bin/`

   – `usr/local/slee/certificates/`

   – `/usr/local/slee/servlet_engine/webapps/`

Caution: For single database system data restoration you also need the last full system backup together with all system data backup files since the latest full system backup. The different backup files needs to be synchronized; never add system data backup files older than the full system backup used.

1. Make sure the MySQL server is shut down. Enter command:

   ```
   /usr/local/mysql/bin/mysqladmin -u root -p shutdown
   ```

2. When prompted for, enter the password for the root database user.

3. Copy the latest full system backup data files to the MySQL data directory `/usr/local/mysql/data`

4. Start MySQL server. Enter commands:

   ```
   cd /usr/local/mysql/
   ./bin/safe_mysqld &
   ```

5. Extract the relevant system data backup files to a directory.

   Note: Relevant system data backup files are the ones taken since last full system backup.

6. Import the system data backups made after the latest full system backup. Change to the directory holding the system data backup and database backup files backed up since last full system backup. Enter command:

   ```
   /usr/local/mysql/bin/mysqlbinlog <backup dir>/query-bin.[0-9].* |
   /usr/local/mysql/bin/mysql -u root -p
   ```

   Replace `<backup dir>` with the directory used in Step 5.

7. When prompted for, enter the password for the root database user.

   All query-bin files are imported and the embedded SQL statements are executed. This procedure may take a few minutes.

   Now the MySQL server should be in the same state as when the latest system data backup was done.

Restore a replicated database system

For dual (replicated) database system data restoration you need the latest performed system data backup.

Note: After the restoration, all data written to the database after the latest backup will be lost. Run backups frequently to avoid to large data loss in case of a database crash.

In a replicated database system, if one database crashes, all information should be present in the still working database. It is possible to save this data when restoring this node, and import this data in a separate MySQL installation to be able to, for instance, dump charging data.

The following references are used below.

Host A: The computer hosting database A.

Database A: The database that will replace the previously malfunctioning database (or standby database if the restoration is a rollback to a previous configuration).

Host B: The computer hosting database B.

Database B: The currently active database used by the system.

1. In **Host B**:

   d. Login in as administrator and open a command window.

2. Login to database B with the MySQL client. Enter command:

   ```
   /usr/local/mysql/bin/mysql -u root -p
   ```

3. When prompted for, enter the password for the database root user.

   The prompt `mysql>` is displayed.

4. Stop the (replication) slave thread. Enter command:.

   ```
   SLAVE STOP;
   ```

5. In **Host A**:

   e. Login in as administrator and open a command window.

6. Make sure the MySQL server to be restored is shut down. Enter command:

   ```
   /usr/local/mysql/bin/mysqladmin -u root -p shutdown
   ```

7. When prompted for, enter the root password.

8. Extract the full system backup files from the backup directory to the home directory of mySQL. The backup directory is configured according to "Setting up backup directories" on page 18-1.

   ```
   cd /usr/local/mysql/
   jar xf <system_backup_file>
   ```

   Where `<system_backup_file>` is the name of the system back-up file.

9. Clear (remove all files and directories in) the MySQL data directory `/usr/local/mysql/data`

10. Unzip and copy the latest system data backup data files to the MySQL data directory `/usr/local/mysql/data`. Check both database A and database B to get the latest backup copy.

    ```
    cd /usr/local/mysql/data
    jar xf <data_backup_file>
    chown -R root:mysql /usr/local/mysql
    chown -R mysql /usr/local/mysql/data
    ```

    Where `<data_backup_file>` is the name of the data back-up file.

11. Open the file `/usr/local/mysql/data/my.cnf`

12. In the file, transform each row starting with the keyword `master` into comments, by inserting a hash (#) character in the beginning of the row.

f. Start **Database A**. Enter commands:

```
cd /usr/local/mysql/
./bin/safe_mysqld &
```

13. In **Host B**:

14. Shut down **Database B**. Enter command:

```
/usr/local/mysql/bin/mysqladmin -u root -p shutdown
```

g. When prompted for, enter the root password.

This will cause BEA WebLogic Network Gatekeeper to switch to **Database A**.

15. Optional step:
Make a copy of the data directory of the mySQL installation.

This copy contains changes made since the latest backup.
This copy can be used to copy to a separate MySQL installation in order to, for example dump charging data or viewing alarms since latest backup. For information on how to import table data files in a MySQL installation, see MySQL Reference Manual.

16. Clear (remove all files and directories in) the MySQL data directory `/usr/local/mysql/data`

17. Unzip and copy the latest system data backup files to the MySQL data directory `/usr/local/mysql/data`. Use the same backup copy as in Step 2 on page 13, sub-step f.

18. Verify that the parameter `master-host` in `my.cnf` in host A is the IP address of **Host B** and vice versa.

19. In **Host B**:

h. Start **Database B**. Enter commands:

```
cd /usr/local/mysql/
./bin/safe_mysqld &
```

Database B will start replicating data updated in **Database A** since **Database B** was shut down.

20. In **Host A**:

i. Open the file `/usr/local/mysql/data/my.cnf`

21. Remove the comment characters, as added in Step 2 on page 13, sub-step h.
22. Login to **Database A**. Enter the following commands:

    ```
    cd /usr/local/mysql/
    ./bin/mysql -u root -p
    ```

23. When prompted for, enter the password for the database root user.

    The prompt `mysql>` is displayed.

24. Change database master to database B. Enter the following commands:

    ```
    CHANGE MASTER TO
       MASTER_HOST='<database B IP address>',
       MASTER_USER='<replication user>',
       MASTER_PASSWORD='<replication password>',
       MASTER_PORT=<database B port>;
    ```

    Where `<database B IP address>`, `<replication user>`, `<replication password>`, `<database B port>` are replaced with the corresponding values, as defined in `my.cnf`.

25. In **Database A** enter command:

    ```
    START SLAVE;
    ```

    Database A starts replicating changes made in **Database B**.

    Verification of restoration of replicated database system

26. In both **Database A** and **Database B**, verify that the database replication is working correctly. Enter commands:

    ```
    SHOW MASTER STATUS;
    ```

    ```
    SHOW SLAVE STATUS;
    ```

27. Cross compare the output values.

    If corresponding, the restoration procedure was successful.

    If the values did not correspond, a corrupt database may the reason. For actions to take, see "Handling corrupt database tables" on page 18-18 or Contact MySQL support.

Database shapshot restoration

Follow the instruction below to perform a backup and restore procedure that can be used when one of the databases in the system has failed and needs to be restored. The procedure assumes that there is still one functional and active database in the system.

When performing a snapshot of the functional database it must be locked for some time in order guarantee a stable copy. During the lock time all write requests towards the database will be blocked. In order to reduce the lock duration it is possible to specify a list of database tables that can be temporary renamed and copied separately in order to reduce the lock duration.

Snapshot

The tables to be separately copied can me managed with the **addMasterSnapshotSpecialCopyTable**, **removeMasterSnapshotSpecialCopyTable** and **listMasterSnapshotSpecialCopyTable** OAM methods in the **SLEE_backup** service.

The data in the specified tables will become unavailable for the duration of the snapshot process but will become available again after completion of the snapshot process. This may cause outstanding requests to be lost.

The following are some examples of tables suitable for separate copy:

- `ic_p_gms_message`
- `ic_slee_alarm`
- `ic_slee_charging`
- `ic_slee_statistics_data`
- `ic_slee_event`

The backup snapshot is created by executing the **createMasterSnapshotForRestore** method in the **SLEE_backup** OAM interface.

Note that during creation of the snapshot the database slave replication thread at the functional database will be stopped. Once the other database host has been restored it must be started again using the **restartSlaveThreadAfterSnapshotRestore** OAM method.

Alarms will be generated to indicate when the snapshot procedure has ended and where it is located.

Pack the backup snapshot files together That is, perform the following commands:

```
cd /usr/local/slee/backup/<snapshot_timestamp>
tar cvf db_snapshot_backup.tar mysql slee_db
```

FTP the backup to the machine with the failed database.

Restoration

Restore the failed database host:

1. Re-install mysql if required.
2. Delete all files under `/usr/local/mysql/data` using:

   ```
   rm -r /usr/local/mysql/data/*
   ```

3. Unpack the backup files under `/usr/local/mysql/data` so that the `mysql` and `slee_db` directories are created under `/usr/local/mysql/data`
4. Changed to correct ownership using:

   ```
   chown -R mysql /usr/local/mysql/data
   ```

   ```
   chgrp -R mysql /usr/local/mysql/data
   ```

5. Execute `postconfig.sh` in `/usr/local/slee/bin` in order to create a proper `my.cnf` file. Executing `postconfig.sh` will also restart the database.
6. Restart the slave replication thread on the original functional active master database host by executing the **restartSlaveThreadAfterSnapshotRestore** OAM method in the **SLEE_backup** service.
7. Check the replication status by executing the **getDatabaseReplicationStatus** OAM method in the **SLEE_backup** service. It should report "OK".

Handling corrupt database tables

If corrupt database tables are discovered during a restoration, they might be recovered. Follow the instructions given in section “Disaster Prevention and Recovery “in MySQL Reference Manual.

Alarm and Fault Handling

The following sections describe WebLogic Network Gatekeeper alarms:

Interpreting alarms

An alarm in the alarm list provides different types of information according to the table below.

Information	Description
Source	Specifies the name of the SLEE service name (software module) that raised the alarm and the IP address of the SLEE the service is installed in.
Severity	Specifies the alarm's severity level. One of the following: 1 - warning 2 - minor 3 - major 4 - critical
Identifier	Specifies the alarm type through a number and heading.
Info	Alarm information provided by the software module the raised the alarm.
Timestamp	Specifies the time and date the alarm was raised.

Clear alarms

Some of the alarms have clear alarms indicating when the condition that caused the alarm has ceased. That is, the condition has gone back to normal. The following combinations of alarms and clear alarms exist:

Type	Alarm
Alarm: Clear alarm:	1012 SLEE: CORBA thread-pool overloaded 1013 SLEE: CORBA thread-pool overload - alarm ceased
Alarm: Clear alarm:	1019 SLEE: SLEE task pool empty 1020 SLEE: SLEE task pool empty - alarm ceased

Type	Alarm
Alarm: Clear alarm:	5408 Plug-in messaging-SMPP: SMSC transmitter connection lost 5409 Plug-in messaging-SMPP: SMSC transmitter reconnected
Alarm: Clear alarm:	5411 Plug-in messaging-SMPP: SMSC transmitter reconnect attempt failed 5409 Plug-in messaging-SMPP: SMSC transmitter reconnected
Alarm: Clear alarm:	5412 Plug-in messaging-SMPP: SMSC receiver connection lost 5413 Plug-in messaging-SMPP: SMSC receiver reconnected
Alarm: Clear alarm:	5415 Plug-in messaging-SMPP: SMSC receiver reconnect attempt failed 5413 Plug-in messaging-SMPP: SMSC receiver reconnected
Alarm: Clear alarm:	5700 Plug-in messaging-CIMD: SMSC login failed 5701 Plug-in messaging-CIMD: SMSC login succeeded
Alarm: Clear alarm:	5705 Plug-in messaging-CIMD: Plug-in not connected to SMSC 5706 Plug-in messaging-CIMD: Plug-in connected to SMSC

Alarm numbering overview

SLEE and SLEE utility alarms

1000-1099 SLEE

1100-1149 SLEE charging

1150-1199 Web server manager

1200-1249 Servlet engine manager

1350-1399 Time server manager

1450-1499 Plug-in manager

3000-3099Policy service

95000-95099Subscription handler

ESPA service capability alarms

11100-11199 ESPA access

2100-2199 ESPA messaging

2200-2299 ESPA call control

2300-2399 ESPA location

2400-2499 ESPA user status

2500-2599 ESPA charging

2600-2699 ESPA user interaction

2700-2799 Subscriber profile

2800-2899 Network initiated call handler

Protocol plug-in alarms

5400-5499 Protocol plug-in messaging/SMPP

5500-5599 Protocol plug-in user location/MPP

5600-5699 Protocol plug-in user status/MPP

5700-5799 Protocol plug-in messaging/CIMD

5800-5899 Protocol plug-in messaging/MM7

5900-5999 Protocol plug-in messaging/MLP

22000-22099 Protocol plug-in OSA access

22200-22299 Protocol plug-in OSA MPCC

22400-22499 Protocol plug-in OSA call UI

SESPA alarms

12100-12199 SESPA access

12200-12299 SESPA user location

12300-12399 SESPA messaging

12400-12499 SESPA messaging UI

12500-12599 SESPA user status

12600-12699 SESPA call UI

12800-12899 SESPA call control

12900-12999 SESPA subscriber profile

Resolving Alarms

1001 SLEE: Service deactivated

Severity

Major

Description

The indicated service has been deactivated because it has raised more critical alarms than allowed. That is, in a service's deployment descriptor it is defined how many critical alarms the service is allowed to raise before it is taken out of service.

What to do

Activate the service again.

1. Start an Network Gatekeeper Management Tool and log in.
2. Select the SLEE the where the deactivated service is installed in the **SLEEs** pane.
3. Select the **SLEE_deployment** service.
4. Select the **activate** method and enter the service name of the service to be activated.
5. Click **Invoke**.

   The service is activated.

If the service keeps raising critical alarms, analyse the reason for those alarms. Trouble report the service to the service supplier if the analyses of the alarms show that the service is faulty.

1002 SLEE: Service data storage failed

Severity

Major

Description

The SLEE was not able to store service data in the database.

Possible reasons:

- Neither the master nor the slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

1. Check that the database is running.

   Enter command `ps -ef|grep safe_mysqld` in a command window. If the database is running, `safe_mysqld` is returned.

2. If the database is not running, start the database on the indicated URL. On the database server, do the following:

   Run the `bin/mysqld_safe &` script in the `/usr/local/mysql/` directory

3. If the database is running, restart the database. To stop the database, do the following:

   Run the `mysqladmin shutdown` script in the `/usr/local/mysql/bin` directory.

   To start the database, see above.

4. Check if the database error log `(/usr/local/mysql/data/<hostname>.err)` shows what caused the switch over.

5. Check the network connection between the SLEE that raised the alarm and the database.

For more information, see MySQL Reference Manual.

1003 SLEE: Service deactivation exception

Severity

Minor

Description

The SLEE had to force the deactivation of the indicated service because an exception was caught from the service when the SLEE tried to deactivate the service.

What to do

Trouble report the service to the service supplier.

1004 SLEE: Service stop exception

Severity

Minor

Description

The SLEE had to force the stopping of the indicated service because an exception was caught from the service when the SLEE tried to stop the service.

What to do

Trouble report the service to the service supplier.

1005 SLEE: Database replication connect failure

Severity

Critical

Description

Unable to connect to both databases when verifying replication of databases.

What to do

Verify that both databases are running.

1006 SLEE: Database replication files differ

Severity

Critical

Description

Database replication files differ more than the maximum allowed value.

The replication mechanism is not able to write data fast enough, or not at all.

What to do

Check the connection between the two databases.

Verify that both databases are running.

1007 SLEE: Database replication file names differ

Severity

Critical

Description

The internal file names used by the database replication process are mismatching. This may occur when changing log file names explicitly, for example during backup.

What to do

If this alarm is generated when not explicitly resetting the logging, the replication files may be out of synchronization. Verify that the replication has not halted due to an error. If the replication has halted, restore the failed database.

1008 SLEE: Database replication status check error

Severity

Critical

Description

Error during check of database replication status. Internal error during database replication check.

What to do

Make sure both databases are running. Restart or restore failed database.

1009 SLEE: Database replication file too large

Severity

Critical

Description

Database replication file is too large.

What to do

Free up disk space. Explicitly change to a new log file by running the reset script

```
/usr/local/slee/bin/dbrunReset.sh
```

1010 SLEE: Database replication files explicitly reset

Severity

Minor

Description

Size of database replication files have reached 90% of maximum allowed size. The files will be gracefully reset.

What to do

No action needed.

1011 SLEE: Faulty username-password combination

Severity

Major

Description

A user tried to perform a OAM method with inadequate user-password combination.

What to do

Examine if there is a fraud attempt.

1012 SLEE: CORBA thread-pool overloaded

Severity

Major

Description

The CORBA thread pool utilization exceeds 80%.

What to do

Increase the CORBA thread pool size or extend the systems capacity. The thread pool size is increased through the `slee_properties.xml` file (**corba_thread_pool** attribute in the **<SLEE_PROPERTIES>** tag). Run the `SLEEConfig.sh` and restart the SLEE.

1013 SLEE: CORBA thread-pool overload - alarm ceased

Severity

Major

Description

The CORBA thread pool utilization has decreased so it is now below 78%.

What to do

-

1014 SLEE: Un-reachable listener object detected

Severity

Major

Description

The SLEE cannot reach an object that has a listener registered.

What to do

Verify that the service owning the listener is activated, that all involved SLEE processes are running, and that there is no network communication problem between the indicated SLEE's server and the server where the un-reachable object executes.

1015 SLEE: Un-reachable listener object removed

Severity

Major

Description

The SLEE has not been able to reach an un-reachable listener object during the configured retry interval and the listener has been removed.

What to do

See alarm*1014 SLEE: Un-reachable listener object detected*.

1016 SLEE: SLEE task could not be scheduled due to full task queue

Severity

Major

Description

A SLEE task could not be scheduled because the SLEE task manager queue was full.

What to do

Increase the SLEE task manager queue size or extend the system capacity. To increase the task queue, select the **SLEE** service in the Network Gatekeeper Management Tool and use commands:

getTaskManagerQueueSize

setTaskManagerQueueSize

1017 SLEE: UNHANDLED exception raised by a SLEE task

Severity

Major

Description

A SLEE task raised an UNHANDLED exception during method doTask.

What to do

Trouble report the service that raised the exception to the service supplier.

1018 SLEE: Un-reachable plug-in object removed

Severity

Major

Description

The SLEE has not been able to reach an un-reachable plug-in object during the configured retry interval and the plug-in has been removed.

What to do

Verify that the plug-in is activated, that all involved SLEE processes are running, and that there is no network communication problem between the indicated SLEE's server and the server where the un-reachable object executes.

1019 SLEE: SLEE task pool empty

Severity

Warning

Description

All threads in the SLEE task pool are currently busy.

What to do

Increase the SLEE task manager thread pool size or extend the system capacity. To increase the task manager thread pool size, select the **SLEE** service in the Network Gatekeeper Management Tool and use commands:

getTaskManagerThreadPoolSize

setTaskManagerThreadPoolSize

1020 SLEE: SLEE task pool empty - alarm ceased

Severity

Warning

Description

Threads are available in the task pool again.

What to do

-

1021 SLEE: Duplicate SLEE timer reference

Severity

Warning

Description

A scheduled timer has failed due to a duplicate timer reference.

What to do

Trouble report the service that raised the exception to the service supplier.

1022 SLEE: Database table replaced

Severity

Warning

Description

The indicated database table has been automatically replaced by the service. May occur when the service is updated and the format of the database table has been changed.

What to do

Contact BEA Support.

1023 SLEE: Database replication error

Severity

Critical

Description

The database replication has halted due to an error in the slave database.

What to do

Log in to the master database and execute the MySQL command SHOW SLAVE STATUS. Refer to the MySQL manual to correct the indicated error.

1024 SLEE: SLEE start-up in progress

Severity

Warning

Description

The indicated SLEE is starting up.

What to do

-

1025 SLEE: SLEE graceful shutdown in progress

Severity

Warning

Description

The indicated SLEE is performing a graceful shutdown.

What to do

-

1026 SLEE: Priority task manager warning level reached

Severity

Minor

Description

Priority task queue utilization level exceeds alarm level.

What to do

Decrease the number of requests sent through the system or increase the system capacity.

1027 SLEE: OAM runtime exception

Severity

Warning

Description

A service OAM method threw a RunTimeException.

What to do

Contact BEA Support and provide the trace information provided in the alarm.

1028 SLEE: Product expiring alarm

Severity

Warning

Description

This product will expire within x hours. It will then automatically shutdown.

What to do

Update the license key for the product. Contact BEA Support.

1029 SLEE: Product expired alarm

Severity

Major

Description

This product has expired, shutting down.

What to do

Update the license key for the product. Contact BEA Support.

1040 SLEE global counter: Counter handler creation failed

Severity

Major

Description

An internal error occurred when the SLEE global counter service tried to create the counter handler for handling volatile counters.

Possible reasons:

- The database is not running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in "1002 SLEE: Service data storage failed" on page 21-6.

1041 SLEE global counter: Periodic cleanup set-up at counter handler creation failed

Severity

Major

Description

Internal error setting up periodic cleanup when the slee global counter service tried to create the counter handler for handling volatile counters.

Possible reasons:

- The database is not running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in "1002 SLEE: Service data storage failed" on page 21-6.

1090 SLEE: CORBA warning received

Severity

Warning

Description

A warning message has been received from the ORB. The complete message can be read in the SLEE trace file `/usr/local/slee/bin/trace/`.

What to do

Analyse the message in the SLEE trace file and take actions accordingly. For more information, refer to section 18 *Exceptions and Error Messages* in ORBacus for C++ and Java.

1091 SLEE: CORBA alarm received

Severity

Major

Description

An alarm has been received from the ORB. The complete message can be read in the SLEE trace file `/usr/local/slee/bin/trace/`.

What to do

Analyse the message in the SLEE trace file and take actions accordingly. For more information, refer to section 18 *Exceptions and Error Messages* in ORBacus for C++ and Java.

1095 SLEE: Database master changed

Severity

Critical

Description

The database master has changed. The change was caused by a failure to create a connection with the previous database master on the indicated URL.

Possible reasons:

- The database is not running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

1096 SLEE: Database connection failed

Severity

Critical

Description

The SLEE has failed to create a connection with the database on the indicated URL.

Possible reasons:

- The database is not running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

1097 SLEE: Database low on disk space

Severity

Major

Description

The database host’s database partition is beginning to run low on available disk space.

What to do

Make more space available on the database partition of the disk. Check the size of the `ic_slee_charging`, `ic_slee_statistics`, `ic_slee_event` and `ic_slee_alarm` tables in the `slee_db` and delete unused data.

If the database uses the same partition as the SLEE, check the number trace files stored in the `/usr/local/slee/bin/trace/` directory.

When the alarm has been received, the low disk space threshold value must be changed to initiate the function again, see *List of Configuration Parameters* - “SLEE and SLEE utility services” on page B-2.

1098 SLEE: Database critically low on disk space, database engine stopped

Severity

Critical

Description

The database was stopped because the database host's database partition was running critically low on available disk space.

What to do

Clean up the file system on the host's database partition and restart the database.

As a first measure, make more space available on the database partition of the disk. Check the size of the `ic_slee_charging`, `ic_slee_statistics`, `ic_slee_event` and `ic_slee_alarm` tables in the `slee_db` and delete unused data.

If the database uses the same partition as the SLEE, check the number trace files stored in the `/usr/local/slee/bin/trace/` directory.

When the alarm has been received, the critically low disk space threshold value must be changed to initiate the function again, see *List of Configuration Parameters* - "SLEE and SLEE utility services" on page B-2.

1099 SLEE: Database partition critically low on disk space, database engine stop failed

Severity

Critical

Description

The indicated database failed to stop when the database host's database partition was running critically low on available disk space.

There is a risk that the system will keep writing data to the database even though it is running out of disk space. This may corrupt the data in the database.

What to do

Clean up the file system on the host's database partition.

As a first measure, make more space available on the database partition of the disk. Check the size of the `ic_slee_charging`, `ic_slee_statistics`, `ic_slee_event` and `ic_slee_alarm` tables in the `slee_db` and delete unused data.

If the database uses the same partition as the SLEE, check the number trace files stored in the `/usr/local/slee/bin/trace/` directory.

Investigate why it was not possible to stop the database.

When the alarm has been received, the critically low disk space threshold value must be changed to initiate the function again, see *List of Configuration Parameters* - "SLEE and SLEE utility services" on page B-2.

1100 SLEE charging: Charging data storage failed

Severity

Critical

Description

The SLEE charging service has failed to write charging data to the database.

Possible reasons:

- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in"1002 SLEE: Service data storage failed" on page 21-6.

1101 SLEE charging: Charging service initialization failed

Severity

Critical

Description

The alarm is raised if the charging service is activated before the database. That is, at installation or system restart, the database has to be started before the SLEE.

What to do

Start BEA WebLogic Network Gatekeeper database before the SLEE at system installation or restart.

1102 SLEE charging: Charging table creation failed

Severity

Critical

Description

An error occurred when trying to create the charging table in the database. The error occurs if the charging service is started before the database. That is, at installation or system restart, the database has to be started before the SLEE.

What to do

Start BEA WebLogic Network Gatekeeper database before the SLEE at system installation or restart.

1350 Time server manager: Time server connection failed

Severity

Major

Description

It was not possible to connect to the network time server through the time server manager.

What to do

Verify the time server configuration parameters, that the network time server is started, and that network time server has access to the network.

1351 Time server manager: Time synchronization failed

Severity

Major

Description

The SLEE has no connection with the network time server. Either is the network time server not running, or a network error/overload has occurred.

What to do

Make sure that the time server is running and can be reached from the SLEE.

1352 Time server manager: Time difference is too large

Severity

Major

Description

The time difference is too large.

What to do

Correct the time manually. Note that this may have influences in, for example, charging records.

1452 Plug-in manager: Request rate could not be re configured according to new node SLA

Severity

Major

Description

This alarm can only be raised if BEA Network Gatekeeper is used together with BEA WebLogic Network Gatekeeper.

The allowed request rate through the plug-in manager could not be updated according to the new node SLA.

What to do

Verify the data in the node SLA and load the SLA again.

1500 SLEE SCS manager: No SCS found

Severity

Major

Description

Found no matching SCSes.

What to do

In SCS_Manager, select **getSCSList** and check that the required SCS exists and is active. For **MESSAGING_TYPE**, check that a criteria has been added.

1501 SLEE SCS manager: SCS overload

Severity

Major

Description

All matching SCSes are overloaded.

What to do

Decrease traffic rate.

1700 SLEE backup: Snapshot backup executed OK

Severity

Warning

Description

Snapshot backup executed OK.

What to do

Refer to backup restoration procedure documentation.

1701 SLEE backup: Unable to perform backup

Severity

Critical

Description

Unable to perform backup.

What to do

Contact BEA Support.

1702 SLEE backup: Un-handled error during backup

Severity

Critical

Description

Un-handled error during backup.

What to do

Contact BEA Support, include all alarm information.

1703 SLEE backup: Unable to create master database connection

Severity

Critical

Description

Unable to perform backup, unable to create master database connection.

What to do

Contact BEA Support.

2101 ESPA messaging: Incoming message storage failed

Severity

Major

Description

The ESPA messaging service could not store an incoming message in the database.

Possible reason:

- The mailbox is not created
- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

Check mailbox

1. Start an Network Gatekeeper Management Tool and log in.
2. Select a SLEE where the ESPA messaging service is installed in the **SLEEs** pane.
3. Double-click the **ESPA_messaging** service in the **Services** pane.
4. Double-click the **listMailboxes** method.
5. Click the **Invoke** button in the **Invoke Method** window.

   The registered mailboxes are displayed in the **Messages** pane.
6. Verify that the indicated mailbox is displayed in the **Messages** pane.

   If not, create the mailbox, see section "Adding mailboxes for an application account" on page 1-20.

   Check database
7. See the *What to do* section in"1002 SLEE: Service data storage failed" on page 21-6.

2102 ESPA messaging: No incoming destination address

Severity

Minor

Description

The ESPA messaging service received an incoming message without a destination address.

What to do

Notify the originator of the message. The originators address is provided in the alarm printout.

2104 ESPA messaging: Plug-in not found

Severity

Major

Description

The ESPA messaging service could not find a messaging protocol plug-in when activated, or an outgoing message has an address format that is not supported by any messaging plug-in.

What to do

If the alarm is raised at service activation, verify that the messaging protocol plug-ins are installed and activate the messaging plug-ins before the ESPA messaging service is activated.

If the alarm is raised when a message with an unsupported address format is received, notify the originator of the message. The originators address is provided in the alarm printout.

2107 ESPA messaging: Charging data storage failed

Severity

Major

Description

The ESPA messaging service could not write charging data to the database.

Possible reasons:

- The SLEE charging service is not installed
- The SLEE charging service is installed but not activated
- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

Verify that the charging service is installed and in the state activated using the **getServices** method in the **SLEE** service. If the charging service is working properly, continue with the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

2108 ESPA messaging: Status update failed

Severity

Major

Description

The ESPA messaging service failed to change the status of a message stored in the database.

Possible reason:

- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

2110 ESPA messaging: No outgoing originating address

Severity

Major

Description

The ESPA messaging service received an outgoing message without an originating address. That is, the message will not be sent because it cannot be charged and not be replied to.

What to do

Notify the enterprise operator.

2111 ESPA messaging: No outgoing destination address

Severity

Major

Description

The ESPA messaging service received an outgoing message without a destination address.

What to do

Notify the enterprise operator.

2112 ESPA messaging: Message not found in database

Severity

Minor

Description

The ESPA messaging service could not find a message with the specified ID in the database. The connection with the database is broken.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

2113 ESPA messaging: Message status update failed

Severity

Minor

Description

The ESPA messaging service could not find a message with the specified ID in the database. The message has been deleted from the database before the status update notification has been received.

What to do

The problem is resolved by the system.

2114 ESPA messaging: Mailbox not found

Severity

Warning

Description

The ESPA messaging service could not find a mailbox for the received message. That is, the message is addressed to BEA WebLogic Network Gatekeeper, but the actual mailbox does not exist. That is, the address of the message is faulty. The message is automatically returned to the sender with a notification.

What to do

The problem is resolved by the system.

2115ESPA messaging: Mailbox existence verification failed

Severity

Major

Description

The ESPA messaging service could not verify if the specified mailbox exists in the database. That is, the connection with the database is broken.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed”.

2118 ESPA messaging: Plug-ins severely overloaded

Severity

Major

Description

All protocol plug-ins of the requested type are severely overloaded. That is, messages cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2122 ESPA messaging: Incoming message without ID

Severity

Minor

Description

The Parlay messaging service received a message without an ID from a protocol plug-in.

What to do

The protocol plug-in that delivered the message to the messaging service is faulty.

2127 ESPA messaging: Mailbox closed due to inactivity

Severity

Warning

Description

The indicated mailbox has been closed due to inactivity. The allowed inactive time period is configurable using the **setMailboxTimeout** method in the **ESPA_messaging** service.

What to do

-

2128 ESPA messaging: Unexpected error message received

Severity

Major

Description

An unexpected error message was received from the plug-in when sending an outgoing message.

What to do

Identify the original alarm from the plug-in and take actions accordingly.

2129 ESPA messaging: Failed to make notification callback

Severity

Minor

Description

Callback to the application failed.

What to do

This alarm could occur when there are temporary network problems.

If the alarm is constantly recurring, you need to verify that the network connection to the application is functioning properly.

Verify that the application is running.

2208 ESPA call control: Database connection failed

Severity

Critical

Description

The ESPA call control service could not use the database. Possible reasons:

- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

2213 ESPA call control: Plug-in not found

Severity

Major

Description

The ESPA call control service could not find a call control protocol plug-in when activated, or a create call leg request has an address format that is not supported by any call control plug-in.

What to do

If the alarm is raised a service activation, verify that the call control protocol plug-ins are installed and activated before the ESPA call control service is activated.

If the alarm is raised when a create call leg request with an unsupported address format is received, notify the originator of the request.

2214 ESPA call control: Plug-ins severely overloaded

Severity

Warning

Description

All protocol plug-ins of the requested type are severely overloaded. That is, call set up requests cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2216 ESPA call control: routeReq timeout detected

Severity

Major

Description

The ESPA call control has issued a routeReq and no response has been received within the default timeout. The call session will be released.

What to do

-

2217 ESPA call control: release call timeout detected

Severity

Major

Description

The ESPA call control has issued a release request and no response has been received within the default timeout. The call session will be released.

What to do

-

2218 ESPA call control: Application supervision timeout detected

Severity

Major

Description

The ESPA call control has issued an eventReportReq and no response has been received within the default timeout. The call session will be released.

What to do

-

2219 ESPA call control: Failed to setup Network Initiated Call Handler Service

Severity

Major

Description

Failed to connect to the Network Initiated Call Handler Service (NICHS).

What to do

Verify that the NICHS is started and in active mode. See "SLEE and SLEE Service Operation" on page 8-1.

Note: The call control service will not be activated if it cannot connect itself to the NICHS.

2220 ESPA call control: Failed to notify application about call event

Severity

Minor

Description

Failed to notify the application of the arrival of a call-related event.

What to do

Verify that the NICHS is started and in active mode. See "SLEE and SLEE Service Operation" on page 8-1.

Note: The call control service will not be activated if it cannot connect itself to the NICHS.

2300 ESPA user location: Plug-ins severely overloaded

Severity

Warning

Description

All protocol plug-ins of the requested type are severely overloaded. That is, location requests cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2301 ESPA user location: Plug-in not found

Severity

Warning

Description

The service could not find a call control protocol plug-in when activated, or a location request has an address format that is not supported by any user location plug-in.

What to do

If the alarm is raised a service activation, verify that the user location protocol plug-ins are installed and activated before the Parlay user location service is activated.

If the alarm is raised when a location request with an unsupported address format is received, notify the originator of the request.

2302 ESPA user location: Charging data storage failed

Severity

Critical

Description

The ESPA user location service cannot write charging data to the database.

Possible reasons:

- The SLEE charging service is not installed
- The SLEE charging service is installed but not activated

- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

Verify that the charging service is installed and in the state activated. If the charging service is working properly, continue with the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

2309 ESPA user location: Periodic location report delivery failed

Severity

Minor

Description

A periodic location report delivery failed because the client was un-reachable.

What to do

It is up to the client to request a new location request.

2400 ESPA user status: Plug-ins severely overloaded

Severity

Warning

Description

All protocol plug-ins of the requested type are severely overloaded. That is, status requests cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2401 ESPA user status: Plug-in not found

Severity

Warning

Description

The ESPA user status service could not find a user status protocol plug-in when activated, or a status request has an address format that is not supported by any user status plug-in.

What to do

If the alarm is raised a service activation, verify that the user status protocol plug-ins are installed and activated before the ESPA user status service is activated.

If the alarm is raised when a status request with an unsupported address format is received, notify the originator of the request.

2402 ESPA user status: Charging data storage failed

Severity

Critical

Description

The Parlay user status service cannot write charging data to the database.

Possible reasons:

- The SLEE charging service is not installed
- The SLEE charging service is installed but not activated

- Neither the master nor slave database is running
- There is a network communication problem between the SLEE and the databases.

What to do

Verify that the charging service is installed and in the state activated. If the charging service is working properly, continue with the *What to do* section in"1002 SLEE: Service data storage failed" on page 21-6.

.

2502 ESPA charging: Plug-ins severely overloaded

Severity

Warning

Description

All protocol plug-ins of the requested type are severely overloaded. That is, charging requests cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2503 ESPA charging: Plug-in not found

Severity

Warning

Description

The ESPA charging service could not find a charging protocol plug-in when activated, or a charging request has an address format that is not supported by any charging plug-in.

What to do

If the alarm is raised a service activation, verify that the charging protocol plug-ins are installed and activated before the ESPA charging service is activated.

If the alarm is raised when a charging request with an unsupported address format is received, notify the originator of the request.

2602 ESPA user interaction: Plug-ins severely overloaded

Severity

Warning

Description

All protocol plug-ins of the requested type are severely overloaded. That is, user interaction requests cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2603 ESPA user interaction: Plug-in not found

Severity

Warning

Description

The ESPA user interaction service could not find a user interaction protocol plug-in when activated, or a user interaction request has an address format that is not supported by any user interaction plug-in.

What to do

If the alarm is raised a service activation, verify that the user interaction protocol plug-ins are installed and activated before the ESPA user interaction service is activated.

If the alarm is raised when an interaction request with an unsupported address format is received, notify the originator of the request.

2605 ESPA user interaction: Found no matching request or notification

Severity

Warning

Description

Found no enabled notification or outstanding sendInfoAndCollect-request matching the arrived message properties. The message will be discarded.

What to do

-

2606 ESPA user interaction: Failed to report notification

Severity

Minor

Description

Failed to notify an application of an network initiated UI-event.

What to do

This alarm could occur when there are temporary network problems.

If the alarm is constantly recurring, you need to verify that the network connection to the application is functioning properly.

Verify that the application is running.

2607 ESPA user interaction: Failed to log charging info

Severity

Major

Description

Failed to log charging info in charging database.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

2608 ESPA user interaction: Delete old request

Severity

Warning

Description

Because of a collision with the primary key in the database an unanswered sendInfoAndCollectRequest was deleted.

What to do

This alarm can be disregarded if it occurs seldom.

If the alarm is constantly recurring, you may need to change the **Sequence number range end ID** parameter, through the **Plugin_messaging_SMPP_SMS** service management interface, see “List of Configuration Parameters” on page B-1.

2609 ESPA user interaction: Message with no destination address

Severity

Warning

Description

A message arrived with no destination address set. The message will be discarded.

What to do

-

2702 ESPA subscriber profile: Plug-ins severely overloaded

Severity

Warning

Description

All protocol plug-ins of the requested type are severely overloaded. That is, subscriber profile requests cannot be sent to the network.

What to do

Install a new instance of the requested protocol plug-in in a server with lower load level. If all servers are running with high load level, it is time to expand the system with more servers. Contact BEA Support.

2703 ESPA subscriber profile: Plug-in not found

Severity

Warning

Description

The ESPA user interaction service could not find a subscriber profile protocol plug-in when activated, or a subscriber profile request has an address format that is not supported by any subscriber profile plug-in.

What to do

If the alarm is raised a service activation, verify that the user profile protocol plug-ins are installed and activated before the ESPA user profile service is activated.

If the alarm is raised when an subscriber profile request with an unsupported address format is received, notify the originator of the request.

2802 Network initiated call handler: No service registered

Severity

Major

Description

No service registered.

What to do

Check that there are call control capabilities installed in the system, that is, multiparty call control (mpcc) and generic call control (gcc) and that the corresponding services are running.

2803 Network initiated call handler: No enabled notification for event

Severity

Major

Description

Received event in interrupt mode with no matching enabled notification request in mode interrupt. Policy service will take control of call.

What to do

Check the enabled notifications (listNotification in gccs and/or mpccs in modules) and verify that they are consistent with the expected client notification state.

2805 Network initiated call handler: Overload

Severity

Major

Description

Service is severely overloaded.

What to do

Decrease traffic.

2806 Network initiated call handler: Unknown error

Severity

Major

Description

Unexpected error.

What to do

Contact BEA Support.

2807 Network initiated call handler: Suspend error

Severity

Major

Description

The service is suspended and cannot process any events.

What to do

Use Network Gatekeeper Management Tool to resume it, see "Changing SLEE state" on page 8-8.

3001 Policy service: Parsing of retraction rule file failed

Severity

Major

Description

The rule engine cannot parse the rule file that retracts all not service-specific objects from the context.

What to do

Verify that the rule file exists.

Verify that the syntax in the rule file is correct. See the log file for the policy service (`policy.log`) for information on the error.

3002 Policy service: Parsing of service-specific rule file failed

Severity

Major

Description

The rule engine cannot parse the service-specific rule file.

What to do

Verify that the rule file exists and that the path to the rule is correct.

Verify that the syntax in the rule file is correct. See the log file for the policy service (`policy.log`) for information on the error.

3005 Policy service: Parsing of service-specific rule file failed at load time

Severity

Major

Description

The policy service cannot parse the service-specific rule file when it is about to be loaded into the database. Probably this is a syntax error in the rule file.

What to do

Verify that the rule file exists and that the path to the rule file is correct.

Verify that the syntax in the rule file is correct. See the log file for the policy service (`policy.log`) for information on the error.

3006 Policy service: Alarm raised from policy rule

Severity

Minor

Description

Failed to match whitelist for service provider.

What to do

Verify that the specified whitelist exists in the **SLEE.list.matcher** service.

3007 Policy service: Denial of service request

Severity

Minor

Description

The policy service denied a service request.

What to do

-

3008 Policy service: Failed to parse node rule file

Severity

Major

Description

Failed to parse node rule file.

What to do

Verify that the node rule file exists and that the path to the node rule file is correct.

Verify that the syntax in the node rule file is correct. See the log file for the policy service (`policy.log`) for information on the error.

3100 Policy service: Total request rate warning level reached

Severity

Minor

Description

The total request rate from WebLogic Network Gatekeeper towards a network node has reached the warning level (default 80%).

What to do

Check the global contract data for the node in the total traffic SLA.

Investigate if it is possible to get access to more capacity in the network node. If that's not possible, decrease the allowed request rate towards the network node in one or more of the service provider traffic SLAs.

3110 Policy service: Total request rate exceeded

Severity

Major

Description

The total request rate from WebLogic Network Gatekeeper towards a network node has exceeded the maximum allowed level defined in the total traffic SLA.

What to do

See alarm "3100 Policy service: Total request rate warning level reached" on page 21-51.

3200 Policy service: Service provider request rate warning level reached

Severity

Minor

Description

The request rate from a specific service provider towards a network node reached the warning level (default 80%).

What to do

Check the node contract data in the service provider traffic SLA.

Consider upgrading the service provider. That is, move the service provider to a service provider group with a SP traffic SLA allowing a higher request rate towards the node.

3210 Policy service: Service provider request rate exceeded

Severity

Major

Description

The request rate for a specific service provider towards a node exceeded the maximum allowed level for that service provider.

What to do

See alarm "3200 Policy service: Service provider request rate warning level reached" on page 21-52.

3300 Policy service: No valid global contract in the Total traffic SLA

Severity

Major

Description

No valid global contract for the node is found in the total traffic SLA.

What to do

Add a valid global contract in the total traffic SLA.

For updating the total traffic SLA, see "Updating the total traffic SLA" on page 6-5.

3310 Policy service: No node contract in the Service Provider traffic SLA

Severity

Minor

Description

No node contract for the node found in the service provider traffic SLA.

What to do

Add a valid node contract in the service provider traffic SLA.

For updating the service provider traffic SLA, see "Updating a service provider traffic SLA" on page 6-3.

5401 Plug-in messaging-SMPP: Plug-in registration failed

Severity

Major

Description

The protocol plug-in failed to register itself in the plug-in manager. The alarm occurs if the plug-in manager is not installed or if it is not in active state.

What to do

Verify that the plug-in manager is active and restart the plug-in.

5403 Plug-in messaging-SMPP: Message sending failed

Severity

Major

Description

The protocol plug-in failed to send the short message to the SMSC.

What to do

Verify the physical connection with the SMSC and that the plug-in is configured properly.

5404 Plug-in messaging-SMPP: Plug-in removal failed

Severity

Major

Description

The protocol plug-in failed to unregister itself from the plug-in manager. The alarm occurs if the plug-in manager is not in active state.

What to do

Verify that the plug-in manager is active and restart the plug-in.

5405 Plug-in messaging-SMPP: Listener notification failed

Severity

Major

Description

The plug-in failed to notify a listener of the result when sending or receiving a message.

What to do

Verify that the generic messaging SCS proxy (**Parlay_messaging** service) owning the listener object is active, that all SLEE processes are running, and that there are no network communication problems between the SLEEs.

5409 Plug-in messaging-SMPP: SMSC transmitter connection established

Severity

Warning

Description

The plug-in has established a connection to the SMSC.

What to do

-

5410 Plug-in messaging-SMPP: SMSC transmitter reconnect procedure timeout

Severity

Warning

Description

The plug-in has failed to reconnect to the SMSC during the configured duration and terminates the reconnection procedure.

What to do

Verify the network connection. Restart the reconnection procedure using the **resetSMPPConnection** method in the **Plugin_messaging_SMPP** service.

5411 Plug-in messaging-SMPP: SMSC transmitter reconnect attempt failed

Severity

Warning

Description

A reconnection attempt in the reconnection procedure has failed.

What to do

The plug-in will keep on trying to connect until it succeeds or until the reconnection procedure times out.

5412 Plug-in messaging-SMPP: SMSC receiver connection lost

Severity

Warning

Description

The plug-in has lost connection with the SMSC.

What to do

Make sure the network connection to the SMSC is working properly.

The plug-in will automatically try to reconnect to the SMSC again. The total reconnection procedure duration and the interval between individual reconnection attempts depends on configuration settings in the **Plugin_messaging_SMPP** service.

5413 Plug-in messaging-SMPP: SMSC receiver connection established

Severity

Warning

Description

The plug-in has established a connection to the SMSC.

What to do

-

5415 Plug-in messaging-SMPP: SMSC receiver reconnect procedure timeout

Severity

Warning

Description

The plug-in has failed to reconnect to the SMSC during the configured duration and terminates the reconnection procedure.

What to do

Verify the network connection. Restart the reconnection procedure using the **resetSMPPConnection** method in the **Plugin_messaging_SMPP** service.

5416 Plug-in messaging-SMPP: SMSC receiver reconnect attempt failed

Severity

Warning

Description

A reconnection attempt in the reconnection procedure has failed.

What to do

The plug-in will keep on trying to connect until it succeeds or until the reconnection procedure times out.

5417 Plug-in messaging-SMPP: Storing message data in database failed

Severity

Major

Description

The plug-in failed to store message data in the database.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

5418 Plug-in messaging-SMPP: Updating message delivery status in database failed

Severity

Major

Description

The plug-in failed to the message delivery status in the database.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

5419 Plug-in messaging-SMPP: Message delivery processing in database failed

Severity

Major

Description

The plug-in failed to store message data in the database.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

5420 Plug-in messaging-SMPP: No listener available for incoming message

Severity

Major

Description

No registered listener was found for the incoming message. The plug-in was unable to deliver the incoming message.

What to do

Verify that the generic messaging SCS proxy (**Parlay_messaging** service) owning the listener object is active, that all SLEE processes are running, and that there are no network communication problems between the SLEEs.

5421 Plug-in messaging-SMPP: SMSC transmitter connection lost

Severity

Warning

Description

The plug-in has lost connection with the SMSC. That is, it failed to send a heartbeat to the SMSC.

What to do

Make sure the network connection to the SMSC is working properly.

The plug-in will automatically try to reconnect to the SMSC again. The total reconnection procedure duration and the interval between individual reconnection attempts depends on configuration settings in the **Plugin_messaging_SMPP** service.

5502 Plug-in user location-MPP: Failed to create provider

Severity

Major

Description

The plug-in failed to connect to the MPC node.

What to do

Verify that the MPC node is running.

Verify that the configuration parameters are correct, see "User location/MPS" on page B-38.

5503 Plug-in user location-MPP: Plug-in registration failed

Severity

Major

Description

The protocol plug-in failed to register itself in the plug-in manager. The alarm occurs if the plug-in manager is not installed or if it is not in active state.

What to do

Verify that the plug-in manager is installed and activated.

5505 Plug-in user location-MPP: Removal failed

Severity

Major

Description

The protocol plug-in failed to unregister itself from the plug-in manager. The alarm occurs if the plug-in manager is not in active state.

What to do

Verify that the plug-in manager is activated.

5506 Plug-in user location-MPP: Connection established

Severity

Warning

Description

The plug-in established connection to the MPC Node.

What to do

-

5507 Plug-in user location-MPP: Reconnection procedure ended

Severity

Warning

Description

The plug-in stopped trying to connect to the MPC Node.

What to do

Restart the reconnection procedure.

Also, see "5502 Plug-in user location-MPP: Failed to create provider" on page 21-61.

5602 Plug-in user status-MPP: Failed to create provider

Severity

Major

Description

The plug-in failed to connect to the MPC node.

What to do

Verify that the MPC node is running.

Verify that the configuration parameters are correct, see "User location/MPS" on page B-38.

5603 Plug-in user status-MPP: Registration failed

Severity

Major

Description

The protocol plug-in failed to register itself in the plug-in manager. The alarm occurs if the plug-in manager is not installed or if it is not in active state.

What to do

Verify that the plug-in manager is installed and activated.

5605 Plug-in user status-MPP: Removal failed

Severity

Major

Description

The protocol plug-in failed to unregister itself from the plug-in manager. The alarm occurs if the plug-in manager is not in active state.

What to do

Verify that the plug-in manager is activated.

5606 Plug-in user status-MPP: Connection established

Severity

Warning

Description

The plug-in established connection to the MPC Node.

What to do

-

5607 Plug-in user status-MPP: Reconnection procedure ended

Severity

Warning

Description

The plug-in stopped trying to connect to MPC node.

What to do

Restart the reconnection procedure.

Verify that the MPC node is running.

Verify that the configuration parameters are correct, see "User location/MPS" on page B-38.

5700 Plug-in messaging-CIMD: SMSC login failed

Severity

Major

Description

The protocol plug-in failed to log in to the SMSC due to a faulty user name and/or password.

What to do

Verify the registered SMSC login parameters with the SMSC responsible.

5701 Plug-in messaging-CIMD: SMSC login succeeded

Severity

Minor

Description

The protocol plug-in has successfully logged in to the SMSC.

What to do

-

5702 Plug-in messaging-CIMD: SMS delivery failed

Severity

Minor

Description

No messaging SCS proxy could be obtained for SMS delivery.

What to do

Verify that messaging SCS proxies are installed in the system and that they are activated.

5703 Plug-in messaging-CIMD: SMSC connection failed

Severity

Major

Description

The protocol plug-in failed to connect to the SMSC.

What to do

Verify the SMSC addressing parameters registered in the plug-in and the SMSCes status with the SMSC responsible.

5704 Plug-in messaging-CIMD: Login request sending failed

Severity

Major

Description

The protocol plug-in failed to send the Login request to the SMSC.

What to do

Verify the SMSC addressing parameters registered in the plug-in and the SMSCes status.

5705 Plug-in messaging-CIMD: Plug-in not connected to SMSC

Severity

Major

Description

The protocol plug-in has detected that it is not connected to the SMSC. The alarm is raised at plug-in start up or if the connection is lost.

What to do

If the alarm is raised at startup, it will automatically cease then the connection is successfully established.

If the alarm is raised during operation, the plug-in will try to re-establish the connection during the specified reconnection time. If this is successful the alarm will cease. Otherwise, the status of the SMSC has to be verified and the connection has to be manually restored through the plug-in's reconnect OAM method.

Alarm 5706 is received as an acknowledgment on the successful connection in all the above cases.

5706 Plug-in messaging-CIMD: Plug-in connected to SMSC

Severity

Minor

Description

The protocol plug-in has successfully connected to the SMSC.

What to do

-

5707 Plug-in messaging-CIMD: Exception when notifying listener

Severity

Major

Description

Failed to notify listener.

What to do

Verify that the SCS ESPA is running.

5708 Plug-in messaging-CIMD: Exception when adding data to database

Severity

Major

Description

Failed to add data to message info database.

What to do

Verify that the database is running.

5710 Plug-in messaging-CIMD: CIMD protocol error in submit response

Severity

Major

Description

Parameter pair mismatch for destination addresses and service center timestamps.

What to do

Report protocol error to SMSC vendor.

5801 Plug-in messaging-MM7: Unable to create SOAP sender

Severity

Major

Description

The protocol plug-in plug-in could not create a SOAP sender.

What to do

Verify the MMSC addressing parameters registered in the plug-in.

5802 Plug-in messaging-MM7: No stored message ID matched message ID in received delivery report

Severity

Major

Description

The protocol plug-in has received a delivery report from the MMSC that could not be be associated with a message ID of previously sent message.

What to do

-

5803 Plug-in messaging-MM7: No message ID contained in received delivery report

Severity

Major

Description

The protocol plug-in has received a delivery report from the MMSC without a message ID.

What to do

-

5804 Plug-in messaging-MM7: Plug-in unable to parse delivery report request

Severity

Major

Description

The protocol plug-in has received a delivery report request from the MMSC that could not be parsed.

What to do

-

5805 Plug-in messaging-MM7: Plug-in unable to parse delivery request

Severity

Major

Description

The protocol plug-in has received a deliver request from the MMSC that could not be parsed.

What to do

-

5806 Plug-in messaging-MM7: No recipient address found in deliver request

Severity

Major

Description

The protocol plug-in could not find a recipient address in a deliver request received from the MMSC.

What to do

-

5807 Plug-in messaging-MM7: Unrecognised address type in deliver request

Severity

Major

Description

The protocol plug-in could not recognise the address type in a deliver request received from the MMSC.

What to do

-

5808 Plug-in messaging-MM7: SOAP request parsing error

Severity

Warning

Description

The protocol plug-in has detected an error when parsing a SOAP request from the MMSC.

What to do

-

5809 Plug-in messaging-MM7: SOAP request handling error

Severity

Major

Description

The SOAP engine has reported that it failed to handle a SOAP request from the MMSC.

What to do

-

5810 Plug-in messaging-MM7: Retrieving simple content data from SOAP message failed

Severity

Warning

Description

The protocol plug-in failed to retrieve a content/attachment data of a MIME simple type from a SOAP message because the data was corrupt.

What to do

-

5811 Plug-in messaging-MM7: Retrieving multiparty content data from SOAP message failed

Severity

Warning

Description

The protocol plug-in failed to retrieve a content/attachment data of a MIME multiparty type from a SOAP message because the data was corrupt.

What to do

-

5812 Plug-in messaging-MM7: SOAP request sending failed

Severity

Major

Description

There was an error trying to send a SOAP request.

What to do

-

5813 Plug-in messaging-MM7: Listener notification failed

Severity

Major

Description

There was an error trying to notify a plug-in listener.

What to do

-

5814 Plug-in messaging-MM7: MM7 server connection lost

Severity

Major

Description

An error was encountered when checking the remote MM7 server using heartbeats. The plug-in has been deactivated.

What to do

Make sure there are no network problems.

5815 Plug-in messaging-MM7: MM7 server connection established

Severity

Major

Description

The connection with the remote MM7 server is OK again and the plug-in has been activated again.

What to do

-

5900 Plug-in messaging-MLP: Reading or writing configuration data failed

Severity

Major

Description

The protocol plug-in failed to read or write configuration data to the database.

What to do

See the *What to do* section in“1002 SLEE: Service data storage failed” on page 21-6.

5902 Plug-in messaging-MLP: Request sending error

Severity

Major

Description

The protocol plug-in failed to send a request to the MLP server.

What to do

Verify the network connection and the MLP server connection data configured in the plug-in.

5903 Plug-in messaging-MLP: Response retrieving error

Severity

Major

Description

The protocol plug-in failed to parse the XML result retrieved from the MLP server.

What to do

Verify the network connection and the MLP server connection data configured in the plug-in. Verify the MLP version used.

7001 SLEE statistics: Failed to store statistics data

Severity

Minor

Description

Failed to store statistics data.

What to do

Check the status of the database and check if the disk is full.

11100 ESPA access: User locked

Severity

Minor

Description

An ESPA user has failed to log in three times and has been locked.

What to do

Unlock the user through the ESPA access OAM interface.

11130 ESPA access: Wrong application ID

Severity

Minor

Description

The application was not allowed to log in. Tried to login with the wrong ID credentials (that is, a non existing service provider account/application account/application instance ID combination) will cause this alarm.

What to do

Make sure the application is provided with the correct ID combination. Note that this alarm may indicate an intrusion attempt.

11131 ESPA access: Wrong application password

Severity

Minor

Description

The application tried to log in with the wrong password.

What to do

Make sure the application is provided with the correct credentials. Note that this alarm may indicate an intrusion attempt.

11132 ESPA access: Locked application log in attempt

Severity

Minor

Description

The application tried to log in after being blocked. Consecutive calls to login after initial lock will cause this alarm.

What to do

Unlock the application. Make sure the application is provided with the correct credentials. Note that this alarm may indicate an intrusion attempt.

11133 ESPA access: Non active application account

Severity

Minor

Description

The application tried to log in on non active account (service provider account, application account or service instance group level).

What to do

Activate the acount on the relevant level if it should be active.

12100 SESPA access: ESPA session logged out

Severity

Minor

Description

ESPA has logged out a SESPA session (application instance) due to too many logged in application instances for the application instance group. The maximum number of concurrent logged in application instances is specified in the application instance group's SLA. The oldest session is logged out first.

What to do

If ESPA logs out active sessions, the SLA has to be re-negonitiated with the service provider. That is, the maximum number of concurrent logged in application instances in the SLA has to be increased.

If an application creates a lot of sessions that are logged out by ESPA, the application might be faulty. That is, the application does not log out un used sessions.

12101 SESPA access: ESPA session error

Severity

Warning

Description

SESPA was unable to recover an ESPA session. That is, the ESPA object was unreachable.

What to do

The application is notified and will log in again and a new session is created.

12200 SESPA user location: Application error

Severity

Minor

Description

Error occurs when invoking an application.

What to do

Check the network connection between the WebLogic Network Gatekeeper and the client.

Check that the client is not overloaded and thereby fails to respond in a timely fashion.

12300 SESPA messaging: Enable Parlay X incoming message notification failed

Severity

Warning

Description

SESPA was unable to enable the Parlay X incoming message notification for the application at restart of the server.

What to do

Manually remove the old notification and create a new notification through the SESPA messaging OAM interface. For more information on how to create a Parlay X incoming message notification, see “Creating an application instance group” on page 5-30.

12301 SESPA messaging: Parlay X incoming message notification failed

Severity

Minor

Description

SESPA was unable to notify an application that a new message is available.

What to do

Verfy that the application is up and running.

12302 SESPA messaging: Parlay X incoming message notification destroyed

Severity

Minor

Description

A Parlay X incoming message notification for an application was destroyed (disabled).

What to do

Create a new notification through the SESPA messaging OAM interface. For more information on how to create a Parlay X incoming message notification, see "Creating an application instance group" on page 5-30.

12400 SESPA messaging UI: Application error

Severity

Minor

Description

Error invoking application.

What to do

Make sure that the application is running and is accessible from the WebLogic Network Gatekeeper.

12401 SESPA messaging UI: Notification error

Severity

Warning

Description

Failed to re-enable notification after service restart.

What to do

The application must manually enable this notification.

12500 SESPA user status: Application error

Severity

Minor

Description

Error invoking application.

What to do

Make sure that the application is running and is accessible from the WebLogic Network Gatekeeper.

12600 SESPA call UI: Application error

Severity

Minor

Description

Error invoking application.

What to do

Make sure that the application is running and is accessible from the WebLogic Network Gatekeeper.

12800 SESPA call control: Notification error

Severity

Warning

Description

Failed to re-enable notification after service restart.

What to do

The application must manually enable this notification.

12801 SESPA call control: Application error

Severity

Minor

Description

Error invoking application.

What to do

Make sure that the application is running and is accessible from the WebLogic Network Gatekeeper.

12900 SESPA subscriber profile: Application error

Severity

Minor

Description

Error invoking application.

What to do

Make sure that the application is running and is accessible from the WebLogic Network Gatekeeper.

22000 Plug-in OSA access: OSA gateway authentication failed

Severity

Major

Description

The OSA access plug-in failed to authenticate with the OSA gateway.

What to do

Verify the OSA gateway connection data registered in "OSA Gateway Connection" on page 7-1 with the OSA gateway operator. Verify that the user certificate is still valid.

22001 Plug-in OSA access: OSA gateway service manager unreachable

Severity

Major

Description

The OSA manager object obtained from the OSA gateway is considered dead. Might be a network problem.

What to do

The OSA gateway plug-in will automatically try to authenticate the OSA gateway at next service request.

22002 Plug-in OSA access: OSA gateway unreachable

Severity

Major

Description

The OSA access plug-in could not reach any of the connected OSA gateways (OSA frameworks) defined. Might be a network problem.

What to do

Verify the network connection.

22003 Plug-in OSA access: No mapping available

Severity

Major

Description

The application requesting a service from the OSA gateway does not have a valid mapping towards the requested OSA service.

What to do

Verify the current mapping. If no mapping exists, create a mapping according to "Connecting an application (account) to an OSA/Parlay gateway" on page 5-20.

22004 Plug-in OSA access: Internal error

Severity

Major

Description

An unexpected internal error has occurred.

What to do

Contact BEA Support.

22101 Plug-in generic UI-HOSA: Message delivery failed - undefined

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_UNDEFINED.

What to do

Contact the HOSA gateway owner.

22102 Plug-in generic UI-HOSA: Message delivery failed - illegal info

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_ILLEGAL_INFO.

What to do

Contact the HOSA gateway owner.

22103 Plug-in generic UI-HOSA: Message delivery failed - ID not found

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_ID_NOT_FOUND.

What to do

Contact the HOSA gateway owner.

22104 Plug-in generic UI-HOSA: Message delivery failed - resource unavailable

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_RESOURCE_
UNAVAILABLE.

What to do

Contact the HOSA gateway owner.

22105 Plug-in generic UI-HOSA: Message delivery failed - illegal range

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_ILLEGAL_RANGE.

What to do

Contact the HOSA gateway owner.

22106 Plug-in generic UI-HOSA: Message delivery failed - improper user response

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_IMPROPER_USER_ RESPONSE.

What to do

Contact the HOSA gateway owner.

22107 Plug-in generic UI-HOSA: Message delivery failed - abandon

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_ABANDON.

What to do

Contact the HOSA gateway owner.

22108 Plug-in generic UI-HOSA: Message delivery failed - no operation active

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_NO_OPERATION_
ACTIVE.

What to do

Contact the HOSA gateway owner.

22109 Plug-in generic UI-HOSA: Message delivery failed - no space available

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_NO_SPACE_AVAILABLE.

What to do

Contact the HOSA gateway owner.

22110 Plug-in generic UI-HOSA: Message delivery failed - resource timeout

Severity

Minor

Description

The HOSA gateway failed to deliver one or more SMSes. The following error message was provided by the HOSA gateway P_UI_ERROR_RESOURCE_TIMEOUT.

What to do

Contact the HOSA gateway owner.

22200 Plug-in OSA MPCC: Internal callback error

Severity

Minor

Description

Callback communication between OSA MPCC plug-in and ESPA (internally in the WebLogic Network Gatekeeper) failed.

What to do

Contact BEA Support.

22201 Plug-in OSA MPCC: OSA error

Severity

Minor

Description

Communication between the plug-in and OSA gateway failed.

What to do

Check the OSA gateway logs to determine what caused the error.

22400 Plug-in OSA call UI: Internal callback error

Severity

Minor

Description

Callback communication between OSA call UI plug-in and ESPA (internally in the WebLogic Network Gatekeeper) failed.

What to do

Contact BEA Support.

22401 Plug-in OSA call UI: OSA error

Severity

Minor

Description

Communication between the plug-in and OSA gateway failed.

What to do

Check the OSA gateway logs to determine what caused the error.

95001 Subscription handler: Subscriber profile plug-in retrieval failed

Severity

Minor

Description

The subscription handler could not find a subscriber profile plug-in when trying to access the subscriber profile database.

What to do

Verify that an active subscriber profile plug-in is available.

95002 Subscription handler: Subscriber profile retrieval failed

Severity

Minor

Description

The subscription handler received an exception when trying to retrieve the subscriber profile for the specified subscriber. Possible cause could be that the subscriber does not have a subscriber profile specified.

What to do

Verify that the subscriber profile exists. Check for alarms from the subscriber profile plug-in.

95003 Subscription handler: Exception received when trying to write subscription data

Severity

Minor

Description

The subscription handler received an exception when trying to write subscription data to the specified subscriber's subscriber profile.

What to do

Make sure the correct database username and password combination is defined in the plug-in. Check the load on the subscriber profile database server.

Check for alarms from the subscriber profile plug-in to get more information.

95004 Subscription handler: Writing subscription data failed

Severity

Minor

Description

A set error was reported by the subscriber profile plug-in or the set request timed out when trying to write subscription data to the specified subscriber's subscriber profile.

What to do

Make sure the correct database username and password combination is defined in the plug-in. Check the load on the subscriber profile database server.

Check for alarms from the subscriber profile plug-in to get more information.

95005 Subscription handler: Exception received when trying to read subscription data

Severity

Minor

Description

An exception occurred when trying to read subscription data from the specified subscriber's subscriber profile.

What to do

Make sure the correct database username and password combination is defined in the plug-in. Check the load on the subscriber profile database server.

Check for alarms from the subscriber profile plug-in to get more information.

95006 Subscription handler: Exception received when verifying a subscription

Severity

Minor

Description

An exception occurred when trying to verify if the specified subscriber has a subscription to the specified application.

What to do

Make sure the correct database username and password combination is defined in the plug-in. Check the load on the subscriber profile database server.

Check for alarms from the subscriber profile plug-in to get more information.

95007 Subscription handler: Reading subscription data failed

Severity

Minor

Description

A get error was reported by the subscriber profile plug-in or the get request timed out when trying to read subscription data from the specified subscriber's subscriber profile.

What to do

Make sure the correct database username and password combination is defined in the plug-in. Check the load on the subscriber profile database server.

Check for alarms from the subscriber profile plug-in to get more information.

CHAPTER 22

System Upgrade

How to upgrade your current system to a new version is dependant on the version you are upgrading to. Version specific instructions are provided by BEA when ordering the new version.

Individual SLEE services can be upgraded in run-time.

To upgrade a SLEE, that specific SLEE has to be shutdown and the SLEE agent must be stopped.

If patches to the current version are provided, instructions on how to install the patch are provided with the patch.

Directory Structure and Contents

The following sections describe the contents of a WebLogic Network Gatekeeper installation:

- "Installation CD" on page A-2
- "Installed system" on page A-3

Installation CD

Structure

The directory structure in Table 22-1 is found on the WebLogic Network Gatekeeper CD-ROM.

Table 22-1 BEA WebLogic Network Gatekeeper CD-ROM directory structure

/	wng/	wng10_hpux.tar.crypt
		wng10_linux.zip
	wng_dev/	wng10_dev.zip

Contents

A brief introduction to the contents of each directory is given below.

- `/wng/wng10_hpux.tar.crypt`

  Contains installation files for WebLogic Network Gatekeeper for HP-UX. It also includes installation files for WebLogic Network Gatekeeper Management Tool for Windows, HP-UX, and Linux.

- `/wng/wng10_linux.zip`

  Contains installation files for WebLogic Network Gatekeeper for Linux. It also includes installation files for WebLogic Network Gatekeeper Management Tool for Windows, HP-UX, and Linux.

- `/wng_dev/wng10_dev.zip`

  Contains installation files for WebLogic Workshop Controls for WebLogic Network Gatekeeper for Windows 2000/XP, installation files for WebLogic Network Gatekeeper Application test environment for Windows2000/XP, and WSDL files for the Web Services interfaces.

Installed system

Structure

At a standard Unix installation, the directory structure in Table 22-2 is created.

Table 22-2 BEA WebLogic Network Gatekeeper Unix Directory Structure

/					
	usr/	local/			
			slee/	bin/	_autoslee
					autosrv
					policy
					services
					trace
				lib	
				servlet_engine	

Contents

A brief introduction to the contents of each directory is given below. For information of which directories to backup at a system backup, see "About system backup" on page 20-2.

- `/usr/local/slee/`

  Contains all directories and files related to BEA WebLogic Network Gatekeeper SLEE.

- `/usr/local/slee/bin/`

  Contains start up scripts and reference files for the name service, repository, and trading service.

- `/usr/local/slee/bin/_autoslee/`

  Contains the jar files of the SLEE utility services.

- `/usr/local/slee/bin/autosrv/`

Contains the jar files of the SLEE services (except the SLEE utility services) that will be automatically started when the SLEE is started or restarted.

- `/usr/local/slee/bin/policy/`

  Contains the policy rule files and a template for writing SLAs.

- `/usr/local/slee/bin/services/`

  The directory where SLEE services will be stored when they are installed in the SLEE. That is, the services working directory.

- `/usr/local/slee/bin/trace/`

  Contains the trace files generated by the trace service.

- `/usr/local/slee/lib/`

  Contains BEA WebLogic Network Gatekeeper executables other than SLEE services. For example the SLEE itself.

- `/usr/local/slee/servlet_engine/`

  Contains all directories and files related to the Tomcat servlet engine.

List of Configuration Parameters

The following sections provide a reference for WebLogic Network Gatekeeper configuration paramters:

- "SLEE and SLEE utility services" on page B-2
- "SLEE start-up parameters" on page B-9
- "SESPA" on page B-13
- "ESPA access and ESPA service capability modules" on page B-15
- "Plug-in manager" on page B-24

SLEE and SLEE utility services

The **Level** column in the tables below indicate how the parameter value is distributed among the SLEE service instances in the system. When **Level** is defined as Node, the value is distributed to all SLEEs in the system where the service is installed. If defined as SLEE, the value is set for the service instance in the current SLEE only.

SLEE

The following configuration parameters can be changed through the **SLEE** service management interface:

Parameter	**Level**	**Description**
Database diskspace warning threshold	SLEE	Specifies a threshold value that raises a warning if the database partition is running out of free diskspace. The threshold value specifies the lowest amount of free diskspace (in kilobyte) allowed before the warning is raises. Default is 1GB (1 000 000 kb).
Database shutdown threshold	SLEE	Specifies a threshold value that initiates a database shutdown if the database partition is running out of free diskspace. The threshold value specifies the lowest amount of free diskspace (in kilobyte) allowed before the shutdown is initiated. Default is 1GB (1 000 000 kb).
Database diskspace monitor interval	SLEE	Specifies the database diskpace monitor interval (in seconds).
Resource sharing context • Name • ORB port • No. of ORB threads • No. of SLEE task threads • SLEE task queue size	SLEE	Specifies data to be used for a resource sharing context. That is, a number of SLEE service sharing a dedicated set of system capacity.
Task manager queue size	SLEE	Specifies at what level (in number task in the queue) the SLEE should be considered to have 100% load.

Parameter	Level	Description
Task manager thread pool size	SLEE	Specifies the number of possible simultaneous JAVA threads in the SLEE and the SLEE services.
Zombie object supervision interval	SLEE	Specifies the time (in seconds) between object supervision heartbeats. The heartbeats are sent to non-responding objects (zombies).
Zombie object supervision timeout	SLEE	Specifies the period (in seconds) heartbeats are sent to non-responding objects before they are assumed dead. That is, the object reference is removed.

Alarm service

The following configuration parameters can be changed through the **SLEE_alarm** service management interface:

Parameter	Level	Description
Alarm broadcast interval	SLEE	Specifies the time interval (in seconds) between alarm broadcasts for the AlarmListenerExt interface listeners
Alarm log filter level	SLEE	Specifies which alarms are logged in the alarm list. The active filter level is represented with a digit according the table below: 1 - all alarms are logged in the alarm list 2 - minor, major and critical are logged 3 - major and critical alarms are logged 4 - only critical alarms are logged

Backup service

The following configuration parameters can be changed through the **SLEE_backup** service management interface:

Parameter	Level	Description
Backup path	SLEE	Specifies the path to the directory where the database backup will be stored.
Database path	SLEE	Specifies the path to the database.
Local database address	SLEE	Specifies the local database address (IP and port). Example: 192.168.1.4:3306
Remote database address	SLEE	Specifies the remote database address (IP and port). Example: 192.168.1.6:3306
SLEE path	SLEE	Specifies the SLEE home directory.

Charging service

The following configuration parameters can be changed through the **SLEE_charging** service management interface:

Parameter	Level	Description
Charging filter	Node	Specifies, for each SCS proxy, based on transaction result which transactions should be stored in the charging database. Possible values for each transaction result: • Completed (true/false) • Partial (true/false) • Failed (true/false)

Event service

The following configuration parameters can be changed through the **SLEE_event** service management interface:

Parameter	Level	Description
Event log filter level	SLEE	Specifies which events are written to the event log. The active filter level is represented with a digit according the table below: 1 - all events are logged 2 - medium and high importance are logged 3 - only high importance events are logged

Service capability manager

The following configuration parameters can be changed through the **SC_manager** service management interface:

Parameter	Level	Description
Service capability manager IOR	Node	Specifies the service capability manager's IOR to be user by the external protocol adapters (external plug-ins).
Criteria	Node	Specifies to which type of service capability an incoming message shall be routed. The routing is based on the destination address of the incoming message. Note, criteria definition is only needed for service capabilities of type MESSAGING_TYPE. • SCS type: MESSAGING_TYPE • SCS properties: SUBTYPE GUI (for ESPA_messaging_userinteraction) or SUBTYPE GMS (for ESPA_messaging) • Criteria: A regular expression for the destination address. For example ^[0-5].* matching all destination addresses starting with 0, 1, 2, 3, 4 or 5. Note, the destination address expressions must match the addresses that are used for mailboxes in ESPA_messaging and instance number ranges in ESPA_messaging_userinteraction.)

Servlet installer

The following configuration parameters can be changed through the **Servlet_installer** service management interface:

Parameter	Level	Description
Servlet installation directory	Node	Specifies the path to the directory where servlets are installed.

SNMP

The following configuration parameters can be changed through the **SLEE_snmp** service management interface:

Parameter	Level	Description
Community	Node	Specifies the snmp community string. Default value: private
Enterprise object identifier	Node	Specifies the object ID for BEA WebLogic Network Gatekeeper. Default value: .1.3.6.1.4.1.2727
Primary manager address • IP address • Port number	Node	Specifies the target address of the primary SNMP manager.
Secondary manager address • IP address • Port number	Node	Specifies the target address of the secondary SNMP manager.
SNMP version	Node	Specifies the SNMP protocol version: 0 - SNMP v1 1 - SNMP v2 (default)
Trap filter level	Node	Specifies which alarms are sent as SNMP traps. The active filter level is represented with a digit according the table below: 1 - all alarms are logged in the alarm list 2 - minor, major and critical are logged 3 - major and critical alarms are logged 4 - only critical alarms are logged
Trap sending repetition	Node	Specifies how many times a trap will be sent. Default value: 1

Statistics service

The following configuration parameters can be changed through the **SLEE_statistics** service management interface:

Parameter	Level	Description
Site ID	Noed	Specifies the an ID that will be included in all statistics reports generated from BEA WebLogic Network Gatekeeper.
Statistics type (list)	Node	Specifies the statistics types to be included in the statistics reports. If a new service is installed, the statistics type(s) used by that service have to be added to the list.
Status	SLEE	Specifies if the statistics service is active or not. That is, if statistics is collected and written to the database or not.

Trace service

The following configuration parameters can be changed through the **SLEE_trace** service management interface:

Parameter	Level	Description
Buffer size	SLEE	Specifies the number of trace messages buffered in the memory before written to disk. Value range: 1-500 messages
Maximum number of trace file	SLEE	Specifies the maximum number of trace files stored for a service. If the number is exceeded, the oldest trace file will be deleted. Value range: 0-10 files
Maximum trace file size	SLEE	Specifies the maximum size of the trace files. Value range: 100-100000 KB
SLEE trace status	SLEE	Specifies if the trace service is active (enabled/disabled) on the SLEE.

SLEE start-up parameters

The following configuration parameters are initialised at SLEE start-up. They are set in the `slee_properties.xml` file found in `/usr/local/slee/bin/` directory.

XML Tag	Parameter Description
`<SLEE_PROPERTIES>`	Specifies properties for the SLEE instance. • `name` A descriptive name. Is used as SLEE instance name. • `access_host` The IP-address or host name used for the default (access) resource sharing context. • `access_port` The port where the default (access) resource sharing context's service accessible CORBA objects, for example ESPA interfaces, are available. • oam_port The IP-address or host name used for the management resource sharing context. • `oam_port` The port where the management resource sharing context's service manageable CORBA objects, that is, the objects presented in the Network Gatekeeper Management Tool, are available. • `corba_timeout` The number of ms before CORBA calls times out. Used for the default (access) resource sharing context and all operator defined resource sharing context. • `corba_oam_timeout` The number of ms before CORBA OAM calls times out. • `corba_connect_timeout` The number of ms before a CORBA connection attempt times out. • `corba_thread_pool` The maximum number of threads in the default (access) resource sharing context's CORBA thread pool. • `corba_mgmt_thread_pool` The maximum number of threads in the management resource sharing context's CORBA thread pool. • `jdbc_connect_timeout` The number of ms before a JDBC connection attempt times out.

XML Tag	Parameter Description
<SLEE_PROPERTIES>	• `jdbc_so_timeout` The number of ms before JDBC requests times out. • `char_encoding` Always set to UTF-8. • `jvm64bit_mode` Specifies (TRUE|FALSE) if the JVM shall be run in 64-bit mode or not. • `start_mem` Specifies the start size, in bytes, of the JVM memory allocation pool. The default value is 64MB. • `max_mem` Specifies the maximum size, in bytes, of the JVM memory allocation pool. This value must a multiple of 1024 greater than 2MB. Append the letter k or K to indicate kilobytes, or m or M to indicate megabytes. • `new_size` Specifies the new size of the JVM young generation heap layout. • `max_new_size` Specifies the maximum new size of the JVM young generation heap layout. • `permanent_size` Specifies the size of the JVM permanent generation heap layout. • `survivor_ratio` Specifies the size of the survivor spaces compared to the eden in the JVM heap layout. • `maxLiveObjectEvacuationRatio` Specifies the maximum percent (0-100) of total space occupied by objects in new space that is expected to survive a scavange garbage collect. • `db_connect_failed_wait_time` Specifies the the time (in seconds) the SLEE will wait between reconnect attempts if no database is available. Default = 10 seconds

XML Tag	Parameter Description
`<SLEE_AGENT>`	Specifies data for the SLEE agent process. • `port` The SLEE agent port on the SLEE host. • `verbose` Specifies (TRUE|FALSE) if the SLEE agent should write information to standard out. Recommended to set to TRUE during system verification and to FALSE during live traffic. • `max_start_attempts` Specifies maximum number of start attempts made by the SLEE agent.
`<SLEE_HOST>`	Specifies the SLEE host’s IP address.
`<SLEE_PATH>`	Specifies the SLEE and database installation directories. • `slee_install_path` The SLEE installation directory. No space are permitted in the directory name. • `database_install_path` The database installation directory. No space are permitted in the directory name.
`<SLEE_REPOSITORY>`	Specifies the port where the SLEE repository is available.
`<SLEE_DB_1>`	Specifies data about the primary database. • `address` Specifies the database host’s IP address. • `port` Specifies the database port on the database host. • `user` • `pwd`

XML Tag	Parameter Description
`<SLEE_DB_2>` (Optional)	Specifies data about the secondary database. • `address` The database host's IP address. • `port` The database port on the database host.
`<SLEE_TIME>`	Specifies data about the time format used. • `format` Specifies the SLEE time format to be used. Specified according to java.text.SimpleDateFormat. • `usegettimeofday` Specifies (TRUE|FALSE) if the JVM shall use the OS time (TRUE) or JVM internal time (FALSE). • `usehighrestime` Specifies (TRUE|FALSE) if the JVM shall use high resolution time (TRUE) or buffered time (FALSE).
`<SLEE_TRACE>`	Specifies start up data for the SLEE trace service. • `verbose` Specifies (TRUE|FALSE) if trace information should be written to standard out. Recommended to set to true during system verification and to false during live traffic. • `enabled` Specifies (TRUE|FALSE) if the trace service is active at SLEE start up. • `port` Specifies the SLEE host port the trace process is listening to. • `trace_db_query_times` Specifies (TRUE|FALSE) if database queries shall traced or not.
`<SLEE_BIDIR>`	Specifies data for the bi-directional CORBA plug-in. • `enabled` Specifies (TRUE|FALSE) if a bi-directional CORBA plug-in is used.

XML Tag	Parameter Description
`<RMI_REGISTRY>`	Specifies data for the RMI registry. • `port` Specifies the SLEE host port for the RMI connection. • `gctimeinterval` Specifies the time (in milliseconds) between RMI garbage collections.
`<MANAGER>`	Specifies the number of OAM transactions to be saved in the Network Gatekeeper Management Tool history file.
`<MANAGER_TRACE>`	Specifies (TRUE|FALSE) if OAM transactions shall be written to the OAM manager history file.
<BACKUP>	Specifies the path to the directory where SLEE backups shall be saved.

SESPA

SESPA access

The following configuration parameters can be changed through the **SESPA_access** service management interface:

Parameter	Level	Description
CORBA connect timeout	Node	Specifies the CORBA connect timeout for the SESPA communication with ESPA.

Parameter	Level	Description
CORBA request timeout	Node	Specifies the CORBA request timeout for the SESPA communication with ESPA.
Load distribution	SLEE	Specifies how the load will be distributed among the SESPA hosts. host - the host's IP address load share - the host's load share in relation to the other hosts. Specified as an integer. Example, for three hosts the load share can be specified as 1-1-1 (equal distribution among the hosts). If one host shall have double load compared to the other to the load share is specified as 2-1-1. That is "load share" is set to 2 for that host and 1 for the other two.

SESPA call control

The following configuration parameters can be changed through the **SESPA_call_control** service management interface:

Parameter	Level	Description
Removal time	SLEE	Specifies the time of day (hh:mm) when removal of old call sessions will be performed.
Storage duration	SLEE	Specifies the number of days a call session will be stored in the database before it is automatically removed.
SQL removal size	SLEE	Specifies the number of old call sessions to be removed per SQL query execution.

SESPA messaging

The following configuration parameters can be changed through the **SESPA_messaging** service management interface:

Parameter	Level	Description
Removal time	SLEE	Specifies the time of day (hh:mm) when removal of old messages will be performed.
Storage duration	SLEE	Specifies the number of days a message will be stored in the database before it is automatically removed.
SQL removal size	SLEE	Specifies the number of messages to be removed per SQL query execution.

ESPA access and ESPA service capability modules

ESPA access

The following configuration parameters can be changed through the **ESPA_access** service management interface:

Parameter	Level	Description
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.

ESPA Charging

The following configuration parameters can be changed through the **ESPA_charging** service management interface:

Parameter	Level	Description
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Request timeout	Node	Specifies the timeout (in seconds) for the asynchronous requests made on the service interface by an application.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.

ESPA call control

The following configuration parameters can be changed through the **ESPA_callcontrol** service management interface:

Parameter	Level	Description
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Request timeout	Node	Specifies the timeout (in seconds) for the asynchronous requests made on the service interface by an application.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.

ESPA call user interaction

The following configuration parameters can be changed through the **ESPA_call_userinteraction** service management interface:

Parameter	Level	Description
Default translation address	Node	Specifies the address to a default announcement that will be used if no specific translation is specified for the announcement ID.
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.
UI timeout	Node	Specifies how long (in seconds) the service capability will wait for a response on a call user interaction request before timing out. Value range: 10-3600 seconds

ESPA messaging

The following configuration parameters can be changed through the **ESPA_messaging** service management interface:

Parameter	Level	Description
Mailbox timeout	Node	Specifies the timeout value for opened mailboxes. The timeout value is specified in seconds. When a mailbox has not been used for this amount of time it is closed.
Maximum number of properties to fetch	Node	Defines the maximum number of message properties to fetch for a message. If the maximum number of properties is larger than the number of properties for a message, all properties will not be fetched. Note, each destination address in a send list counts as one property.

Parameter	Level	Description
Notification callback time before dead	Node	Specifies how long notification callback-interfaces shall be considered to be 'zombies' (not responding to heartbeat supervision) before considered dead and removed from the notification. If a notification only has one callback-interface set and this is considered to be dead the notification will be discarded.
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Removal time	Node	Specifies the time of day when old messages (see storage duration) are automatically removed from the system.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.
Simultaneously deleted messages	SLEE	Specifies the number of messages to be deleted per SQL query execution.
Storage duration	Node	Specifies the number of days a message will be stored in the mailbox before it is automatically removed.

ESPA messaging user interaction

The following configuration parameters can be changed through the **ESPA_messaging_userinteraction** service management interface:

Parameter	Level	Description
Address configuration • address plan • address presentation • address screening	Node	Specifies what address-parameters shall be used in the address that is used as 'sent from' address when sending a message to a user. That is, when invoking sendInfoReq or sendInfoAndCollectReq on IpUI. address plan: 0 = P_ADDRESS_PLAN_NOT_PRESENT 1 = P_ADDRESS_PLAN_UNDEFINED 2 = P_ADDRESS_PLAN_IP 3 = P_ADDRESS_PLAN_MULTICAST 4 = P_ADDRESS_PLAN_UNICAST 5 = P_ADDRESS_PLAN_E164 (default) 6 = P_ADDRESS_PLAN_AESA 7 = P_ADDRESS_PLAN_URL 8 = P_ADDRESS_PLAN_NSAP 9 = P_ADDRESS_PLAN_SMTP 10 = P_ADDRESS_PLAN_MSMAIL 11 = P_ADDRESS_PLAN_X400 12 = P_ADDRESS_PLAN_SIP 13 = P_ADDRESS_PLAN_ANY address presentation: 0 = P_ADDRESS_PRESENTATION_ UNDEFINED (default) 1 = P_ADDRESS_PRESENTATION_ALLOWED 2 = P_ADDRESS_PRESENTATION_ RESTRICTED 3 = P_ADDRESS_PRESENTATION_ ADDRESS_NOT_AVAILABLE address screening: 0 = P_ADDRESS_SCREENING_ UNDEFINED (default) 1 = P_ADDRESS_SCREENING_USER_ VERIFIED_PASSED 2 = P_ADDRESS_SCREENING_USER_ NOT_VERIFIED 3 = P_ADDRESS_SCREENING_USER_ VERIFIED_FAILED 4 = P_ADDRESS_SCREENING_NETWORK

Parameter	Level	Description
Default plug-in type	Node	Specifies what type of plug-in that shall be used * for user interaction if the policy service is unavailable or if the type is not specified in the SLA. Valid types: • USSD • SMS • GUI
GUI instance number range	SLEE	Specifies address ranges to be used as destination addresses for the end-users' answers. Over-lapping ranges between service instances are not allowed. The size of the range defines how many outstanding requests can be handled by the service instance at a time. Individual range size can be increased by adding digits in the end of the start and end values. Example: the range 1231000-1231999 can be increased to 12310000-12319999.
Notification callback time before dead	Node	Specifies how long notification callback-interfaces shall be considered to be 'zombies' (not responding to heartbeat supervision) before considered dead and removed from the notification. If a notification only has one callback-interface set and this is considered to be dead the notification will be discarded.
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.
UI timeout	Node	Specifies how long (in seconds) the service capability will wait for a response on a user interaction request before timing out. Value range: 10-3600 seconds

ESPA Subscriber profile

The following configuration parameters can be changed through the **ESPA_subscriber_profile** service management interface:

Parameter	Level	Description
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.

ESPA User location

The following configuration parameters can be changed through the **ESPA_user_location** service management interface:

Parameter	Level	Description
Maximum number of outstanding addresses	Node	Specifies the maximum number of location addresses (numbers) that can be registered for periodic user location at the same time.
Minimum interval between periodic location requests	Node	Specifies minimum allowed time interval (in milliseconds) between location requests when periodic user location is used.
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Plug-in type request level error callback	Node	Specifies if the plug-ins that makes one error callback if the entire request failed or if the plug-in makes one error callback for each failed address in the request. TRUE - one error callback for the whole request FALSE - one error callback for each failed address

Parameter	Level	Description
Request timeout	Node	Specifies the timeout (in seconds) for the asynchronous requests made on the service interface by an application.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.

ESPA User status

The following configuration parameters can be changed through the **ESPA_user_status** service management interface:

Parameter	Level	Description
Overload level	SLEE	Specifies the load percentage defining when the service will raise an overloaded alarm.
Plug-in type request level error callback	Node	Specifies if the plug-ins that makes one error callback if the entire request failed or if the plug-in makes one error callback for each failed address in the request. TRUE - one error callback for the whole request FALSE - one error callback for each failed address
Request timeout	Node	Specifies the timeout (in seconds) for the asynchronous requests made on the service interface by an application.
Severe overload level	SLEE	Specifies the load percentage defining when the service will raise a severely overloaded alarm.

Plug-in manager

The following configuration parameters can be changed through the **Plugin_manager** service management interface:

Parameter	Level	Description
Plug-in types (list)	Node	Specifies the types of network and SCS plug-ins that can be installed. If the plug-in type is not registered before the plug-in is installed, the plug-in cannot register in the plug-in manager. Plug-in types for the core plug-ins are provided as default.

Network plug-ins

ESPA access

The following configuration parameters can be changed through the **Plugin_OSA_access** service management interface:

Parameter	Level	Description
Keystore password	Node	Specifies the password used when storing and removing user certificates and private keys in the ESPA Access/OSA plug-in's keystore.
Policy based routing enabled	Node	Specifies if policy based routing is enabled or not. Must be set to TRUE if the policy based routing shal be.

ESPA generic UI/OSA (HOSA)

The following configuration parameters can be changed through the **Plugin_OSA_GUI** (**Plugin_HOSA_GUI**) service management interface:

Parameter	**Level**	**Description**
Language	SLEE	Specifies the value for the language parameter to be used in the sendInfoReq and sendInfoAndCollectReq requests.
Requested response	SLEE	Specifies the value for the requested response parameter to be used in the sendInfoReq and sendInfoAndCollectReq requests. Defines if a response is required from the call user interaction service, and any action the service should take. 1 - RESPONSE REQUIRED The User Interaction Call shall send a response when the request has completed. 2 - LAST ANNOUNCEMENT IN A ROW This is the final announcement within a sequence. It might, however, be that additional announcements will be requested at a later moment. The UI call service may release any used resources in the network. The UI object will not be released. 4 - FINAL REQUEST This is the final request. The UI object will be released after the information has been presented to the user.
Repeat indicator	SLEE	Specifies how many time an announcement or voice prompt shall be sent to the end users. If 0 (zero) is specified,
Minimum no. of characters	SLEE	Specifies the minimum number of characters (digits) to be collected after an announcement/voice prompt.
Maximum number of characters	SLEE	Specifies the maximum number of characters (digits) to be collected after an announcement/voice prompt.
End sequence	SLEE	Specifies the character(s) which will terminate an input of variable length.

Parameter	Level	Description
First character timeout	SLEE	Specifies the maximum allowed time period between an annoncement has been completed or interruped and the first character (digit) is entered. If the timer times out, the input is regarded to be erroneous.
Inter-character time out	SLEE	Specifies the maximum allowed time period between entering two subsequent characters (digits) in a response. If the timer times out, the input is regarded to be erroneous.
Enable Notification Restoration	SLEE	Defines if automatic restoration of registered notifications shall be performed towards an underlying Generic UI OSA (HOSA) SCS. If enabled, BEA WebLogic Network Gatekeeper restores the notification listeners periodically. The time period is defined in Notification Restoration Interval. This is used when the underlying OSA/Parlay Gateway does not restore registered notifications after a restart. This is the case for, for example Ericsson NRG.
Notification Restore Interval	SLEE	The time in seconds between each notification restoration process.

ESPA user location/OSA

The following configuration parameters can be changed through the **Plugin_OSA_UL** service management interface:

Parameter	Level	Description
Maximum number of addresses per request	SLEE	Specifies the maximum number of adresses allowed per one user location request.

ESPA user status/OSA

The following configuration parameters can be changed through the **Plugin_OSA_US** service management interface:

Parameter	Level	Description
Maximum number of addresses per request	SLEE	Specifies the maximum number of adresses allowed per one user status request.

Messaging/CIMD

The following configuration parameters can be changed through the **Plugin_messaging_cimd** service management interface:

Parameter	Level	Description
Alive message interval	SLEE	Specifies the interval between link test messages in seconds. 0 (zero) disables the test messages sending.
SMSC connection info	SLEE	Specifies information about the WebLogic Network Gatekeeper OSA Gateway connection. • host: The SMSC IP in IPv4, or host name. • port: The port number to connect to. • user ID: Identity used to login. Max. 32 characters. Leading or trailing spaces are not allowed. • password: Password used to login. Max. 32 characters. Leading or trailing spaces are not allowed. • subaddress: Defines a unique index (0-9) for a plug-in instance. This is useful when several plug-in instances are connected on the same user id. A negative value indicates that sub addressing shall not be used. • window size: Defines the window size, i.e. the maximum number of concurrently outstanding un-acked submits. A negative value indicates that the window size shall not be specified in the login. Value range: 1-128

Parameter	Level	Description
Overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Severe overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.
Database cleaner parameters	SLEE	Specifies parameters for the store and forward database cleaner service: • Invocation time: Time of day when the service shall be invoked (hh:mm) • Invocation interval: How often (no. of days between invocations) the service shall be invoked • Age of requests (hours) to be deleted
Database query size	SLEE	Specifies the maximum number of queries to be processed, that is, deleted at a time.

Messaging/SMPP SMS

The following configuration parameters can be changed through the **Plugin_messaging_SMPP_SMS** service management interface:

Parameter	Level	Description
Connect delay value	SLEE	Specifies the interval (in seconds) between SMSC reconnect attempts within a reconnect procedure.
Connect total time value	SLEE	Specifies the duration (in minutes) of an SMSC reconnect procedure. A reconnect procedure includes several SMSC reconnect attempts.
Database cleaner parameters	SLEE	Specifies parameters for the store and forward database cleaner service: • Invocation time: Time of day when the service shall be invoked (hh:mm) • Invocation interval: How often (no. of days between invocations) the service shall be invoked • Age of requests (hours) to be deleted

Parameter	Level	Description
Database query size	SLEE	Specifies the maximum number of queries to be processed, that is, deleted at a time.
Enquire link request timer value	SLEE	Specifies the how long (in milliseconds) the plug-in will wait for a response to the enquire link request before the connection is considered dead.
Enquire link timer value	SLEE	Specifies the interval (in minutes) between the enquire link requests sent to the SMSC. Sending this request to the SMSC keeps the connection alive. If 0 (zero) is specified, the enquire link sending is turned off.
ESME address range	SLEE	Specifies the address range of the SMSes to be sent to BEA WebLogic Network Gatekeeper. The address range is specified as a UNIX regular expression.
ESME numbering plan indicator	SLEE	Specifies the numbering plan indicator for the addresses specified in the “ESME address range” parameter.
ESME password	SLEE	Specifies the password used by BEA WebLogic Network Gatekeeper when connecting to the SMSC as an ESME.
ESME system ID	SLEE	Specifies the system ID used by BEA WebLogic Network Gatekeeper when connecting to the SMSC as an ESME.
ESME system type	SLEE	Specifies the system type used by BEA WebLogic Network Gatekeeper when connecting to the SMSC as an ESME.
ESME type of number	SLEE	Specifies the type of number for the addresses specified in the “ESME address range” parameter.
Overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Request timer value	SLEE	Specifies the value (in milliseconds) of the timer used when sending messages. When the timer expires, the plug-in assumes that the message sending has failed.

Parameter	Level	Description
Sequence number range end ID	SLEE	Specifies the last number in the sequence number range. The ID manager will not generate IDs larger than the specified value.
Sequence number range start ID	SLEE	Specifies the first number in the sequence number range. The ID manager will generate IDs beginning with the specified value
Severe overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.
SMSC default alphabet	SLEE	Specifies the default alphabet used by the SMSC. This is specified in the plug-in for the characters to be decoded correctly. The following encoding schemes are supported: • All encoding schemes supported by JAVA. For example: - ASCII - Cp1252 - ISO8859_1
SMSC IP address	SLEE	Specifies the SMSC host's IP address.
SMSC port	SLEE	Specifies the SMSC host's port number.
User text max length	SLEE	Specifies the maximum number of characters allowed in an Parlay message.

Messaging/SMPP USSD

The following configuration parameters can be changed through the **Plugin_messaging_SMPP_USSD** service management interface:

Parameter	Level	Description
Connect delay value	SLEE	Specifies the interval (in seconds) between SMSC reconnect attempts within a reconnect procedure.
Connect total time value	SLEE	Specifies the duration (in minutes) of an SMSC reconnect procedure. A reconnect procedure includes several SMSC reconnect attempts.
Database cleaner parameters	SLEE	Specifies parameters for the store and forward database cleaner service: • Invocation time: Time of day when the service shall be invoked (hh:mm) • Invocation interval: How often (no. of days between invocations) the service shall be invoked • Age of requests (hours) to be deleted
Database query size	SLEE	Specifies the maximum number of queries to be processed, that is, deleted at a time.
Enquire link request timer value	SLEE	Specifies the how long (in milliseconds) the plug-in will wait for a response to the enquire link request before the connection is considered dead.
Enquire link timer value	SLEE	Specifies the interval (in minutes) between the enquire link requests sent to the SMSC. Sending this request to the SMSC keeps the connection alive. If 0 (zero) is specified, the enquire link sending is turned off.
ESME address range	SLEE	Specifies the address range of the SMSes to be sent to BEA WebLogic Network Gatekeeper. The address range is specified as a UNIX regular expression.
ESME numbering plan indicator	SLEE	Specifies the numbering plan indicator for the addresses specified in the “ESME address range” parameter.

Parameter	Level	Description
ESME password	SLEE	Specifies the password used by BEA WebLogic Network Gatekeeper when connecting to the SMSC as an ESME.
ESME system ID	SLEE	Specifies the system ID used by BEA WebLogic Network Gatekeeper when connecting to the SMSC as an ESME.
ESME system type	SLEE	Specifies the system type used by BEA WebLogic Network Gatekeeper when connecting to the SMSC as an ESME.
ESME type of number	SLEE	Specifies the type of number for the addresses specified in the “ESME address range” parameter.
Overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Request timer value	SLEE	Specifies the value (in milliseconds) of the timer used when sending messages. When the timer expires, the plug-in assumes that the message sending has failed.
Sequence number range end ID	SLEE	Specifies the last number in the sequence number range. The ID manager will not generate IDs larger than the specified value.
Sequence number range start ID	SLEE	Specifies the first number in the sequence number range. The ID manager will generate IDs beginning with the specified value
Severe overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.
User text max length	SLEE	Specifies the maximum number of characters allowed in an Parlay message.
USSD gateway address	SLEE	Specifies the USSD host’s IP address.
USSD gateway port	SLEE	Specifies the USSD host’s port number.

MMS/EAIF

The following configuration parameters can be changed through the **Plugin_mms_EAIF** service management interface:

Parameter	Level	Description
MMS server configuration	SLEE	Specifies the configuration for the connection with the MMS server • IP - The MMS server's IP address. • SENDPORT - The MMS server port that reicives MMS messages. • RECIVEPORT - The plug-in client port that recives MMS messages.
Overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Response delay	SLEE	Specifies the response delay (in milliseconds) when running running asynchronous mode. The specified value must be greater than 0 (zero).
Send mode	SLEE	Specifies the send mode according to the following: 1 - Synchronous 2 - Asynchronous
Severe overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.

MMS/MM7

The following configuration parameters can be changed through the **Plugin_messaging_MM7** service management interface:

Parameter	Level	Description
Attachment format	SLEE	Specifies the format used for attachments. One of the following: • Dime • Mime (default)
Database cleaner parameters	SLEE	Specifies parameters for the store and forward database cleaner service: • Invocation time: Time of day when the service shall be invoked (hh:mm) • Invocation interval: How often (no. of days between invocations) the service shall be invoked • Age of requests (hours) to be deleted
Database query size	SLEE	Specifies the maximum number of queries to be processed, that is, deleted at a time.
Default destination	SLEE	Specifies a default destination address for incoming messages without a destination address. If set to an empty string, incoming messages without a destination address will be rejected.

Parameter	Level	Description
Heartbeat configuration	SLEE	Specifies the plug-in to MM7 server heartbeat function configuration: • Heartbeat URL: The (MM7 server) URL to use for the heartbeats. • Heartbeat interval: The interval between heartbeats in milliseconds. Set the interval to 0 if the heartbeat mechanism shall be disabled. • Heartbeat content match: The content retrieved from the specified URL will be matched with the specified heartbeat content match and the check is interpreted as OK if they match. Set the heartbeat content match parameter to an empty string if no content match shall be performed. • Explicitly activate plug-in: Set to true if the plug-in should be explicitly activated. This is useful when setting the interval to 0 for disabling the heartbeat and the plug-in should be activated. Example: If the URL is set to http://192.168.1.4:8080/status/status.txt and status.txt contains the text “MM7 server OK”, the plug in will match this text against the text specified in heartbeat content match. If they match, the connection will be considered OK.
HTTP basic authentication	SLEE	Specifies if HTTP basic authentication is enabled (TRUE|FALSE) or not.
HTTP basic authentication details	SLEE	Specifies the user name and password to be used for the HTTP basic authentication.
Is active	SLEE	Specifies (true|false) if the plug-in shall explicitly activated even if the heartbeat function indicates that the MM7 server is not responding. That is, if there is something wrong with the heartbeat function itself.
MM7 version	SLEE	Specifies the MM7 version used. The following are supported: • 5.3.0 • ericsson_mm7_1_0

Parameter	Level	Description
MMS relay/server address	SLEE	Specifies the path used in the http request to the MMS relay/server.
MMS relay/server URN	SLEE	Specifies the MMS relay/server URN (Uniform Resource Name)
Overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Read report	SLEE	Specifies if read reports are requested (TRUE|FALSE) or not.
Report address	SLEE	Specifies the report address to be used when sending messages to an Ericsson MMSC that requires the report address element.
Sequence number range end ID	SLEE	Specifies the last number in the sequence number range. The ID manager will not generate IDs larger than the specified value.
Sequence number range start ID	SLEE	Specifies the first number in the sequence number range. The ID manager will generate IDs beginning with the specified value
Severe overload percentage	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.
Value added service ID	SLEE	Specifies the VAS (Value Added Service) ID to be used for BEA WebLogic Network Gatekeeper If left empty, the Application Instance Group IDApplication ID the application belongs to is used.
Value added service provider ID	SLEE	Specifies the VASP (Value Added Service Provider) ID to be used for BEA WebLogic Network Gatekeeper. If left empty, the Service Provider IDthe application belongs to is used.

User location/MLP

The following configuration parameters can be changed through the **Plugin_user_location_MLP** service management interface:

Parameter	Level	Description
Default MLP response request	SLEE	Specifies the default MLP response request type. If set to NOT_USED, the **<eqop>** tag will not be used in the SOAP requests. The following are supported: 0 - NO_DELAY 1 - LOW_DELAY 2 - DELAY_TOL 3 - NOT_USED
Heartbeat check interval	SLEE	Specifies the interval (in milliseconds) between MLP server heartbeat checks. Heart beats are only sent if the connection with the MLP server is lost.
MLP password	SLEE	Specifies BEA WebLogic Network Gatekeeper password used when connecting to the MLP server. The password is provided by the MLP owner.
MLP requestor ID	SLEE	Specifies BEA WebLogic Network Gatekeeper requestor ID. If set to an empty string, the **<requestorid>** tag will not be used in the SOAP requests. The requestor ID is provided by the MLP owner.
MLP server URL	SLEE	Specifies the MLP server's URL.
MLP service ID	SLEE	Specifies BEA WebLogic Network Gatekeeper service ID. If set to an empty string, the **<serviceid>** tag will not be used in the SOAP requests. The service ID is provided by the MLP owner.
MLP user ID	SLEE	Specifies BEA WebLogic Network Gatekeeper user ID used when connecting to the MLP server. The user ID is provided by the MLP owner.
Overload level	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.

Parameter	Level	Description
Request buffer	SLEE	Specifies if request buffering shall used (TRUE|FALSE) or not. If not used requests will be rejected if the MLP server does not respond. If used, the requests will be buffered and sent to the MLP server when the connection is re-established.
Request buffer flush interval	SLEE	Specifies the interval (in milliseconds) between flushes when emptying the request buffer.
Request buffer flush size	SLEE	Specifies the number of requests sent in each flush when emptying the request buffer.
Request buffer request interval	SLEE	Specifies the interval (in milliseconds) between the requests within a flush when emptying the request buffer.
Severe overload level	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.

User location/MPS

The following configuration parameters can be changed through the **Plugin_user_location_MPS** service management interface:

Parameter	Level	Description
MPC address	SLEE	The IP address of the MPC server.
MPC port	SLEE	The port number to connect to on the MPC server.
MPC user ID	SLEE	BEA WebLogic Network Gatekeeper user ID used when connecting to the MPC server. The user ID is provided by the MPC owner.
MPC password	SLEE	BEA WebLogic Network Gatekeeper password used when connecting to the MPC server. The password is provided by the MPC owner.

Parameter	Level	Description
Overload level	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Severe overload level	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.

User Status/MPS

The following configuration parameters can be changed through the **Plugin_user_status_MPS** service management interface:

Parameter	Level	Description
MPC address	SLEE	The IP address of the MPC server.
MPC port	SLEE	The port number to connect to on the MPC server.
MPC user ID	SLEE	BEA WebLogic Network Gatekeeper user ID used when connecting to the MPC server. The user ID is provided by the MPC owner.
MPC password	SLEE	BEA WebLogic Network Gatekeeper password used when connecting to the MPC server. The password is provided by the MPC owner.
Overload level	SLEE	Specifies the load percentage defining when the plug-in will raise an overloaded alarm.
Severe overload level	SLEE	Specifies the load percentage defining when the plug-in will raise a severely overloaded alarm.

Servlet engine manager

The following configuration parameters can be changed through the **Servlet_engine_manager** service management interface:

Parameter	Level	Description
Port	SLEE	Specifies the port number on which the servlet engine is configured to listen for http connections.

Embedded Tomcat

The following configuration parameters can be changed through the **Embedded_Tomcat** service management interface:

Parameter	Level	Description
Catalina home directory	SLEE	Specifies the path to the Tomcat servlet engine
IP address	SLEE	Specifies the local IP address used for listening
Connectors • port number • protocol type • maximum no. of connections to accept • minimum no. of threads • maximum no. of threads	SLEE	Specifies connectors. That is, connects a protocol type to a port and defines related configuration data. Valid protocol types are: http and ajs
HTTPS Connectors • port number • maximum no. of connections to accept • minimum no. of threads • maximum no. of threads • use SSL client authentication (Y/N) • keystore file • keystore password	SLEE	Specifies https connectors. The keystore file parameter includes the directory path (including file name) for the user certificate.

Network time server manager

The following configuration parameters can be changed through the **Time_server_manager** service management interface:.

Parameter	Level	Description
Server address	Node	Specifies the IP address of the system time server.
Synchronization interval	Node	Specifies the time period (in milliseconds) between the time synchronizations. The shortest recommended interval is 10.000 ms.
Time difference alarm	Node	Specifies the maximum time difference (in milliseconds), at synchronization, between the SLEE time and the time server time that is allowed without raising an alarm.
Maximum time difference for automatic syncronization	Node	Specifies the maximum time difference (in milliseconds) that is allowed for making an automatic synchronization between the SLEE time and the time server time. If the time difference exceeds the specified value, the syncronization has to be made manually.

User Certificates and Private Keys

The following sections describe how to work with certificates and private keys:

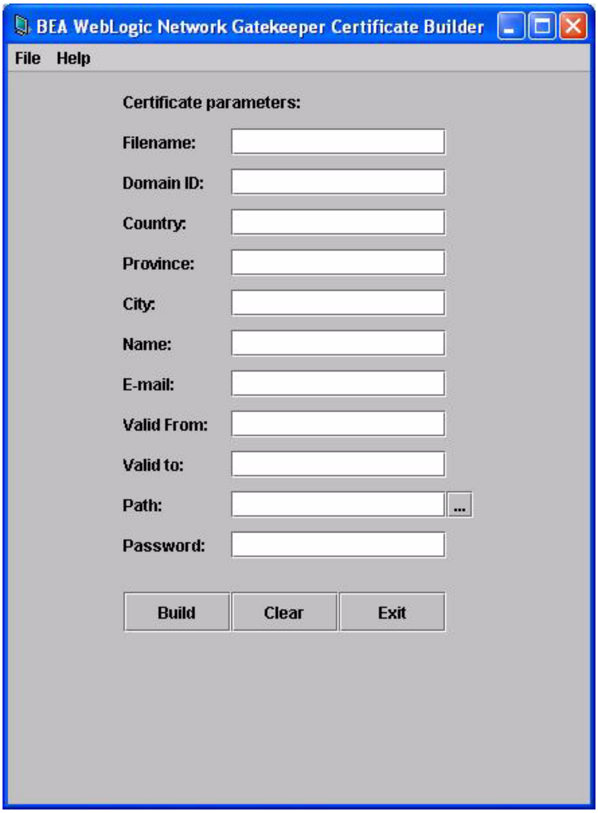
About user certificates and private keys

An application using network services through an OSA/Parlay gateway acts as an OSA/Parlay client towards the OSA/Parlay gateway. The OSA/Parlay client and the OSA/Parlay gateway's framework authenticate using user certificates and private keys.

When an application account is registered, an OSA/Parlay client for the application is created. This OSA/Parlay client imports the OSA/Parlay gateway's user certificate and provides its user certificate to the OSA/Parlay gateway. A part of creating the OSA/Parlay client is to generate the OSA/Parlay client's user certificate and private key.

About the certificate builder

The certificate builder is a tool for generating user certificates and private keys. It can be used stand alone and through an Network Gatekeeper Management Tool. The same functions are provided in both cases. The stand alone version of the certificate builder is shown in Figure 22-1.



BEA WebLogic Network Gatekeeper Certificate Builder

Certificate parameters:

Filename:

Domain ID:

Country:

Province:

City:

Name:

E-mail:

Valid From:

Valid to:

Path:

Password:

Figure 22-1 Stand alone Certificate Builder

Some fields in the certificate builder are used differently depending on what function the user certificate and private key is generated for. The specific usage of all fields are described in Table 22-3.

Table 22-3 Description of the Fields in the Certificate Builder

Field	Description
Filename	Specifies the file names of the generated user certificate and private key pair. **Example:** If `Filename` is set to `myApplication`, your files will be named: • `myApplication.key` (the private key) • `myApplication.der` (the user certificate).
Domain ID	The clientAppID (appID\entOpID) related to the application's OSA/Parlay client should be entered. The clientAppID is provided by the OSA/Parlay gateway operator.
Country	The country BEA WebLogic Network Gatekeeper is located in.
Province	The province or state BEA WebLogic Network Gatekeeper is located in.
City	The city BEA WebLogic Network Gatekeeper is located in.
Name	Contact person at your organization.
E-mail	The contact person's e-mail address.

Field	Description
Start date	The first date (YYYY-MM-DD) the certificate will be valid.
End date	The last date (YYYY-MM-DD) the certificate will be valid.
Path	The path to the directory where the user certificate and private key will be stored. Only existing directories can be specified. When importing a private key from a directory there must be only two files in the directory. That is, the private key and its user certificate. Therefore, it is recommended that you create a new directory for each pair of private key and user certificate you create.
Password	Defines a password that will be needed when importing the private key. Keep a note of the password, you will need it later. Note that this is the private key's password. When you import the private key in the keystore, you will also need the keystore's password. The keystore's password is defined the first time you import a private key or user certificate in the keystore.

Generating certificates and private keys

Follow the instruction below to generate a user certificate and private key pair.

If you perform the task through an Network Gatekeeper Management Tool, remember that the user certificate and private key will be stored on the server the Network Gatekeeper Management Tool is connected to. That is, where the SLEE runs.

Using the certificate builder stand alone

1. Start the certificate builder.

   j. Open a command window.

2. Go to the `/usr/local/slee/bin/` directory.
3. Start the certificate builder. Enter command: `./runCertBuilder.sh`
4. Enter the user certificate and private key data according to Table 22-3 on page 4.
5. Generate the user certificate and private key. Click the **Build** button.

   The user certificate and private key files are stored in the specified directory.

Using the certificate builder through an Network Gatekeeper Management Tool

1. Start an Network Gatekeeper Management Tool and log in.
2. Select any SLEE.
3. Double-click the **cert_builder** service.
4. Double-click the **buildCertificate** method.
5. Enter the user certificate and private key data according to Table 22-3 on page 4.
6. Click **Invoke**.

   The user certificate and private key files are stored in the specified directory.

Writing Service Level Agreements

The following sections describe how to write service level agreements:

Service level agreement XML file overview

The applications access rights to BEA WebLogic Network Gatekeeper ESPA service capabilities are specified in Service Level Agreement (SLA) XML files. There are SLAs on two levels, service provider and application level. The SLAs on the two levels are related to the service provider groups and and application groups. If the SLA on the service provider level is more restrictive than on application level, the value specified on service provider level will be used . That is, it is always the most restrictive value that applies.

An SLA template can be found in the `/usr/local/slee/bin/policy/sla_template` directory.

The SLA contains two main types of information specified by the attributes in the `<Sla>` tag and the contents of the `<serviceContract>` tags. Listing D-1, “Service level agreement XML file overview,” on page D-2 shows the service provider level SLA XML file’s main structure and the relation between the `<Sla>` and the `<serviceContract>` tags. Differences between the SLA files on service provider and application level are described in the tag descriptions below the listing.

Listing D-1 Service level agreement XML file overview

```
<Sla serviceProviderGroupID=”spGroup1" <!-- or applicationGroupID -->
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="file:./policy/sla_schema/sla_file.xsd"
>

<serviceContract>
  <!--service contract data for service capability 1-->
</serviceContract>

<serviceContract>
<!--service contract data for service capability 2-->
</serviceContract>

<serviceContract>
<!--service contract data for service capability 3-->
</serviceContract>

<serviceContract>
<!--service contract data for service capability n-->
</serviceContract>

</Sla>
```

<Sla>

This tag contains a number of service contracts specifying under which conditions a an application is allowed to access and use service capabilities.

The **serviceProviderGroupID** attribute specifies service provider group the service provider is related to. For SLAs on application level the **applicationGroupID** attribute is used instead. It specifies the application group the application i related to.

The **xmlns:xsi** and **xsi:noNamespaceSchemaLocation** attributes contains processing information and should not be changed.

<serviceContract>

These tags contain contractual data specifying under which conditions an application is allowed to access and use specific service capabilities. One `<serviceContract>` tag is needed for each service capability an application shall have access to.

What data to write in the `<serviceContract>` tag for each service capability is described in the following sections.

Charging service contract data

Listing D-2, "Charging service contract data," on page D-4 shows the tags available for the charging service contract and the order they have to appear in.

Listing D-2 Charging service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_charging</scs>

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>createChargingSession</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>createChargingSession</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>creditAmount</methodName>
   </blacklistedMethod>
   <blacklistedMethod>
      <methodName>creditUnit</methodName>
   </blacklistedMethod>
</methodAccess>

<currencyRestriction> <!-- Optional -->
   <allowedCurrency>
      <currencyCode>USD</currencyCode>
      <minAmount>1</minAmount>
      <maxAmount>10</maxAmount>
   </allowedCurrency>
   <allowedCurrency>
      <currencyCode>EUR</currencyCode>
      <minAmount>1</minAmount>
      <maxAmount>10</maxAmount>
   </allowedCurrency>
</currencyRestriction>

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- createChargingSession
- creditAmount
- creditUnit
- debitAmount
- debitUnit
- directCreditAmount
- directCreditUnit
- directDebitAmount
- directDebitUnit
- getChargingSession

- reserveAmount
- reserveUnit

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- createChargingSession
- creditAmount
- creditUnit
- debitAmount
- debitUnit
- directCreditAmount
- directCreditUnit
- directDebitAmount
- directDebitUnit
- getChargingSession
- reserveAmount
- reserveUnit

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- createChargingSession
- creditAmount
- creditUnit
- debitAmount

- debitUnit
- directCreditAmount
- directCreditUnit
- directDebitAmount
- directDebitUnit
- getChargingSession
- reserveAmount
- reserveUnit

<currencyRestriction>

This tag is used to specify the currencies allowed to use in the transactions handled by the charging service. The currency code is specified according to the ISO 4217 standard. To avoid too small and too large amounts in transactions, it is possible to specify a maximum and a minimum amount for each currency.

One `<allowedCurrency>` tag (including the `<currencyCode>`, `<minAmount>`, and `<maxAmount>` tags) is needed for each allowed currency. If all currencies are allowed, the tag is deleted or commented out.

Generic call control service contract data

Listing D-3, “Generic call control service contract data,” on page D-8 shows the tags available for the generic call control service contract and the order they have to appear in.

Listing D-3 Generic call control service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_generic_call_control</scs>

<maxNoOfActiveCalls>1000</maxNoOfActiveCalls> <!-- Optional -->

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>createCall</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>createCall</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>changeCallNotification</methodName>
   </blacklistedMethod>
</methodAccess>

<allowedGccEvents>OFFHOOK_EVENT
ANSWER_FROM_CALL_PARTY</allowedGccEvents> <!-- Optional -->

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<maxNoOfActiveCalls>

This tag [Row <Input/Output>] is used to specify the maximum number active calls the application is allowed to have. If there is no restriction, the tag is deleted or commented out.

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- callEventNotify
- changeCallNotification
- createCall
- enableCallNotification
- reportNotification
- route

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- callEventNotify
- changeCallNotification
- createCall

- enableCallNotification
- reportNotification
- route

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- callEventNotify
- changeCallNotification
- createCall
- enableCallNotification
- reportNotification
- route

<allowedGccEvents>

This tag is used block the application from listening to network events. The allowed events are listed in the tag and separated with a space. The following events are available:

- UNDEFINED
- OFFHOOK_EVENT
- ADDRESS_COLLECTED_EVENT
- ADDRESS_ANALYSED_EVENT
- CALLED_PARTY_BUSY
- CALLED_PARTY_UNREACHABLE
- NO_ANSWER_FROM_CALLED_PARTY
- ROUTE_SELECT_FAILURE
- ANSWER_FROM_CALL_PARTY

If the application is allowed to listen to all events, the tag should be deleted or commented out.

Generic messaging service contract data

Listing D-4, "Generic messaging service contract data," on page D-12 shows the tags available for the generic messaging service contract and the order they have to appear in.

Listing D-4 Generic messaging service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_messaging</scs>

<allowedCharging> <!-- Optional -->
   <allowedChargingList>0,1 0,5 1 2 3 4 5 10</allowedChargingList>
</allowedCharging>

<maxMessageSize>160</maxMessageSize> <!-- Optional -->

<allowedMmCharging> <!-- Optional -->
   <allowedChargingList>1 5 10 15 20 25 30</allowedChargingList>
</allowedMmCharging>

<maxMmMessageSize>100000</maxMmMessageSize> <!-- Optional -->

<allowedContentTypes> <!-- Optional -->
   <allowedContentTypeList>4 5 9 10</allowedContentTypeList>
<allowedContentTypes>

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>putMessage</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
  <methodRestriction>
    <methodName>putMessage</methodName>
    <reqLimit>20</reqLimit>
    <timePeriod>1000</timePeriod>
  </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
  <blacklistedMethod>
    <methodName>putMnMessage</methodName>
  </blacklistedMethod>
</methodAccess>

<gmsEventCriteria> <!-- Optional -->
  <allowedGmsEvent>
    <eventName>MESSAGE_ARRIVED</eventName>
  </allowedGmsEvent>
</gmsEventCriteria>

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<allowedCharging>

This tag is used for specifying the allowed charging amuonts for SMSes. The amounts are specifed as a string with spaces between the allowed amounts.

<maxMessageSize>

This tag is used for specifying the maximum number characters allowed in a SMS message. This size can be larger than 160. In this case, the message will be split by the messaging plug-ins.

<allowedMmCharging>

This tag [Row is used for specifying the allowed charging amuonts for MMSes. The amounts are specifed as a string with spaces between the allowed amounts.

<maxMmMessageSize>

This tag is used for specifying the maximum size of a MMS message in bytes.

<allowedContentTypes>

This tag is used for specifying which content types are allowed in MMS messages. The allowed content types are specified as a string with spaces between the values representing the content types.

Value	Content type
0	UNDEFINED
1	APPLICATION_MULTIPART_MIXED
2	APPLICATION_MULTIPART_RELATED
3	APPLICATION_SMIL
4	IMAGE_GIF
5	IMAGE_JPEG
6	IMAGE_PNG
7	IMAGE_TIFF
8	IMAGE_WBMP
9	TEXT_HTML
10	TEXT_PLAIN
11	TEXT_WML
12	AUDIO_AMR
13	AUDIO_WAVE
14	AUDIO_MP3
15	AUDIO_AU

Value	Content type
16	AUDIO_AIF
17	AUDIO_SND
18	AUDIO_RA
19	AUDIO_MID

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- createFolder
- enableMessagingNotification
- getMessage
- messagingEventNotify
- openMailbox
- putMessage
- putMmMessage

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- createFolder
- enableMessagingNotification

- getMessage
- messagingEventNotify
- openMailbox
- putMessage
- putMmMessage

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- createFolder
- enableMessagingNotification
- getMessage
- messagingEventNotify
- openMailbox
- putMessage
- putMmMessage

<gmsEventCriteria>

This tag is used to block the application from listening to network events. Since only two events are available, MESSAGE_ARRIVED and MESSAGE_DELIVERY_STATUS, the allowed event is entered in the tag.

If the application is allowed to listen to both events, the tag should be deleted or commented out.

Generic user interaction service contract data

Listing D-5, "Generic user interaction service contract data," on page D-17 shows the tags available for the user interaction service contract and the order they have to appear in.

Listing D-5 Generic user interaction service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_generic_user_interaction</scs>

<uiResourceType>USSD</uiResourceType>
<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>createUICall</methodNameGuarantee>
      <reqLimitGuarantee>50</reqLimitGuarantee>
      <timePeriodGuarantee>6000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>createUICall</methodName>
      <reqLimit>100</reqLimit>
      <timePeriod>60000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>sendInfoAndCollectReq</methodName>
   </blacklistedMethod>
</methodAccess>

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<uiResourceType>

This tag is used to specify the messaging type the application uses for generic user interaction. The following messaging types are supported:

- SMS
- USSD

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- createUI
- sendInfoReq
- sendInfoAndCollectReq

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- createUI
- sendInfoReq
- sendInfoAndCollectReq

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- createUI
- sendInfoReq
- sendInfoAndCollectReq

Multiparty call control service contract data

Listing D-6, "Multiparty call control service contract data," on page D-20 shows the tags available for the multiparty call control service contract and the order they have to appear in.

Listing D-6 Multiparty call control service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_call_control</scs>

<maxNoOfActiveCalls>1000</maxNoOfActiveCalls> <!-- Optional -->
<maxNoOfCallLegsInCall>31</maxNoOfCallLegsInCall> <!-- Optional -->

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>createCall</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>createCall</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>createChargingSession</methodName>
   </blacklistedMethod>
</methodAccess>

<allowedMpccEvents>ADDRESS_COLLECTED ANSWER
ORIGINATING_CALL_ATTEMPT</allowedMpccEvents> <!-- Optional -->

</serviceContract>
```

<startdate>

This is a general tag, see “Service capability common service contract data” on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<maxNoOfActiveCalls>

This tag is used to specify the maximum number active calls the application is allowed to have. If there is no restriction, the tag is deleted or commented out.

<maxNoOfCallLegsInCall>

This tag is used to specify the maximum number call legs in a call the application is allowed to have. If there is no restriction, the tag should be deleted or commented out.

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- createCall
- createCallLeg
- createNotification
- reportNotification
- route

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- createCall
- createCallLeg
- createNotification
- reportNotification
- route

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- createCall
- createCallLeg
- createNotification
- reportNotification
- route

<allowedMpccEvents>

This tag is used block the application from listening to network events. The allowed events are listed in the tag and separated with a space. The following events are available:

- ADDRESS_ANALYSED
- ADDRESS_COLLECTED
- ANSWER
- ALERTING
- ORIGINATING_CALL_ATTEMPT

- ORIGINATING_CALL_ATTEMPT_AUTHORISED
- ORIGINATING_SERVICE_CODE
- ORIGINATING_RELEASE
- TERMINATING_CALL_ATTEMPT
- TERMINATING_CALL_ATTEMPT_AUTHORISED
- TERMINATING_SERVICE_CODE
- TERMINATING_RELEASE
- REDIRECTED
- UNDEFINED
- QUEUED

If the application is allowed to listen to all events, the tag should be deleted or commented out.

Subscriber profile service contract data

Listing D-7, "Subscriber profile service contract data," on page D-24 shows the tags available for the subscriber profile service contract and the order they have to appear in.

Listing D-7 Subscriber profile service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_subscriber_profile</scs>

<permission>Read/Write</permission> <!-- Optional -->

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>getInfoProperty</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>getInfoProperty</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>setInfoProperty</methodName>
   </blacklistedMethod>
</methodAccess>

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<permission>

This tag specifies if the application's subscriber profile users have read and write access or read access only. Possible values are "Read/Write" or "Read".

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- getInfoProperty
- getSubscriberProfile
- setInfoProperty

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- getInfoProperty
- getSubscriberProfile
- setInfoProperty

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- getInfoProperty
- getSubscriberProfile
- setInfoProperty

User interaction service contract data

Listing D-8, “User interaction service contract data,” on page D-26 shows the tags available for the user interaction service contract and the order they have to appear in.

Listing D-8 User interaction service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_user_interaction</scs>

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>createUICall</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>createUICall</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>sendInfoAndCollectReq</methodName>
   </blacklistedMethod>
</methodAccess>

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<serviceCode> - Application level SLAs only

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- createUICall
- sendInfoReq
- sendInfoAndCollectReq

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- createUICall
- sendInfoReq
- sendInfoAndCollectReq

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- createUICall
- sendInfoReq
- sendInfoAndCollectReq

User location service contract data

Listing D-9, "User location service contract data," on page D-29 shows the tags available for the user location service contract and the order they have to appear in.

Listing D-9 User location service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_user_location</scs>

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>locationReport</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>locationReport</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction>

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>periodicLocationReport</methodName>
   </blacklistedMethod>
</methodAccess>

</serviceContract>
```

<startdate>

This is a general tag, see “Service capability common service contract data” on page D-33 for a description.

<enddate>

This is a general tag, see “Service capability common service contract data” on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<serviceCode>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- extendedLocationReport
- locationReport
- periodicLocationReportStartReq

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- extendedLocationReport
- locationReport
- periodicLocationReportStartReq

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- extendedLocationReport
- locationReport
- periodicLocationReportStartReq

User status service contract data

Listing D-10, "User status service contract data," on page D-31 shows the tags available for the user status service contract and the order they have to appear in.

Listing D-10 User status service contract data

```
<serviceContract>
<startDate>2003-01-01</startDate>
<endDate>2004-01-01</endDate>
<scs>ESPA_user_status</scs>

<serviceCode>45</serviceCode> <!-- Optional -->

<guarantee> <!-- Optional -->
   <methodGuarantee>
      <methodNameGuarantee>statusReport</methodNameGuarantee>
      <reqLimitGuarantee>10</reqLimitGuarantee>
      <timePeriodGuarantee>1000</timePeriodGuarantee>
   </methodGuarantee>
</guarantee>

<restriction> <!-- Optional -->
   <methodRestriction>
      <methodName>statusReport</methodName>
      <reqLimit>20</reqLimit>
      <timePeriod>1000</timePeriod>
   </methodRestriction>
</restriction

<methodAccess> <!-- Optional -->
   <blacklistedMethod>
      <methodName>createChargingSession</methodName>
   </blacklistedMethod>
</methodAccess>

</serviceContract>
```

<startdate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<enddate>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<scs>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<serviceCode>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description.

<guarantee>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to guarantee the access for the following methods:

- statusReportReq

<restriction>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to restrict the access for the following methods:

- statusReportReq

Note: Since only one method is available for user status, the `<restriction>` and `<methodAccess>` tags cannot exist together in the same service contract.

<methodAccess>

This is a general tag, see "Service capability common service contract data" on page D-33 for a description. It is possible to block the access for the following methods:

- statusReportReq

Note: Since only one method is available for user status, the `<restriction>` and `<methodAccess>` tags cannot exist together in the same service contract.

Service capability common service contract data

<startdate>

This tag specifies the date the application can start using the service capability . Use format YY-MM-DD.

Note that a later start date on the service provider level service contract overrides this date.

<enddate>

This tag specifies the last date the application can use service capability . Use format YY-MM-DD.

Note that an earlier end date on the service provider level service contract overrides this date.

<scs>

This tag specifies the SLEE service name of the ESPA service capability. The SLEE service name is the same as displayed in Network Gatekeeper Management Tool.

<serviceCode>

This tag is used to specify a serivce code that can be used for charging purposes. A service code specified by the application will be replaced with this code.

<guarantee>

This tag is used to specify a number of method requests the service provider or application is guaranteed during a specified time period (in milliseconds). That is, method requests from service providers and applications having the method tagged as guaranteed will have precedence before requests from service providers and applications not having the method tagged as guaranteed.

One `<guarantee>` tag (including the `<methodName>`, `<reqLimit>`, and `<timePeriod>` tags) is needed for each method that should have guaranteed usage.

<restriction>

This tag is used to restrict the number of method requests the application is allowed to do during a specified time period (in milliseconds). One `<methodRestriction>` tag (including the

`<methodName>`, `<reqLimit>`, and `<timePeriod>` tags) is needed for each method that should have restricted usage.

If the application does not have any usage restrictions within the allowed methods, the whole `<restriction>` tag should be deleted or commented out.

<methodAccess>

This tag is used to block the application from accessing one or more methods in the service capability . One `<blacklistedMethod>` (including the `<methodName>` tag) is needed for each blocked method.

If the application is allowed to access all methods, the whole `<methodAccess>` tag should be deleted or commented out.

Writing Network SLA Files

The following sections describe network SLA files:

SLA file overview

The network SLA files are written in XML. Depending on which level they are used, total traffic or service provider traffic, the XML SLA file looks slightly different. A SLA template that can be used for SLA files on both levels can be found in the following directory:

```
/usr/local/slee/bin/policy/sla_template
```

Service provider traffic SLA file

The service provider traffic SLA file consists of a **<sla>** tag containing one or more **<nodeContract>** tags as shown in Listing E-1, "Service provider traffic SLA file," on page E-2. The **serviceProviderGroupID** attribute specifies service provider group the SLA file is valid for. The structure and contents of the **<nodeContract>** tag is further described in "Contract data" on page E-3.

Listing E-1 Service provider traffic SLA file

```
<Sla serviceProviderGroupID="spGroup1"

  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:noNamespaceSchemaLocation="file:./policy/sla_schema/node_sla_file.xsd"
>

<nodeContract>

    <!--Contract data for network node 1-->

  </nodeContract>

<nodeContract>

    <!--Contract data for network node 2-->

  </nodeContract>

<nodeContract>

    <!--Contract data for network node n-->

  </nodeContract>

</Sla>
```

Total traffic SLA file

The total traffic SLA file consists of a **<sla>** tag containing one or more **<globalContract>** tags as shown in Listing E-2, "Total traffic SLA file," on page E-3. In this case, the **serviceProviderGroupID** attribute is left empty. The structure and contents of the **<globalContract>** tag is further described in "Contract data" on page E-3.

Listing E-2 Total traffic SLA file

```
<Sla serviceProviderGroupID=""
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="file:./policy/sla_schema/node_sla_file.xsd"
>
<globalContract>
    <!--Contract data for network node 1-->
  </globalContract>
<globalContract>
    <!--Contract data for network node 2-->
  </globalContract>
<globalContract>
    <!--Contract data for network node n-->
  </globalContract>
</Sla>
```

Contract data

The **<nodeContract>** and **<globalContract>** tags contains the same set of sub-tags that define under which conditions a network node can be accessed. See Listing E-3, "<nodeContract> and <globalContract> tag contents," on page E-4. The contents of each tag is further described below the listing.

Listing E-3 <nodeContract> and <globalContract> tag contents

```
<startDate>2001-06-01</startDate>

<endDate>2010-06-01</endDate>

<serviceType>USER_LOCATION_TYPE</serviceType>

<nodeID>UserLocationNode_A</nodeID>

<nodeRestrictions>

  <nodeRestriction>

    <overloadLimit>80</overloadLimit>

    <severeOverLoadLimit>90</severeOverLoadLimit>

    <maxSizeOfSendList>8</maxSizeOfSendList>

    <reqLimit>3</reqLimit>

    <timePeriod>1000</timePeriod>

  </nodeRestriction>
```

<startDate>

This tag specifies the date the service provider or WebLogic Network Gatekeeper can start accessing the network node. Use format YY-MM-DD.

<endDate>

This tag specifies the last date (expiry date) the service provider or WebLogic Network Gatekeeper can access the network node. Use format YY-MM-DD.

<serviceType>

This tag specifies the type of service provided by the network node according to the service types registered in the plug-in manager. Available service types can be listed using the **getTypeList** OAM method through the **Plugin_manager** service.

<nodeID>

This tag specifies the network node's node ID as registered in the Plug-in manager. Registered nodes can be listed using the **getIdList** OAM method through the **Plugin_manager** service.

<nodeRestrictions>

This tag contains one node restriction tag including sub-tags. See below.

<nodeRestriction>

This tag contains sub-tags that specify how much traffic the service provider or WebLogic Network Gatekeeper is allowed to send towards the network node and under which conditions. See below.

<overloadLimit>

This tag specifies when the underlying network node is considered to be overloaded. If this value is exceeded, an alarm is raised.

The value depends on how the network node reports its load. For example, one node can report the load as a value between 0-10 where 7 represents overloaded, and another node reports load as a value between 0-100 where 80 represents overloaded.

<severeOverLoadLimit>

This tag specifies when the underlying network node is considered to be severely overloaded. If this value is exceeded, further requests are rejected and exceptions are sent to the application.

The value depends on how the network node reports its load.

<maxSizeOfSendList>

This tag specifies how many destination addresses can be included in a request to the network node. The tag is optional and is used for the following service types:

- MESSAGING_TYPE
- USER_LOCATION_TYPE
- USER_STATUS_TYPE

If the send list size is exceeded, the whole request is rejected and an exception is sent to the requesting application.

<reqLimit>

This tag specifies a number of requests. It is used to restrict the number of service requests allowed during a specified time period.

An alarm is raised when the warning level (80% default, configurable through the rule) is exceeded. If the request limit is reached, further requests are rejected and exceptions are sent to the requesting applications.

<timePeriod>

This tag specifies the time period (in milliseconds) during which the request limit is valid.

Writing OAM Batch Files

The following sections describe how to use OAM batch files:

- "OAM batch file example" on page F-2
- "Executing an OAM batch file" on page F-2

OAM batch file example

The following shows a an example of an OAM batch file called `updateFriends.txt`. The friends and acquaintances lists are imaginary services that keeps track of a person's friends and acquaintances. Using the batch file, four persons are added to the acquaintances list and one person is moved from the acquaintances list to the friends list.

Listing F-1 OAM Batch file example

```
service Acquaintances
method addPerson
“Donald”
“Doris”
“Mary”
“Mike”
removePerson “John”
Friends:addPerson “John” “36”
```

The service **Acquaintances** is selected.

Since four persons are to be added, the method **addPerson** is selected. By selecting the method, you do not have to specify the method again until you want to use method.

The four persons are added to the acquaintances list. Note that strings have to be put within quotation marks.

To remove a person, the **removePerson** method is used. Since only one person is removed it is unnecessary to select the method and specify the parameters on a separate rows.

Finally, the removed person is added to the friends list. Since the Friends service is used only once, both the method and parameters are specified on the same row as the service. Note that parameters are separated by a space.

Executing an OAM batch file

Store the OAM batch file in the `bin` directory on the SLEE host where the used SLEE services are installed. for example `/usr/local/slee/bin/` directory on BEA WebLogic Network Gatekeeper host.

After connecting the text based Network Gatekeeper Management Tool to the SLEE, the OAM batch file is executed using the command:

```
exec "updateFriends.txt"
```

The OAM batch file can also be executed from an Network Gatekeeper Management Tool, see "Network Gatekeeper Management Tool" on page 3-1.

It is also possible to store the OAM batch files in other directories than the `bin` directory. The `exec` command is then used with an absolute or relative path. The relative path with the `bin` directory as starting point. Note that the path has to be specified as a Java string, for example: "`C:\\batch_files\\updateFriends.txt`" and "`/usr/local/batch_files/updateFriends.txt`".

References

Product Description - BEA WebLogic Network Gatekeeper

Application Developer's Guide - Parlay X Web Services for BEA WebLogic Network Gatekeeper

Application Developer's Guide - Extended Web Services for BEA WebLogic Network Gatekeeper

API Descriptions - Parlay X Web Services for BEA WebLogic Network Gatekeeper

API Descriptions - Extended Web Services for BEA WebLogic Network Gatekeeper

User's Guide - BEA WebLogic Network Gatekeeper Application Test Environmnet

Standards API specifications

Parlay X specifications

See http://www.parlay.org

Database

MySQL Reference Manual

Orb

ORBacus for C++ and Java

Servlet engine

Tomcat Servlet Engine documentation