HP OpenView Service Oriented Architecture Manager

Administrator Guide

Version: 2.11

Windows, HP-UX, Linux

Aug 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Linux is a U.S. registered trademark of Linus Torvalds

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation

UNIX® is a registered trademark of The Open Group

Support

You can visit the HP OpenView web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

Table of Contents

1

Introduction

This chapter covers general information about the *Administrator Guide* as well as technical overview information about the HP OpenView Service Oriented Architecture (SOA) Manager software. The technical overview information is fundamental to understanding and using the software. Read this information carefully before setting up the software in a test or enterprise environment.

Document Overview

The *SOA Manager Administrator Guide* provides instructions for setting up, configuring, and using the SOA Manager software. The chapters in the book are organized by feature with more generic features explained first. It is suggested that new users proceed through the chapters sequentially since the features become more complex in each successive chapter.

The guide does not detail the SOA Manager's implementation of standard WS-based management protocols. These standards define how to manage resources (including Web services) using Web services technology. The SOA Manager currently implements the Web Service Management Framework (WSMF), which is an HP-authored precursor version of standard WS-based management protocols.

Audience

The *Administrator Guide* is primarily intended for Administrators and Developers who are responsible for integrating and enabling Web services-based applications and management solutions in their IT environments. In addition, the guide is intended for Business Managers who are responsible for monitoring the health of Web services-based business applications. In addition, customers, partners, and industry analysts can read this chapter to get a technical overview of the SOA Manager software.

Prerequisites

To use this guide, users must have a fundamental knowledge of Web services principals, Java platform technologies, and software management principals. In addition, users must have basic experience deploying Web services-based applications.

Component Overview

The SOA Manager software allows an organization to dynamically manage the SOA resources that are deployed in an enterprise. The software is comprised of a set of core components that are distributed in an IT environment. The core components that are discussed in this section include:

- **Network Services Server** – A central management server that works to collect management data and present the data in a meaningful context. The data is collected from any number of WSM Agents and/or WSM Brokers.
- **WSM Agents** – Web Services Management (WSM) agents that provide management capabilities for Web services containers and their hosted Web services. The agents are integrated with the Web services container.
- **WSM Broker** – A proxy server process that provides management capabilities for Web services containers and their hosted Web services. The Broker is a separate process from the Web services container.

The following graphic shows a conceptual view of these components.

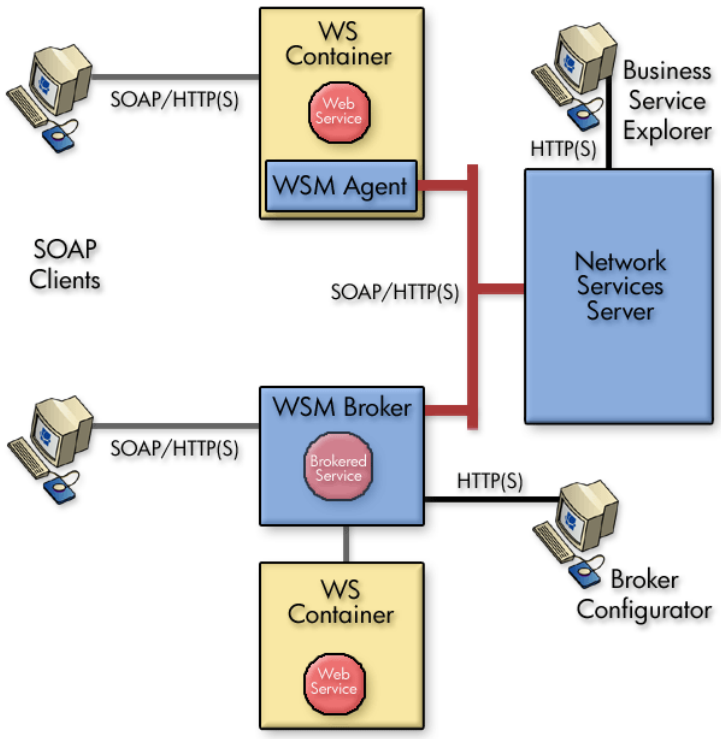


Figure 1-1: Conceptual View of SOA Manager Software Components

Network Services Server

The Network Services Server is a central management server that runs in a single Java Virtual Machine (JVM) process and includes a J2EE-based administrative console called the Business Service Explorer (BSE). A typical SOA Manager installation includes a single Network Services server that interacts with any number of WSM Agents and/or WSM Brokers. The communication between the software components is SOAP over HTTP(S). This communication channel is often referred to as the management channel. See Figure 1-1 above.

The server's primary functions are outlined below and discussed throughout this guide.

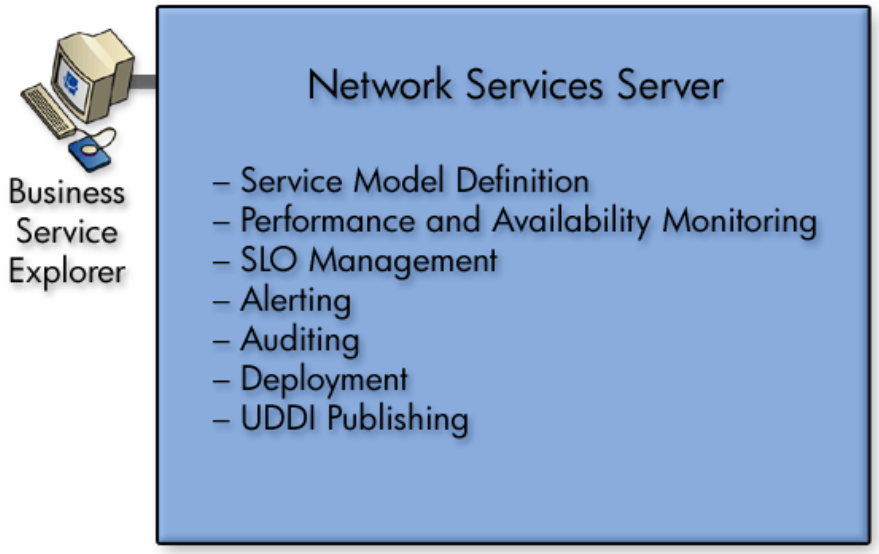


Figure 1-2: Network Services Server Functions

Service Model Definition

The Network Services Server maintains service model definitions. A service model definition allows a user to define an end-to-end model that encompasses business services and their relationships to actual IT resources. The service model is a distinguishing characteristic from other management solutions and is essential to understanding how SOA resources are managed using the SOA Manager software. The service model includes software assets (such as Web services), and also includes virtualized IT infrastructure components (such as Web services containers). A service model is defined using the BSE console and contains the following elements:

- **IT Service** – The virtualization of management information or capabilities of a group of IT resources of a certain type. The current version of SOA Manager implements and understands the following types of IT services: Web service Container IT services (Web service containers such as .NET and WebLogic Server), Web service Intermediary IT services (Web services proxies such as the WSM Broker), Database IT services, Message Oriented Middleware (MOM) IT services, and Host IT services. The model definition also includes the owners and stakeholders of an IT service.

- **Business Service** – A business service represents some business application that is offered by a business manager to either internal or external customers. Currently, the SOA Manager only implements one type of business service, which is a Web service. Multiple Web services can be part of a single business service. A business service definition is created and then bound to the IT Services that are required to deliver the business application. The model definition also allows relationships between business services. Such relationships can be used to provide root cause analysis and impact analysis.

The service model (including IT services and Business services) allow Business Managers, Developers, IT Operations and IT Support personnel to work together when defining, creating, deploying, and managing services. Ultimately, the service model definition links business operations with IT operations and automates many of the tasks that are required to deliver service-based applications.

Performance and Availability Monitoring

The Network Services Server aggregates management data that is collected by WSM Agents and/or WSM Brokers that are registered as IT services in the Network Services Server. The BSE is then used to view the collected data. Two types of management data are collected: performance metrics and availability status.

Performance metrics are collected over time and show the overall health and performance of the resources that are contained in a business service. Different metrics are collected depending on the type of resource being managed.

Availability status shows whether or not the IT services that are part of the overall service model are operational. The availability of an IT service typically provides the first indication that a business service is not operational.

SLO Management

The Network Services Server allows Service Level Objectives (SLO) to be defined for performance metrics. The SLO definition includes acceptable warning-level and breach-level limits. When an SLO limit is reached, an alert is raised. The BSE is used to define SLO threshold values and also to view any SLO alerts. SLOs allow operators to react and adapt to degrading services.

Alerting

The Network Services Server provides alerting capabilities for management events. There are generally three types of alerts: SLO alerts, availability alerts, and business content alerts. SLO alerts are raised whenever an SLO limit is reached. Availability alerts are raised whenever the status of an IT service changes. Lastly, business content alerts are raised when specific content is contained in the SOAP request and/or response message for a Web service.

Alert messages include information such as the origin, severity, and description of the alert. Alerts are viewed using the BSE and can be sent to email recipients, an SNMP TRAP, and to a log file. Alerts are persisted to the SOA Manager's database. The BSE is also used to create alert recipients and manage alerts (i.e. acknowledge alerts).

Auditing

The Network Services Server aggregates Web service message trace information that is collected by WSM Agents and/or WSM Brokers. Trace information provides historical data related to a Web service's performance, access history, security, size, source and destination endpoints, successes, failures, and can also include the SOAP request-response payloads and profile data.

Trace information is persisted to the SOA Manager's database at regular intervals. The BSE is used to view the trace information and generate reports.

Deployment

The Network Services Server can deploy a deployment unit to remote WS Containers/Brokers that are registered in the Network Services Server as an IT service. In the current release, deployment units represent Web services that are packaged in a WS Container's/Broker's deployment format (e.g. `.ear`, `.jar`, `.msi`, etc...). Any Web services that are contained in the deployment unit are automatically discovered at the time of deployment. Remote deployment saves time and allows business services to scale as service demands increase.

UDDI Publishing

The Network Services Server can be configured to use a UDDI registry. The BSE is used to publish management Web services for IT services and business services to the registry. Using a registry allows the assets that are defined in the service model to be reused by other applications.

WSM Agents and WSM Broker Components

The WSM Agents and WSM Broker are responsible for providing manageability for Web services and their WS container. The Agents and Broker are also responsible for exposing management data to the Network Service Server using standard WS-based management Web services.

The SOA Manager software provides a WSM Agent (called the J2EE Agent) for the WebLogic Server WS container and a WSM Agent (called the .Net Agent) for the .NET WS container. The WSM Agents are integrated with their respective containers and run in the same process as the container. Configuration files are used to configure the agents.

The WSM Broker is a separate server process that runs in a single JVM process and includes an administrative console called the Broker Configurator. The WSM Broker is a WS intermediary and can be used to add manageability to any WS container. The Broker provides manageability by using a brokered service (a proxy to the service being managed). A brokered service must be created for each Web service that you want to manage. Brokered services are created using the Broker Configurator.

Figure 1-3 below provides a view of the components associated with the WSM Agents and the WSM Broker.

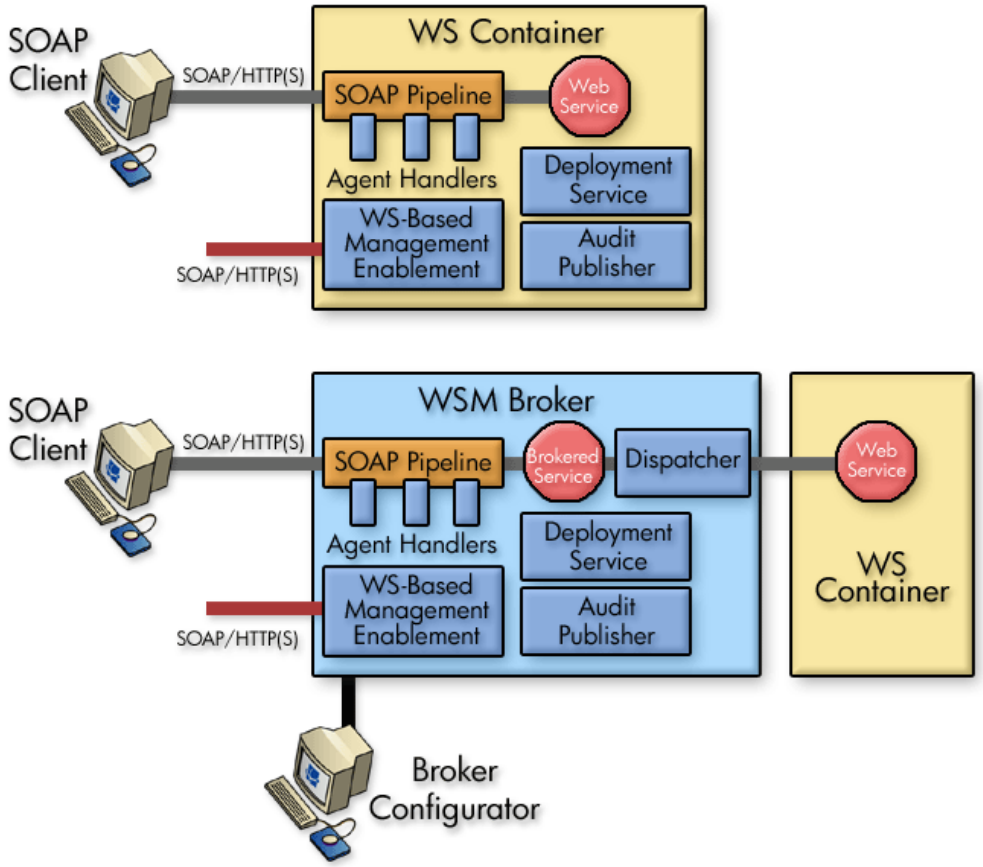


Figure 1-3: WSM Agents and WSM Broker components

Agent Handlers

The J2EE Agent and Broker collect management data through the use of Agent Handlers that are arranged in a handler chain. The agents are preconfigured to use a set of handlers that include (but not limited to) a monitoring handler, business metric handler, and auditing handler. Configuring the handlers is done differently for the J2EE Agent and the Broker.

Each SOAP message passes through the handler chain during a service request and response. Figure 1-4 is a common view of the handler chain. For detailed information about installing and configuring the J2EE Agent and Broker, see the *WSM J2EE Agent Administrator Guide* and the *WSM Broker Administrator Guide* respectively. These guides are located in the `/Documentation` directory of the distribution.

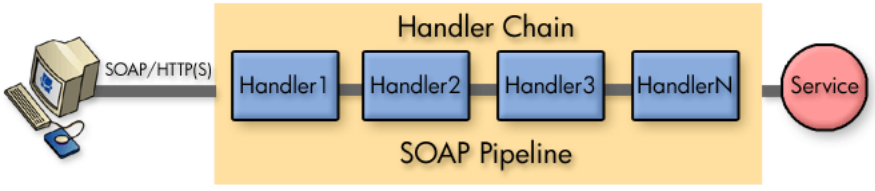


Figure 1-4: Management Handler Chain

The .NET Agent uses a Dynamic-Link Library (DLL) that monitors SOAP requests and responses. The DLL uses SOAP Extensions to gather management information for Web services. Figure 1-5 shows a common view of .NET management. For detailed information about installing and configuring the .NET Agent, see the *WSM .NET Agent Administrator Guide* located in the `/Documentation` directory of the distribution.

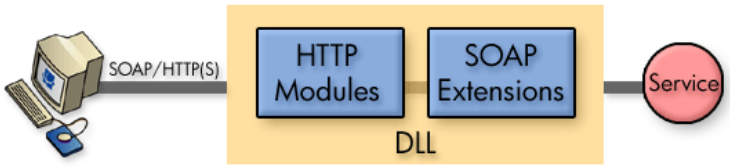


Figure 1-5: .NET Management

WS-Based Management Enablement

The WS-based management enablement layer is deployed into the Web service container or intermediary as a Web services application. The application is used by the Network Services server to get management data and also converts WS management interactions into interactions with the native management platforms. (i.e., JMX invocations for J2EE platforms, and WMI invocations for .NET platform.)

The SOA Manager currently implements an HP-authored precursor version of standard WS-based management protocols. These protocols are used by the WS-based management enablement layer.

Deployment Service

Each agent contains a Deployment Service that is used to deploy/undeploy deployment units (`.msi`, `.war`, etc…) in a managed domain. This mechanism allows IT administrators to quickly add or change application resources as required. The deployment service works together with the Network Service Server's deployment functionality.

Audit Publisher

The Audit Publisher is responsible for publishing trace messages (including payload) to the Audit Service in the Network Services server. The trace information is viewed using the BSE.

Dispatcher

The Dispatcher is an HTTP(S) client that dispatches requests from a brokered service to the actual Web service endpoint. The dispatcher is only a component of the WSM Broker.

Security

The SOA Manager software can be secured in several ways. First, management communication between the Network Services Server and the WSM Agents and/or WSM Brokers can be secured using SSL and HTTPS. The communication channel between these core components is often referred to as the management channel. This channel contains sensitive management information and can also be used to affect the resources that are being managed. For this reason, security on this channel is very important.

Second, the SOA Manager software provides security capabilities when using a WSM Broker. The capabilities can secure communication between a SOAP client, the WSM Broker, and the final Web service endpoint. This communication channel is often referred to as the application channel. Communication on this channel can be secured at both the transport layer (SSL and HTTPS) and at the message layer (WS-Security). This type of security is often implemented when a WS container does not offer native security support.

In both cases, identity management is handled by a tight integration with HP OpenView Select Access. This integration can also be used to provide authorized users access to the BSE and Broker Configurator.

This guide only covers management channel security, Select Access integration, and securing the BSE and Broker Configurator console using Select Access. For instructions on securing the application channel when using a Broker, refer to the *WSM Broker Administrator Guide*.

Integration Points

The SOA Manager software provides many integration points that allow custom integrations with existing software assets in an IT environment. Integrations with the SOA Manager software provide greater reusability and the flexibility to create solutions that are specific to a particular IT environment. This guide does not provide detailed integration instructions. Detailed instructions for common integrations are provided in the *SOA Manager Integrator Guide*, located in the `/Documentation` directory of the distribution.

SOA Manager Roles

As described above, the SOA Manager's service model facilitates better alignment among three functional groups within an enterprise: line of business or business teams, application development teams, and application and operations support. This alignment is enabled by capturing the concept of a business service in the model and providing the three groups with interfaces to interact with the model.

Line of Business Perspective

A line of business manager (LOBM) drives the creation and functional definition of any business service. A business service represents an IT implementation of a business product offered by the LOBM to business consumers such as customers, partners and suppliers. Subsequently, the LOBM is also motivated to define appropriate Service Level Objectives (SLO) for the business service and ensure operational compliance of the business service with the desired SLO.

For example, a LOBM decides that they need to offer an Order Status Query service to customers. The service needs to be available to consumers between certain business hours and return responses within some defined response time.

Development Team Perspective

Once the LOBM defines the business service, an Architect identifies how the architecture of the business service is to be broken up into different and distributed types of elements in the IT environment that execute in some coordinated manner. These different types of elements typically have different groups responsible for deploying and supporting them. The infrastructure for supporting these different IT element types is represented by an IT service. An Architect creates a model of the business service which also includes IT services.

One such IT service is the creation, deployment, and on-going support of a Web service implementation. The development team is responsible for implementing the Web service. Once they create the implementation, they capture the deployment unit for that implementation as an asset of the IT service representing the Web service implementation.

Another example of an IT service is the configuration and support of an entry within the WSM Broker. The brokering of an existing Web service may be required to interpose manageability or perform some kind of translation of semantics or technical protocol. A Web Services Management team within IT may be responsible for maintenance of such a broker. They may create the configuration of this asset and save the configuration as an asset of the IT service representing Web service brokering.

IT Operations and Support Perspective

IT operations teams must deploy the implementation assets captured in the IT service model by the Architect, onto appropriate IT resources to create running instances of IT services. Some coordination is required to configure the connections between the IT services. For example, someone must keep the Web Services Broker up-to-date to forward messages to one or more deployed Web service implementation endpoints.

Once the business service is made operational by connecting together the IT services, IT operations and support teams must monitor and maintain underlying resources for the implementations to keep these IT services running smoothly and ensure that the operation of the business service complies with the desired SLO. Additionally, they need to rapidly respond to changing needs of the business service by making appropriate changes to the underlying IT services.

Improving Business IT Alignment and Providing IT Automation

The functional groups can achieve better communication through the shared context provided by the business service. When the LOBM requires changes, they drive them through the business service, thus the involved IT Operations and Support teams can quickly affect the underlying IT services. Implementation changes directed at development teams can be prioritized by understanding the affected business services.

Repetitive tasks, such as deploying software and configuring connectivity between underlying IT services, can be automated by leveraging the metadata captured in the service model.

Life Cycle Stages

Web services, like all managed resources, have a life cycle. The SOA Manager software provides a clear life cycle definition for Web services. This definition provides an efficient and calculated method for managing Web services. The life cycle is comprised of two areas:

- **A Permanent Management Model**: The structure, relationships, policies, and assets are captured in the service model definition and are applied at runtime for management functions.
- **Transient Managed Resources**: Resources such as Web service containers and Web services that can be created, destroyed, and relocated anytime as required.

Figure 1-6 shows the stages of the life cycle and the relationship between the permanent management model and transient managed resources.

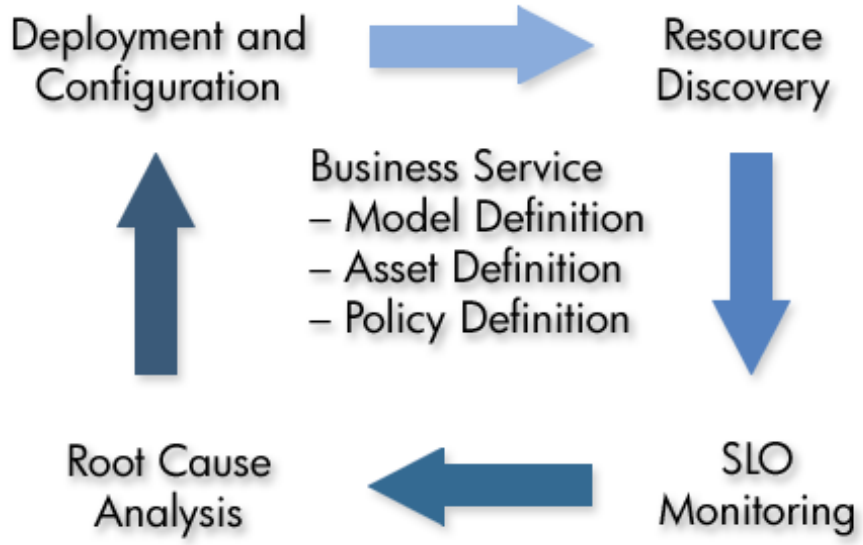


Figure 1-6: Life Cycle Stages

Model Definition

The structure, relationships, policies, and assets described in the service model are captured using the BSE. The BSE is not only used to create business service models, it is also used to view the business services, including their associated model. The underlying service model is architected to be interchangeable so that it can be created and manipulated by other tools or products (i.e., other Service Management products from HP).

Resource Discovery

At runtime, all managed Web services and Web services containers in the environment are registered using the BSE. Once resources are registered with the Network Services server, various IT services then identify resources contained in them by using identity matching patterns. This allows the IT services map to automatically reflect deployed resources in the IT services.

SLO Monitoring

Once IT services identify underlying resources, an SLO monitoring engine uses SLO values to monitor the performance of the underlying resources. SLO warning and breaches are detected and such events can be mapped to different types of responses. The most common response today is to send an email to the configured recipient, but this mechanism is flexible and can be mapped to any required automatic execution.

Problem Resolution

Once SLO warning and breach alerts are raised, the BSE can be used to navigate the virtual service and resource relationships to troubleshoot and isolate problems using root cause analysis or impact analysis.

Deployment and Configuration

Deployment assets captured in IT services can be deployed against target Web services containers. A corresponding un-deploy mechanism is provided as well.

WSM Deployment Scenarios

This section describes two basic deployment scenarios when setting up the SOA Manager's software components. The first scenario is a Broker-based scenario and the second is WSM agent-based scenarios. The deployment scenario you select is ultimately based on your business requirements and your services environment. Because the enterprise is increasingly becoming heterogeneous, it is likely that your environment will include a mix of the deployment scenarios discussed in this section.

The two scenarios discussed in this section are not meant to be inclusive of all possible deployment scenarios and are only meant to establish a foundation for understanding how the SOA Manager's software components are used together.

Broker-Based Scenario

A broker-based scenario utilizes one or more WSM Brokers to collect management data for Web services that are deployed in a WS Container. The Broker acts as a proxy to the container and does not need to be co-located with the container. The Broker provides manageability by using a brokered service (a proxy to the service being managed). A brokered service must be created for each Web service that you want to manage. For more information on installing and configuring the WSM Broker, see the *WSM Broker Administrator Guide*.

Runtime requests are sent through a brokered service and dispatched to the actual requested service implementation running in a WS Container. Management data is collected by handlers during the requests and responses that are sent through the brokered service.

A single instance of the WSM Broker can manage multiple brokered services. In addition, multiple brokers can be used on a single host or distributed across hosts. In scenarios where a single service is replicated across multiple machines, management data and metrics are aggregated. The Broker can also be used for services that are being managed by WSM Agents in order to leverage the security capabilities of the Broker.

Figure 1-7 shows a broker-based scenario that includes scaling for multiple WS Containers using multiple Brokers.

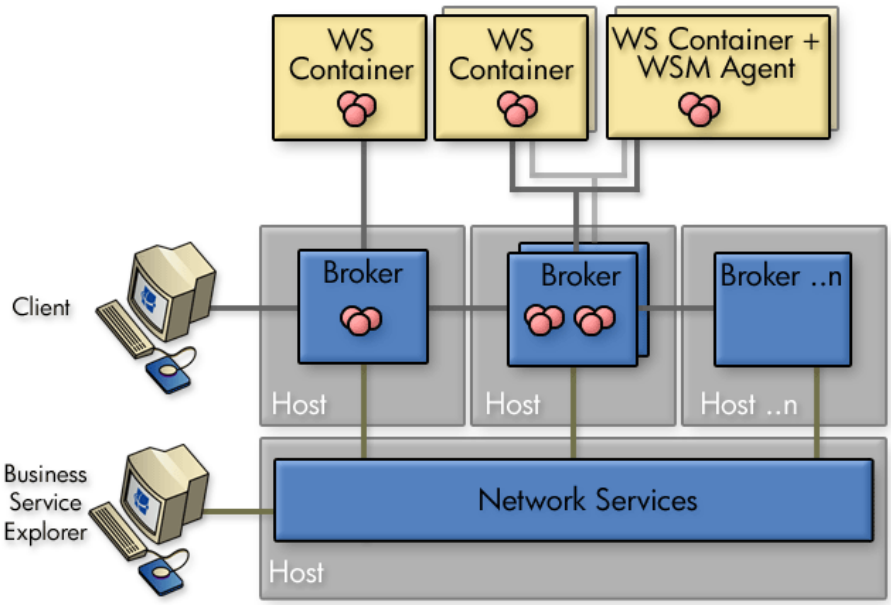


Figure 1-7: Broker-Based Scenarios

WSM Agent-Based Scenario

A WSM Agent-based scenario utilizes agents that are integrated into a WS Container. The WSM Agents run in the same process as the WS Container. There is an agent for the WebLogic Server WS Container and the Microsoft .NET WS Container.

Any number of WSM Agents can be used in a production environment. In scenarios where a single service is replicated across multiple machines, management data and metrics are aggregated. For more information on installing and configuring the WSM Agents, see the *WSM J2EE Agent Administrator Guide* and the *WSM .NET Agent Administrator Guide* respectively.

Figure 1-8 shows a WSM Agent-based scenario that mixes both a .NET Agent as well as a J2EE Agent.

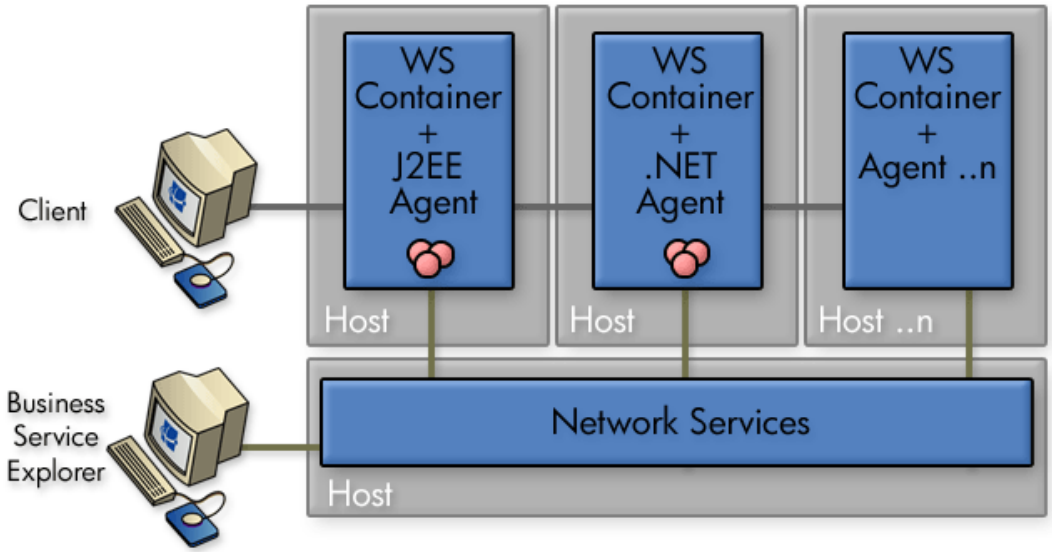


Figure 1-8: WSM Agent Scenario

Broker vs. Agent Deployment

This following table shows a quick overview of when to consider using the different WSM deployment methods.

Table 1-1: Sample Table

Brokered Web services	Agents
You do not have control of the deployment environment or the Web service itself (for example, if you want to monitor an external Web service that is part of a composite application).	You control the deployment environment and are planning to deploy to either a WLS or IIS container (for example, a Web service that is developed internally). You must keep your platform version in synch with SOA Manager Agent releases.

Brokered Web services	Agents
You have multiple instances of your Web service running on different containers and you want the Broker to determine which end point to route to at run-time (for example, load balancing and fail-over routing).	You want to monitor the health of the WLS or IIS container as well as the Web service itself.
You want to secure an individual Web service using an Authentication, Authorization, Audit (AAA) product like HP Select Access and the container it is running in does not provide native security.	You are already securing the WLS or IIS container the Web service is running in using an Authentication, Authorization, Audit (AAA) product like HP OpenView Select Access.
	You prefer not to separately deploy and manage extra servers (Broker) for managing Web services and are concerned about the latency imposed by using brokered Web services. Agents impose less latency than Brokers because there is no extra process hop.

2

Getting Started

The topics in this chapter provide instructions for completing basic tasks that are associated with using the SOA Manager software and are specific to Network Services. The chapter includes:

- Finance Example Overview
- Starting and Stopping the Network Services
- Starting the Business Services Explorer
- Configuring HTTP Settings
- Configuring an Oracle Database
- Configuring a UDDI Registry
- Adding People
- Using XPL Logging
- Using XPL Tracing

Finance Example Overview

A Web services-based example application is provided in the distribution and can be used to test the SOA Manager software. The Finance application is included as a convenience if you do not have a Web service-based application to test with while setting up the software. The Finance application is also used as part of the SOA Manager HTML-based tutorials that are located in the `/Documentation` directory of the distribution. The tutorials also include setup instructions.

The Finance application is located in the `/Examples` directory of the distribution. The example includes a Web service for the Tomcat, BEA WebLogic Server (WLS), and the .NET platform. In addition, a client is included with the example. The client is only available for the Windows platform.

The Microsoft .NET Redistributable Package and Microsoft WSE 2.0 must be installed on the computer where the Finance application client is installed.

Setting Up the Finance Application

To set up the Finance application:

1. Deploy the finance service (`axis.war`, `finance-service.ear`, or `FinanceServiceInstaller.msi`) to either the Tomcat, WLS, or .NET platform respectively.
2. Install the Finance client, using `/Examples/FinanceService/client/FinanceSetup.msi`.
3. From the directory where you installed the Finance client, click `FinanceClient.exe`. The HP Finance Client (.NET) application starts.
4. Click the **Configuration** tab.
5. In the Server URL field, enter URL for the deployed finance server. For example,

   When using Tomcat enter:

   `http://<host:port>/axis/services/FinanceServiceSoap?wsdl`

   When using WLS enter:

   `http://<host:port>/FinanceService/FinanceService`

   When using .NET enter:

   `http://<iis_host>/FinanceService/FinanceService.asmx`
6. Click **Apply**.
7. Click the **Quotes and Information** tab.
8. In the Symbol field, enter `hpq` and click **Get Quote**. The quote information is returned in the Results section. You can also enter `MSFT`, `IBM`, and `BEAS`. Any other symbol will generate an exception.

Starting the Network Services

A script for both Windows and UNIX is provided to start the Network Services server. The script is located in <*install_dir*>`/bin/win32` and <*install_dir*>`/bin/unix` respectively.

Windows users can choose to create product icons during the SOA Manager installation. If you accepted the default program group during installation, you can start the Network Services server by clicking **Start | Program Files | SOA Manager 2.1 | Network Services**.

Make sure an environment variable MIP_JAVA_HOME was created during the SOA Manager installation. The Network Service server will not start if the environment variable is not set. This variable must be set to the JDK you want the Network Services to use. See the *SOA Manager Installation Guide* for Java version requirements.

To start the Network Services server:

1 Open a command prompt.

2 Depending on your platform, change directories to <*install_dir*>\bin\win32 or <*install_dir*>\bin\unix.

3 Run the networkservices startup script. The console outputs log messages as the Network Services starts. The Network Services has started when you see the message:

```
MIP Server startup completed in # seconds.
```

During the SOA Manager installation, you had the option to install Network Services as a Windows Service. If you chose this option, the Network Services is already running. Attempting to start Network Services again causes an error.

Installing the Network Services as a Windows Service

If you choose not to install the Network Services as a Windows service during the installation, a batch script is provided that installs the Network Services as a Windows service. This allows the server to automatically start whenever Windows is started. The script can also be used to remove the Network Services from being a Windows service.

To install the Network Services as a Win 32 Service:

1 Open a command window.

2 Change directories to <*install_dir*>\bin\win32\services.

3 Run service-manager.bat and specify the following arguments:

```
service-manager.bat -install networkservices <install_dir>
```

The service has been successfully installed when the following message appears in the console:

```
Service "HP OpenView SOA Manager v2.1 networkservices" installed.
```

The script configures the network services server to automatically start the next time Windows is started. You must use the Windows Computer Management Console to change this behavior.

To remove the service, run the service-manager script and specify -remove. For example,

```
service-manager.bat -remove networkservices <install_dir>
```

Stopping the Network Services

The Network Services server can be stopped using the stop process methods that are appropriate for the host operating system.

Windows

Switch to the command window where the server process is running and type `Ctrl+c`. Then type `y` to terminate the process.

If the Network Services server is running as a Windows service, the service must be stopped. To stop a Windows service, open the Control Panel and select **Administrative Tools**. From the Administrative Tools screen, select **Services**. From the Services screen, right-click the Network Services service and select **Stop**.

UNIX

When using Linux or HP-UX, open a terminal window and issue the following command:

```
ps -ef | grep java
```

The command lists all current Java processes, including the process number. Find the Network Services server process and issue the `kill` command to stop the process. For example:

`kill` <*process number*>

Starting the Business Service Explorer

The Network Services server is administered through the Business Service Explorer (BSE). The BSE is a Web application that runs on port 5002. A different port can be specified in the <*install_dir*>`\conf\networkservices\mipServer.xml` file.

To start the BSE:

1. Start the Network Services as described above.
2. Open a Browser.
3. Enter the following URL and substitute <*host*> with the host name where the Network Services server is running:

   `http://<host>:5002/bse`
4. The default credentials are `admin` for the user name and `password` for the password.
5. Click **Login**. The Business Service List screen displays.

The Network Services server version (including installed patches) is located above the copyright statement at the bottom of each page.

Assigning Access to the BSE Console

The <*install_dir*>\conf\networkservices\mipServer.xml file allows you to define user credentials for accessing the BSE console. In particular, you can define user names and passwords for accessing the console. A single role, admins, has been implemented. All users must be associated with this role. This feature is typically only used while testing the SOA Manager software.

The SOA Manager also integrates with Select Access, which can be used to secure access to the BSE console. See Chapter 10 "Integrating with Select Access" for more information. Select Access is the preferred method for securing access to the BSE console in production installations.

To add access rights for a user:

1. Stop the Network Services if it is currently started.
2. Use a text editor to open <*install_dir*>\conf\networkservices\mipServer.xml.
3. Comment out the following entry:

```
<entry name="com.hp.mip.security.provider.console">default</entry>
```

4. Add a new user and password entry. For example:

```
<entry name="com.hp.mip.server.security.user">Joe User</entry>
<entry name="com.hp.mip.server.security.password">password</entry>
```

5. Save and close the file.
6. Restart the Network Services.

Configuring HTTP Settings

The Network Services server contains an HTTP server. The server is used to accept HTTP requests for the BSE.

This section covers:

- Configuring the HTTP Server Port Number
- Configuring the HTTP Server Thread Settings

Configuring the HTTP Server Port Number

The Network Services contain a Java HTTP Server that listens for HTTP messages and is used by the BSE console. The HTTP Server is configured in the <*install_dir*>\conf\networkservices\mipServer.xml file. The default port used by the HTTP Server is 5002. If port 5002 is currently being used, the Network Services will not start.

To configure the port number:

1. Stop the Network Services if it is currently started.
2. Use a text editor to open <*install_dir*>\conf\networkservices\mipServer.xml.

3 Change the port number for the `com.hp.http.server.port` entry. For example:

```
<entry name="com.hp.http.server.port">5003</entry>
```

4 Save and close the file.

5 Restart the Network Services.

Configuring HTTP Server Thread Settings

You can change the manner in which the HTTP server manages threads. Thread management can help increase performance and improve latency for the HTTP Server. There are three thread settings:

- `<entry name="com.hp.http.threads.max">` – The maximum number of threads allowed to be used by the HTTP server.
- `<entry name="com.hp.http.threads.min">` – The minimum number of threads allowed to be used by the HTTP server.
- `<entry name="com.hp.http.threads.maxIdle">` – The maximum amount of time in milliseconds that an HTTP server thread can remain idle.

To configure the HTTP server thread settings:

1 Stop the Network Services if it is currently started.

2 Use a text editor to open <*install_dir*>`\conf\networkservices\mipServer.xml`.

3 Configure the HTTP Server Thread settings. For example:

```
<entry name="com.hp.http.threads.max">50</entry>
<entry name="com.hp.http.threads.min">2</entry>
<entry name="com.hp.http.threads.maxIdle">60000</entry>
```

4 Save and close the file.

5 Restart the Network Services.

Configuring the Refresh Setting

The BSE contains a refresh feature that periodically auto-refreshes screens that have dynamic information. If this feature is disabled, you must manually refresh a screen to view the most current information. The feature can be configured to refresh at any interval (in Seconds).

The refresh feature is disabled by default. When enabled, the refresh image in the top right corner of the BSE is animated. This feature can also be enabled/disabled by clicking on the refresh image.

To configure the refresh setting:

1 Log in to the BSE.

2 From the BSE main tool bar, click **Settings**. The Settings screen displays.

3 From the General Settings tab, enter the interval (in Seconds) to wait before an auto-refresh.

4 Click to select the **Refresh enabled** check box.

5 Click **Update Settings**.

Configuring an Oracle 9i Database

The Network Service persists service messages, service trace messages, and alerts to a database. The SOA Manager software includes the HSQL database which is a light-weight database. This database can be used for testing. However, for production environments, a database schema for creating the data tables in Oracle 9i is provided. See the Oracle 9i documentation if you are not familiar with creating data tables using a schema file.

The schema for creating the tables in Oracle is located at <*install_dir*>\data\oracle\CollectionService-Create-Oracle9i.SQL. After you create the database and run the schema, configure the Network Services to use the database.

You must copy the 9.2.0.5.0 version of the oracle thin JDBC driver (oracle_ojdbc14.jar and oracle_nls_charset12.jar) into the <*install_dir*>/lib/ext directory. These .jar files are available from the Oracle website.

To configure the Network Services to use the Oracle 9i database:

1 Stop the Network Services server if it is currently started.

2 Open <*install_dir*>\conf\networkservices\mipServer.xml.

3 Uncomment the Database Properties section and add your database information. For example:

```
<entry name="com.hp.db.demo">false</entry>

<!-- The demo entry must be set to false. -->

<entry name="com.hp.db.driver">
   oracle.jdbc.driver.OracleDriver</entry>
<entry name="com.hp.db.url">
   jdbc:oracle:thin:@host:1521:DB1</entry>
<entry name="com.hp.db.user">admin</entry>
<entry name="com.hp.db.password">admin</entry>
```

4 Save and close the file.

5 Restart the network services.

Configuring Timezones

Oracle database versions less than 9.2.0.5 use the small time zone file (`timezone.dat`) by default. This file does not contain several time zone region names including many European time zone names. If you are running the Network Services server in a time zone that is not in the Oracle small time zone file, check to see if the time zone is in the large time zone file (`timezlrg.dat`).

If your Oracle installation is on UNIX, you can configure Oracle to use the large time zone file by setting an environment variable:

```
ORA_TZFILE=$ORACLE_HOME/oracore/zoneinfo/timezlrg.dat
export ORA_TZFILE
```

If your Oracle installation is on Windows, you must modify the Windows registry and add the `ORA_TZFILE` parameter to the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOMEID` subkey and set it to `$ORACLE_HOME/oracore/zoneinfo/timezlrg.dat`.

You must restart the Database for the change to take effect.

Performing Database Maintenance

As with all databases, you must monitor the database and periodically do maintenance to control the size of the database. Some example SQL scripts are provided to remove old alerts and trace messages from the SOA Manager database. The SQL scripts are located in:

<*install_dir*>`\data\oracle\CleanAlerts-Preview-Oracle9i.SQL`

<*install_dir*>`\data\oracle\CleanAlerts-Oracle9i.SQL`

<*install_dir*>`\data\oracle\CleanAudits-Preview-Oracle9i.SQL`

<*install_dir*>`\data\oracle\CleanAudits-Oracle9i.SQL`

Migrating an SOA Manager Database

The SOA Manager's distribution includes a script to migrate an SOA Manager 2.0 database to a 2.1 database. The script preserves current 2.0 data in the database.

To migrate the database:

1. Stop the 2.1 Network Services server if it is currently started.
2. Run the migration script, <*2.1_install_dir*>`/data/oracle/Upgrade2.0Db-Oracle9i` to migrate 2.1 database.
3. Start the 2.1 version of network services.
4. From a browser go to `http://`<*host*>`:5002/bse/support/clean_versions.jsp`. This page is used to correct defects in a migrated SOA Manager 2.0 database.

5 Click **Remove** to remove excess rows. This operation could take several minutes up to an hour to complete depending on the number of rows. The web page shows the progress as rows are removed.

Configure a UDDI Registry

A UDDI Registry must be configured with Network Services server before you can use the BSE to publish the SOA Manager's assets to the registry.

If your UDDI Registry is accessed using SSL, you must configure the Network Services server's SSL settings. See Chapter 9, "Using SSL for the Management Channel."

To register a UDDI Registry:

1 From the BSE main tool bar, click **Settings**. The Settings screen displays.

2 Click the **UDDI Settings** tab.

3 Enter the UDDI Registry settings:

- **Username for UDDI Publishing**: A user's name used to access the registry.
- **Password for UDDI Publishing**: The user's password.
- **UDDI Registry Inquiry URL**: The URL used to connect to the registry and make inquiries. For example, `http://<host>:<port>/uddi/inquiry`.
- **UDDI Registry Publish URL**: The URL used to connect and publish to the registry. For example, `http://<host>:<port>/uddi/publishing`.
- **Maximum Rows Returned for Provider Query**: Constrains the number of Providers that are returned when the UDDI Registry is queried.

4 Click **Save**.

5 Restart the Network Service server.

UDDI Settings can also be manually entered in *<install_dir>*`\conf\networkservices\mipServer.xml`.

Adding People

There are often different people or groups of people that play important roles in the management of the SOA Manager's assets (i.e., business and IT services). Business and IT service lists in the BSE can be filtered by people and their roles. For example, the user can choose to only display services that are owned by the finance department. The service filters are saved in the user's session.

The SOA Manager does not attempt to replicate the features of an identity management server, but provides some basic contact information while allowing associations to people and groups in a directory server.

There are two roles within SOA Manager that a person can assume:

- **Owner**: The owner of a business or IT service is generally responsible for lifecycle management and publishing of the service.
- **Support**: The person or group responsible for supporting deployed instances of the service.

The owner and support roles are assigned to business services and IT services. This is discussed in more detail in subsequent chapters.

To add people:

1 From the BSE main tool bar, click the **People** tab. The People screen displays.

2 Click **Add**. The Create People screen displays.

3 Complete the following the fields:

— **Name** – Common name used to identify the party.

— **Email** – Email address that can be used to contact the party.

4 Click **Save**. The People screen displays, and the new party is listed.

Using XPL Logging

SOA Manager uses HP OpenView Cross Platform (XPL) logging. Installation, configuration, and usage are described below.

Installing XPL Logging

During the SOA Manager installation, you may have been prompted to select the HP OpenView installation and data directories. You will only be prompted for this information if this is the first time you have installed an HP OpenView product.

The default value for the installation directory is `C:\Program Files\HP OpenView` on Windows and `/opt/OV` on UNIX. The default value for the data directory is `C:\Program Files\HP OpenView\data` on Windows and `/var/opt/OV` on UNIX. The Network Services log files are created in the log subdirectory of the data directory. If you do not run Network Services as an administrator, you may need to change the permissions for the log subdirectory.

XPL Tools

The HP OpenView Cross Platform Component contains logging and tracing tools. If you need to change the default log file configuration parameters, install the component. Run the appropriate installer in the /Support directory of the SOA Manager CD.

Configuring XPL

The Network Services automatically creates log files in the log subdirectory of the HP OpenView data directory. The Network Services log file name has the format:

networkservices[unique].sequence.locale

For example:

`networkservices0.0.en_US`

This file is the first network services log file created for the US English locale.

Network Services creates a log file for an English locale and a second file for your system's locale if it is different from English.

The Network Services creates up to 10 log files, each file containing up to 1 megabyte of data. The log files will have sequence numbers 0 through 9. When the maximum number of log files is exceeded, the sequence 0 log file is overwritten.

You can change the maximum number of log files and log file size using the HP OpenView Cross Platform tool, `ovconfchg`. After installing the HP OpenView Cross Platform Component, this program is in the `/bin` directory of the HP OpenView installation directory. An example of using this tool is shown below.

```
ovconfchg -ns xpl.log.OvLogFileHandler -set filecount 12
-set filesize 2
```

This command sets the maximum number of log files to 12 and the maximum log file size to 2 megabytes.

Restart the Network Services Server for the new configuration to take effect.

You can see the current configuration using this command:

`ovconfget`

For more information about `ovconfchg` and `ovconfget`, see the help documentation in the help subdirectory of the HP OpenView installation directory.

Configuring Log Levels

You can change the Network Services log levels using the BSE. Alternatively, you can change the log levels by editing the `logging.properties` file in the JDK `/lib` directory or the `xpllogging.properties` in the <*install_dir*>`/conf/networkservices` directory. The log levels are: `SEVERE`, `WARNING`, `INFO`, `FINE`, `FINER`, and `FINEST`. By default the log level is set to `INFO`.

Using the BSE

The edit/query log level feature provides the ability to edit/query log levels for different log categories that are configured for the Network Services. Different log levels and log categories provide varying levels of log details that can help identify process events that are occurring in the Network Services server.

To edit/query log levels:

1. From the BSE main toolbar, click **Settings**. The Settings screen displays and the General Settings tab is selected by default.
2. Click the **Edit/Query BSE Log Levels**. The Edit/Query Log Levels screen displays in a new browser window. The default root logger and its current log level displays.
3. Using the Log Level drop-down list, select a new log level.
4. Click **Update Settings**. The log level for this logger is updated on the Network Services server. The log file will now display any log messages that are sent to this log level. If no code uses this logger or this particular log level, than no new messages are displayed.
5. In the Logger field, change the Root logger to `MIP`. Any string can be entered in the Logger field. You can also set the log level for individual packages. The Network Services packages begin with `com.hp.ov.mip`.
6. Click **Query**. The Log Level field updates and displays the current log level for the logger. If you query a logger that is not currently implemented, the Log Level field displays Unknown. If you save a logger that is not currently implemented in the Network Services, the logger is created on the Network Services and the log level selected is set. Although, since no code is using the logger, no new messages are displayed.
7. Repeat steps 3 and 4 to change the log level.
8. Click **Cancel** to close the Edit/Query Log Levels screen.

Using JRE Properties File

You can change the log level for Network Services by editing the `logging.properties` file in the `JRE /lib` directory. You must restart Network Services for the changes take effect. For example, you can add the following line to the end of the file:

```
com.hp.ov.mip.level = FINE
```

This sets the log level for the Network Services to `FINE`.

Using the XPL Properties File

You can change the log level for Network Services by editing the `xpllogging.properties` in the <*install_dir*>`/conf/networkservices` directory. You must restart Network Services for the changes take effect. For example, you can add the following line to the end of the file:

```
com.hp.ov.mip.level = FINE
```

This sets the log level for Network Services to `FINE`.

Viewing Logs

You can use an editor or the BSE to view the Network Services log files. From the BSE main toolbar, click **Settings** to go to the settings page and then click **View BSE Log**. Alternatively, use an editor to view the network services log files in the HP OpenView data log directory.

Using XPL Tracing

SOA Manager uses the HP OpenView Tracing tools for tracing. Refer to the *HP OpenView Tracing Concepts Guide* for detailed information on how to use the trace feature. The guide is located on the SOA Manager CD in the `/Documentation` directory.

Installation

Before beginning this procedure, verify if the HP OpenView Tracing tools are already installed on your system. You can check to see if the trace server is installed. On UNIX, the trace server is installed as `/opt/OV/lbin/xpl/trc/ovtrcd`. On Windows, the trace server is installed as `C:\Program Files\HP OpenView\bin\ovtrcsvc.exe`.

The tracing tools are located on the SOA Manager CD in the `/Support` directory.

Windows

To install the tracing tools on a Windows system, double-click on `/Support/HPOvXpl-<version>-release.msi`.

HP-UX

To install the tracing tools on an HP-UX system, run:

```
swinstall -s /Support/HPOvXpl-<version>-HPUX11.0-release.depot \*
```

Linux

To install the tracing tools on a Linux system, run:

```
rpm -Uhv /Support/HPOvXpl-<version>-Linux2.4-release.rpm
```

Example Configuration Entries

The following SOA Manager entries are example entries for the XPL configuration file:

```
TCF Version 3.2
APP: "networkservices"
SINK: Socket "system1.acme.com" "node=192.1.60.106;"
TRACE: "mip.config" "Operation" Info Error
TRACE: "mip.config" "Parameters" Info Error
TRACE: "mip.config" "Procedure" Info Error
TRACE: "mip.metrics" "Operation" Info Error
TRACE: "mip.metrics" "Parameters" Info Error
TRACE: "mip.metrics" "Procedure" Info Error
TRACE: "mip.slos" "Operation" Info Error
TRACE: "mip.slos" "Parameters" Info Error
TRACE: "mip.slos" "Procedure" Info Error
TRACE: "mip.deploy" "Operation" Info Error
TRACE: "mip.deploy" "Parameters" Info Error
TRACE: "mip.deploy" "Procedure" Info Error
```

3

Managing Resources Using IT Services

This chapter provides instruction for creating and maintaining IT services as well as registering IT service resources. These tasks are completed using the BSE. IT services are part of the service model definition and an integral part of managing SOA resources using the SOA Manager software.

Overview

An IT service is an abstract concept that can mean different things to different people. Within the scope of the SOA Manager's service model, an IT service is the virtualization of management information and capabilities of a group of IT resources. The IT service can represent a single IT resource or can be a collection of resources that are managed together in some meaningful way. Typically, this model is used to organize resources that are similar. For example, an IT service could be used to organize all the managed WS containers for a specific application.

The IT services that are supported include:

- **WS Container Services**: This type of IT service captures the management of WS containers and their hosted Web services. The WS container IT service supports the deployment, discovery, and SLO monitoring of a Web service implementation deployed to multiple Web services containers. A WS container must expose its manageability using a WSM Agent (J2EE or .NET).
- **WS Intermediary Services**: This type of IT service captures the management of WS intermediaries and their hosted brokered services. The WS intermediaries IT service supports the deployment, discovery, and SLO monitoring of a brokered service. The WSM Broker is a WS intermediary.
- **Database Services**: This type of IT service is used to capture the management of databases that are used by a service-based application. You can also create a database IT service for the SOA Manager's database.

- **Host Services**: This type of IT service is used to capture the management capabilities of a host that is part of a grid that is built using the Globus Toolkit (a de-facto open source grid middleware). The manageability characteristics of a Globus grid-based host are accessed using Globus's Monitoring and Discovery Service (MDS) component. Moreover, the MDS component utilizes the Ganglia monitoring system as an information provider to capture low-level metrics and attributes of resources such as CPU load or number of processes. Globus Toolkit and Ganglia are not packaged with the SOA Manager product. For more information about the Globus Toolkit and Ganglia, refer to Globus Toolkit (version 4) and Ganglia Monitoring System. HP grid-related offerings can be found at http://www.hp.com/go/grid.
- **MOM Services**: This type of IT service is used to capture the management of JMS servers. The JMS server must expose its manageability using the MOM Agent. The current SOA Manager release only supports the JMS server included with WebLogic Server.

Figure 3-1 below shows a conceptual view of an IT services for both a WS container IT service and a WS intermediary IT service.

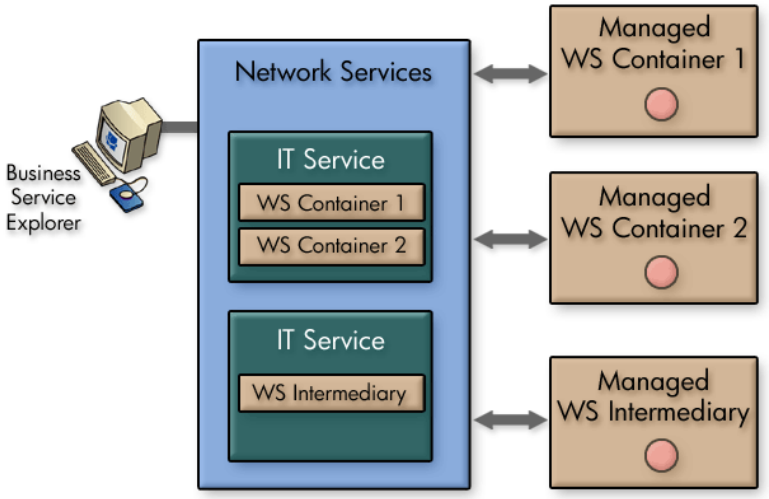


Figure 3-1: Conceptual View of IT Services

Creating IT Services

This section provides instructions for creating an IT service using the BSE. The instructions are specific to the type of IT service that is being created. Once an IT service is created, you can register any number of resources to the IT service. Instructions for registering resources to an IT service are provided in the "Registering Resources" section below.

Create a WS Intermediary IT Service

To create a WS intermediary IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.
2. From the WS Intermediary Services section, click **Add**. The Add WS Intermediary Service screen displays.
3. Complete the following fields:
   - **Name**: A descriptive name for the IT service.
   - **Description**: A description for the IT service.
   - **Owner**: Use the drop-down list to select an owner of the IT service. The owner of an IT service is generally responsible for lifecycle management and publishing of the service. See the "Adding People" section in Chapter 2.
   - **Support**: Use the drop-down list to select a support person of the IT service. The person or group responsible for supporting deployed instances of the service. See the "Adding People" section in Chapter 2.
   - **Availability**: This check box indicates that an alert is generated when the IT service is not operational (e.g., when a managed WS intermediary that is contained in the IT service is not available).
   - **Alert Recipients**: The alert categories that are used for this IT service. Use the respective drop-down lists to select alert categories for both degraded and failed alerts. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 "Using Alert Notifications."
4. Click **Save**. The IT service is created and its view screen displays.
5. Repeat this procedure to create additional WS intermediary IT services or refer to the "Registering Resource" section to add a resource to this IT service.

Create a WS Container IT Service

To create a WS container IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.
2. From the WS Container Services section, click **Add**. The Add WS Container Service screen displays.

3 Complete the following fields:

- **Name**: A descriptive name for the IT service.
- **Description**: A description for the IT service.
- **Owner**: Use the drop-down list to select an owner of the IT service. The owner of an IT service is generally responsible for lifecycle management and publishing of the service. See the “Adding People” section in Chapter 2.
- **Support**: Use the drop-down list to select a support person of the IT service. The person or group responsible for supporting deployed instances of the service. See the “Adding People” section in Chapter 2.
- **Availability**: This check box indicates that an alert is generated when the IT service is not operational (e.g., when a managed WS container that is contained in the IT service is not available).
- **Alert Recipients**: The alert categories that are used for this IT service. Use the respective drop-down lists to select alert categories for both degraded and failed alerts. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 “Using Alert Notifications.”

4 Click **Save**. The IT service is created and its view screen displays.

5 Repeat this procedure to create additional WS container IT services or refer to the “Registering Resource” section to add a resource to this IT service.

Create a Database IT Service

A database IT service pings a database every 30 seconds to see if it is responding. It is configured using the standard JDBC driver settings which are summarized below. If the database IT service fails to ping the database, it will generate an alert.

To create a database IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.

2 From the Database Services section, click **Add**. The Add New Database Service screen displays.

3 Complete the following fields:

- **Name**: A descriptive name for the database IT service.
- **Version**: A version for the database IT service
- **Description**: A description for the database IT service.
- **Driver**: The database’s JDBC driver type. You can only select Oracle or Hypersonic.
- **URL**: The driver-specific URL used to connect to your database.
- **Login**: The login name for the user account used to access the database.
- **Password**: The password for the user account used to access the database–if applicable. The password field can be left blank.

- **Owner**: Use the drop-down list to select an owner of the IT service. The owner of an IT service is generally responsible for lifecycle management and publishing of the service. See the "Adding People" section in Chapter 2.
- **Support**: Use the drop-down list to select a support person of the IT service. The person or group responsible for supporting deployed instances of the service. See the "Adding People" section in Chapter 2.
- **Availability**: This check box indicates that an alert is generated when the database IT service is not operational (i.e., when a ping of the database fails).
- **Alert Recipients**: The alert category that is used for this IT service. All alerts that are generated for this IT service will be sent to this category. Use the drop-down list to select an alert category. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 "Using Alert Notifications."

4 Click **Save**. The database IT service is created and its view screen displays.

5 Repeat steps 2 through 4 to create additional database IT services.

Create a Host IT Service

A host IT service tries to connect to a Globus MDS component or a Ganglia monitoring system to see if it is responding and to collect metrics such as processor load and available virtual memory. If the connection fails, an alert is generated. A system running a Globus MDS or Ganglia Monitoring Daemon is required to complete these steps. Additional information about the Globus Toolkit and Ganglia are included in Chapter 3 of the *Concepts Guide*.

To create a host IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.

2 From the Host Services section, Click **Add**. The Add New Host Service screen displays.

3 Complete the following fields:

- **Name**: A descriptive name for the host IT service.
- **Version**: A version for the host IT service.
- **Description**: A description for the host IT service.
- **URL**: The URL to connect to either a Ganglia Monitoring Daemon service (e.g., <*host*>:`8649`) or the URL to connect to the Globus MDS component (e.g., <*host*>:`8080`) that is deployed to the Tomcat servlet container or to the standalone SOAP container bundled with the Globus Toolkit.

  Replace <*host*> with the full DNS name of the server. Ports `8649` and `8080` are used as examples. Change these values if a different port is being used.
- **Owner**: Use the drop-down list to select an owner of the IT service. The owner of an IT service is generally responsible for lifecycle management and publishing of the service. See the "Adding People" section in Chapter 2.

- **Support**: Use the drop-down list to select a support person of the IT service. The person or group responsible for supporting deployed instances of the service. See the “Adding People” section in Chapter 2.
- **Availability**: This check box indicates that an alert is generated when the host IT service is not operational (i.e., connection to the Ganglia Daemon fails).
- **Alert Recipients**: The alert category that is used for this IT service. All alerts that are generated for this IT service will be sent to this category. Use the drop-down list to select an alert category. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 “Using Alert Notifications.”

4 Click **Save**. The IT service is created and its view screen displays.

5 Repeat this procedure to create additional host IT services.

Create a MOM IT Service

To create a MOM IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.

2 From the MOM Services section, click **Add**. The Add New MOM Service screen displays.

3 Complete the following fields:

- **Name**: A descriptive name for the IT service.
- **Description**: A description for the IT service.
- **Owner**: Use the drop-down list to select an owner of the IT service. The owner of an IT service is generally responsible for lifecycle management and publishing of the service. See the “Adding People” section in Chapter 2.
- **Support**: Use the drop-down list to select a support person of the IT service. The person or group responsible for supporting deployed instances of the service. See the “Adding People” section in Chapter 2.
- **Availability**: This check box indicates that an alert is generated when the IT service is not operational (i.e., when a JMS server that is contained in the IT service is not available).
- **Alert Recipients**: The alert categories that are used for this IT service. Use the respective drop-down lists to select alert categories for both degraded and failed alerts. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 “Using Alert Notifications.”

4 Click **Save**. The IT service is created and its view screen displays.

5 Repeat this procedure to create additional MOM IT services or refer to the “Registering Resource” section to add a resource to this IT service.

Registering Resources

This section provides instructions for registering resources to an IT service. The instructions should be completed after completing the instructions in the "Creating IT Services" section above. The instructions in this section are organized based on the type of resource that is registered.

Registering WS Container and WS Intermediary Resources

When a managed WS container or WS intermediary is registered, its hosted Web services or brokered services are automatically discovered and registered as well. As services are added and removed from a WS container or WS intermediary, they are automatically added and removed from the IT service.

To register a container or intermediary resource:

1 Make sure the managed WS containers or WSM Brokers that you want to register are started.

Instructions for setting up managed WS containers and the WSM Broker are located in separate administrator guides. The guides are located in the `/Documentation` directory of the distribution.

Some Network Services features may not work as expected when using WS container/intermediary versions that are different than the Network Services server version. It is recommended that the Network Services server version and the WSM Agents and WSM Broker versions match.

2 From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.

3 Select the IT service you want to contain the resource. The IT Services View screen displays for the selected IT service.

4 From the Contained Resources section, click **Add**. The Add WS Intermediary / Container screen displays.

5 From the **Type** drop-down box, select the type of resource you want to register.

6 Using the fields provided, enter the host and port where the managed resource is installed. For WLS, you will also need to supply the Standalone Server name or Cluster name where the WSM J2EE Agent is installed.

The WSM Agents and the WSM Broker publish their management interface (WSDL) to a URL. The BSE uses the information entered in this step to construct the URL. Once you become familiar with the URL format, you can use the URL text box to enter the URL to the management WSDL.

7 Click the SSL check box if you want the management channel to this resource to be secured. To use this feature you must first set up the appropriate security components. See the "Using SSL for the Management Channel" chapter.

8 Click **Add**. The Add WS Intermediary / Container screen redisplays and the Contained Web Services section lists the Web services that are discovered in the managed WS Container/WS intermediary.

9 Click **Add**. The WS Intermediary / Container View screen displays and the Contained Web Services section lists the resources that are now registered in the IT service.

10 Repeat this procedure to register additional resources for this IT service.

Registering MOM Resources

Managed JMS servers are registered within a MOM IT service. When a JMS server is registered, all queues and topics in the JMS server are automatically discovered and registered in the Network Services server.

To register a JMS server:

1 Make sure the managed JMS servers that you want to register are started.

Instructions for setting up a MOM Agent to manage JMS servers are located in the *WSM J2EE Agent Administrator Guide*. Setup the MOM Agent before completing the instructions in this section.

2 From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.

3 From the MOM IT Services section, select the MOM IT service you want to contain the resource. The MOM Service screen displays.

4 From the Contained Resources section, click **Add**. The Add MOM Server screen displays.

5 In the Host field, enter the host where the MOM Agent is deployed.

6 In the Port field, enter `7001`.

Or,

In the WSDL Location field, enter the URL to the MOM Agent's management Web service WSDL as follows:

`http://<host>:<port>/MOM/MOMAgent?WSDL`

7 Click **Add**. The MOM Servers screen displays and lists all the discovered JMS servers including any discovered topics and queues.

8 Select the JMS Server resource that is to be included in this IT service.

9 Click **Add**. The resource is added to the IT service.

10 Repeat this procedure to register additional resources for this IT service.

Registering Host Resources

A host IT service is used to register the hosts on which the Ganglia monitoring system and/or the Globus MDS components are installed.

To register a host:

1. Make sure the hosts that you want to register are operational.
2. From the BSE main tool bar, click **IT Services**. The IT Service Summary screen displays.
3. From the Host Services section, select the Host IT service to which you want to register the resource. The Host Service Details screen displays.
4. From the Contained Resources section, click **Add**. The Add Host screen displays and lists any discovered hosts.
5. From the list of discovered hosts, select a host to be included in this Host IT service.
6. Click **Add**. The Host Service Details screen displays and lists the new host as well as the status of the host.
7. Repeat this procedure to register additional resources for this IT service.

Managing Web Service Resources

Registered resources have a view screen that provides details about the resource as well as basic operations that allow you to interact and manage the resource.

From this screen, you can:

- Select a Web or brokered service to view its details
- View log traces for the resource
- Check the availability of a resource
- View/Acknowledge alerts that are currently active for a resource
- Delete a resource

Viewing Registered Resources

To view details about a registered resource:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view. The IT Services View screen displays for the selected IT service.
3. From the Contained Resources section, click a resource to view it. The resource's view screen displays. Each service in the resource is listed in the Contained Web services section. You can click a service link to view the service's details including a performance graph and a list of web service operations. In addition, you can click an operation to see its properties and performance graph.

Viewing Log Traces

The log trace feature is a convenient way to view the log file for a registered WS container/intermediary from within the BSE without having to log on to multiple remote computers. The log traces are used to troubleshoot problems or to verify that a WS container/intermediary is operating successfully.

To view Log Traces:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view. The IT Services View screen displays for the selected IT service.
3. From the Contained Resources section, click a resource to view it.
4. From the Logging Level section, click **View Log**. A new browser window displays and lists the last 20 log messages.
5. Use the text box to change the amount of entries to be displayed.
6. Click **Go** to refresh the window.
7. When you are done viewing the log messages, click **Close** to close the browser window.

Editing and Querying Log Levels

The edit/query log level feature provides the ability to query/edit log levels for different loggers that are configured in a managed a WS container/intermediary. Different log levels and loggers provide varying levels of log details that can help identify process events.

A WS container/intermediary contains a predefined set of loggers. For .NET, two categories (WSMF and WsmfLibs) are used. For WLS containers and Broker-based intermediaries, loggers are defined in each agent's XPL configuration file. In addition, any custom loggers that are implemented in a WS container/intermediary can also be configured.

To edit/query log levels:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view. The IT Services View screen displays for the selected IT service.
3. From the Contained Resources section, click a resource to view it.
4. From the Logging Level section, click **Edit/Query Log Levels**. The Edit/Query Log Levels screen displays in a new browser window. The default root logger and its current log level displays.
5. Using the Log Level drop-down list, select a new log level.

6 Click **Save**. The log level for this category is updated on the WS container or WS intermediary. The log file will now display any log messages that are sent to this category's log level. If no code uses this logger or this particular log level, then no new messages are displayed.

7 In the Logging Category field, replace `MIP` with a logging category that is implemented on this WS container/intermediary. Any string can be entered in the Logging Category field.

8 Click **Query**. The Log Level field updates and displays the current log level for the category.

If you query a logging category that is not currently implemented in the WS container/intermediary, the Log Level field displays `Unknown`. If you save a logging category that is not currently implemented, the logging category is created and the log level selected is set. Although, since no code is using the logging category, no new messages are displayed.

9 Repeat steps 5 and 6 to change the log level for the logger.

10 Click **Cancel** to close the Edit/Query Log Levels screen.

Enabling Availability Notifications

The availability feature allows an alert notification to be sent to alert recipients whenever a registered WS container/intermediary is not available. Enabling this feature will quickly notify individuals when a WS container/intermediary is not operational and can help you determine why a Web service is failing.

To enable availability notifications:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of IT services, click the IT service you want to view.

3 From the Contained Resources section, click a resource to view it.

4 From the Status section, click **Edit Alerts**. The Availability screen displays.

5 From the Availability section, click the **Alert when unavailable** check box. A check indicates that availability notifications are enabled.

6 From the Alert Recipients section, use the Alert Recipient drop-down list to select a Recipient Category to receive the alert. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 “Using Alert Notifications.”

7 Click **Save**. Alerts are displayed in the Resource Alerts section.

To see a generated availability alert, manually shutdown the WS container/intermediary for which you enabled availability alerts. Refresh the screen. An alert message displays in the Alerts section and indicates that the WS container/intermediary is unavailable. Restart the WS container/intermediary. When the WS container/intermediary becomes available, an alert message displays in the Alerts section and indicates that the WS container/intermediary is available.

Deleting a Resource

You can delete an IT service resource at any time. This procedure is typically completed when a WS container/intermediary host is decommissioned or no longer used to host Web services. When you delete a WS container/intermediary, it is removed from the Network Services. If the resource is part of an IT service, it is removed from the IT service as well.

Deleting a WS container/intermediary also removes its Web services (or brokered services).

To deregister a WS container or WS intermediary:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view.
3. From the Contained Resources section, click a resource to view it.
4. Click **Remove**. A remove screen displays in a new browser window.
5. Click **Remove**. The Business Services screen displays.
6. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
7. From the list of IT services, click the IT service you want to view. The resource is removed from the Contained Resources section.

Managing WS Intermediary/Container IT Services

The View IT Service screen provides details about an IT service. The screen is a convenient way to view managed WS containers/intermediaries from the context of their IT service. From this screen, you can:

- View an IT service's details
- Edit an IT service
- Add/Remove resources from an IT service
- View/Acknowledge alerts that are currently active for the IT service
- Publish IT services to a UDDI registry
- Delete a WS container/intermediary IT service

Viewing a WS Container/Intermediary IT Service

An IT service's view screen provides information about the IT service, such as alerts, as well as features for editing the IT service.

To view an IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays. Alert and status information for each IT service is also listed.

2 Select the IT service you want to view. The view screen displays and contains a section for general information, a section for alerts, and a section that lists all WS container/intermediary resources that are contained in the IT service. The Contained Resources section also lists the current version of the WS container/intermediary resource as well as the resource's management WSDL.

Some Network Services features may not work as expected when using WS container/intermediary versions that are different than the Network Services server version. It is recommended that the Network Services server version and the WSM Agents and WSM Broker versions match.

Adding Resources

Any WS container/intermediary that is already registered with the Network Services can be added to an IT service. Typically, this procedure is used to add a WS container/intermediary in multiple IT services or move a WS container/intermediary between IT services. The later is required when you delete an IT service.

To add a WS container/intermediary to an IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of IT services, click the IT service you want to configure. The view screen displays for the selected IT service.

3 From the Contained Resources section, click **Edit**. The Edit WS Intermediary / Container IT Service screen displays.

4 From the list of WS containers or WS intermediaries, click the **Contains** check box for each resource you want to add to this IT service. A check mark indicates that the WS container/intermediary is selected.

5 Click **Save**.

Removing Resources

To remove a managed WS container/intermediary from an IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of IT services, click the IT service you want to configure. The view screen displays for the selected IT service.

3 From the Contained Resources section, click **Edit**. The Edit WS Intermediary / Container IT Service screen displays.

4 From the list of WS containers/WS intermediaries, click the **Contains** check box for each resource you want to remove from this IT service. An empty check box indicates that the resource is no longer selected.

5 Click **Save**.

Enabling Availability Notifications

Availability notifications generate alerts for an IT service whenever a managed WS container/intermediary that is contained in the IT service fails. This can be used to troubleshoot any problems that are encountered when managing Web services. Alerts are sent to an alert category which contains any number of alert recipients. For more information on setting up alert recipients and creating alert recipient categories, see chapter 5 “Using Alert Notifications”.

The IT service list indicates the alert status of all IT services. The View IT Service screen provides the details of the alert and also indicates which managed WS container/intermediary caused the alert.

It is good practice to enable availability notifications for a managed WS container/intermediary that is contained in an IT service. See the above section “Enabling Availability Notifications” for more information.

To enable availability notifications for an IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view. The view screen displays for the selected IT service.
3. Click **Edit**. The Edit WS Intermediary / Container IT Service screen displays.
4. From the Availability section, click the check box to enable availability notifications. A check indicates that availability notifications are enabled.
5. From the Alert Recipients section, use the drop-down list to select an alert category for both the Degraded and Unavailable availability status.
6. Click **Save**.

Publishing to a UDDI Registry

The BSE can publish IT services to a UDDI registry. IT services that are published to a UDDI registry can be reused by other applications. To use the UDDI feature, you must have a UDDI registry that is configured for use with the Network Services server. To configure a UDDI registry, see “Configure a UDDI Registry” in Chapter 2.

To publish an IT service to a UDDI registry:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view. The view screen displays for the selected IT service.
3. Click **Publish**. The Publish IT Service screen displays.
4. Using the Provider drop-down list, select a Business Entity in the UDDI registry.
5. Click **Publish**.

Deleting a WS Container/Intermediary IT Service

You can delete an IT service at any time. When you delete an IT service, its alerts are removed and its UDDI entries are deleted from the UDDI registry; however, any managed WS containers/intermediaries that are contained in the IT service are not removed from the Network Services and can be added to another IT service.

To delete an IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of IT services, click the IT service you want to view. The view screen displays for the selected IT service.
3. From the IT Service section, click **Remove**. A warning screen displays.
4. Click **Remove**. The IT Services Summary screen displays and the IT service is removed.

Managing Database IT Services

The Database Service Details screen provides details about a database IT service. From this screen, you can:

- View a database IT service's details
- Edit a database IT service
- View/Acknowledge alerts that are currently active for the database IT service
- Publish database IT services to a UDDI registry
- Delete a database IT service

Viewing a Database IT Service

To view a database IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the Database Services section, select the database IT service you want to view. The Database Service Details screen displays. The screen contains a section for general information and a section for alerts.

Editing a Database IT Service

To edit a database IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the Database Services section, select the database IT service you want to edit. The Database Service Details screen displays.

3 From the Database Service section, click **Edit**. The Edit Database Service screen displays.

4 Modify the provided fields. For field descriptions, see the "Creating a Database IT Service" section.

5 Click **Save**. The Database Service Details screen displays. The alert section indicates when the database IT service is operational.

Publishing to a UDDI Registry

The BSE can publish database IT services to a UDDI registry. Database IT services that are published to a UDDI registry can be reused by other applications. To use the UDDI feature, you must have a UDDI registry and configure the registry with the Network Services server. To configure a UDDI registry, see "Configure a UDDI Registry" in Chapter 2.

To publish a database IT service to a UDDI registry:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the Database Services section, select the database IT service you want to view. The Database Service Details screen displays.

3 From the Database Service section, click **Publish**. The Publish IT Service screen displays.

4 Using the Provider drop-down list, select a Business Entity in the UDDI registry.

5 Click **Publish**. The Database Service Details screen displays.

Deleting a Database IT Service

You can delete a database IT service at any time. When you delete a database IT service, it is removed from the Network Services server. In addition, all alerts for the database IT service are resolved and its UDDI entries are deleted from the UDDI registry.

To delete a database IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of Database IT services, click the IT service you want to delete. The Database Service Details screen displays.

3 From the Database Service section, click **Remove**. A warning screen displays.

4 Click **Remove**. The IT Services Summary screen displays and the database IT service is removed.

Managing Host IT Services

The Host Service Details screen provides details about a host IT service. From this screen, you can:

- View a host IT service's details
- Edit a host IT service
- View/Acknowledge alerts that are currently active for the host IT service
- Publish host IT services to a UDDI registry
- Delete a host IT service

Viewing a Host IT Service

To view a host IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the Host Services section, select the host IT service you want to view. The Host Service Details screen displays. The screen contains a section for general information, a section for alerts, and a section that displays all hosts that are registered within the host IT service.

Editing a Host IT Service

To edit a host IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the Host Services section, select the host IT service you want to edit. The Host Service Details screen displays.
3. From the Host Service Details screen, click **Edit**. The Edit Host IT Service screen displays.
4. Modify the fields. For field descriptions, see the “Creating a Host IT Service” section.
5. Click **Save**. The Host Service Details screen displays. The alert section indicates the host IT service’s status.

Enabling Availability Notifications

Availability notifications generate alerts for an IT service whenever a host that is contained in the IT service fails. This can be used to troubleshoot any problems that are encountered when managing grid hosts. Alerts are sent to an alert category which contains any number of alert recipients. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 “Using Alert Notifications”.

The host IT service list indicates the alert status of all host IT services. The View IT Service screen provides the details of the alert and also indicates which managed host caused the alert.

To enable availability notifications for a host IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the list of host IT services, click the host IT service you want to view.
3. Click **Edit**. The Edit IT Service screen displays.
4. From the Availability section, click the check box to enable availability notifications. A check indicates that availability notifications are enabled.
5. From the Alert Recipients section, use the drop-down list to select the default alert category where the alerts will be sent.
6. Click **Save**.

Publishing to a UDDI Registry

The BSE can publish host IT services to a UDDI registry. Host IT services that are published to a UDDI registry can be reused by other applications. To use the UDDI feature, you must have a UDDI registry and configure the registry with the Network Services server. To configure a UDDI registry, see “Configure a UDDI Registry” in Chapter 2.

To publish a host IT service to a UDDI registry:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the Host Services section, select the host IT service you want to view. The Host Service Details screen displays.
3. From the Host Service Detail screen, click **Publish**. The Publish IT Service screen displays.
4. Using the Provider drop-down list, select a Business Entity in the UDDI registry.
5. Click **Publish**. The Host Service Details screen displays.

Deleting a Host IT Service

You can delete a host IT service at any time. When you delete a host IT service, its alerts are resolved, its UDDI entries are deleted from the UDDI registry, and all of its registered hosts are removed from the SOA Manager.

To delete a host IT service:

1. From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.
2. From the Host Services section, click the IT service to be deleted. The Host Service Details screen displays.

3 From the Host Service section, click **Remove**. A warning screen displays.

4 Click **Remove**. The IT Services Summary screen displays and the host IT service is removed.

Managing MOM IT Services

The View MOM IT Service screen provides details about a MOM IT service. The screen is a convenient way to view managed JMS servers from the context of their IT service. From this screen, you can:

- View a MOM IT service's details
- Enable Availability Notifications
- Publish MOM IT services to a UDDI registry
- Delete a MOM IT service

Viewing a MOM IT Service

An IT service's view screen provides information about the MOM IT service, such as alerts, as well as features for editing the IT service.

To view a MOM IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays. Alert and status information for each IT service is also listed.

2 Select the MOM IT service you want to view. The view screen displays and contains a section for general information, a section for alerts, and a section that lists all JMS servers that are contained in the IT service.

Enabling Availability Notifications

Availability notifications generate alerts for an IT service whenever a managed JMS server that is contained in the IT service fails. This can be used to troubleshoot problems that are encountered when managing MOM resources. Alerts are sent to an alert category which contains any number of alert recipients. For more information on setting up alert recipients and creating alert recipient categories, see chapter 6 "Using Alert Notifications".

The MOM IT service list indicates the alert status of all MOM IT services. The View IT Service screen provides the details of the alert and also indicates which managed WS JMS server caused the alert.

To enable availability notifications for a MOM IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of MOM IT services, click the MOM IT service you want to view. The view screen displays for the selected IT service.

3 Click **Edit**. The Edit MOM IT Service screen displays.

4 From the Availability section, click the check box to enable availability notifications. A check indicates that availability notifications are enabled.

5 From the Alert Recipients section, use the drop-down list to select an alert category for both the Degraded and Unavailable availability status.

6 Click **Save**.

Publishing to a UDDI Registry

The BSE can publish MOM IT services to a UDDI registry. IT services that are published to a UDDI registry can be reused by other applications. To use the UDDI feature, you must have a UDDI registry that is configured for use with the Network Services server. To configure a UDDI registry, see "Configure a UDDI Registry" in Chapter 2.

To publish an IT service to a UDDI registry:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of IT services, click the MOM IT service you want to view. The view screen displays for the selected IT service.

3 Click **Publish**. The Publish IT Service screen displays.

4 Using the Provider drop-down list, select a Business Entity in the UDDI registry.

5 Click **Publish**.

Deleting a MOM IT Service

You can delete a MOM IT service at any time. When you delete a MOM IT service, its alerts are removed and its UDDI entries are deleted from the UDDI registry; however, any managed JMS servers that are contained in the IT service are not removed from the Network Services and can be added to another IT service.

To delete an IT service:

1 From the BSE main tool bar, click **IT Services**. The IT Services Summary screen displays.

2 From the list of MOM IT services, click the MOM IT service you want to view. The view screen displays for the selected IT service.

3 From the IT Service section, click **Remove**. A warning screen displays.

4 Click **Remove**. The IT Services Summary screen displays and the IT service is removed.

4

Using Business Services

This chapter provides instructions for constructing service models from the context of business services. Business services are an essential part of the service model definition and are the main context from which a service model is constructed and viewed. An overview is included that introduces the business service concept as well as other service model conventions.

Overview

A business service is the virtualization of some business application that is offered by a business manager to either internal or external customers. Currently, the SOA Manager only implements one type of business service, which is a Web service. This chapter only covers business services as they relate to the management of Web services.

Business services are used to better align business managers, IT/operation administrators, and application developers. In this model, business managers define the business service; application developers architect and develop a services-based solution; while administrators deploy and manage the solution across the enterprise. This orchestration is captured in the service model and allows an organization to quickly react and adapt to business changes.

Some of the benefits of managing Web services using a service model are listed below.

- A business service provides different views of a Web service that are relevant to all stakeholders. The stakeholders collaborate in the complete lifecycle of Web services that are delivered and managed as business services.
- A business service includes various metrics, operations, and events that support the paradigm of assess, advise, and act.
- Repetitive tasks such as deploying software and configuring connectivity between underlying IT services are automated by leveraging the meta-data captured in the service model.
- Business services are represented as a standards-based managed object that can be integrated into current management products or used as an integration point between management products that need to coordinate adaptive behavior.

- Business services can be published to a UDDI registry. The registry allows business services to be discovered and used by any management products that support UDDI.

Conceptual Architecture

Business services are part of the service model definition. Business services are defined using the BSE. The BSE is a business service designer that is used to capture the structure, relationships, policies, and assets of a business service.

As part of the business services definition, a business service configuration is created and bound to an IT service and its managed resources. For each IT service type, a corresponding business service configuration type is available. For more information on IT services, see Chapter 3, “Managing Resources Using IT Services”.

The configuration types include:

- Web Service Container configurations
- Web Service Intermediary configurations
- Database Services configurations
- Host Services configurations
- MOM Services configurations

The use of configurations allows the model to provide automation features such as automatic resource discovery, automatic resource deployment, and automatic endpoint routing.

Figure 4-1 shows a generic view of the relationship between a business service, a business service configuration, and an IT service.

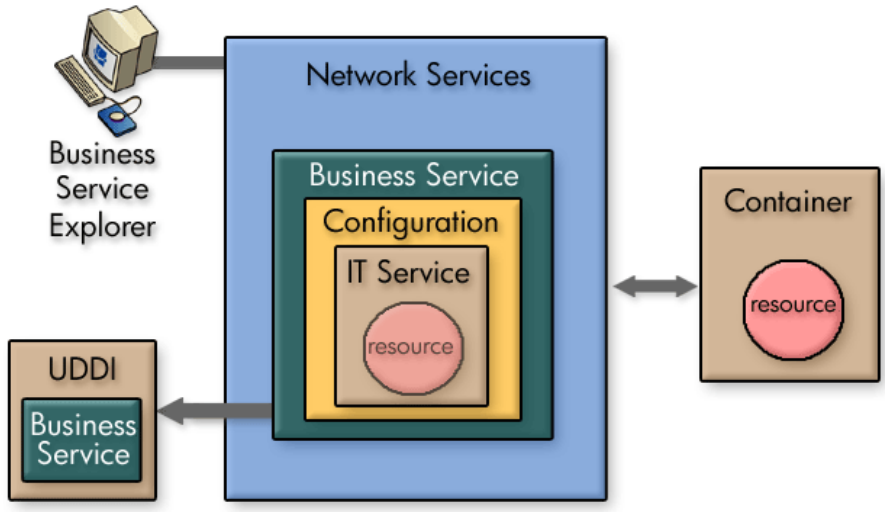


Figure 4-1: Generic view of the business service model

Service Models

This section discusses some basic service model use cases that are supported by the SOA Manager. The examples do not include every potential service model use case and should be considered a starting point for understanding service models.

Model – Business Service

A service model can contain multiple business services. A business service can also be related to other business services. The relationship between business services must be explicitly defined (see "Selecting Dependencies for a Business Service" later in this chapter). Figure 4-2 below shows a service model that contains three business services and one business service relationship.

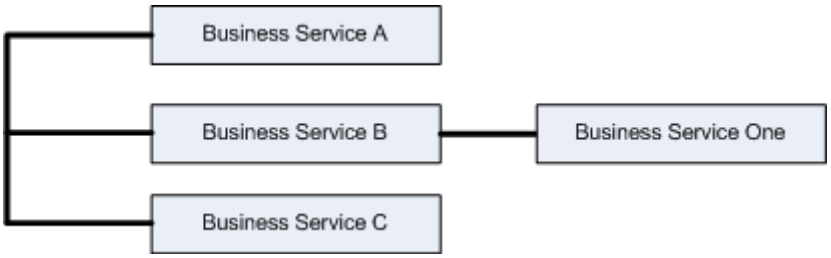


Figure 4-2: Model – Business Services

Model – Web Services Only

Business services contain the representation of Web services that are being managed. A business service can contain multiple Web services. Any Web service can be designated as an entry point to the model (see "Step 5: Designate the Entrypoint" later in this chapter). Figure 4-3 below shows some basic ways a service model can be constructed to represent Web services. The star indicates entrypoints to the model.

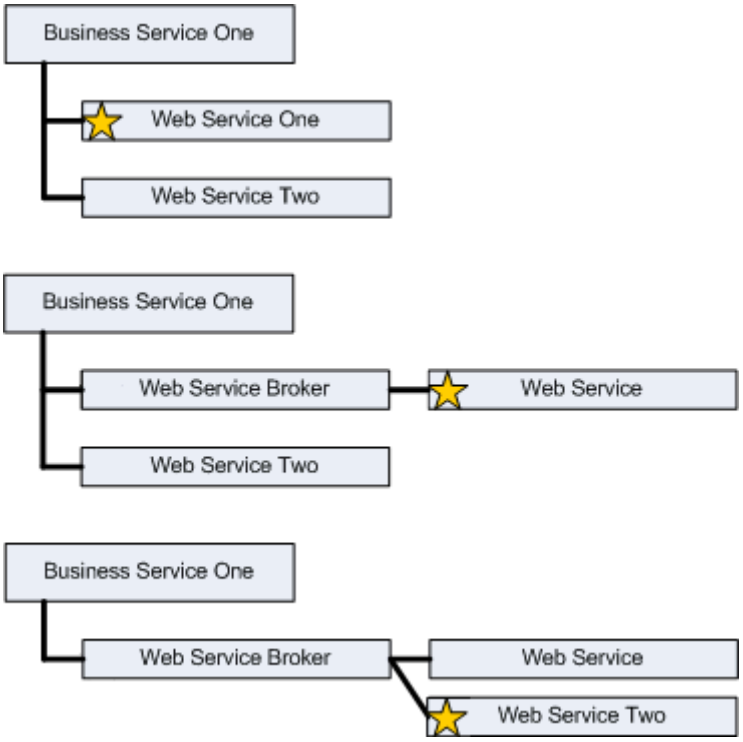


Figure 4-3: Model – Web Service Only

Model – Heterogeneous

Lastly, a business service can contain many resources that are part of an SOA environment. In most cases, these resources are related to the Web service. The service model captures these resources as part of the business service. Figure 4-4 below shows some possible ways a business service might include different resources as part of its model. The star indicates entrypoints to the model.

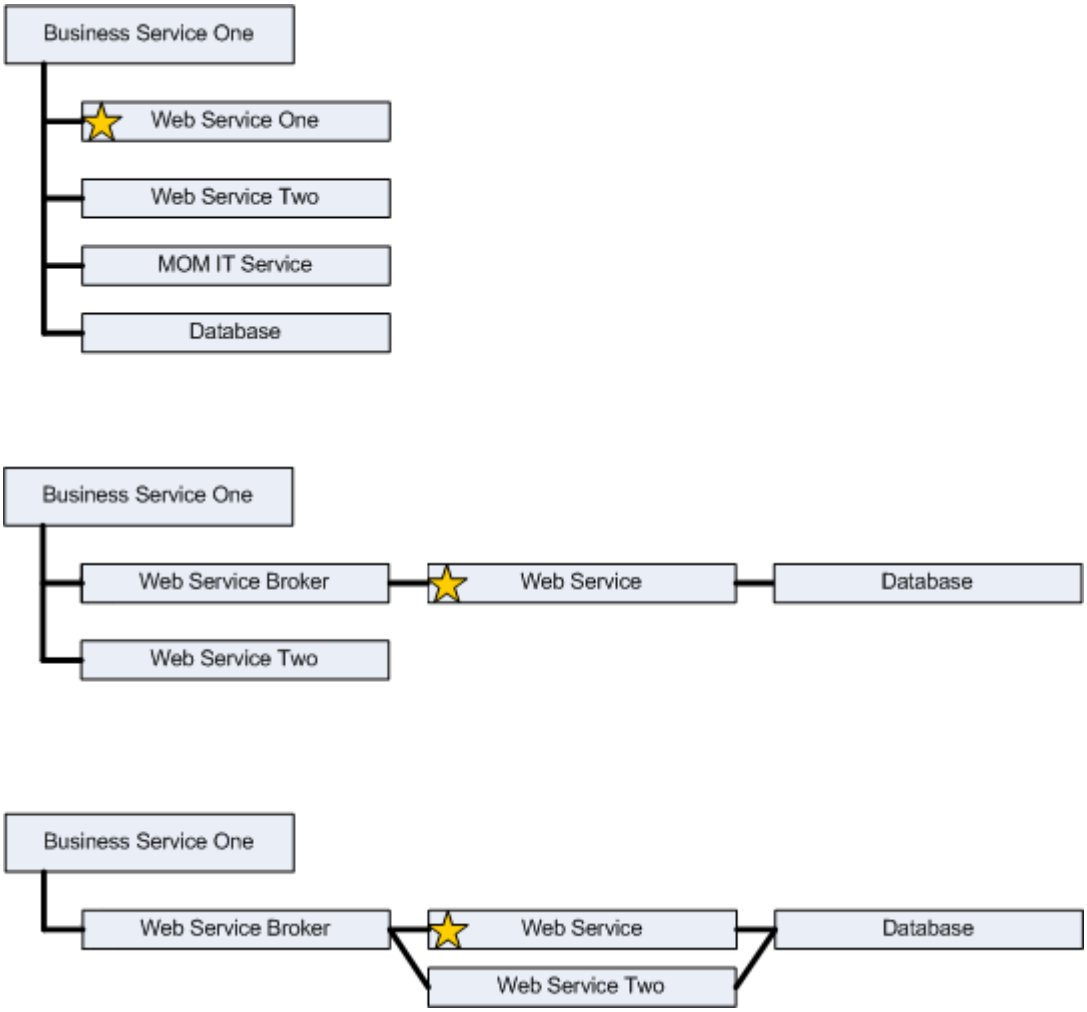


Figure 4-4: Model – Heterogeneous

Defining Business Services

Business services are defined using the BSE. When you define a business service, you create the business service and then add a configuration for the business service. The configuration is bound to an IT service that contains the resources that are being managed. The definition process is broken down into the following three steps:

- Create a business service
- Add a Configuration
- Add a Resource

Step 1: Create a Business Service

To create a business service:

1. From the BSE main tool bar, click the **Business Services** tab. The Business Service List screen displays.
2. Click **Add**. The Create Business Service screen displays.
3. Complete the following fields:
   - **Name**: Enter a user-friendly name for this business service.
   - **Version**: Enter a version number for this business service.
   - **Description**: Enter a description for this business service.
   - **Route Propagated Alerts to Category**: Use the drop-down list to select a default alert category to be used for this business service. If you are not sure which category to use, leave the `Default` category.

     Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on creating alert categories as well as alert recipients, see chapter 6 “Using Alert Notifications.”
   - **Route Business Content Alerts to Category**: Use the drop-down list to select a default alert category to be used for business content alerts for this business service. If you are not sure which category to use, leave the `Default Business Content` category.

     Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on business content alerts, creating alert categories, as well as alert recipients, see chapter 6 “Using Alert Notifications.”
4. Click **Add**. The Business Service List screen redisplays and lists the business service.
5. Repeat this procedure to create additional business services as required.

Step 2: Import Existing IT Services

IT service configurations are used to link a business service with an IT service. An IT service contains the resources that are managed within a business service. A corresponding configuration type exists for each IT service type. In addition, any number of IT service configurations can be included in a business service. Each IT service configuration can include resource configurations that contain the resources of the corresponding IT service that are to be managed within the business service.

To select any subset of the existing IT services, create corresponding IT service configurations and the resource configurations, all in one screen:

1. From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.
2. From the Model section, use the Add drop-down list and select Link IT services.
3. The ‘Link to existing IT Services’ screen displays. Select the IT services and resources to be managed within this business service.

4 Click **Link**. The Business Service View screen redisplays and the Model section lists the new configurations as dependencies for this business service.

Steps 3 “Add an IT Service Configuration” and Step 4 “Add a Resource Configuration” provide an alternate approach for what step 2 accomplishes. Continue with Step 5.

Step 3: Add an IT Service Configuration

IT service configurations are used to link a business service with an IT service. An IT service contains the resources that are managed within a business service. A corresponding configuration type exists for each IT service type. In addition, any number of IT service configurations can be included in a business service.

To add an IT service configuration to a business service:

1 From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.

2 From the Model section, use the Add drop-down list and select the configuration type that corresponds to IT service that contains the resource to be managed within this business service. The Add New Configuration screen displays for the selected configuration type.

3 Complete the following fields:

- **Name**: Enter a user-friendly name for this configuration.
- **Version**: Enter a version number for this configuration.
- **Description**: Enter a description for this configuration.
- **Owner**: Use the Owner drop-down list to select an owner of the configuration.
- **Support**: Use the Support the drop-down list to select a support person of the configuration.

Before you can assign an owner or support person, the person must be added to the Network Services Server. See the “Adding People” section in Chapter 2.

- **Route propagated Alerts to Category**: Use the drop-down list to select a default alert category to be used for this configuration. If you are not sure which category to use, leave the `Default` category.

  Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on creating alert categories as well as alert recipients, see chapter 6 “Using Alert Notifications.”

- **Bind to IT Service**: Use the drop-down list to select the IT Service that contains the resources to be managed in this business service.

4 Click **Save**. The Business Service View screen redisplays and the Model section lists the new configuration as a dependency for this business service.

5 Repeat this procedure to add additional configurations as required.

Step 4: Add a Resource Configuration

This step is used to add a resource configuration that contains the resources that are to be managed within the business service. Resources are added in the context of the configuration type that corresponds to the type of resource being managed.

Brokered Web services and Web services can also be added to a configuration by importing a WSDL. See the "Importing a WSDL" section below.

Web Service

To add a Web/brokered service resource configuration to an IT service configuration:

1. From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.
2. From the Model section, use a Web service container/intermediary configuration's Add drop-down list and select **Add New Web Service Configuration**. The Add New Configuration screen displays.
3. Complete the following fields:
   - **Name**: Enter a user-friendly name for this configuration.
   - **Version**: Enter a version number for this configuration.
   - **Description**: Enter a description for this configuration.
   - **Owner**: Use the Owner drop-down list to select an owner of the configuration.
   - **Support**: Use the Support the drop-down list to select a support person of the configuration.

     Before you can assign an owner or support person, the person must be added to the Network Services Server. See the "Adding People" section in Chapter 2.

   - **Default Alert Categories**: Use the drop-down list to select a default alert category to be used for this configuration. If you are not sure which category to use, leave the `Default` category.

     Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on creating alert categories as well as alert recipients, see chapter 5 "Using Alert Notifications."
   - **Route Business Content Alerts to Category**: Use the drop-down list to select a default alert category to be used for business content alerts for Web/brokered Service that are contained in this configuration. If you are not sure which category to use, leave the `Default Business Content` category.
   - **Deployment**: Click the check box if you would like to enable the deployment feature. This feature allows you to deploy a Web/brokered service to a managed WS container/intermediary or undeploy the service from a managed WS container/intermediary. Disregard this field if the Web/brokered service for this business service is already deployed to a managed WS container/intermediary.

If you select the Deployment check box, additional fields display that allow you to select whether you would like to either deploy or undeploy as well as options for selecting a deployment unit. For more information on automatic deployment, see chapter 8 “Using Deployment.”

— **Resource Discovery**: Use the drop-down list to select the Web/brokered service to be contained in this configuration. The list contains all services that are discovered when a managed Web service container/intermediary is registered as an IT Service. See the “Managing Resources Using IT Services” chapter.

Or,

Use the text box to enter the namespace and local name of the Web/brokered service in the form *{namespace}localname* (e.g., `{http://mycompany.com}MyService`). The values to use in the pattern can be obtained by inspecting a Web service’s WSDL. The *namespace* corresponds to the Web service’s targetNamespace, and the *localname* refers to the service name.

A discovery pattern is typically used when adding a Web/brokered service to the service model before the service is actually deployed to a container/intermediary that is registered as an IT service. Once the service is deployed, the pattern is used to automatically discover and add the service to this configuration.

4 Click **Save**. The Business Service View screen redisplays and lists the Web/brokered service as part of the configuration.

5 Repeat this procedure to add additional resource configurations.

Importing a WSDL

The import WSDL feature is used to add a Web service or brokered Web service to a configuration based on a WSDL file. If the WSDL file defines a service that currently exists in a registered IT service, it is automatically mapped to this configuration. Moreover, if the service is not currently deployed, you can still import the WSDL. Once the service is deployed, it will automatically be discovered and added to the appropriate configuration.

1 From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.

2 From the Model section, use a Web service container/intermediary configuration’s Add drop-down list and select **Import WSDL**. The Import Web Service WSDL screen displays.

3 In the Browse Local WSDL file field, enter the location of the WSDL or click the **Browse...** button to locate the WSDL.

Or,

In the Specify Remote WSDL URL field, enter the URL to the WSDL.

If there is no service defined in the WSDL file, the operation fails without any error in the BSE. In addition, the WSDL files cannot contain external links.

4 Click **Import**. The Business Services View screen displays and the model section is updated. All operations discovered in the WSDL are also listed.

Manually Adding Operations

Web service operations can be added to the service model allowing for fine grained manageability at the operation level. Web service operations are automatically discovered and added to the service model when the import WSDL feature is used. However, you can also manually add any operations:

To manually add operations:

1 From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.

2 From the Model section, use a Web service configuration's Add drop-down list and select **Add New Web Service Operation Configuration**. The Add New Configuration screen displays.

3 Complete the following fields:

- **Name**: Enter a user-friendly name for this configuration.
- **Version**: Enter a version number for this configuration.
- **Description**: Enter a description for this configuration.
- **Owner**: Use the Owner drop-down list to select an owner of the configuration.
- **Support**: Use the Support the drop-down list to select a support person for the configuration.

Before you can assign an owner or support person, the person must be added to the Network Services Server. See the "Adding People" section in Chapter 2.

- **Route Propagated Alerts to Category**: Use the drop-down list to select a default alert category to be used for this configuration. If you are not sure which category to use, leave the `Default` category.

  Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on creating alert categories as well as alert recipients, see chapter 6 "Using Alert Notifications."

- **Operation Name**: Use the drop-down list to select an operation that appears in the Web service WSDL file or use the text box to enter the operation name as it appears in the WSDL file.

4 Click **Save**. The Business Service View screen displays and the operation is listed within the model section.

MOM Destination

To add a JMS topic or queue to a MOM service configuration:

1 From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.

2 From the Model section, use a MOM configuration's Add drop-down list and select **Add New MOM Destination Configuration**. The Add Configuration screen displays.

3 Complete the following fields:

— **Name**: Enter a user-friendly name for this configuration.

— **Version**: Enter a version number for this configuration.

— **Description**: Enter a description for this configuration.

— **Owner**: Use the Owner drop-down list to select an owner of this configuration.

— **Support**: Use the Support the drop-down list to select a support person of this configuration.

Before you can assign an owner or support person, the person must be added to the Network Services Server. See the "Adding People" section in Chapter 2.

— **Route Propagated Alerts to Category**: Use the drop-down list to select a default alert category to be used for this configuration. If you are not sure which category to use, leave the `Default` category.

Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on creating alert categories as well as alert recipients, see chapter 6 "Using Alert Notifications."

— **Resource Discovery**: Use the drop-down list to select the topic or queue to be contained in this configuration. The list contains all topics and queues that are discovered when a managed JMS server is registered as an IT Service. See the "Managing Resources Using IT Services" chapter.

Or,

Use the text box to enter the queue or topic name in the following format `Queue:`<*queue_name*> or `Topic:`<*topic_name*>. For example:

```
Queue:MyQueue
```

A discovery pattern is typically used when adding a MOM destination configuration to the service model before a JMS topic or queue is actually deployed. Once the topic or queue is deployed, the pattern is used to automatically discover and add the topic or queue to the configuration.

4 Click **Save**. The Business Service View screen redisplays and lists the topic or queue as part of the MOM configuration.

5 Repeat this procedure to add additional configurations to the MOM configuration.

Host

To add a host to a host service configuration:

1 From the Business Services List screen, click a business service. The Business Service View screen displays for the selected business service.

2 From the Model section, use a host service configuration's Add drop-down list and select **Add New Host Service Configuration**. The Add New Configuration screen displays.

3 Complete the following fields:

— **Name**: Enter a user-friendly name for this configuration.

- **Version**: Enter a version number for this configuration
- **Description**: Enter a description for this configuration.
- **Owner**: Use the Owner drop-down list to select an owner of the configuration
- **Support**: Use the Support the drop-down list to select a support person of the configuration.

Before you can assign an owner or support person, the person must be added to the Network Services Server. See the "Adding People" section in Chapter 2.

- **Route Propagated Alerts to Category**: Use the drop-down list to select a default alert category to be used for this configuration. If you are not sure which category to use, leave the `Default` category.

  Click **Edit Categories** to edit an alert category or create additional alert categories. For more information on creating alert categories as well as alert recipients, see chapter 6 "Using Alert Notifications."

- **Resource Discovery**: Use the drop-down list to select the host to be contained in this configuration. The list contains all the hosts that are part of the host IT service to which this configuration is bound. Hosts that have already been selected are excluded. See the "Managing Resources Using IT Services" chapter.

  A discovery pattern is typically used when adding a host configuration to the service model. Any host that has been added as a contained resource to the bound host IT service can be discovered automatically and selected for the host configuration.

4. Click **Save**. The Business Service View screen redisplays and lists the host as part of the host service configuration.
5. Repeat this procedure to add additional configurations to a host service configuration.

Step 5: Designate the Entrypoint

A business service can contain several different IT configurations and resource configurations. Any of the resource configurations can be designated as the entrypoint. Entrypoints are being used in SOA Manager to designate the resource configuration that is the most important. After an entrypoint is assigned, the user can set policies on the business service, and SOA Manager is able to filter and propagate alerts accordingly.

A service model can become very complex depending on the number of assets that are defined in the model. By designating a resource configuration as an entrypoint, all relevant alerts are propagated to the Business Service. In other words, an entrypoint acts as a designated alert filter mechanism. It is important to note that in a given business service only one resource configuration can be designated as the entrypoint.

To designate or change the entrypoint for a business service:

1. From the business service view screen, expand the Add drop-down list next to the name of the business service in the Model section. Select **Select Entrypoint**.

2 On the next screen, select the radio button for the resource configuration that should be the entrypoint.

3 Click **Save**.

Selecting Dependencies for a Business Service

This section describes how to add or remove explicit dependencies from a business service's model definition. The dependencies include other business services, configurations, and resources that have already been added as part of the business service definition process. Dependencies allow alerts to be propagated from a dependency to its business service. In the absence of explicit dependencies, for example, alerts will be propagated from service configurations to their contained resource configurations, and not vice-versa. Therefore explicit dependencies are needed for a business service to receive alerts from the contained resources.

A business service may use, or be used by, any number of other business services. The relationship between business services can be expressed as A uses B and B is used by A. This relationship has to be known and declared in the business service model and represents a dependency relationship between the Web services in one business service to that in another. This dependency relationship is used for impact analysis and root cause analysis.

Monitoring a business service that uses other business services allows you to perform root cause analysis to determine which related business services are degrading. Conversely, monitoring a business service that is used by other business services allows you to perform impact analysis to determine how a business service's performance affects related business services.

To add or remove dependencies from a business service's model definition:

1 From the Business Service List screen, select a business service to view its details. The Business Services View screen displays for the selected business service.

2 From the Model section, use the Add drop-down menu next to the business service's name and click 'Select Dependencies'.

3 From the list of resources, click the check box to add or remove a resource. A check mark next to the resource indicates that it is currently a dependency of the business service.

4 Click **Save**. The Business Services View screen displays and the model section is updated to display the explicit dependencies.

Adding Routing Targets

The routing target feature is used to add additional endpoints to a brokered service. The endpoints must first be deployed to a Web service container or intermediary that is registered as an IT service and bound to a business service.

Routing targets are automatically added to the brokered service's list of available endpoints able to service a request at runtime. When a brokered service contains multiple endpoints, requests are dispatched to the endpoints using a round robin load balancing scheme.

To add a routing target:

1 From the Business Services List screen, expand a business service to view its contained configurations.

2 From a Web Service Intermediary configuration, click the Web service configuration to which you want to add additional routing targets. The View Web Service Configuration screen displays.

3 From the Web Service Configuration section, click **Edit**. The Edit Web Service Configuration screen displays.

4 Click to select the Endpoint Update Policy check box. A check indicates that the routing feature is enabled.

5 Click **Save**. The View Web Service Configuration screen redisplays.

6 From the Routing Table section, click **Edit**. The Select Resources screen displays. The screen lists all the Web services that are in the business service. The Web services are organized by type.

7 From the list of Web services, click the check box to add the Web services as a routing target. A check mark indicates an active routing target.

8 Click **Save**. The Web Service View screen displays and the Routing Table lists all routing targets.

Assigning Owner and Support Roles

Business services, configurations, and resources can be assigned to an owner or a support person. Once assigned, you can filter business services and configurations based on the owner or support person.

Before you can assign an owner or support person, the person must be added to the Network Services Server. See the "Adding People" section in Chapter 2.

Business Service Roles

To assign owner and support roles for a business service:

1 From the Business Service List screen, select a business service to view its details. The Business Services View screen displays for the selected business service.

2 Click the **Edit** link in the Business Service section. The Edit Business Service screen displays.

3 Use the Owner drop-down list to select an owner of the business service. The owner of a business service is generally responsible for lifecycle management and publishing of the service. If needed, click the check box for sending email alerts to this person.

4 Use the Support the drop-down list to select a support person of the business service. The person or group is responsible for supporting deployed instances of the service. If needed, click the check box for sending email alerts to this person.

5 Click **Save**. The Business Services View screen redisplays.

6 From the BSE main tool bar, click the **Business Services** Tab. The Business Services List screen displays.

7 Use the **Filter 'By Person' and 'By Role'** drop-down lists to filter the list based on business service owners and roles.

IT Service Configuration Roles

To assign owner and support roles for a business service configuration:

1 From the Business Service List screen, expand a business service to view its IT service configurations.

2 Click an IT service configuration. The Configuration View screen displays.

3 Click the **Edit** link. The Edit Configuration screen displays.

4 Use the Owner drop-down list to select an owner of the configuration. The owner of a configuration is generally responsible for lifecycle management and publishing of the service. If needed, click the check box for sending email alerts to this person.

5 Use the Support the drop-down list to select a support person of the configuration. The person or group is responsible for supporting the contained resources of an IT service. If needed, click the check box for sending email alerts to this person.

6 Click **Save**. The Configuration View screen redisplays.

7 From the BSE main tool bar, click the **Business Services** Tab. The Business Services List screen displays.

8 Use the **Filter 'By Person' and 'By Role'** drop-down lists to filter the list based on IT service configuration owners and roles.

Resource Configuration Roles

To assign owner and support roles for a resource configuration:

1 From the Business Service List screen, expand a business service to view its IT service configurations.

2 Expand an IT service configuration to view its resource configurations.

3 Click the resource configuration. The corresponding View screen displays.

4 Click the **Edit** link. The Edit Configuration screen displays.

5 Use the Owner drop-down list to select an owner of the resource configuration. The owner of a resource is generally responsible for the development of the resource. If needed, click the check box for sending email alerts to this person.

6 Use the Support the drop-down list to select a support person of the resource. The person is responsible for the ongoing maintenance of the resource. If needed, click the check box for sending email alerts to this person.

7 Click **Save**. The Configuration View screen redisplays.

8 From the BSE main tool bar, click the **Business Services** tab. The Business Services List screen displays.

9 Use the **Filter 'By Person' and 'By Role'** drop-down lists to filter the list based on resource configuration owners and roles.

Operation Roles

To assign owner and support roles for a Web service operation configuration:

1 From the Business Service List screen, expand a business service to view its IT service configurations.

2 Expand an IT service configuration to view its resource configurations.

3 Expand a Web service configuration to view its operation configuration.

4 Click an operation configuration. The View Web Service Operation Configuration screen displays.

5 Click the **Edit** link. The Edit Configuration screen displays.

6 Use the Owner drop-down list to select an owner of the operation configuration. The owner of an operation configuration is generally responsible for the development of the operation. If needed, click the check box for sending email alerts to this person.

7 Use the Support the drop-down list to select a support person of the operation configuration. The person is responsible for the ongoing maintenance of the operation configuration. If needed, click the check box for sending email alerts to this person.

8 Click **Save**. The View Web Service Operation Configuration screen redisplays.

9 From the BSE main tool bar, click the **Business Services** Tab. The Business Services List screen displays.

10 Use the **Filter 'By Person' and 'By Role'** drop-down lists to filter the list based on operation configuration owners and roles.

Publishing Business Services to a UDDI Registry

The BSE can publish business services to a UDDI registry. Business services that are published to a UDDI registry can be reused by other applications. To use the UDDI feature, you must have a UDDI registry and configure the registry with the Network Services server. To configure a UDDI registry, see "Configure a UDDI Registry" in Chapter 2.

You must publish the business service's dependencies before the business service. Publish consumed business services, Web service Intermediary/Container IT services, database IT services, and MOM IT services first. See chapter 3 for details on publishing these dependencies.

To publish a business service to the registry:

1 From the Business Service List screen, select a business service to view its details. The Business Service's View screen displays.

2 Click the **Publish** link next to the Business Service section. The Publish Business Service screen displays.

3 Complete the following fields:

- **Management Web Service Provider**: Select the provider for the business service. Select a Business Entity name from the drop-down list of Business Entities in the UDDI registry.
- **Web Service Provider** (optional): Select the provider for the Web service. This is the Web service managed by the BSE business service. Select a Business Entity name from the drop-down list of Business Entities in the UDDI registry. If the Web Service is already in the UDDI registry, SOA Manager will not change the existing entries. If the service is already in the registry, the Web Service provider parameter is not used.
- **Web Service Name**: The name of the web service.

4 Click **Publish**. The Business Service View screen displays. If an error occurs, the error is shown in red at the top of the Publish Business Service screen.

When you delete a Web service Intermediary/Container Configuration, its UDDI entries are deleted.

When you delete a business service, the business service and Web service Intermediary/Container Configuration UDDI entries are deleted. The UDDI registry entities corresponding to Web services are not deleted.

JMS Support

The UDDI feature also supports business services that include JMS resources. The following support is included for JMS:

- A `TModel` for the JMS transport is published with the name `hp-com:jms`.
- A functional business service binding template containing:
  - an access point with the following attributes:

    `destinationStyle`, `initialContextFactory`, `jmsVendorURI`, `jndiConnectionFactoryName`, `jndiDestinationName`, `jndiProviderUrl`
  - A binding `TModel` with a keyed reference for the JMS transport in the category bag.

Reusing a Business Service

The BSE allows you to import and export business services. This simplifies and saves time when moving business services between environments (e.g., development to production).

SOAM version 2.1 supports importing a business service that was created using version 2.0. The business service is automatically updated to a 2.1 compliant business service. In particular, the import updates:

- Business services and their contained intermediary configurations, container configurations, database service configurations
- Business Service relationships
- SLOs defined for intermediary configurations and/or container configurations

Exporting a Business Service

To export a business service:

1 From the Business Service List screen, select a business service to view its details. The Business Services View screen displays for the selected business service.

2 Click the **Export** link in the Business Service section. The Export Business Service screen displays.

3 Click **Download**.

4 The file download dialog box for your browser displays.

5 Use the download dialog box to save the business service.

Importing a Business Service

To import a business service:

1 From the Business Service List screen, click the **Import** link. The Import Business Services screen displays

2 Use the **Browse** Local Business Service Jar field to enter the location to a business service JAR file.

Or,

Use the Specify Remote Business Service Jar URL field to enter the URL to a business service JAR file.

3 Click **Import**. The Business Service List screen displays and the business service is listed. It may take several seconds for the business service to be deployed and to display on the list.

Deleting a Configuration

Configurations can be deleted without deleting the business service. When deleting a configuration, all pending alerts for the configuration are acknowledged, UDDI entries in the UDDI registry are deleted, and SLO alerts are no longer triggered Any configuration contained in this configuration is also removed.

To delete a business service configuration:

1. Click the **Business Services** tab to view the Business Services List screen.
2. From the Business Service List screen, expand a business service to view its configurations.
3. Select the configuration to be deleted. The Configuration View screen displays for the selected configuration.
4. From the Configuration View screen, click **Remove** next to the Configuration section. The Remove screen displays.
5. Click **Remove**. The Business Service View screen displays and the configuration is no longer listed as part of the business service.

Deleting a Business Service

You can delete a business service. When you delete the business service, business service configurations are deleted; pending alerts for this business service are acknowledged; dependencies on the business services are removed; and SLOs and alerts are no longer triggered for this service. If the business service was published to a UDDI registry, it is deleted from the registry as well. However, the functional business service UDDI registry entries are not deleted.

To delete a business service:

1. Click the **Business Services** tab to view the Business Services List screen.
2. From the Business Service List screen, select a business service to view its details. The Business Services View screen displays for the selected business service.
3. From the Business Services View screen, click **Remove** next to the Business Service section. The Delete Business Service screen displays.
4. Click **Remove**. The Business Service List screen displays and the business service is no longer listed.

5

Monitoring Performance and SLO

This chapter provides instructions for monitoring the performance of resources that are contained in a business service. In addition, the chapter provides instructions for defining Service Level Objectives (SLO) to help ensure that resources are performing within acceptable limits.

Overview

Performance metrics are collected over time and allow you to view the overall health and performance of the resources that are contained in a business service. Each resource type (excluding database resources) has a unique set of performance metrics that are captured at the point closest to the consumers of the resource. They are the closest approximation of performance and availability, computed by monitoring real transactions without doing externally probed synthetic transactions.

In addition to monitoring performance metrics, a business manager can define overall SLOs for a resource's performance metrics. The SLOs are used to set desired operating limits for the resource. Also, a business manager can set overall SLOs on the business service. These SLOs are used to set desired operating limits for the resource designated as the entrypoint for the business service. When the business service or resource limits are violated, an SLO alert is generated and notifies key stakeholders of the violation. Such alerts help minimize downtime and help ensure maximum availability.

Viewing Performance Metrics

Performance metrics are viewed within the BSE console on a resource's view screen. The resource must be contained within a business service before you can view the resource's performance metrics or set SLO limits.

To view a resource's performance metrics:

1 Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Services List screen, expand a business service to view its contained configurations.

3 Click the resource configuration you want to view. The appropriate view screen displays. Performance information is located in the Performance section of the screen.

Changing the Monitoring Interval

The monitoring interval for the Performance section can be adjusted depending on how closely you want to monitor a resource. The Choose View: drop-down list in the Performance section is used to select a monitoring interval. The Summary table and Performance Graph automatically change based on the selected Monitoring interval.

Adjusting the time interval allows you to choose how closely to monitor a resource. For example, a Web service resource that typically experiences heavy loads may require a Minute-by-Minute view of the metrics; whereas, a moderately used Web service resource may only require an Hour-by-Hour view of the metrics.

The following monitoring intervals are available:

- **6 Minutes** – Metrics are displayed for the last Six Minutes in Minute intervals. The exact time interval being evaluated is listed in the table heading. The One Minute detail table provides performance data based on a specific Minute within the last Six Minutes of operation. Use the mouse to roll the pointer along the performance graph and click to select a specific Minute. The details of the selected Minute are displayed in the 1 Minute Detail table. The exact Minute selected is shown in the table heading.
- **1 Hour** – Metrics are displayed for the last Hour in Ten Minute intervals. The exact time interval being evaluated is listed in the table heading. The Five Minute detail table provides performance data based on a specific Five Minute interval within the last hour of operation. Use the mouse to roll the pointer along the performance graph and click to select a specific Five Minute interval. The details of the selected interval are displayed in the 5 Minute Detail table. The exact interval selected is shown in the table heading.
- **1 Day** – Metrics are displayed for the last Day in 4 Hour intervals. The exact time interval being evaluated is listed in the table heading. The One Hour detail table provides performance data based on a specific hour within the last Twenty Four Hours of operation. Use the mouse to roll the pointer along the performance graph and click to select a specific Hour interval. The details of the selected Hour are displayed in the 1 Hour Detail table. The exact Hour selected is shown in the table heading.
- **Lifetime** – Metrics are displayed for the complete life (Uptime value) of the resource. The lifetime interval does not include a details section or a performance graph.

Web Service Performance Metrics

The Performance section of a Web service's view screen gives an overall view of how the Web service is performing. In addition, if the service model contains specific operations for a Web service, then a Performance section also displays on each Web service operation's view screen. This allows you to view performance down to the operation level. In such cases, the Availability and Uptime metrics for Web service operations have the same values as the Availability and Uptime of the operation's Web service.

The following table defines each of the metrics that are collected for a Web service.

Table 5-1: Web service Performance Metrics

Metric	Value
Availability (%)	The percentage of successful Web service requests sent during the configured interval. If there is traffic (requests are going through), then Availability % = successful requests / total request (i.e., if 5 requests go through, and 4 succeed, availability is 80%). If no requests are sent, the field is left blank. If a WS container/intermediary goes down, the Uptime percentage gradually goes down to zero. The value gradually goes to zero because the Network Services server intermittently tries to contact a WS container/intermediary and assumes the WS container/intermediary will recover.
Average Response Time (ms)	The average amount of time in milliseconds for a successful Web service response. If no requests are sent during an interval, this field is left blank.
Failure Count	The total number of failed Web service invocations.
Maximum Response Time (ms)	The maximum amount of time in milliseconds for a successful Web service response. If no requests are sent during an interval, this field is left blank.
Minimum Response Time (ms)	The minimum amount of time in milliseconds for a successful Web service response. If no requests are sent during an interval, this field is left blank.
Security Violations	The total number of times a security violation occurred.
Success Count	The total number of successful Web service invocations.
Total Requests	The total number of Web service requests.
Uptime (%)	The percentage over time that a Web Service has been available. It is the availability of the service that is being measured and does not depend on any traffic/messages. At every poll interval, statistics for a service are gathered. If the service returns the statistics, then it is considered available. To change the poll interval, see "Changing the Service Polling Interval" below.
Uptime	The current uptime state. This is different than the Uptime (%) metric, which represents the historical uptime state.

Performance Graph

The Web services performance graph provides a visual view of the performance metrics based on the current monitoring interval. The graph includes the following elements:

- **Green line**: represents the average response time in milliseconds during a given time interval
- **Gray Column**: represents the total number of successful requests during a given time interval
- **Red Column**: represents the total number of faults during a given time interval
- **Yellow Bullet**: represents the occurrence of one or more security violations for the given time interval

The Throughput fields are calculated for the currently selected monitoring interval. For the Six Minute and One Hour intervals, throughput is success/Minute. For the Day interval, throughput is success/Hour. The lifetime interval does not provide the throughput metric. The fields include:

- **avg**: the average number of successful requests based on the selected time interval
- **peak**: the greatest number requests for the selected time interval

Changing the Service Polling Interval

The Network Services periodically polls services to ensure their availability and update their performance metric values.

To change the service polling interval:

1. Stop the Network Services server if it is currently started.
2. Use a text editor to open <*install_dir*>`\conf\networkservices\mipServer.xml`.
3. Add an entry for `com.hp.service.polling.interval` and enter a value in Milliseconds. For example:

   ```
   <entry name="com.hp.service.polling.interval">60000</entry>
   ```

4. Save and close the file.
5. Restart the Network Services server.

MOM Destination Performance Metrics

The Performance section of a MOM Destination's view screen gives an overall view of how the topic or queue is performing. The following table defines each of the metrics that are collected for the destination.

Table 5-2: MOM Destination Performance Metrics

Metric	Description
Pending Count (msg)	The number of pending messages in the topic or queue for the specified time interval.

Metric	Description
Maximum Pending Count (msg)	The greatest number of pending messages in the topic or queue for the specified time interval.
Minimum Pending Count (msg)	The least number of pending messages in the topic or queue for the specified time interval.
Average Pending Count (msg)	The average number of pending messages in the topic or queue for the specified time interval.
Uptime (%)	The percentage over time that a topic or queue has been available. At every poll interval, statistics for the destination are gathered. If destination returns the statistics, then the destination is considered available.

Performance Graph

The MOM Destination performance graph provides a visual view of the pending count over the current monitoring interval. The graph includes the following elements:

- **Green line**: represents the number of messages that are pending for the topic or queue for a selected time interval

Host Performance Metrics

The Performance section of a Host's view screen shows the amount of system resources that are being utilized on the system Host computer. The following table defines each of the metrics that are collected for the host.

The SOA Manager integrates with MDS from the Globus Toolkit to report host performance metrics. Correct reporting depends on the integration of MDS with Ganglia, both of which are external to the SOA Manger product. These metrics are only reported correctly for those host platforms where Ganglia can be configured to capture the metrics. Work with HP Services for technical support on host metrics.

Table 5-3: Host Performance Metrics

Metric	Description
Processor Load	The average amount of processor load being experienced on the host over the last 1 minute. Processor Load is different than CPU utilization. The former polls the operating system's job queue and averages the number of processes waiting for the processor over a 1 minute window. When the processor load of a host is high, other tools should be used to analyze the CPU utilization of different processes on that host.

Metric	Description
Available Virtual Memory (MB)	The amount of virtual memory available on the host.
Available Disk Space (MB)	The amount of physical disk space available on the host.
Availability (%)	The percentage of availability throughout the uptime of the host.
Virtual Memory Utilization (%)	The percentage of virtual memory being utilized throughout the uptime of the host.
Disk Space Utilization (%)	The percentage of disk space being utilized throughout the uptime of the host.

Performance Graph

The Host performance graph provides a visual view of the processor load over the current monitoring interval. The graph includes the following elements:

- **Blue column**: represents the process load on the host computer for a selected time interval

Monitoring SLO

A resource has some SLO definitions that are related to the overall performance objectives of a business service. As part of the model definition process, appropriate SLO threshold values are defined for a resource's performance metrics. When thresholds are violated, an alert is generated.

In addition, a business service has SLO definitions for the overall performance objectives of a business service. The business service SLO thresholds are defined for performance metrics in the resource designated as the entrypoint for the business service. Changing the thresholds in the business service, changes the thresholds in the entrypoint and vice-a-versa. When business service SLO thresholds are violated, an alert is generated for the business service.

Alerts are displayed in the Alerts section and can also be sent to email recipients. Refer to Chapter 6, "Using Alert Notifications", for more information on alerts.

An Example Scenario

The following example demonstrates a scenario where an SLO is defined to ensure that a server is not getting overloaded with Web service requests. The example uses fictitious values that may not be valid in your environment.

A WS Container can process a maximum of 1000 requests per minute. Because the application's availability is a top priority, you want to be notified when the server is reaching its maximum request limits.

For this scenario, you could configure the Total Requests performance metric to have an SLO Warning value of `>500` and an SLO Breach value of `>750`. When the Total Request reaches `501`, an SLO alert is generated. You now know that at least 501 requests are being processed per minute. When the Total Request reaches `751` requests per minute, an SLO alert is generated. You now know that loads are increasing. If you do not react, you may reach the WS Container's maximum process capacity and the availability and health of the application may be compromised. Therefore, you deploy another instance of the application to another WS Container to compensate for the increased demand.

Defining SLO Values for a Resource

SLO threshold values are accessed from the Performance section of a resource configuration's view screen. The SLO feature is not enabled by default and must be enabled separately for each resource. Depending on the resource, different performance metrics can be assigned an SLO threshold value.

To define SLO values:

1. Click the **Business Services** tab to view the Business Services List screen.
2. From the Business Services List screen, expand a business service to view its contained configurations.
3. Click the resource configuration for which you want to define SLO values. The resource view screen displays for the selected resource.
4. From the Performance section, click **Edit SLOs**. The Edit Configuration Performance screen displays.
5. Use the option boxes to select the metrics you want to enable for SLO monitoring.
6. Using the SLO Warning column, enter SLO warning threshold values for the metrics you enabled. When a warning value is reached, an SLO Warning Alert is generated.
7. Using the SLO Breach column, enter SLO breach threshold values for the metrics you enabled. When a breach value is reached, an SLO Breach Alert is generated.

   You do not have to enter a value for both SLO Warning and SLO Breach, but you must enter a value for at least one of them for each enabled metric.

8. From the Alert Recipients section, select an alert recipient category for both SLO Warning and Breach alerts. Refer to Chapter 6, "Using Alert Notifications", for more information on alert categories.
9. Click **Save**. The resource's view screen displays.

Defining SLO Values for a Business Service

SLO threshold values are accessed from the business service's view screen. The SLO feature is not enabled by default. The thresholds are defined for performance metrics in the resource designated as the entrypoint for the business service. Changing the thresholds in the business service, changes the thresholds in the entrypoint and vice-a-versa. If the entrypoint is changed to another resource of the same type, the business service SLOs are preserved, and the new entrypoint's thresholds are changed to match the business service ones. Depending on the type of entrypoint resource, different performance metrics can be assigned an SLO threshold value.

To define SLO values:

1. Click the **Business Services** tab to view the Business Services List screen.
2. Click on the business service for which you want to define SLO values. The business service view screen displays the selected business service.
3. Click **Policy**.
4. If the business service does not have an entrypoint, the Select Entrypoint screen displays.
   - Select the resource to use as the entrypoint.
   - Click on **Save**.
5. The Edit Configuration Performance screen displays.
6. Use the option boxes to select the metrics you want to enable for SLO monitoring.
7. Using the SLO Warning column, enter SLO warning threshold values for the metrics you enabled. When a warning value is reached, an SLO Warning Alert is generated.
8. Using the SLO Breach column, enter SLO breach threshold values for the metrics you enabled. When a breach value is reached, an SLO Breach Alert is generated.

   You do not have to enter a value for both SLO Warning and SLO Breach, but you must enter a value for at least one of them for each enabled metric.
9. From the Alert Recipients section, select an alert recipient category for both SLO Warning and Breach alerts. Refer to Chapter 6, "Using Alert Notifications", for more information on alert categories.
10. Click **Save**. The business service's view screen displays.

Enabling Availability Notifications for a Resource

The SLO availability feature allows a breach alert notification to be sent to alert recipients whenever a resource is unavailable. Enabling this feature quickly notifies individuals that a resource is not operational and can help you resolve problems in a timely fashion.

To enable availability notifications:

1. Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Services List screen, expand a business service to view its contained configurations.

3 Click the resource configuration for which you want to enable availability notifications. The resource view screen displays for the selected resource.

4 From the Performance section, click **Edit SLOs**. The Edit Configuration Performance screen displays.

5 From the Availability section, select the **Alert when unavailable** check box.

6 Click **Save**.

Enabling Availability Notifications for a Business Service

The SLO availability feature allows a breach alert notification to be sent to alert recipients whenever the resource designated as the business service entrypoint is unavailable. Enabling this feature quickly notifies individuals that a business service is not operational and can help you resolve problems in a timely fashion.

To enable availability notifications:

1 Click the **Business Services** tab to view the Business Services List screen.

2 Click the business service for which you want to enable availability notifications. The business service view screen displays for the selected business service.

3 Click **Policy**.

4 If the business service does not have an entrypoint, the Select Entrypoint screen displays.

— Select the resource to use as the entrypoint.

— Click on **Save**.

5 The Edit Configuration Performance screen displays.

6 From the Availability section, select the **Alert when unavailable** check box.

7 Click **Save**.

Changing the SLO Polling Interval

The SLO Engine evaluates performance metric against SLO values every 6 minutes by default. An SLO is evaluated every minute using the last 6 minutes worth of data.

The preferable SLO window is 6 minutes. In addition, the SLO window should never be set to less than 1 minute.

To change the SLO polling interval:

1 Stop the Network Services server if it is currently started.

2 Use a text editor to open <*install_dir*>`\conf\networkservices\mipServer.xml`.

3 Add a `com.hp.mip.slo.windowSize` entry. Possible values are:

— Numerical values in milliseconds. For example, to set the window size to 6 minutes, specify 600000.

— `OneMinute`, `FiveMinutes`, `FifteenMinutes`, `OneHour`, `EightHours`, and `Life`. For example:

```
<entry name="com.hp.mip.slo.windowSize">FiveMinutes</entry>
```

4 Save and close the file.

5 Restart the Network Services server.

Viewing a Business Service's Status Details

A business service's status is used to monitor whether a business service is currently operating under normal conditions. Typically, an alert for a business service changes the status of the business service (i.e., an availability alert or SLO alert). The status of a business services is reported on the Business Services List as well as on a Business Service's View screen, which also provides details about the cause of a status change.

To view a business service's status details:

1 Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Service List screen, select a business service to view its details. The Business Service View screen displays for the selected business service.

6

Using Alert Notifications

This chapter provides instructions for configuring and using the alert notification features included with the SOA Manager. The instructions include creating alert recipients and alert recipient categories. In addition, this chapter covers two alert types: SLO Alerts and Business Content Alerts. An overview and conceptual architecture of the alert notification feature are also provided.

Overview

The alert notification feature is used to notify recipients when events occur that may impact network or business operation performance. When events occur, alerts are automatically sent to any number of alert recipients so that appropriate actions can be taken. In general, alerts help maintain efficient applications and help stop problems before they impact performance or breach business rules. Specifically, alerts are useful for:

- Troubleshooting – Alerts provide event details that can be used to see why a business service or its contained Web service may be failing.
- Monitoring – Alerts allow personnel to be notified of current performance metric values and react to unwanted situations before they escalate and degrade performance.
- Content Monitoring – Alerts can notify recipients when a specific value (i.e., order > $25,000.00) is found in a SOAP message.
- SLO Management – Alerts can safeguard against metric values that may be elevating past SLO levels.
- SNMP Management – Alerts in the SOA Manager can be integrated with SNMP management solutions.

Conceptual Architecture

The Network Service server contains a Notification Server which manages alerts through an Alert service. The Alert service generates the alerts, persists the alerts to the database, and sends the alerts to an alert category. An alert category organizes and manages alert recipients. The BSE is used to configure alert categories and alert recipients. Figure 6-1 shows a conceptual architecture of the alert feature.

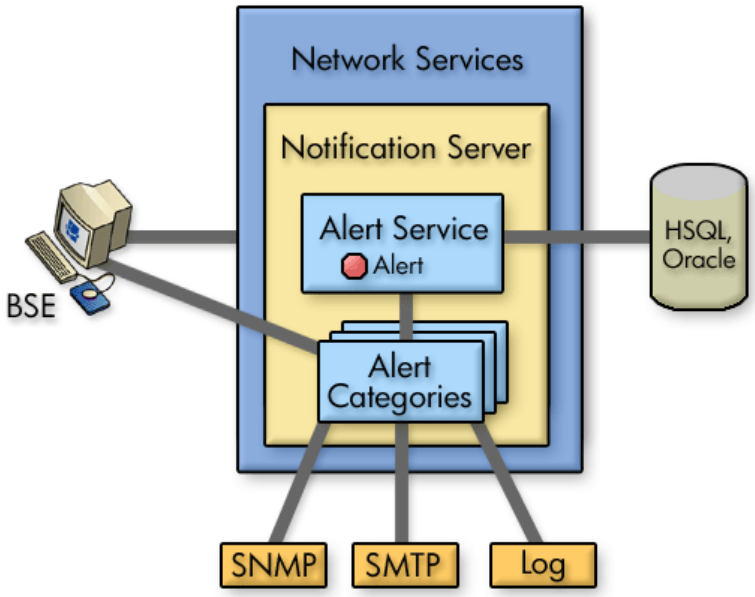


Figure 6-1: Alert Conceptual Architecture

Global Alert List

The global alert list is accessed by clicking the Alerts tab on the BSE main tool bar. The list is a global list of alerts and includes all alerts from all resources. The global alert list has two views Active Alerts and Acknowledged Alerts. The Active Alerts view lists all current alerts. The Acknowledged Alerts view displays the manually acknowledged alerts and automatically acknowledged alerts. When a new alert comes in, it will auto acknowledge all relevant alerts from the same source.

Resource Alert List

Alerts are also viewable on the Business Service View screen, Configuration View screen, IT Service View screen, Web Service View screen, and Web Service Operation View screen. These screens show the alerts that are specific to these resources.

Initially, active alerts for a selected resource are displayed. However, the **Show Acknowledged** link changes the alert view to Acknowledged Alerts. From the Acknowledged Alerts view, click **Show Active** to return to the Active Alerts view. Click an alert link to display the global alert list for the selected resource.

Alert Icons

Alert messages are associated with an icon that depicts the alert's severity. The following table lists the alert icons used by the BSE and provides a description for each icon.

Table 6-1: Alert Icon Descriptions

Alert Icon	Description
	Normal alert
	Informational alert
	Warning alert–low severity
	Minor alert–medium severity
	Major alert–serious severity
	Failed alert–critical severity
	Disabled

Alert Propagation

The Alert Service uses alert propagation to govern how alerts are propagated among associated resources in the service model. Alert propagation facilitates identifying alerts and troubleshooting events as they arise and ensures that alerts for low-level resources are noticed within the context of higher-level resources of the service model.

The resources that listen for alert changes include: business services, IT service configurations, and Web service configurations and Web service operations.

The rules for Alert propagation are as follows:

- If any configuration gets an alert, its related resources are notified. The notified resource in turn may or may not generate an alert on itself, which in turn could cause an alert on its related resources. In general, alerts tend to flow from a business service down through its resources.

  For example, when a Web service configuration violates an SLO, the Web service operation will not propagate that alert. However, if the Web service configuration is unavailable, the Web Service operation also becomes implicitly unavailable and this causes a new alert to be generated against the Web service operation.
- Any alerts for an entrypoint of a business service are propagated up to the business service.
- Any alert for a configuration are propagated to any dependent configurations.

An example of alert propagation can be seen when a managed WS container fails. The fail event causes an alert and status change for the WS container. In addition, the IT service and the business service that contains the WS container also generate an alert and status change. When the WS container recovers, the alert and status returns to normal and the alert and status for the IT service and business service recover as well.

The Alert column is used to monitor alert propagation. The column is visible on the Business Services screen as well as most view screens. The columns display the most severe current alert among associated assets in the service model. Acknowledging/Deleting the alert does not change any associated resources' status. Only a recovery alert changes the alert status.

A resource can have many different concurrent alert severities; however, the worst alert is always shown. In addition, each issue is resolved independently from the others. For example, if a business service contains two resources which have a status of severe, and one resource returns to normal, the business service continues to have a status of severe until the other resource also returns to normal.

SLO Alerts

SLO alerts notify recipients when an SLO threshold value for a performance metric is exceeded. For more information on defining SLO threshold values, see Chapter 5 "Monitoring Performance and SLO". There are four types of SLO alerts:

- SLO Normal () – An alert that is generated when the SLO threshold value is within normal levels or when a threshold value has returned to an acceptable level. This is a low-level alert and typically no action is required.
- SLO Warning () – An alert that is generated when the SLO Warning threshold value for a business metric is exceeded. This is a medium-level alert and should be used to indicate that a minor event has occurred that may impact an SLO.
- SLO Breach () – An alert that is generated when the SLO Breach threshold value for a business metric is exceeded. This is a high-level alert and should be used to indicate that a major or critical event has occurred and needs immediate attention.
- SLO Operational () – An alert that is generated when a component in the service model is not operational or unavailable. Operational alerts can be enabled for IT services, business services, configurations, and resources.

Assigning an SLO Alert to an Alert Category

When SLO alert threshold values are violated, an alert is generated and forwarded to all recipients in a recipient category that is assigned to an SLO alert type (warning or breach). See the "Setting Up Alert Recipients" category below for creating alert recipients and recipient categories.

To assign an SLO Alert Type to an Alert Category:

1 Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Services List screen, expand a business service to view its contained configurations.

3 Click the resource configuration you want to view. The appropriate view screen displays.

4 From the Performance section, click **Edit SLOs**. The Edit Configuration Performance screen displays.

5 In the Alert Recipients section, use the drop-down lists to select a recipient category for each SLO alert type.

6 Click **Save**.

Configuring the SLO Alert Polling Interval

The SLO Engine evaluates performance metric values against SLO threshold values. When the metric value violates the SLO threshold value, an alert is generated. The values are evaluated every minute by default.

To change the SLO polling interval:

1 Stop the Network Services server if it is currently started.

2 Use a text editor to open <*install_dir*>`\conf\networkservices\mipServer.xml`.

3 Add a `com.hp.mip.slo.windowSize` entry. Possible values are `OneMinute`, `FiveMinutes`, `FifteenMinutes`, `OneHour`, `EightHours`, and `Life`. The default is `OneMinute`. For example:

```
<entry name="com.hp.mip.slo.windowSize">FiveMinutes</entry>
```

4 Save and close the file.

5 Restart the Network Services server.

Business Content Alerts

Business content alerts notify alert recipients when specific content is contained in a SOAP message. Business content alerts are useful because they allow you to react to events that can potentially have an impact on business operations. For example, if you are managing an order process service, you could receive an alert when:

- An important client is using the service
- An order total is greater than $25,000.00
- A specific product is ordered
- A specific product is shipped

Business content alerts display on three screens in the BSE: a business service view screen, a Web service configuration view screen, and the alert list screen. A business content alert is generated for the Web service configuration associated with the Web service that sends the alert to the Network Services server; this alert has a severity level of `normal`. Another alert is generated for the business service that contains the Web service configuration; this alert has a severity level of `informational`.

There is a special alert category that is used for business content alerts, the `Business Content Alert Category`. This category is set for the business service and for the Web service configuration. If the category is not set for the Web service configuration, then the business service setting is used for the Web service configuration alerts. For more information on alert categories, see the “Setting Up Alert Recipients” section later in this chapter.

Defining a Business Content Alert

The Broker and WSM Agents contain a business content alert handler that is used to define a business content alert. Business content alerts are defined differently for the Broker and WSM Agents. Before you can view a business content alert for a Web service, the Web service must be contained in a business service.

Defining a business content alert requires knowledge of the W3C XPath expression language. It is beyond the scope of this documentation to cover the details of XPath. Several books on XPath are available and you can also refer to the W3C website for details. If you are not familiar with XPath, you should consult a developer before defining a business content alert.

WSM Broker

You can enable a broker agent’s business content handler using the Broker Configurator. The handler must be enabled for each brokered service that you create. You can enable the handler when you first create the brokered service or you can edit a brokered service at any time and enable the handler. The following procedure enables the handler for a brokered service and defines a business content alert using the Finance Service as an example. See the *Broker Configurator Online Help* for additional information on creating brokered services.

To enable the handler and define a business content alert:

1. Start the Broker Configurator.
2. From the Action column, click **edit** for the brokered service you want to configure. The Service Configuration screen displays.
3. From the Features section, click the Business Content Alerting check box. A check mark indicates that the option is selected and that business content alerting is enabled. The business content alerting parameters display.
4. Define the business metric using the parameter fields provided:
   - **Name:** Enter a user friendly name to identify the alert (i.e., `HPQ Alert`).
   - **Operation:** Enter an operation in the service that contains the business content you want to monitor. The XPath expression is applied to the operation (i.e., `getInfo`).
   - **Alert applies to**: Select when you want the broker to search for the operation. You can select to search during requests or responses.

- **Expression**: Enter an XPath expression which selects the business content from the operation. For example, `//ns1:InfoRequest/ns1:symbol/text()`. This expression traverses the SOAP message for the `InfoRequest` node and selects the text found for the `symbol` child node.
- **Message**: Enter a user friendly message that is sent with the alert (i.e, `A ${name} alert has occurred`).
- **Dynamic Properties**: Enter a dynamic variable defined within the message. The Name field corresponds to the variable name. The XPath field corresponds to an XPath expression used to update the variable. For example: (i.e., **Name**: `name` **Xpath**: `//s:Envelope/s:Body/t:InfoRequest/t:symbol/text()`
- **Namespace Prefixes**: Enter any name space prefixes that appear in the XPath expression (i.e., **prefix**: `ns1` **URI**: `http://wsm.hp.com/Finance/Request`).

5 At the bottom of the screen, click **Save**. The Brokered Services screen displays and the brokered service is automatically deployed. The deployment is complete when the status changes to `Operational`.

6 Send the Web service a request that uses the operation that is being monitored by the BusinessMetricHandler handler. An alert is sent to the BSE.

7 From the BSE Business Services list, select the business service that contains the brokered service for which the business content alert was defined. The Business Service View screen displays and the alert is listed in the Alerts section.

WSM J2EE Agent

You can enable a J2EE agent's business content alert handler using the Web service's `web-services.xml` file. See the *WSM J2EE Agent Administrator's Guide* for additional information on configuring handlers when using a J2EE agent.

To enable the handler and define a business content alert:

1 Stop the WebLogic Server (WLS), where the J2EE Agent is running, if it is currently started.

2 Use a text editor to open a Web service's `web-services.xml` file. The file is typically located in a Web application's `/WEB-INF` directory.

3 Add the following XML content within the `<web-services>` root element.

```
<handler class-name=
        "com.hp.wsm.agent.bizmetrichandler.BusinessMetricHandler">
   <init-params>
      <init-param value="" name=""/>
   </init-params>
</handler>
```

4 Configure the handler's parameters using name/value pairs as shown below. The Finance Service is used an example.

```
<handler class-name=
   "com.hp.wsm.agent.bizmetrichandler.BusinessMetricHandler">
   <init-params>
      <init-param value="FinanceService" name="catalog"/>
      <init-param value="FinanceService" name="servicename"/>
      <init-param value="FinanceServiceSoap"
                  name="serviceporttype"/>
      <init-param value="http://wsm.hp.com/finance"
                  name="servicenamespace"/>
      <init-param value="symbol" name="Name"/>
      <init-param value="InfoRequest" name="OperationName"/>
      <init-param value="//n1:InfoRequest/n1:symbol"
                  name="Expression"/>
      <init-param value="true" name="ProcessRequest"/>
      <init-param value="false" name="ProcessResponse"/>
      <init-param value="false" name="ProcessFault"/>
      <init-param value="http://wsm.hp.com/Finance/Request"
                  name="xmlns:n1"/>
      <init-param value="An InfoRequest alert has occurred"
                  name="message" />
      <init-param value="//s:Envelope/s:Body/t:InfoRequest/
                         t:symbol/text()"
                  name="dynamicprop:p1" />
   </init-params>
</handler>
```

- **catalog**: Enter the Web application's name.
- **servicename**: Enter the Web service's name.
- **serviceporttype**: Enter the port type as defined in the WSDL file for the Web service.
- **Name**: Enter a user friendly name to identify the alert.
- **OperationName**: Enter an operation in the service that contains the business content you want to monitor. The XPath expression is applied to the operation.
- **Expression**: Enter an XPath expression which selects the business content that will trigger an alert
- **ProcessRequest**: Allows a request to be processed. Valid values are `true` or `false`.
- **ProcessResponse**: Allows a response to be processed. Valid values are `true` or `false`.
- **ProcessFault**: Allows a fault to be processed. Valid values are `true` or `false`.
- **Namespace Prefixes**: Enter any namespace prefixes that appear in the XPath expression are entered as prefix/namespaceURI pairs.
- **Message**: Enter a user friendly message that is sent with the alert.
- **Dynamic Properties**: Enter a dynamic variable defined within the message pattern. The value is an XPath expression used to update the variable.

5. Save and close the file.
6. Restart WLS for the changes to take effect.
7. Send a Web service request that uses the operation that is being monitored by the BusinessMetricHandler handler. An alert is sent to the BSE.

8 From the BSE Business Services list, select the business service that contains the managed Web service for which the business content alert was defined. The Business Service View screen displays and the alert is listed in the Alerts section.

WSM .Net Agent

The .NET Agent Business Metric SOAP extension is enabled by modifying a Web service application's `Web.config` file. The file can be edited using an XML editor or a text editor. The following instructions enable the extension and also demonstrate how to define a business content alert using the Finance Service as an example.

To define a business content alert:

1 Using a text editor, open the FinanceService's `Web.config` file. For example:

```
C:/Inetpub/wwwroot/FinanceService/Web.config
```

2 Edit the file by adding a `<services>` node within the `<configuration>` node.

3 Create a `<service>` node within the `<services>` node and include a `name` attribute that contains the Web service name. For example:

```
<services>
   <service name="FinanceService.asmx">
```

4 Define the business content alert within a `<bizmetric>` node as shown below.

```
<bizmetric>
    <name>HPQ Info</name>
    <expression>
       //s:Envelope/s:Body/t:InfoRequest/t:symbol[text() = 'HPQ']
    </expression>
    <message>InfoRequest = ${company}</message>
    <operation>getInfo</operation>
    <direction>REQUEST</direction>
    <properties>
      <property>
        <name>company</name>
        <value>text()</value>
      </property>
    </properties>
    <namespaces>
      <property>
        <name>s</name>
        <value>http://schemas.xmlsoap.org/soap/envelope/</value>
      </property>
      <property>
        <name>t</name>
        <value>http://wsm.hp.com/Finance/Request</value>
      </property>
    </namespaces>
</bizmetric>
```

5 Use the fields to enter the alert policy:

— **Name:** A user friendly name to identify the alert.

— **Expression**: An XPath expression which selects the business content from the operation.

- **Message**: A user friendly message that is sent with the alert. Any alert service variables can also be used in the message. Alert variables are described in the BSE.
- **Operation:** The operation in the service that contains the business content you want to monitor.
- **Direction**: When to search for the operation. Valid entries are `REQUEST`.
- **Properties**: A dynamic variable defined within the message. The `name` attribute corresponds to the variable name. The `value` attribute corresponds to an XPath expression used to update the variable.
- **Namespace**: Any namespace prefixes that appears in the XPath expression. The `name` attribute refers to namespace prefix. The `value` attribute refers to the namespace URI.

6 Save and close the file.

7 Send a Web service request that uses the operation that is being monitored by the Business Metric SOAP extension. An alert is sent to the BSE.

8 From the BSE Business Services list, select the business service that contains the managed Web service for which the business content alert was defined. The Business Service View screen displays and the alert is listed in the Alerts section.

Troubleshooting Business Content Alerts

The following steps can help troubleshoot configuration issues related to business content alerts.

Network Services Setup

- Ensure the WS container/intermediary that should be raising the Business Content Alerts is registered with Network Services and is reachable.

  In the BSE, select the IT service that contains the WS container/intermediary and ensure that the Availability field displays the value **Operational** (also indicated by a green check).

- Ensure that Network Services subscribes to the WS container/intermediary for Business Content Alerts.

  Edit the `xpllogging.properties` file in the <*install_dir*>`/conf/networkservices` directory and increase the log level for the logger:
  `com.hp.ov.mip.wsm.sn.monitoring.notification.BusinessContentMonitoringService.level=FINE`.

  Restart Network Services. When the WS container/intermediary is re-added at startup, there should be log messages for each WS container/intermediary indicating whether or not it believes the WS container/intermediary supports Business Content Alerts, and if so, showing that the Network Services has subscribed for Business Metric `raiseAlert` events.

Service Setup

- In the WSM Agent, ensure that the handler that should be raising Business Content Alerts is configured to raise Business Content Alerts.
  - When using the WSM Broker:

    View the Service Details page and ensure that the Business Content Alert section is selected and that the details are filled in correctly.

    On the Services list, ensure that the Service is deployed and using the current configuration. The words "(changed on disk)" should not appear next to the Service in the Service list. If it does appear, undeploy and redeploy the Service.
  - When using the WSM J2EE Agent:

    View the Web applications `web-services.xml` configuration file and ensure that the `BusinessMetricHandler` has been added to the handler chain and is properly configured. You must restart the WLS for any changes to `web-services.xml` to take effect.
  - When using the WSM .NET Agent:

    Make sure that the `BusinessMetricPolicy` is defined and a business content alert is configured in the `Web.config` file for the Web service application.

Invocations

- Check that the invocations that should be triggering the Business Content Alert are actually reaching the configured WS container/intermediary.
  - When using the WSM Broker:

    View the Service Details page and ensure that the Logging option is selected for the Service.

    Edit the `xpllogging.properties` file in the <*install_dir*>/`conf/broker` directory and set the logger `service.`<*service name*> to `INFO`. For example, for a Service named FinanceServiceProxy, the following line should be added:

    ```
    com.hp.ov.mip.service.FinanceServiceProxy.level=INFO
    ```

    Restart the Broker.

    Send an invocation through the broker. The request and response messages should display in the Broker Configurator (if the broker is not running as a win32 service) and in the broker log file.
  - When using the WSM J2EE Agent:

    Edit the logging.properties file in the JRE /lib directory and add the logger:

    ```
    com.hp.ov.mip.wsm.commons.net.level=WARNING
    ```

    Restart WLS.

    Send an invocation to the Web service. The request and response messages should appear in the domain log file (i.e., `bea/user_projects/domains/`<*domain*>/<*domain*>`.log`).
  - .NET does not currently log request or response payloads.

- Confirm that the message body (request or response, depending on the Business Content Alert configuration) contains the necessary data to trigger the configured Business Content Alert.
  - When using the WSM Broker:

    Confirm that the operation name specified in the Operation field of the Business Content Alert configuration matches the Request Operation name in the log file.

    Confirm that the XPath expression will select the correct node in the request or response body (depending on whether Request Message or Response Message was selected in the alert configuration).

    Confirm that the namespace prefixes used in the XPath expression are correctly defined in the alert configuration.
  - When using the WSM J2EE Agent:

    Confirm that the operation name of the invoked method matches the value of the `OperationName` parameter in the `web-services.xml` file.

    Confirm that the XPath expression will select the correct node in the request body, response body, or fault.

    Confirm that the namespace prefixes used in the XPath expression are correctly defined in the `web-services.xml` file.
  - When using the WSM .NET Agent:

    Confirm that the service being invoked is the service for which the Business Content Alert is configured.

    Confirm that the XPath expression specified in the `Web.config` file selects the correct node in the request.

    Confirm that the condition specified in the XPath expression exists in the selected node (i.e., if the alert specifies that the value must equal `foo`, the node text value should be `foo`).

    Confirm that the namespace prefixes used in the XPath expression are correctly defined in the `Web.config` file for Web service application.
- Check that the WS container/intermediary is raising the alert.
  - When using the WSM Broker:

    Edit the `xpllogging.properties` file in the <*install_dir*>/`conf/broker` directory and set the logger:

    ```
    com.hp.ov.mip.wsm.sn.router.xml.bizmetrichandler.level=WARNING
    ```

    Restart the Broker.

    Send an invocation through the broker. A log message should appear in the log file indicating that a `BusinessMetricAlert` for metric <*metric name*> is being sent.
  - When using the WSM J2EE Agent:

    Edit the `logging.properties` file in the JRE /lib directory and add the category:

    ```
    com.hp.ov.mip.wsm.impact.sba.controller.service.event=
    WARNING
    ```

Restart WLS.

Send an invocation through the broker. Log messages should appear in the domain log file (i.e., bea/user_projects/domains/<*domain*>/<*domain*>.log) indicating that a `BusinessMetricAlert` is being sent.

— .NET does not currently log the sending of BusinessMetricAlerts.

- Check that Network Services is receiving the alert.

  If the alert is received, the `BusinessContentMonitoringService` and the `AlertDispatcher` will log any problems that occur processing the alert. Otherwise, the alert should display in the Alert List.

  No positive debug logs exist in the `BusinessContentMonitoringService` to indicate normal processing of Business Content Alerts.

Customizing Alert Messages

Customizing alert messages provides a greater level of granularity when describing the reasons for an alert and can help create more meaningful messages that are specific to an enterprise. Detailed and familiar alert messages can improve issue resolution as well as maintain overall performance.

Alert messages are created using a default message that contains information about the alert (i.e., alert severity, source, timestamp, etc…). However, you can customize any alert message to include additional information. The information can be text that you add to the message and can also include dynamic properties that are exposed by the Alert Service.

Alert messages can be customized only after an alert is generated for the first time. After the message is customized, all subsequent messages of the same alert type will contain the custom message.

To customize and alert:

1. From the BSE main tool bar, click the **Alerts** tab. The Alert List screen displays.
2. Click the Alert Id number for the alert type whose message you want to customize. The Basic Details screen displays. Basic details as well as specific properties of the alert message are listed.
3. From the Message row, click **format**. The Edit Alert Message screen displays.
4. In the message text box, customize the default message. You can use text as well as any dynamic properties that are listed in the Dynamic Values table. Dynamic properties must be entered using the format `${`*property_name*`}`.
5. To preview the message, click **Test**.
6. Click **Save**. The next time an alert of this type is generated, it will contain the custom message.
7. Click **Done**.

8 Repeat this procedure to customize additional alert messages for an alert type.

Acknowledging Alerts

Alerts that are resolved must be acknowledged and removed from the BSE. If the alert is listed on multiple View screens, then acknowledging an alert removes it from the View screens as well.

To acknowledge alerts:

1 From the BSE main toolbar, click the **Alerts** tab. The Alerts List screen displays.

2 Use the option boxes to select which alerts you want to acknowledge, or select the option box in the table head to remove all alerts.

3 Click **Acknowledge Selected**. All the selected alerts are removed from the Alerts List as well as the alert section of a view screen.

Acknowledging alerts from the BSE does not remove alerts from the SOA Manager database.

Querying Alerts

All alerts are stored in the Network Services database. The alerts remain in the database even after they have been removed from the BSE. The query link allows the user to find audit traces in the database that may be related to an alert.

This feature is the same as the audit feature. Using this feature returns audit traces, which include alerts. See Chapter 7 “Using Auditing” for more information on the Auditing feature.

1 From the BSE main tool bar, click the **Alerts** tab. The Alert List screen displays.

2 Click the Alert Id number for the alert type you want to query. The Basic Details screen displays. Basic details as well as specific properties of the alert message are listed.

3 From the Message row, click **query**. The Query screen displays.

4 Use the **Start Date** fields to enter the query’s start date and start time.

5 Use the **End Date** fields to enter the query’s end date and end time.

6 Using the Service drop-down lists, to select which service to query.

7 If you want to query the alerts based on a specific authenticated security principal (authenticated user), enter the user name in the **User** text box.

8 Click **Query**. The results of the query are listed in the Results section.

9 Click on a timestamp to view audit details.

Setting Up Alert Recipients

When an alert is generated, it is sent to recipients that are part of a recipient category. Alert recipients include:

- BSE Console – Alerts are sent to the BSE console. Depending on the source of the alert, the alert is listed on the Alerts are also viewable on the Business Service View screen, Configuration View screen, and Resource View screens. All alerts are listed on the Alert List screen.
- SNMP – Alerts are sent to an SNMP log category that is configured to send the log message to an SNMP TRAP.
- SMTP – Alerts are sent as an email message to any number of email addresses.
- Log File – Alerts are sent to a log category and published using the output method defined by the category.

Recipient categories are used to organize recipients because they provide an efficient method of supporting multiple recipients for an alert. Several default categories are provided that you can customize. In addition, you can create your own recipient categories.

Modifying an Existing Recipient Category

To modify an existing recipient category:

1. From the BSE main tool bar, click **Settings**. The Settings screen displays.
2. Click the **Alert Settings** tab. The Alert Settings screen displays.
3. Under the Service alerts assigned to *category* ... section, click the recipient category you want to modify. The Edit Alert Category screen displays.
4. From the list of targets, select the targets to be included in the category.
5. Click **Update Alert Targets**.

Creating Recipient Categories

To create a new recipient category:

1. From the BSE main tool bar, click **Settings**. The Settings screen displays.
2. Click the **Alert Settings** tab. The Alert Settings screen displays.
3. Under the Service alerts assigned to *category* ... section, enter a name for the new alert category.
4. Click **Add Category**. The new category is listed in the list of available categories.

Adding Alert Recipients to a Recipient Category

To add alert recipients to an alert category:

1. From the BSE main tool bar, click **Settings**. The Settings screen displays.
2. Click the **Alert Settings** tab. The Alert Settings screen displays.
3. Under the Service alerts assigned to *category* ... section, click the recipient category you want to modify. The Edit Alert Category screen displays.
4. Select the targets to be included in the category.
5. Click **Update Alert Targets**. The Alert Settings screen displays and lists the recipients associated with the recipient category.

Creating Email Recipients

The SMTP feature uses the server's native SMTP service to send emails to an email recipient. If the SMTP service is not activated, you must activate the service before emails can be sent. See your operating system's documentation for instructions on enabling the SMTP service.

To create an email recipient:

1. From the BSE main tool bar, click **Settings**. The Settings screen displays.
2. Click the **Alert Settings** tab. The Alert Settings screen displays.
3. Under the Assigned alerts can be sent to *target* ... section, click **Add New Target**. The Add Alert Target screen displays.
4. From the drop-down list, select **email**.
5. In the text field, enter a name for the recipient.
6. Click **Add Target**. The Alert Settings screen displays and the new recipient is listed in the list of available recipients.
7. If the email settings haven't been configured, click the **Email Settings** tab. The Email Settings screen displays. Enter the email properties using the fields provided:
   - **Email Support**: Select Enable.
   - **SMTP Host**: The server's host name.
   - **Port**: The port on which the SMTP service is running.
   - **User**: The administrator's user name that has access rights to use the SMTP service on the server. Any user that has access to the SMTP service can be used.
   - **Password**: The administrator password that has access rights to use the SMTP service on the server. Any user that has access to the SMTP service can be used.
   - **Sender**: The email sender.

   Click **Save**.
8. Click the **Alert Settings** tab.

9 Under the Assigned alerts can be sent to *target* ... section, click on the new email recipient to edit its properties. The Edit Target screen displays.

10 Enter the email properties using the fields provided:

— **To**: The recipient's email address.

— **Subject**: The subject of the email.

— **Body**: A message to be displayed in the body of the email message. The body can use any dynamic values as listed in the Dynamic Values section.

11 Click **Test** to test if the configuration you entered is valid and works correctly.

12 Click **Save**. The Alert Settings screen displays.

13 For the new email recipient, click **Start** to activate the recipient.

Creating Log Recipients

The log feature uses the Log4j logging implementation to send an alert to a log category that publishes the alert to the output specified by the log category. Log categories are configured in the `logging.properties` file in the *<install_dir>*`\conf\networkservices` directory.

To create a log recipient:

1 From the BSE main tool bar, click **Settings**. The Settings screen displays.

2 Click the **Alert Settings** tab. The Alert Settings screen displays.

3 Under the Assigned alerts can be sent to *target* ... section, click **Add New Target**. The Add Alert Target screen displays.

4 From the drop-down list, select **log4j**.

5 In the text field, enter a name for the recipient.

6 Click **Add Target**. The Alert Settings Screen displays and the new recipient is listed in the list of available recipients.

7 Under the Assigned alerts can be sent to *target* ... section, click on the new log recipient to edit its properties. The Edit Target screen displays.

8 Enter the log properties using the fields provided:

— **category**: The log category that the alert is sent to. Any category that is in the logging.properties file can be used. The `default` category publishes outputs to the network services console.

— **level**: The logging level to use. The log levels are: `DEBUG`, `INFO`, `WARN`, and `ERROR`. By default the log level is set to `WARN`. If you want to use a different level, you must assign the category's level appropriately in the `logging.properties` file.

— **message**: A message to be displayed in the log. The message can use any dynamic values as listed in the Dynamic Values section.

If you change `logging.properties`, you must restart the network services server for the changes to take effect.

9 Click **Test** to test if the configuration you entered is valid and works correctly.

10 Click **Save**. The Alert Settings screen displays.

11 For the new log recipient, click **Start** to activate the recipient.

Creating SNMP Recipients

The SNMP feature uses the Log4J logging implementation to send an alert to a special SNMP log category (log4j.category.com.hp.wsm.sn.notification.target.snmp). The SNMP log category is set to publish the alert message to an SNMP TRAP. You can configure the location of the SNMP TRAP in <*mip_installation_dir*>`/conf/networkservices/logging.properties`. See the "Getting Started" chapter for more information on logging.

Before configuring an SNMP recipient, you must configure your SNMP TRAP settings. The SNMP TRAP settings indicate the location and configuration of your SNMP TRAP. These settings are located in <*install_dir*>`/conf/networkservices/logging.properties`. You must restart the network services server for the changes to take effect.

To create an SNMP recipient:

1 From the BSE main tool bar, click **Settings**. The Settings screen displays.

2 Click the **Alert Settings** tab. The Alert Settings screen displays.

3 Under the Assigned alerts can be sent to *target* ... section, click **Add New Target**. The Add Alert Target screen displays.

4 From the drop-down list, select **log4j**.

5 In the text field, enter a name for the recipient.

6 Click **Add Target**. The Alert Settings Screen displays and the new recipient is listed in the list of available recipients.

7 Under the Assigned alerts can be sent to *target* ... section, click on the new log recipient to edit its properties. The Edit Target screen displays.

8 Enter the log properties using the fields provided:

- **category**: Enter the SNMP log category `log4j.category.com.hp.wsm.sn.notification.target.snmp`.
- **level**: Enter `INFO` for the level.
- **message**: A message to be displayed in the log. The message can use any dynamic values as listed in the Dynamic Values section.

9 Click **Test** to test if the configuration you entered is valid and works correctly.

10 Click **Save**. The Alert Settings screen displays.

11 For the new recipient, click **Start** to activate the recipient.

7

Using Auditing

This chapter outlines the auditing capability in the SOA Manager and its possible applications. It provides an architectural overview of the technical components that collaborate to enable auditing. The chapter also includes instructions for configuring the various participating components.

Overview

Auditing refers to the capturing of information related to message exchanges with managed Web services into a central database. An audit message trace contains information related to performance, security, size, source and destination endpoints, successes and failures (i.e., SOAP faults), and can also include the SOAP request-response payloads and profile data.

Trace information is persisted to a database at regular intervals. You can use the BSE to view message trace information; moreover, trace information can be reused by other applications. In general, the audit traces are useful for:

- Troubleshooting – You can verify exactly which messages are failing and possible reasons why they are failing.
- Security Auditing – You can discover when and by whom Web services are being used.
- Billing – An application can use trace information for billing (i.e., the number of times a Web service was accessed by a particular client).
- Non-repudiation – You can securely reproduce messages exchanged with a Web service.
- Service Level Agreement (SLA) – You can integrate trace information with analytic products that provide SLA reporting.

Architecture

The audit architecture is comprised of several distributed components. These components are listed here and Figure 7-1 shows the general runtime flow of the components.

- **Audit Handlers** – The WSM agents (J2EE, .NET) and the Broker can be configured to contain audit handlers. When messages pass through the Web service, they are captured, along with their context information, by the audit handler. Information collected by the audit handlers is sent to the audit publisher.
- **Audit Publishers** – The WSM agents each contain an audit publisher. The audit publisher is responsible for publishing the trace information to the audit service that is part of the Network Services server.

  When a WSM Agent (J2EE, .NET) or Broker is registered with the Services Network, the Audit Service registers itself as a listener for Audit Traces with the Audit Publisher using a WSMF Notification subscription. This is how the Publishers know how to find the Audit Service.
- **Audit Service** – The audit service runs in the Network Services server and receives published trace information from all audit publishers. The audit service is also responsible for saving the information to the database.
- **Database** – The database stores all trace information.

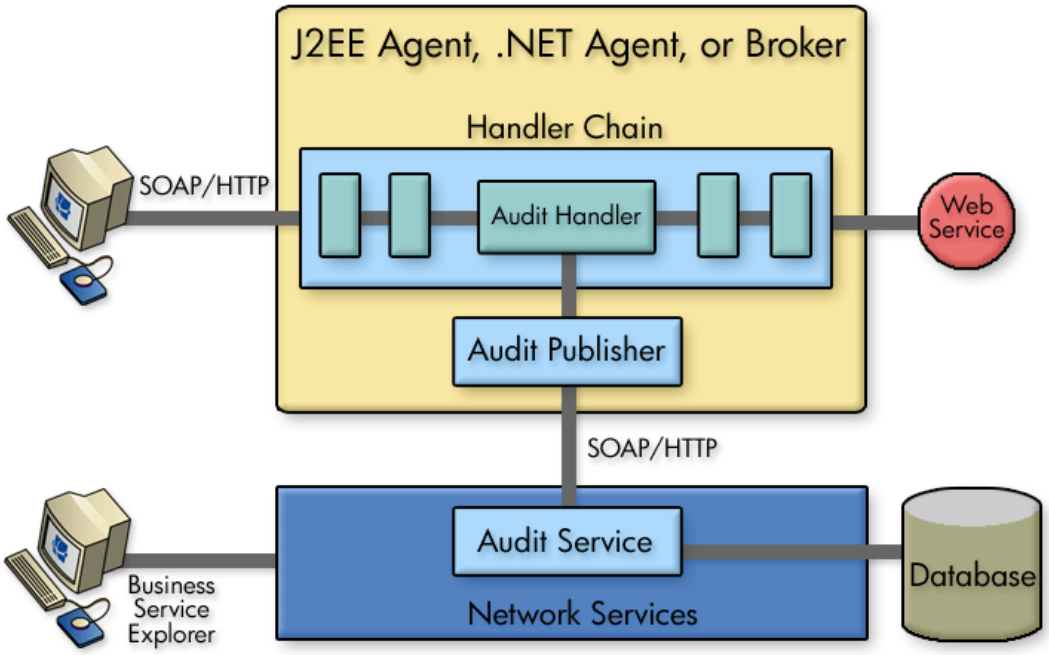


Figure 7-1: Audit Architecture

Setting Up the Audit Components

The components of the audit feature must be set up before message trace information is collected and stored in the database and viewed using the BSE. To set up the auditing components you must:

- Enable the Audit Handler
- Configure the Audit Publisher
- Configure the Database

Enable the Audit Handler

The WSM Agents and the broker contain a group of handlers that are responsible for gathering management data for a Web service. Enabling an agent's audit handler is achieved differently for the Broker and WSM Agents.

The audit handler for the J2EE Agent and the .NET Agent is enabled by default.

WSM Broker

You can enable a broker's audit handler using the Broker Configurator. The audit handler must be enabled for each brokered service that you create. You can enable auditing when you first create the brokered service or you can edit a brokered service at any time to enable auditing. The following procedure enables the audit handler for a brokered service which has already been created. See the *Broker Configurator Online Help* or the *WSM Broker Administrator Guide* for additional information on creating brokered services.

To enable the audit handler:

1. Log in to the Broker Configurator.
2. From the Action column, click **edit** for the brokered service you want to configure. The Service Configuration screen displays.
3. From the Features section, click the **Auditing** check box. A check indicates that the auditing is selected and that traces will be sent to the audit database.
4. If you want the audit handler to capture profile data, click to select the **Include detailed traces** check box. This feature captures the outcome of a Web service invocation as it passes through each handler in the handler chain for a brokered service.
5. If you want to also collect a message's SOAP payload, use the Payload Option drop-down list to select whether you want the payload to be collected for requests, responses, or both requests and responses.
6. Use the options provided to select whether you want the payload for all messages (successful and failed) or just for failed messages.

7 At the bottom of the screen, click **Save Changes**. The Brokered Services screen displays and the brokered service is automatically deployed. The deployment is complete when the status changes to `operational`. You may need to refresh the screen to see the status change.

WSM J2EE Agent

The WSM J2EE Agent automatically adds an audit handler to every Web service it discovers. The handler is enabled in a Web service's `web-services.xml` file. See the *WSM J2EE Agent Administrator Guide* for additional information on configuring handlers when using a J2EE Agent.

WSM .NET Agent

The .NET Agent's Audit SOAP extension is enabled for either specific Web services or for all Web services. The following instructions are applicable when enabling Auditing for a specific Web service. See the *WSM .NET Agent Administrator Guide* for additional information on configuring SOAP extensions.

To enable the audit SOAP extension for a specific Web service:

1 Use a text editor to open an application's `Web.config` file.

2 Edit the file by adding a `<services>` node within the `<configuration>` node.

3 For each Web service, create a `<service>` node within the `<services>` node and include a `name` attribute that contains the Web service name. For example:

```
<services>
   <service name="FinanceService.asmx">
```

4 Within the `<service>` node add an `<audit>` node and include a `payload-option` and `payload-filter` attribute. For example:

```
<services>
   <service name="FinanceService.asmx">
      <audit payload-option="REQUEST-RESPONSE"
             payload-filter="ALL" />
   </service>
</services>
```

— **payload-option**: Defines what payloads to audit. Valid entries are `REQUEST`, `RESPONSE`, `REQUEST-RESPONSE`, or `NONE`.

— **Payload-filter**: Defines when to capture the payload. Valid entries are `ALL` or `ERROR`. Setting this attribute to `ALL` captures payloads that are successful and payloads that encountered errors.

5 Repeat Steps 3 and 4 to enable auditing for additional Web service in the application.

6 Save and close the file.

Configure the Audit Publisher

The WSM Agents and Broker contain an audit publisher that is responsible for sending trace information to the Network Services' audit service. Configuring an agent's audit publisher is achieved differently for the Broker and WSM Agents.

There are two properties you can configure for the audit publisher. The properties define the number of trace messages (bucket size) to send to the audit service and the interval (in milliseconds) to wait before sending trace messages. Trace messages are published based on whichever value is reached first.

A small bucket size or interval means trace messages are published very often and may produce unwanted overhead that affects performance. A large bucket size or interval means trace messages will not be available for a long time and could hinder you from detecting and correcting problems or security violations. These properties should be set according to your business and application requirements.

WSM Broker

To configure the audit publisher for the Broker:

1. Stop the Broker if it is currently started.
2. Use a text editor to open <*install_dir*>\conf\broker\mipServer.xml.
3. Edit the audit publisher entries for `interval` and `threshold`. The `interval` value is in Milliseconds and the `threshold` value is the total number of trace messages:

```
<entry name="com.hp.audit.publisher.interval">100000</entry>
<entry name="com.hp.audit.publisher.threshold">10</entry>
```

4. Save and close the file.
5. Restart the Broker for the changes to take effect.

WSM J2EE Agent

In addition to the audit publisher properties for interval and trace, the J2EE Agent's publisher also controls whether or not a messages' SOAP payload is sent. These settings are also discussed in this procedure.

To configure the audit publisher:

1. Stop the WebLogic server, where the J2EE Agent is running, if it is currently started.
2. Use a text editor to open <*j2ee_agent_install_dir*>\config\agent.xml.
3. Under the `<components>` node, find the `<component>` element with the `id` attribute `Auditing`.
4. Edit the `publishInterval` and `traceThreshold` parameters. The `publishInterval` value is in milliseconds and the `traceThreshold` value is the total number of trace messages:

```
<parameters>
   <parameter name="traceThreshold" value="200" />
   <parameter name="publishInterval" value="3600000" />
</parameters>
```

5. Within the same node, you can configure whether you want a message's SOAP payload to be sent with the trace information. For example:

```
<parameter name="payloadOption" value="request-response" />
<parameter name="payloadFilter" value="all" />
```

- `payloadOption` – Valid values are `none`, `request`, `reponse`, and `request-response`.
- `payloadFilter` – Valid values are `all`, and `failure`. The `all` value sends payload for both failed and successful messages.

6 Save and close the file.

7 Restart the WebLogic server for the changes to take effect.

WSM .NET Agent

The audit publisher for the .NET Agent is configured using a Web service that comes with the .NET Agent. The Web service is called `RemoteConfig.asmx` and is only accessible from the computer that is hosting the .NET agent.

To configure the audit publisher:

1 From the computer that is hosting the .NET Agent, open a browser.

2 Go to the following URL:

`http://<DotNetAgentHost>/hpwsm/RemoteConfig.asmx`

Replace <*DotNetAgentHost*> with the with the fully qualified DNS name of the computer.

3 From the RemoteConfig Web service, click **SetAuditBucketSize**. The SetAuditBucketSize operation screen displays.

4 Using the bucketSize text box, enter the total number of trace messages as an integer.

5 Click **Invoke** to set the bucket size. The SetAuditBucketSize operation is run and a new browser window displays with a blank screen.

6 Close the blank browser window.

7 From the browser window for the SetAuditBucketSize operation screen, click the browser's **Back** button. The RemoteConfig Web service displays.

8 From the RemoteConfig Web service, click **SetAuditInterval**. The SetAuditInterval operation screen displays.

9 Using the intervalSeconds text box, enter the trace interval in Milliseconds as an integer.

10 Click **Invoke**. The SetAuditInterval operation is run and a new browser window displays with a blank screen.

11 Close all browser windows.

Configure the Database

Message trace information is sent to the Network Services' audit service and stored in a database. The Network Services server includes an embedded instance of the HSQL database (http://hsqldb.sourceforge.net/) that is enabled by default. This database can be used for testing. However, for production environments, a database schema for creating the data tables in Oracle 9i is provided. See the Oracle documentation if you are not familiar with creating data tables using a schema file. As with all databases, you must monitor the database and periodically do maintenance. For the auditing feature, the number of trace messages will continue to grow in size. You should periodically retire old data before it becomes unmanageable. See the "Performing Database Maintenance" section in Chapter 2.

Configuring the HSQL Database

The default installation of the Network Services server is configured to use the embedded HSQL database. This is reflected in:
<*install_dir*>\conf\networkservices\mipServer.xml.

```
<entry name="com.hp.db.demo">true</entry>
```

Once this entry is set to `demo=true`; remaining values related to JDBC URL, user name, etc. are ignored and will use the following default values. These default values are not reflected in the xml file but hard-coded in the Network Service server:

```
<entry name="com.hp.db.driver">org.hsqldb.jdbcDriver</entry>
<entry name="com.hp.db.url">
   jdbc:hsqldb:E:\<install_dir>\data\sn</entry>
<entry name="com.hp.db.user">sa</entry>
<entry name="com.hp.db.password"></entry>
```

HSQL comes with a swing-based GUI Database Manager that can be used to view trace information in the Audit tables and perform routine maintenance. The class for starting the database manager is located in the <*install_dir*>/lib/ext/hsqldb.jar. The full class name is `org.hsqldb.util.DatabaseManager` and can be started from the command line.

Configuring an Oracle 9i Database

A schema for creating the audit tables in Oracle 9i is located at <*install_dir*>\data\oracle\CollectionService-Create-Oracle9i.SQL. After you create the database and create the schema, configure the Network Services server to use the database.

You must copy the 9.2.0.5.0 version of the oracle thin JDBC driver (`oracle_ojdbc14.jar` and `oracle_nls_charset12.jar`) into the <*install_dir*>/lib directory.

To configure the Network Services server to use the Oracle 9i database:

1. Stop the Network Services server if it is currently started.
2. Open <*install_dir*>\conf\networkservices\mipServer.xml.

3 Add your database information in the DB Properties section. For example:

```
<entry name="com.hp.db.demo">false</entry>

<!-- The demo entry must be set to false. -->

<entry name="com.hp.db.driver">
   oracle.jdbc.driver.OracleDriver</entry>
<entry name="com.hp.db.url">
   jdbc:oracle:thin:@host:1521:DB1</entry>
<entry name="com.hp.db.user">admin</entry>
<entry name="com.hp.db.password">admin</entry>
```

4 Save and close the file.

5 Restart the network services.

Viewing Audit Information

The BSE allows you to query trace messages that are stored in the SOA Manager database. You can query successful messages and failed messages. For each trace message, you can see detailed trace information.

To view audit information:

1 Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Services List screen, expand a business service to view its contained configurations and Web services configurations.

3 Click the Web service configuration you want to view or expand the configuration and click a specific operation. The appropriate view screen displays.

4 From the 1 hour summary table, click the success value (to query trace messages for successful requests) or failure value (to query trace messages for failed requests). The View Failures or View Successes screen displays depending on the value selected.

5 In the Query section, configure the following query fields:

- **Search For:** Select the **Success** and/or the **Failure** check boxes.
- **Service:** Use the drop-down lists to constrain the query by business service, IT service or Web/brokered service.
- **Start Date:** Use the fields to enter a specific start date and start time for the query to match.
- **End Date:** Use the fields to enter a specific end date and end time for the query to match.
- **User:** Enter a user in the field if you want query the trace messages based on a specific authenticated security principal (authenticated user) that made the request.

6 Click **Query**. The results of the query are listed in the Results section.

7 Click on a trace message's Timestamp to view trace information details as well as Profile Data.

Viewing Reports

The BSE allows you to query the SOA Manager database and produce business service reports. The reports can be generated for any business service over any specified period of time. The reports are:

- Service Level by Consumer Reports
- Audit Message Traces Reports

Service Level by Consumer Reports

The Service Level by Consumer report provides the following statistics:

- Request Count
- Success Count
- Failure Count
- Availability Percentage
- Max Response Time
- Min Response Time.

To view Service Level by Consumer reports:

1. From the BSE main tool bar, select **Reports**. The Reports screen displays.
2. Click **Service Level by Consumer**. The Service Level by Consumer screen displays.
3. Complete the following fields:
   - **Consumer:** Use the drop-down list to select a specific consumer of the business service to include in the query. To include all the consumers of a service, select **ALL**.
   - **Service:** Use the drop-down list to select the business service on which to constrain the report.
   - **Start Date:** Use the fields to enter a specific start date and start time for the query to match.
   - **End Date:** Use the fields to enter a specific end date and end time for the query to match.
   - **Interval:** Use the drop-down list to select a predefined interval of time on which to constrain the report. For example, if you select `1/2/05 10 AM PST` as the start date, and `1/3/05 10 AM PST` as the end date, and interval as an hour, the report will contain around 24 rows, one for each hour between 1/2/05 10 AM and 1/3/05 10 AM. Each row is labeled with the timestamp for the hour it represents.
4. Click **Query**. The results of the query are listed under the Service section.

Audit Message Traces Reports

This report allows you to view audit message trace information.

To view Audit Message Traces reports:

1. From the BSE main tool bar, select **Reports**. The Reports screen displays.
2. Click **Audit Message Traces**. The View Success and Failures screen displays.
3. In the Query section, configure the following query fields:
   - **Search For:** Select the **Success** and/or the **Failure** check boxes.
   - **Service:** Use the drop-down lists to constrain the report by business service, IT service or Web/brokered service.
   - **Start Date:** Use the fields to enter a specific start date and start time for the query to match.
   - **End Date:** Use the fields to enter a specific end date and end time for the query to match.
   - **User:** Enter a user in the field if you want query the trace messages based on a specific authenticated security principal (authenticated user) that made the request.
4. Click **Query**. The results of the query are listed under the Service section.
5. Click on a trace message's Timestamp to view trace information details as well as Profile Data.

Troubleshooting

Problems that are encountered when using the auditing feature are often related to database setup. It is recommended that before implementing an Oracle database that you test the audit feature using the preconfigured HSQL database included with SOA Manager. The following tips may also help you isolate problems:

- Ensure you have configured Audit handlers appropriately.
- When using Oracle, ensure that the 9.2.0.5.0 version of the oracle thin JDBC driver (`oracle_ojdbc14.jar` and `oracle_nls_charset12.jar`) are copied into the <*install_dir*>`/lib directory`.
- Make sure the Broker or WSM Agent's publisher threshold value or interval value has been met. That is, you have waited the interval's value in Milliseconds, or you have sent enough requests to the managed Web service to satisfy the threshold value. If one of these values has not been met, trace messages will not be published. During testing, it may be useful to use small values for these settings so that trace messages are published frequently.
- Verify that messages are being sent to the database by checking the database file to see if it is increasing in size. When using the HSQL Database, the data file to check is <*install_dir*>`\data\hsqldb\sn.script`.
- Make sure you are using your database's correct driver package for JDBC persistence. When using the HSQL database the correct driver is already defined.

- Check for any reported errors in the standard out log messages for the Network Services console and the Network Services log file (<*install_dir*>`\log\networkservices.log`).
- Check for any reported errors in the log files for the Broker or WSM Agents:
  - J2EE Agent log messages are found in the WebLogic Server's standard out and the Server's log file. (i.e., `C:\bea\user_projects\domains\mydomain\mydomain.log`).
  - Broker log messages are sent to the standard out and to the broker's log file (<*install_dir*>`\log\broker.log`).
  - .NET Agent log messages are sent to the agent's log file located at (<*IIS_directory*>`/hpwsm/Log/HpWsmAgent.log`).

8

Using Deployment

This chapter provides instructions for using the SOA Manger's deployment feature. The chapter also includes overview information as well as the deployment feature's architecture.

Overview

The SOA Manager's deployment feature deploys a deployment unit to a managed WS Container/Intermediary that is registered in the Network Services server. The deployment feature is used from within the BSE and allows you to update Web services or brokered services that are being managed as business services.

In general the deployment feature addresses two common use cases. First, the deployment feature allows you to deploy new versions of a Web service that are contained in a business service. Web services, as with all application types, typically change over time. They may initially be deployed in a development environment and go through several iterations while they are being developed and tested. Once deployed to a production environment, new features may be added or bugs may be fixed.

Second, the deployment feature allows you to deploy instances of a Web service to compensate for increased demand during heavy loads.

The deployment feature addresses the dynamic nature of the enterprise and provides the following benefits:

- Allows adaptability – The deployment feature provides the ability to react quickly when performance is degrading or failing.
- Promotes business service reuse – The deployment feature deploys updated Web services to a managed WS Container/Intermediary within the context of a business service. The business service remains valid even when the services contained in the business service are changing.
- Allows ease of deployment – The deployment feature allows Web services to be deployed without having to know the deployment technology implemented by a WS Container/Intermediary.

- Promotes separation of the production and development environment – The deployment feature simplifies and standardizes the movement of Web services from a development environment to a production environment.

Architecture

The deployment architecture is comprised of distributed components. These components are listed here and Figure 8-1 shows the general runtime flow of the components.

- **Deployment Service Adapter** – The deployment service adapter runs in the Network Services server and sends a deploy request to a WSM agent's deploy service. As part of the request, the deployment unit's name and URL are sent.
- **Deploy Service** – The WSM agents (J2EE, .NET) and the WSM Broker each contain a deployment service that is responsible for deploying a deployment unit. The deploy service is itself exposed as a Web service and leverages the deployment features of the WS Container/Intermediary.

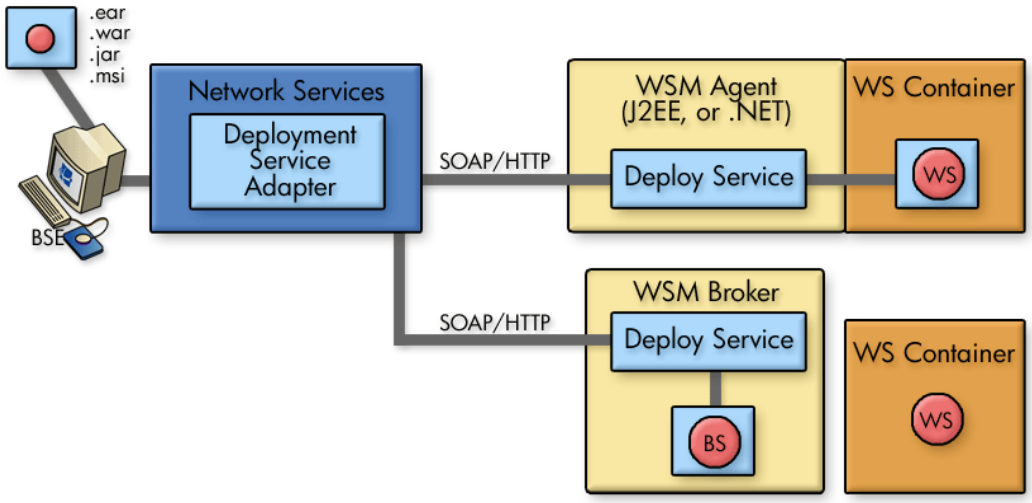


Figure 8-1: Deployment Architecture

Valid Deployment Units

The deployment feature deploys deployment units. Deployment units are different depending on the platform to which they are deployed. For WLS and .NET, a deployment unit represents the artifacts (Web services) that are to be managed. For a Broker, a deployment unit represents a brokered service, which includes the management capabilities (interposed) for a Web service.

The following sections describe the deployment unit types that are available for each platform.

WLS Deployment Units

A valid WLS deployment unit is an Enterprise ARchive (`.ear`) or a Web ARchive (`.war`). In WLS, a Web service is typically packaged as a `.war`, which is then packaged as an `.ear`. However, a `.war` can also be used without being packaged within an `.ear`. It is beyond the scope of this documentation to explain how to define and package Web services when using WLS. If you are not familiar with these procedures, see the WLS documentation.

.NET Deployment Units

The Windows Installer (`.msi`) for the Web service implementation is the only supported deployment unit for the Windows platform. It is beyond the scope of this documentation to explain how to define and package Web services when using .NET. If you are not familiar with these procedures, see the .NET documentation.

Broker Deployment Units

A brokered service configuration is captured in a Java ARchive (`.jar`) file. This deployment unit includes the service definition (WSDL), the management features for the service (configured policy handler pipeline), and the endpoints used to fulfill service requests. These assets defined in the jar file are proprietary in nature and work only with the WSM Broker.

A brokered service is a proxy to a service's endpoints. Therefore, the deploy service cannot be used to deploy Web services directly to a WS Container. A Web service to be managed must be deployed to a WS Container before a business service is updated with a new brokered service.

A deployment unit is automatically created when you define a brokered service using the Broker Configurator. The deployment unit is stored as a `.jar` in the <*install_dir*>`/conf/broker` directory. The deployment unit contains:

- `service.wsdl` – This file contains a service's definition without the SOAP address (endpoints) for a service.
- `service.xml` – This file contains a service's endpoints and also the management capabilities that will be interposed for the service.

Typically, a brokered service is created and configured in a development environment using a development instance of a WSM Broker. When a business service needs to be updated, the deployment feature is used to deploy the brokered service deployment unit to the production instance of a WSM Broker.

If the Web service's endpoints in the development environment are different than the endpoints in the production environment, you must change the endpoint values that are defined in the deployment unit's `service.xml` file.

Deploying a Deployment Unit

The BSE console is used to deploy a deployment unit. Deployment is performed either when adding a resource (Web/brokered service) to a business service or when editing an existing resource that is contained in a business service. In both cases, the deployment fields are the same.

The procedure below updates an existing resource in a business service with a Web/brokered service implementation. It is assumed that the resource is not currently bound to any underlying implementation.

Before completing the procedure, make sure you have created a deployment unit and know where it is located. In addition, the target WS container/intermediary must be started.

To deploy a deployment unit:

1 Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Services List screen, expand a business service to view its configurations.

3 Click the Web service configuration to which you want to deploy a deployment unit. The View Web Service Configuration screen displays.

4 From the Web Service Configuration View screen, click **Edit**. The Edit Web service screen displays.

5 Click the Deployment check box to enable the deployment feature and display the deployment fields. A check mark indicates that the feature is enabled.

6 From the Desired state options, select **Deployed**.

7 In the Upload a new deployment unit field, enter the location to a deployment unit, or click **Browse...** to locate and select a deployment unit. For example `c:\temp\Myapp.ear`.

A deployment unit that contains multiple Web services (e.g., .ear or .msi) can be configured for different Web services in the same business service.

8 In the resource discovery text box, enter the namespace and local name of the Web/brokered service in the form *{namespace}localname* (e.g., `{http://mycompany.com}MyService`). The values to use in the pattern can be obtained by inspecting a Web service's WSDL file. The *namespace* corresponds to the Web service's *targetNamespace*, and the *localname* refers to the service name.

9 Click **Save**. The View Web Service Configuration screen displays. It may take several minutes for the deployment to occur. The Deployment field indicates the status of the deployment. Refresh the screen periodically until the status is normal. This is indicated by a green check.

10 From the Deployment field, click **Status**. The Deployment Status screen displays and indicates the status and state of the deployment.

If the status does not change to indicate that deployment has finished, check that the correct discovery pattern is configured in the resource discovery text box in the Web service configuration. If the wrong discovery pattern is entered, deployment will not complete.

Detailed information about deployment status is also logged to the Network Services' log file.

Undeploying a Deployment Unit

The deployment feature allows you to undeploy a deployment unit that is contained in a managed WS container/intermediary. For managed WS containers, this feature removes the Web service from the WS container. For the WSM Broker, this feature removes the brokered service from the WSM Broker; however, the final endpoint is unaffected.

To undeploy a deployment unit:

1. Click the **Business Services** tab to view the Business Services List screen.
2. From the Business Services List screen, expand a business service to view its configurations.
3. Click the Web service configuration that contains the Web/brokered service that you want to undeploy. The View Web Service Configuration screen displays.
4. From the Web Service View screen, click **Edit**. The Edit Web service screen displays.
5. If the deployment feature is disabled, click the Deployment check box to enable the deployment feature and display the deployment fields. A check mark indicates that the feature is enabled.
6. From the Desired state options, select **Undeployed**.
7. Use the drop-down list to select the deployment unit that is to be undeployed.
8. Click **Save**. The View Web Service Configuration screen displays. It may take several minutes for the undeployment to occur. The Deployment field indicates the status of the undeployment. Refresh the screen periodically until the status is normal. This is indicated by a green check.
9. From the Deployment field, click **Status**. The Deployment Status screen displays and indicates the status and state of the undeployment.

Detailed information about undeployment status is logged to the Network Services' log file.

9

Using SSL for the Management Channel

This chapter describes how to secure the management channel and the management components that are used in the SOA Manager. Users should be familiar with general security principals and SSL security before completing the instructions in this chapter. In particular, users should be familiar with Key Stores and should have SSL certificates, including Certificate Authority (CA) root certificates, for the servers being used to implement the SOA Manager solution.

This chapter does not include instructions for securing the application channel. Application channel security for the WSM Broker is located in the *WSM Broker Administration Guide*.

In addition, this chapter does not include instructions for using Select Access for identity management. See the next chapter, “Integrating with Select Access” for instructions on using Select Access.

Overview

The SOA Manager management channel contains sensitive data about Web services that are being managed. The data include performance data, auditing data, and business content data. More importantly, the management channel exposes interfaces that are used to interact with a WS Container/Intermediary and its deployed services. The potential for security violations and malicious attacks does exist and should be considered when setting up the WSM solution.

The management channel is secured at the transport layer (HTTP) using SSL. SSL provides the means to implement authentication, confidentiality, and data integrity. SSL is used to secure the management communication between the Network Services, WSM Agents, and WSM Broker and is also used to secure communication to the BSE and Broker Configurator.

Architecture

The Network Services server communicates with the WSM Agents and the WSM Broker using a WS-based management channel. The channel utilizes a WS-based management protocol (SOAP over HTTP). Figure 9-1 below provides a view of the components in the management channel and the communication between those components.

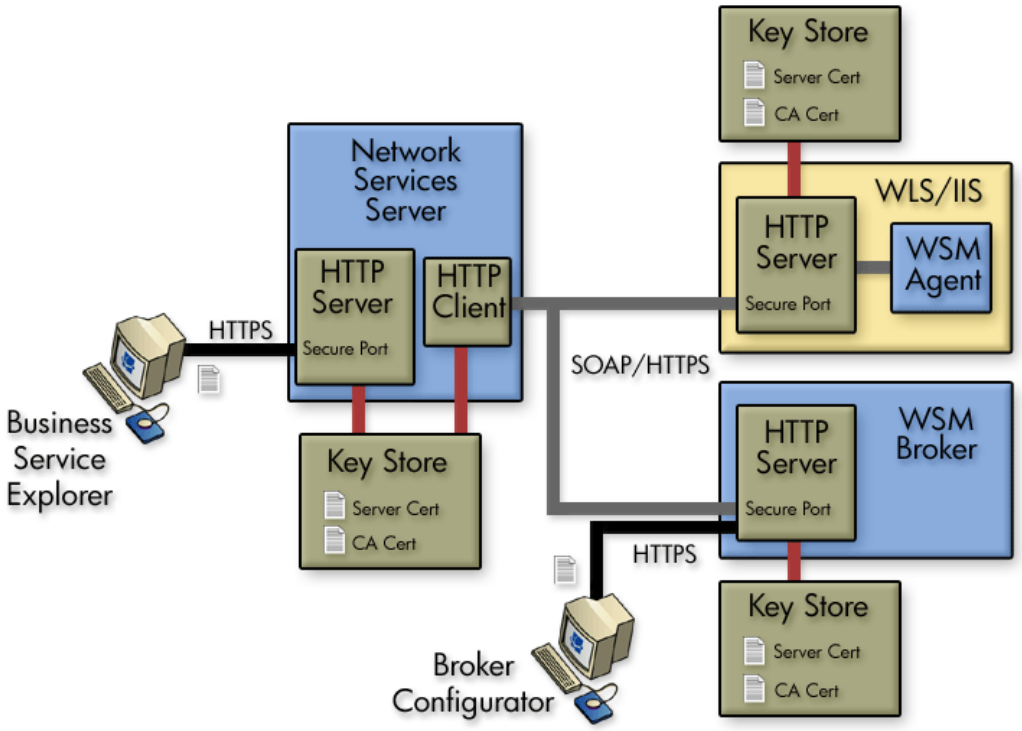


Figure 9-1: Management Channel Security

The Network Services contains both an HTTP Server and an HTTP Client. The Server and Client utilize the same SSL implementation and Key Store. Management data travels between the Network Services' HTTP Client and the HTTP Servers for the Broker and WSM Agents. The Broker contains its own HTTP Server, while the WSM Agents, which are integrated with their respective WS Container, leverage their container's HTTP Server and SSL implementation.

Figure 9-1 shows the Network Services server and the Broker on separate hosts. If the Network Services server and the WSM Broker are co-located on the same host, then they share the same SSL implementation and Key Store. This scenario may be applicable during testing.

The Key Stores for the Network Services Server and the Broker can be either a Java Key Store or a PKCS12 Key Store. Both IIS and WLS use their native Key Stores. The CA's root certificate for all servers in the management channel must be located in the Network Services' Key Store. The Network Services' JDK Trust Store can also be used to store CA root certificates.

Lastly, the BSE and the Broker Configurator Web applications can be configured to use a secure port. This is particularly important when accessing these applications from remote computers. In such scenarios, the CA's root certificate must be installed in each browser that accesses the applications.

Setting Up SSL

This section provides instructions that are used to implement SSL security between the management components of the WSM solution. Using SSL ensures that management data is secured and that the BSE and Broker Configurator are accessed in a secure manner.

Assign Key Stores and Trust Stores

The steps in this section detail how to assign Key Stores and Trust Stores for the various management servers used in the WSM solution. Before you complete the instructions in this section, make sure that each server participating in the WSM solution contains an SSL certificate which has been verified by a Certificate Authority (CA).

See Appendix A in the *WSM Broker Administrator Guide* for information on creating Java Key Stores and server certificates.

Network Services

The steps below detail how to assign a Key Store and Trust Store for use by the Network Services server. Because the Network Services server acts as an HTTP client, its Trust Store must contain the CA root certificate for each server participating in the WSM solution. If each server is verified by the same CA, then only a single CA root certificate is required.

To configure a Key Store and Trust Store for the Network Services server:

1. Stop the Network Services server if it is currently started.
2. Use a text editor to open <*install_dir*>`\conf\mipServer.xml`.
3. Use the following example and enter the properties for your Key Store and Trust Store. Each property is described following the example.

```
<entry name="com.hp.mip.security.server.keystore.type">
   jks</entry>
<entry name="com.hp.mip.security.server.keystore.location">
   C:\\temp\\MyKeystore.jks</entry>
<entry name="com.hp.mip.security.server.keystore.password">
   MyPassword</entry>
<entry name="com.hp.mip.security.server.privatekey.alias">
   MyAlias</entry>
<entry name="com.hp.mip.security.server.privatekey.password">
   MyPassword</entry>
<entry name="com.hp.mip.security.server.truststore.type">
   jks</entry>
<entry name="com.hp.mip.security.server.truststore.location">
   <jdk_install>/jre/lib/security/cacerts</entry>
<entry name="com.hp.mip.security.server.truststore.password">
   MyPassword</entry>
```

- **Keystore Type**: The entry can either be a Java Key Store (`jks`) or a PKCS12 Key Store (`pks`).
- **Keystore Location**: Enter the full path to the Key Store.
- **Keystore Password**: Enter the password for the Key Store.
- **Private Key Alias**: Enter the private key alias for the Key Store.
- **Private Key Password**: Enter the private key password for the Key Store.
- **Truststore Location**: Enter the full path to the Trust Store.
- **Truststore Password**: Enter the password for the Trust Store.
- **Truststore Type**: The entry can either be a Java Key Store (`jks`) or a PKCS12 Key Store (`pks`).

If your CA trusted roots certificates are stored together with the server certificate in the Key Store, enter the same Key Store values for the Trust Store. In such scenarios, the Key Store is considered the Trust Store.

4 Save and Close the file.

WSM Broker

The steps below detail how to assign a Key Store and Trust Store for use by the Broker. If the Broker is co-located with the Network Services server, they share the same Key Store and Trust Store. That is, assigning a Key Store and Trust Store for the Network Services also assigns the Key Store and Trust Store for the Broker.

To assign a Key Store and Trust Store the Broker:

1 Start the Broker Configurator.

2 From the Configurator's main tool bar, click **SSL Settings**. The SSL Settings screen displays.

3 Set the following properties:

- **Keystore Location**: Enter the full path to the Key Store (i.e., *C:\\temp\\MyKeystore.jks*).

- **Keystore Password**: Enter the password for the Key Store.
- **Keystore Type**: The entry can either be a Java Key Store (`jks`) or a PKCS12 Key Store (`pks`).
- **Private Key Alias**: Enter the private key alias for the Key Store.
- **Private Key Password**: Enter the private key password for the Key Store.
- **Truststore Location**: Enter the full path to the Trust Store (i.e., *<jdk_install>/jre/lib/security/cacerts*).
- **Truststore Password**: Enter the password for the Trust Store.
- **Truststore Type**: The entry can either be a Java Key Store (`jks`) or a PKCS12 Key Store (`pks`).

If your CA certificates are stored together with the server certificate in the Key Store, enter the same Key Store values for the Trust Store. In such scenarios, the Key Store is considered the Trust Store.

4 From the bottom of the screen, click **Save**.

WSM Agents

The WSM Agents are integrated with their respective WS Containers (IIS or WLS) and leverage their container's HTTP Server and SSL implementation. Please see the IIS or WLS SSL documentation for instructions on configuring a Key Store and Trust Store.

Configure SSL Settings

The steps in this section detail how to configure SSL on the management servers that are participating in the WSM solution. This typically includes enabling an SSL implementation and defining an HTTPS port.

Network Services

To configure SSL settings in the Network Services server:

1 Use a text editor to open *<install_dir>*`\conf\networkservices\mipServer.xml`.

2 Enter the following properties:

```
<entry name="com.hp.http.server.securePort">port_number</entry>
<entry name="com.hp.mip.security.server.webapps.secure">
   true</entry>
```

- **Secure Port**: The Network Services secure port that is used to accept HTTPS requests from the BSE. Any open port can be used.
- **Webapps Secure**: Enables SSL on the Network Services server. Valid entries are **true** and **false**.

3 Save and close the file.

4 Start the Network Services server.

WSM Broker Management Channel

To configure management channel SSL settings in the WSM Broker:

1. Stop the Broker if it is currently started.
2. Use a text editor to open <*install_dir*>\conf\broker\mipServer.xml.
3. Set the com.hp.mip.security.server.management.webapps.secure element to true.

```
<entry name="com.hp.mip.security.server.management.webapps.
   secure">true</entry>
```

4. Specify a port value for the com.hp.http.server.secureManagementPort element. Make sure the port is not being used by any other application on your system.

```
<entry name="com.hp.http.server.secureManagementPort">443</entry>
```

5. Save and close mipserver.xml.
6. Start the Broker server.

Broker Configurator

To configure the Broker Configurator to use SSL:

1. Stop the Broker if it is currently started.
2. Use a text editor to open <*install_dir*>\conf\broker\mipServer.xml.
3. Set the com.hp.mip.security.server.webapps.secure element to true.

```
<entry name="com.hp.mip.security.server.webapps.secure">
   true</entry>
```

4. Specify a port value for the com.hp.http.server.securePort element. Make sure the port is not being used by any other application on your system.

```
<entry name="com.hp.http.server.securePort">-1</entry>
```

5. Save and close mipserver.xml.
6. Start the Broker server.

WSM Agents

The WSM Agents are integrated with their respective WS Container (IIS or WLS) and leverage their container's HTTP Server and SSL implementation. Please see the IIS or WLS SSL documentation for instructions on enabling SSL and defining secure ports.

Registering a Secure Managed WS Container/Intermediary

Managed WS Containers/Intermediaries that run on a secure server are registered with the Network Services server using the BSE in the same manner as non-secure managed WS Containers/Intermediaries. However, because a managed WS Containers/Intermediaries runs on a secure server, the server's secure port must be used.

Because the Network Services server acts as an HTTP Client, its Trust Store must contain the CA root certificate for each managed WS Containers/Intermediaries server participating in the WSM solution. If each server is verified by the same CA, then only a single CA root certificate is required.

To register a secure managed WS container/intermediary:

1. Make sure the managed WS container/intermediary that you want to register is started.
2. From the BSE main tool bar, click the **IT Services** tab. The IT Service Summary screen displays.
3. Select the IT service you want to contain the WS container/intermediary. The IT Services View screen displays for the selected IT service
4. From the Contained Resources section, click the **Add** link. The Add WS Intermediary / Container screen displays.
5. From the **Type** drop-down box, select the type of resource you want to register.
6. Using the fields provided, enter the host and secure port where the managed WS container/intermediary is installed.
7. Click to select the **SSL** check box.
8. Click **Add**. The Add WS Intermediary / Container screen redisplays and lists the Web services that were discovered in the managed WS container/WS intermediary.
9. Click **Add**. The WS Intermediary / Container View screen displays and lists the resources that are now registered in the Network Services. The Management Interface (WSDL) field indicates an HTTPS URL.
10. Repeat this procedure to register additional secured managed WS containers/intermediaries.

Accessing the BSE

When using SSL, the BSE is accessed through the Network Services server's secure port (see "Configuring SSL Settings" above). Any browser used to access the BSE must contain a CA root certificate from the CA that was used to verify the Network Services server's SSL certificate. See your browser's documentation for information on installing a CA's trusted root certificate.

To access the BSE:

1. Open a Browser.
2. Enter the following URL and substitute <*host*> with the DNS host name where the Network Services server is running and <*secure_port*> with the server's secure port:

   `https://<host>:<secure_port>/bse`

Accessing the Broker Configurator

When using SSL, the Broker Configurator is accessed through the Broker's secure port (see "Configuring SSL Settings" above). Any browser used to access the Broker Configurator must contain a CA root certificate from the CA that was used to verify the Broker's SSL certificate. See your browser's documentation for information on installing a CA's trusted root certificate.

To access the Broker Configurator:

1. Open a Browser.
2. Enter the following URL and substitute <*host*> with the DNS host name where the Network Services server is running and <*secure_port*> with the server's secure port:

   `https://<host>:<secure_port>/console`

10

Integrating with Select Access

This chapter describes how to set up and configure the Select Access integration for the Network Services and WSM Broker. To complete the instructions in this chapter you need:

- A general understanding of the Select Access Policy Builder
- Access (local or remote) to a Select Access Server Version 6.1
- A Select Access Installation CD Version 6.1
- General Understanding of the SOA Manager

Overview

Select Access provides an identity management solution for securing access to IT services and resources. Select Access is used for securing access on both the application channel and the management channel.

For the management channel, Select Access can be used to replace the default security provider that controls access to the BSE and the Broker Configurator Web applications. This allows for single sign-on scenarios where policies for user authentication are pre-established in the enterprise. See the "Authenticating BSE and Broker Configurator Login" section below after completing the instructions for setting up the Select Access integration.

For the application channel, Select Access is used to provide authentication and authorization for consumers of Web services. Select Access integration for the application channel requires the Broker to mediate Web service communication. See the "Using the Broker's Security Features" chapter in the *WSM Broker Administrator Guide* for detailed instructions on setting up application channel security when using the Broker.

Architecture

The Select Access integration is the same for both the Network Services and the WSM Broker. As part of the integration, a Select Access Enforcer plug-in is used to mediate between the SOA Manager Security API and the Select Access Validator. Figure 10-1 shows the different aspects of the integration.

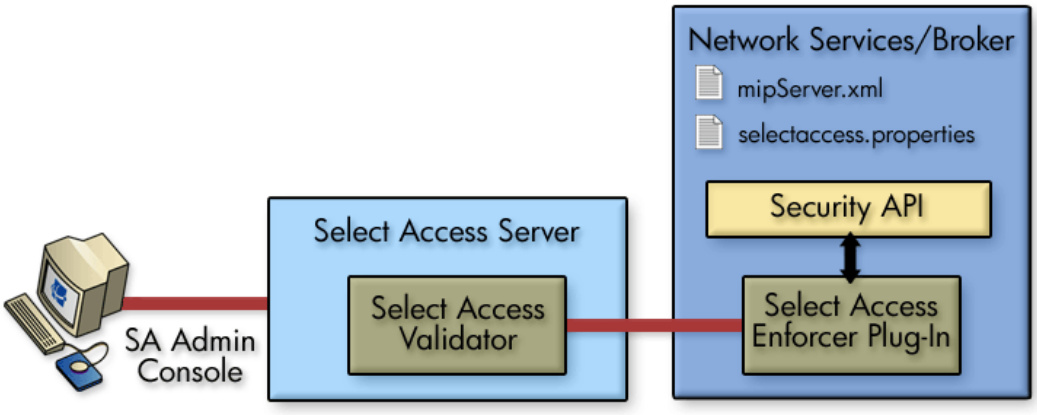


Figure 10-1: Select Access Integration

There are two configuration files that are used in the integration: `mipServer.xml` and `selectaccess.properties`. The Network Services and the Broker each contain their own version of these files. The files are located in <*install_dir*>`/conf/networkservices/` and <*install_dir*>`/conf/broker/` respectively. The `mipServer.xml` file provides entries that define Select Access as the default security provider, while `selectaccess.properties` defines properties that are used by the Select Access Enforcer. Both of these files are discussed in this chapter.

The Select Access Administration console is used to define resources that are to be secured as well as create polices and permissions for those resources. If you are not familiar with Select Access, you may need to consult the Select Access documentation while completing some of the instructions in this section.

Setting Up the Select Access Integration

The Select Access integration must be set up and configured before using Select Access with SOA Manager. This entails tasks that are performed on the Network Services and WSM Broker servers, as well as tasks that are performed on the Select Access Administration Server using the Select Access Administration console.

Install the Select Access Servlet Enforcer

The Select Access Servlet Enforcer must be installed on the same machine as the Network Services server as well as any computers that are hosting the WSM Broker. If the Network Server and the Broker are co-located on the same computer, The Enforcer only has to be installed once. This may be typical during testing scenarios.

To install the Select Access Servlet Enforcer:

1 Place the Select Access 6.1 installation CD in the CD ROM drive and close the tray. The installation's start screen displays.

2 If this is the first time a Select Access component is being installed on this system:

- Click **Next**.
- Read and agree to the License Agreement.
- Select the location where you would like to install Select Access Components. (i.e., `C:\Select Access`).
- Click **Next**.

Or,

If you have previously installed Select Access components on this system:

- Click **Modify – Install new components on this host**.
- Click **Next**.
- Read and agree to the License Agreement .
- Click **Next**.

3 From the Choose HP OpenView Select Access Components screen, select the **Servlet Enforcer Plugin**. Click **Next**.

4 Click **Install**.

5 When asked if you would like to configure the components now, select **YES** and click **Next**. This will launch the Select Access Setup Tool.

6 From the welcome screen, click **Next**. Keep clicking **Next** until you are asked to configure the Generic Enforcer Plugin. Follow the instruction and choose the location of the enforcer file, and click **Configure**.

Generic Enforcer Plugin is the same as Servlet Enforcer Plugin.

7 Provide the requested information to contact the Select Access Administration Server and click **Next**. Make sure to use an IP address.

8 In the Setup Options section, select **Typical** and click **Next**.

9 Click **Finish**.

10 Click **Next** on all the remaining prompts and close the wizards.

Copy the Required Jars

Once the Select Access Generic Enforcer is installed, move the required Enforcer's JAR files into the SOA Manager `/lib` directory. This procedure must be completed on every system where the Select Access Enforcer was installed.

To copy the required jars:

1. Stop the Network Service and/or Broker if they are currently started.
2. From the SOA Manager CD, copy `/Addons/mip-addons.jar` to <*install_dir*>`/lib/addons`.
3. Change directories to the directory where the Enforcer was installed, and copy the following JAR files to <*install_dir*>`/lib/addons`.
   - activation.jar
   - castor-0.9.3.19.jar
   - EnforcerAPI.jar
   - jakarta-oro-2_0.jar
   - jdom.jar
   - ldapjdk.jar
   - msgsresources.jar
   - protomatter.jar
   - shared.jar
   - xercesImpl.jar
   - xml.jar
   - xml-apis.jar
4. From <*install_dir*>`/lib/addons` directory, rename `xml.jar` to `AAA_sa_xml.jar`.
5. Move `AAA_sa_xml.jar` to `<install_dir>/lib`.

Configure the Network Services to Use Select Access

Two procedures are used to configure the Network Services to use Select Access:

- Modify Security Provider Settings for Select Access
- Modify the Select Access Enforcer Properties File

Modify Security Provider Settings for Select Access

The Select Access security provider replaces the default Network Services' security provider to provide security functions for BSE authentication.

To modify the security provider settings:

1. Stop the Network Services server if it is currently started.
2. Use a text editor to open <*install_dir*>`/conf/networkservices/mipServer.xml`.

3 Add security provider names to the `com.hp.mip.security.providers` entry, separated by a semicolon. For example, to add the Select Access security provider to the provider list, use the following entry:

```
<entry name="com.hp.mip.security.providers">default; SelectAccess
</entry>
```

4 Change the name of the console's security provider:

```
<entry name="com.hp.mip.security.provider.console">default</entry>
```

The above setting configures Select Access as the security provider for authentication when accessing the BSE.

5 Add the security provider configuration file path entry. For example, when using the Select Access security provider:

```
<entry name="com.hp.mip.security.provider.SelectAccess">
   C:\\<install_dir>\\conf\\networkservices\\selectaccess.properties
</entry>
```

It is recommended that the full path to the Select Access properties file be used.

6 Save and close `mipServer.xml`.

Modify the Select Access Enforcer Properties File

The Network Services must be configured to use the Select Access Enforcer at runtime.

To modify the Select Access Enforcer properties file:

1 Use a text editor to open *<install_dir>*`/conf/networkservices/selectaccess.properties` and configure the following settings:

```
Select AccessLoggingName = AxisEnforcer
EnforcerDebugLevel = 9
```

```
#SelectAccess service for basic authentication
```

```
HttpServiceProtocol = HTTP
```

`HttpServiceHost =` *<network_services_host_name>*

`HttpServicePort =` Port where the Network Services server is servicing requests. Default is 5002.

```
#SelectAccess service for certificate-based authentication
```

```
HttpsServiceProtocol = HTTPS
```

`HttpsServiceHost =` *<network_services_host_name>*

`HttpsServicePort =` Port where Network Services server is servicing SSL requests. Default is 8443

```
#SelectAccess service authentication resource path
```

```
AuthenticationResource = /authentication
```

`EnforcerConfigFile =` Specify the full path to the enforcer.xml file (i.e., `C:\\Program Files\\HP OpenView\\Select Access\\bin\\enforcer.xml`).

The above settings will be needed when defining a Select Access service.

2 Save and close `selectaccess.properties`.

3 Restart the Network Services server and ensure there are no errors when starting.

Configure the Broker to Use Select Access

Two procedures are used to configure the Broker to use Select Access:

- Modify Security Provider Settings for Select Access
- Modify the Select Access Enforcer Properties File

Modify Security Provider Settings for Select Access

The Select Access security provider replaces the default Broker security provider to provide security functions for Broker console authentication, web service request authentication and authorization, and security auditing.

To modify the security provider settings:

1 Stop the Broker if it is currently started.

2 Use a text editor to open <*install_dir*>`/conf/broker/mipServer.xml`.

3 Add security provider names to the `com.hp.mip.security.providers` entry, separated by a semicolon. For example, to add the Select Access security provider to the provider list, add the following entry:

```
<entry name="com.hp.mip.security.providers">default; SelectAccess
</entry>
```

4 Change the name of the security provider in the security service entries, for example:

```
<entry name="com.hp.mip.security.provider.console">default</entry>

<entry name="com.hp.mip.security.provider.authorization">
SelectAccess
</entry>

<entry name="com.hp.mip.security.provider.authentication">
SelectAccess
</entry>

<entry name="com.hp.mip.security.provider.auditing">
default
</entry>
```

The above settings configure Select Access as the security provider for authorization and authentication. The default security provider is used for the Broker Configurator and security auditing.

5 Add the security provider configuration file path entry. For example, when using the Select Access security provider:

```
<entry name="com.hp.mip.security.provider.SelectAccess">
   C:\\<install_dir>\\conf\\broker\\selectaccess.properties
</entry>
```

It is recommended that the full path to the Select Access properties file be used.

6 Save and close `mipServer.xml`.

Modify the Select Access Enforcer Properties File

The Broker must be configured to use the Select Access Enforcer at runtime.

To modify the Select Access Enforcer properties file:

1 Use a text editor to open <*install_dir*>`/conf/broker/selectaccess.properties` and configure the following settings:

```
Select AccessLoggingName = AxisEnforcer
EnforcerDebugLevel = 9

#SelectAccess service for basic authentication

HttpServiceProtocol = HTTP
HttpServiceHost = <broker_host_name>
HttpServicePort = Port Broker is servicing requests on.  Default is 9032.

#SelectAccess service for certificate-based authentication

HttpsServiceProtocol = HTTPS
HttpsServiceHost = <broker_host_name>
HttpsServicePort = Port Broker is servicing SSL requests on. Default is 8443

#SelectAccess service authentication resource path

AuthenticationResource = /authentication

EnforcerConfigFile = Specify the full path to the enforcer.xml file (i.e.,
C:\\Program Files\\HP OpenView\\Select Access\\bin\\enforcer.xml).
```

The above settings will be needed when defining a Select Access service.

2 Save and close `selectaccess.properties`.

3 Restart the Broker and ensure there are no errors when starting.

Authenticating BSE and Broker Configurator Login

The following instructions demonstrate how to use Select Access to authenticate users that log in to the BSE and the Broker Configurator. Before you complete this section, you must complete the “Setting Up the Select Access Integration” section above.

Define a Select Access Resource Server for the BSE

When the Select Access security provider is specified in the Network Service properties file, <*install_dir*>/conf/networkservices/mipServer.xml, the BSE automatically uses that security provider to authenticate a login. However, you must create a Select Access resource for the BSE using the HP OpenView Select Access Policy Builder.

To define a Select Access Service for the BSE:

1 From the Select Access Policy Builder Resources Tree, right-click Resource Access and select **New** | **Folder**. The New Folder dialog box displays.

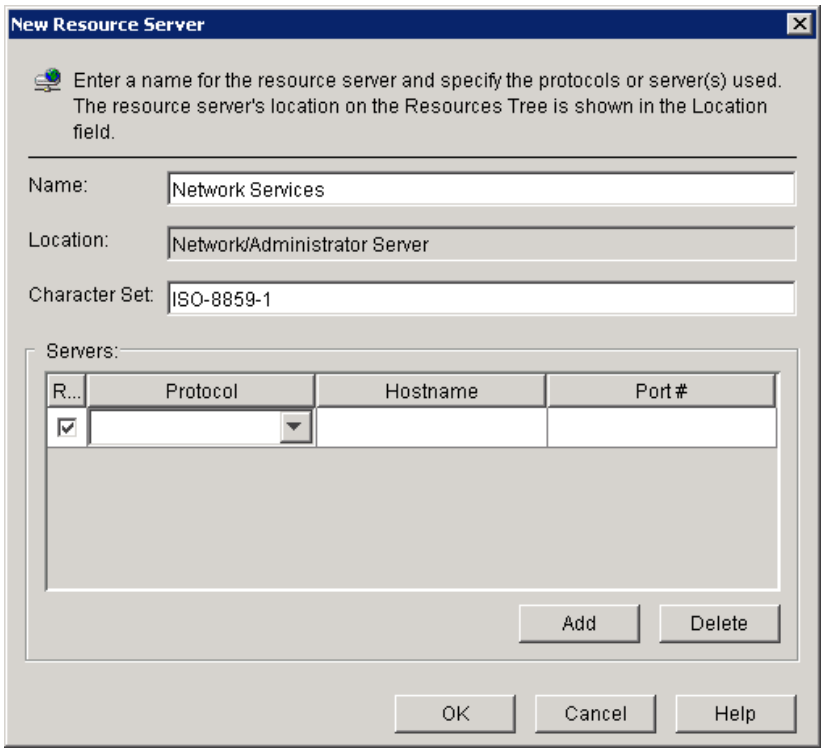
2 In the Name field, enter a name for the folder.

3 Click **OK**. When asked to clear the Policy Validator cache, select **OK**. The folder is created and is added to the Policy Builder Resources Tree under Resource Access.

4 Right-click the newly created folder and select **New** | **Resource Server**. The New Resource Server dialog box displays.

5 In the Name box, enter a name for this new resource server (i.e., Network Services). Any name that clearly identifies the server can be used.

6 On the bottom of the window click **Add**. A new entry displays under the Servers section.



7 Enter the following information for the server where the BSE is located:

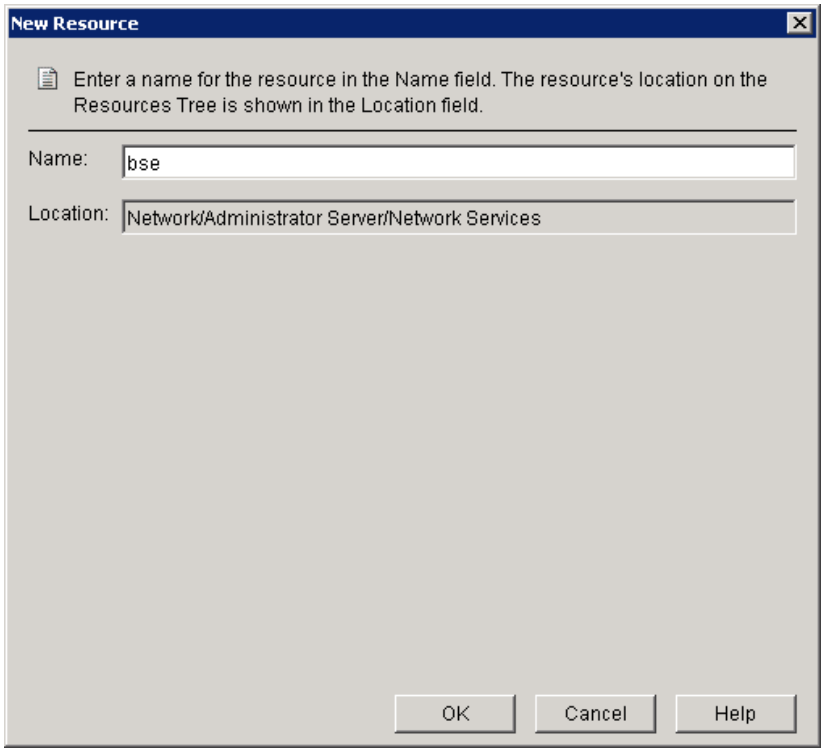
- **Protocol**: The protocol used to access the BSE (`HTTP` or `HTTPS`).
- **Hostname**: <*network_services_host_name*>
- **Port #**: The BSE's port number (`5002`).

8 Click **OK** to close this dialog box. When asked to clear the validators cache, select **OK**. The resource server is listed in the Policy Builder Resources Tree.

9 From the Policy Builder Resources Tree, right-click on the newly created resource server and select **New | Resource** from the menu. The New Resource dialog box displays.

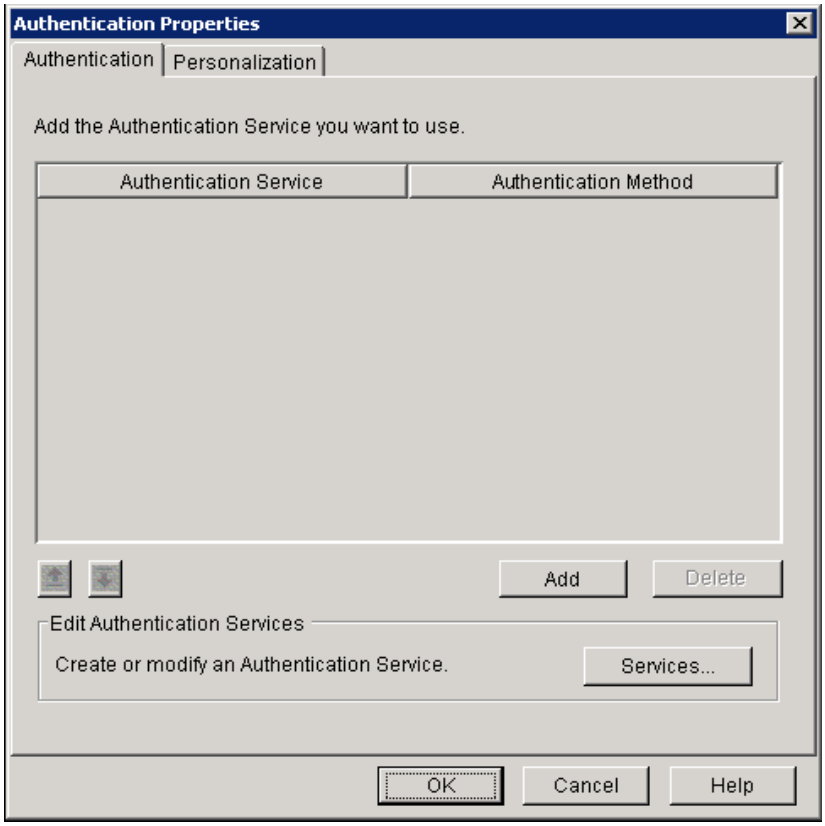
10 In the Name field, enter the resource name `bse` as shown below. This name corresponds to the resource as it appears in the URL to access the BSE. For example:

`http://`*<network_services_host_name>*`:5002/`**bse**).



11 Click **OK** to save this new Select Access resource. When asked to clear the validators cache, select **OK**. The resource is listed under the service in the Policy Builder Resources Tree. You now have a new resource defined which is used to authenticate BSE users.

12 From the Policy Builder Identities Tree, right-click the first column on the same row as the resource server for the Network Services, select **Enable Select Auth** from the pop-up menu. The Authentication Properties dialog box displays.



13 Click **Add**. The Available Authentication Services dialog box displays.

14 Select the password authentication service and click **Add**. The service is listed in the Selected Services column.

15 Click **OK**. The Authentication service is added to the list of authentication services in the Authentication Properties dialog box.

16 Click **OK**. When asked to clear the Policy Validator cache, select **OK**. The Select Auth icon shows that Select Auth for the selected resource server is enabled.

17 Use the Identities Tree to assign users of the BSE resource.

Define a Select Access Service for the Broker Configurator

When the Select Access security provider is specified in the Broker's properties file, <*install_dir*>`/conf/broker/mipServer.xml`, the Broker Configurator automatically uses that security provider to authenticate a login. However, you must create a Select Access resource for the Broker Configurator using the Select Access Policy Builder.

To define a Select Access Service for the Broker:

1 From the Select Access Policy Builder Resources Tree, right-click Resource Access and select **New | Folder**. The New Folder dialog box displays.

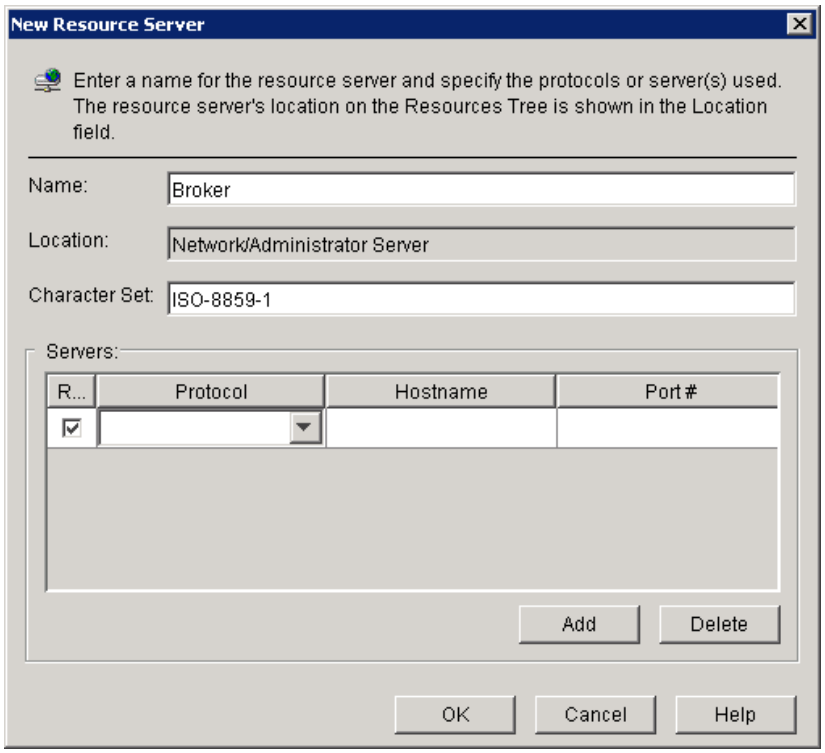
2 In the Name field, enter a name for the folder.

3 Click **OK**. When asked to clear the Policy Validator cache, select **OK**. The folder is created and is added to the Policy Builder Resources Tree under Resource Access.

4 Right-click the newly created folder and select **New | Resource Server**. The New Resource Server dialog box displays.

5 In the Name box, enter a name for this new resource server (i.e., Broker). Any name that clearly identifies the server can be used.

6 On the bottom of the window click **Add**. A new entry displays under the Servers section.



7 Enter the following server information for the server where the Broker is located:

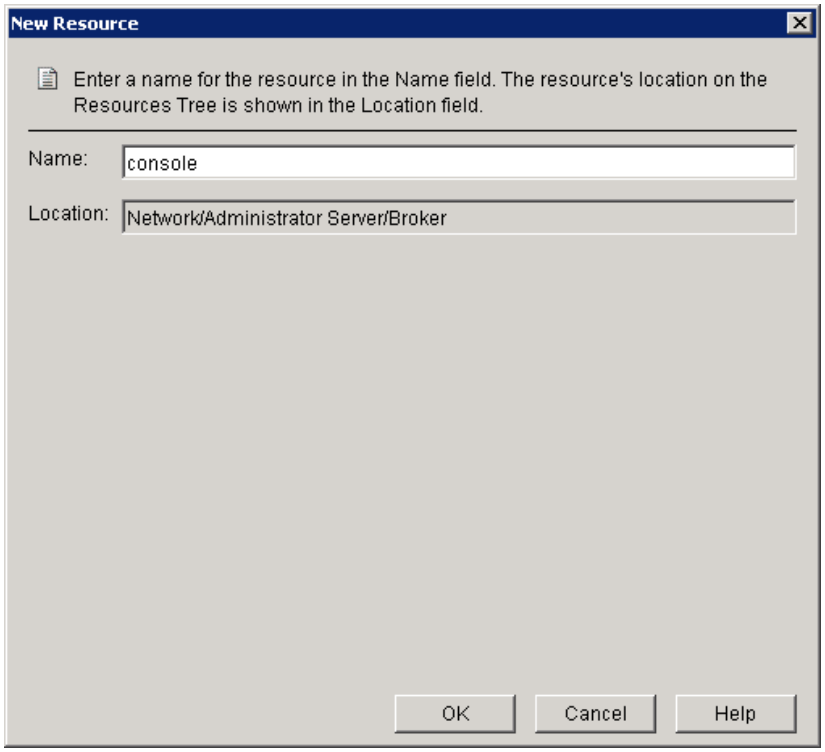
- **Protocol**: The protocol used to access the Broker Configurator (`HTTP` or `HTTPS`).
- **Hostname**: <*broker_host_name*>.
- **Port #**: The Broker Configurator's port number (`9032`).

8 Click **OK** to close this dialog box. When asked to clear the validator's cache, select **OK**. The resource server is listed in the Policy Builder Resources Tree.

9 From the Policy Builder Resources Tree, right-click on the newly created resource server and select **New | Resource** from the menu. The New Resource dialog box displays.

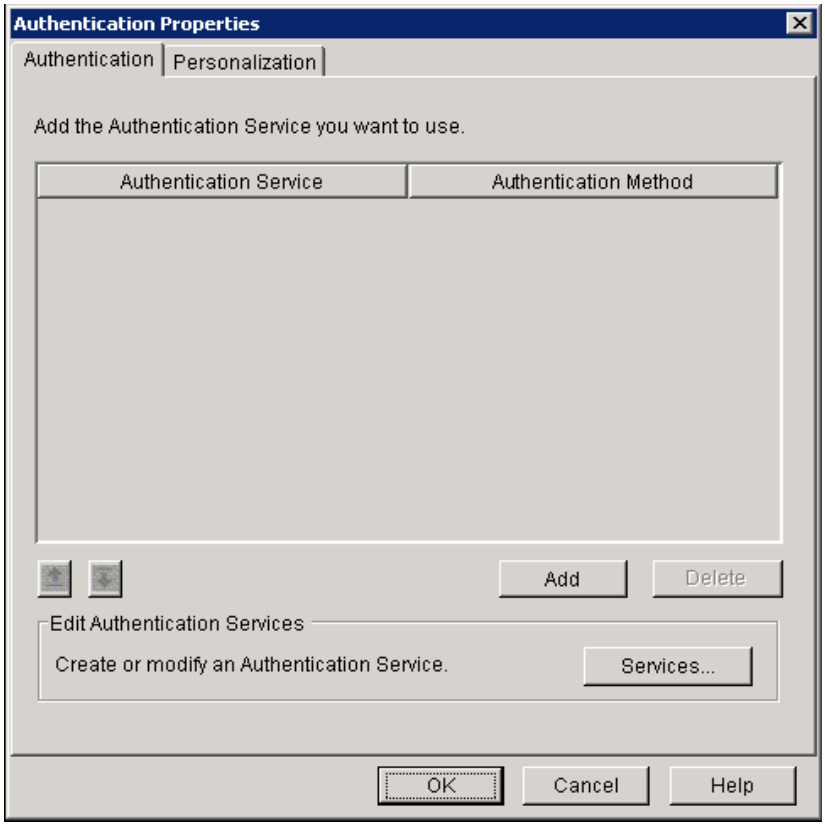
10 In the Name field, enter the resource name `console` as shown below. This name corresponds to the resource as it appears in the URL to access the Broker Configurator. For example:

`http://`<*broker_host_name*>`:9032/`**console**).



11 Click **OK** to save this new Select Access resource. When asked to clear the validator's cache, select **OK**. This resource is now listed under the service in the Policy Builder Resources Tree. You now have a new resource defined which is used to authenticate Broker Configurator users.

12 From the Policy Builder Identities Tree, right-click the first column on the same row as the resource server for the Broker, select **Enable Select Auth** from the pop-up menu. The Authentication Properties dialog box displays.



13 Click **Add**. The Available Authentication Services dialog box displays.

14 Select the password authentication service and click **Add**. The service is listed in the Selected Services column.

15 Click **OK**. The Authentication service is added to the list of authentication services in the Authentication Properties dialog box.

16 Click **OK**. When asked to clear the Policy Validator cache, select **OK**. The Select Auth icon shows that Select Auth for the selected resource server is enabled.

17 Use the Identities Tree to assign users of the BSE resource.

11

Troubleshooting

This chapter provides common troubleshooting tasks when using the Network Services.

Installation and Configuration Problems

Errors occurred during installation

Receive an error message at the end of the installation:

```
The installation of HP OpenView SOA Manager is finished, but some
errors occurred during the install. Please see the installation log
for details.
```

Solution:

1. Check the `<SOAM dir>/HP_OpenView_SOA_Manager_InstallLog.xml` log file for errors.
2. If you see install file errors, `<action name="Install File" status="error" />`, it means you only copied the `HPSOAManagerInstaller.bin` file from the SOA Manager installation CD to the system. You need to copy all of the files that are on the CD in the `../Installation` directory to the system where you're trying to install network services.

AutoPass fails to install

Receive an error dialog during installation:

```
AutoPass, the OpenView licensing tool, failed to install properly.
This installation will abort.  Please refer to the <temp
dir>\AutoPass_install.log log file for more details.
```

Solution:

1. Check to see if the `<temp dir>\AutoPass_install.log` log file exists.
2. If the log file exists, check for errors.

3 If the log file doesn't exist, check to see if there are non-English characters in the `<temp dir>` name. AutoPass has a bug where it doesn't allow non-English characters in path names. If there are non-English characters in the `<temp dir>` name:

   a Uninstall the Network Services.

   b Save the value of the `TMP` environment variable.

   c Change the `TMP` environment variable to a directory with all English characters.

   d Install the Network Services.

   e Change the value of the `TMP` environment variable back to its original value.

Unable to add Broker to WS Intermediary Service

Receive the message:

`http://<broker system>:<broker port>/wsmf/services/Runtime$service=Wsee?wsdl does not seem to be a valid WSEE or is offline.`

Solution:

1 Check to see if the WSM Broker is available. Access the URL from a browser.

2 If the URL is accessible, make sure you can access each imported WSDL and schema. For example, the following is a portion of a WSDL displayed in the browser.

```
<wsdl:import location=
  "http://ovw017.cup.hp.com:9032/wsmf_generated/WS-Events.wsdl"
  namespace="http://schemas.hp.com/wsmf/2003/03/Events#" />
  ...
  <xsd:import namespace=
    "http://openview.hp.com/xmlns/mip/2005/03
      /mip-manageability.xsd"
    schemaLocation="http://ovw017.cup.hp.com:9032/wsmf_generated
      /mip-manageability.xsd" />
  ...
```

In the browser, access:

`http://<broker system>:<broker port>/wsmf_generated/WS-Events.wsdl`
`http://<broker system>:<broker port>/wsmf_generated/mip-manageability.xsd`.

3 If the URL is not accessible, make sure the Broker is running. If the broker is not running, start it up. If the broker is running, look in the log file to see if there are any errors.

Runtime Problems

Could not start monarch-sba

When trying to start network services, receive a message:

```
[WARN] unable to locate tools.jar, possible non-sun jvm?
```

and later

```
[SEVERE]; Could not start monarch-sba: java.lang.Exception: Monarch
did not initialize
```

Solution:

Verify that the environment variable `MIP_JAVA_HOME` is assigned to the Java 1.4 SDK and not the JRE.

When trying to start network services, receive a message:

```
[SEVERE]; Could not start monarch-sba: java.lang.Exception: Monarch
did not initialize.
```

Solution:

1. Turn on logging for the Smart Business Agent (SBA) to get more details about the problem.
   a. Change directories to `<install_dir>/conf/networkservices`.
   b. Edit the `logging.properties` file.
      – Change `log4j.category.com.hp.wsm.impact=OFF` to `log4j.category.com.hp.wsm.impact=INFO, ROLL_FILE`
      – Add the following to the end of the file

```
# ROLL_FILE - rolling file appender that writes the logs to
the file system
#
log4j.appender.ROLL_FILE=org.apache.log4j.
   RollingFileAppender
log4j.appender.ROLL_FILE.File=C:\\temp\\soam-ns-sba.log
log4j.appender.ROLL_FILE.MaxFileSize=512KB
log4j.appender.ROLL_FILE.MaxBackupIndex=1
log4j.appender.ROLL_FILE.layout=org.apache.log4j.
   PatternLayout
log4j.appender.ROLL_FILE.layout.ConversionPattern=-->
   %d{yyyyMMdd|HH:mm:ss}|%p|%t|%c{5}|%m%n
```

2. Restart Network Services.
3. Look for errors in the `C:\temp\soam-ns-sba.log` file.

Failed to initialize listener

When trying to start network services, receive a message:

```
…;SEVERE;An error occurred while initializing the MIP Server: … :
failed to initialize listener
```

Solution:

1. Check to see if the Network Services is already running. If you are running on Windows and selected to install network services as a service during the installation process, network services is automatically started when you reboot the system.
2. If Network Services is not running, then another application must be using the port. By default, the Network Services uses port 5002. Change the Network Services to use a different port.
   a. Change directories to `<soam_home>/conf/networkservices`.
   b. Edit the `mipServer.xml` file. Change the `<entry name="com.hp.http.server.port">5002</entry>` property.
   c. Start the Network Services.

Timezone error when using Oracle 9i

Receive the message when starting the Network Services:

```
java.sql.SQLException: ORA-01882: timezone region not found
```

Solution:

1. Verify that the Oracle JDBC driver version is 9.2.0.5.0. The Network Services prints out the JDBC driver information at startup to `stdout`.
2. Make sure your timezone is in the timezone file Oracle is using. The following is from Chapter 2 "Creating an Oracle Database" in the *Oracle 9i Database Administrator's Guide Release 2 (9.2)*:

   "Oracle uses a time zone file, located in the Oracle home directory, as the source of valid time zones. If you determine that you need to use a time zone that is not in the default time zone file (`timezone.dat`), but that is present in the larger time zone file (`timezlrg.dat`), then you must set the `ORA_TZFILE` environment variable to point to the larger file."

Performance data not showing up in Business Service

Requests are sent to the service but the performance data is not updated in the Business Service.

Solution:

Verify service is a resource in the Business Service:

1. Click the **Business Services** tab to view the Business Services List screen.

2 From the Business Services List screen, expand a business service to view its contained configurations.

3 Click the resource configuration you want to view. The appropriate view screen displays. The service should be listed in Discovered Resources at the bottom of the window. If the service is not listed, verify that the configuration is bound to the IT Service that contains the container/intermediary the service is in. The **Bind to IT Service** field should contain a value.

4 If there is no value for the **Bind to IT Service** field, click on the **Edit** link next to Configuration: <*container name*>. Select the correct IT Service for the **Bind to IT Service** field in the configuration details window.

5 If there is a value for the Bind to IT Service field:

a Click on the value to get the IT Service View screen. Scroll down to the bottom of the window and verify that the service's container/intermediary is in the Contained Resources section. If the service's container/intermediary is not in the Container Resources section, click on the **Add** link and add it.

b Check that the Resource Discovery value is correct. The format for the resource discovery is *{namespace}localname* where namespace is the service's target namespace and localname is the service's name. For example, if the service is the FinanceService with the following WSDL, the resource discovery is: `{http://wsm.hp.com/finance}FinanceServce`.

```
<definitions targetNamespace="http://wsm.hp.com/finance">
  <types>
  ...
  </types>
  <message name="getQuote">
    <part name="parameters" element="partns:QuoteRequest">
    </part>
  </message>
  ...
  <portType name="FinanceServiceSoap">
    <operation name="getQuote">
      <input message="tns:getQuote">
      </input>
      <output message="tns:getQuoteResponse">
      </output>
    </operation>
  </portType>
  <binding type="tns:FinanceServiceSoap"
    name="FinanceServiceSoap">
    <soap:binding style="document"
      transport="http://schemas.xmlsoap.org/soap/http">
    </soap:binding>
    <operation name="getQuote">
      <soap:operation style="document" soapAction="">
      </soap:operation>
      <input>
        <soap:body namespace=http://wsm.hp.com/finance
          use="literal">
        </soap:body>
      </input>
      <output>
        <soap:body namespace=http://wsm.hp.com/finance
          use="literal">
        </soap:body>
```

```
        </output>
      </operation>
    </binding>
    <service name="FinanceService">
      <port name="FinanceServiceSoap"
        binding="tns:FinanceServiceSoap">
        <soap:address location=
           "http://ovw017.cup.hp.com:7001
            /FinanceService/FinanceService">
        </soap:address>
      </port>
    </service>
  </definitions>
```

Performance graph error on HP-UX and Linux

The performance graph located in the Performance section of a view screen does not display when the Network Services Server is installed on HP-UX or Linux.

The performance graph is implemented using Java Swing libraries. The libraries require that the server have an X server display defined. If the display is not defined, the performance graph fails.

To define an X server display:

1 On the Network Services server, create a `DISPLAY` environment variable that contains the X server's display name of the form *hostname:displaynumber.screennumber*. For example:

```
export DISPLAY=Myserver.com:0.0
```

This variable defines that the display is located on `Myserver.com` and that the default display and screen number will be used.

2 In addition to the `DISPLAY` variable, you must give clients the ability to access the X server's display. This can be done using X host. For example:

```
xhost +
```

3 Restart the Network Services Server process.

Broker audit traces not showing up in BSE

When querying for audit messages in the BSE, there are no audit messages returned in the query.

Solution:

Verify the clock synchronization. If the broker is running on a different system than the Network Services, verify that the clocks are synchronized.

Verify auditing is enabled for the brokered service:

1 In the Broker Configurator, click on the Brokered Service for which you are not seeing audit messages.

2 In the Features section on the Service Details page for the service, confirm that **Auditing** is checked. If this is not checked, then edit the Service settings and check the **Auditing** feature to enable auditing. Check to see if Audit messages are now displaying.

Verify the audit message is being received by the Network Services:

1 In the `<install_dir>\conf\networkservices\xpllogging.properties` file, set the logging level for Network Service to `fine`:

```
com.hp.ov.mip.level = FINE
```

2 Restart the Network Services.

3 Confirm that network services subscribes for audit messages. Look for the following message in the trace file:

```
Jul 5, 2005 9:56:35
AM;157;13;com.hp.wsm.sn.monitoring.collectionservice.CollectionSer
vice;wseeAdded;com.hp.ov.mip.Auditing;INFO;><Subscribing to wsee
http://<Service-Host>:9032/wsmf/services/Runtime$service=Wsee?wsdl
listening for audit events
```

4 Send a request to the service so an audit message is generated. Confirm that trace message is being received by network services. Look for the following message in the trace file:

```
Jul 5, 2005 9:58:04
AM;581;19;com.hp.wsm.sn.monitoring.collectionservice.CollectionSer
vice;handleNotify;com.hp.ov.mip.Auditing;FINE;>!<Received audit
messages

Source: http://<Service-
Host>:9032/wsmf/services/Runtime$service=Wsee?wsdl

Event:
http://schemas.hp.com/mip/2004/WsExecutionEnvironment/Event/Messag
eTraceNotificaTion
```

If the message is there, then you know the Network Services has received the audit message. Go through the rest of the trace messages to pinpoint the problem.

If the message is not there, then you know the Network Services has not received the audit message. Read the next section.

Verify audit message is being sent by the Broker:

1 In the `<install_dir>\conf\broker\xpllogging.properties`, set the logging level for the Broker to `FINE`:

```
com.hp.ov.mip.level = FINE
```

2 Delete the `9032MipNotificationManager.xml` file to clean up the subscriptions. On Windows, it's in the `\tmp` directory. On UNIX, it's in the `/var/tmp` directory.

3 Restart the Broker.

4 Restart the Network Services to make sure that the Network Services subscribes to the Broker. Wait until you see the following message in the Network Services log file:

```
Jul 5, 2005 9:56:35
AM;157;13;com.hp.wsm.sn.monitoring.collectionservice.CollectionSer
vice;wseeAdded;com.hp.ov.mip.Auditing;INFO;><Subscribing to wsee
http://<Service-Host>:9032/wsmf/services/Runtime$service=Wsee?wsdl
listening for audit events
```

5 Send a request to the service so that an audit message is generated.

6 Verify that the message was dispatched from the Broker. You should see the following log messages in the Broker's log file:

```
Jul 5, 2005 9:58:03
AM;269;16;com.hp.wsm.sn.router.server.audit.MessageTraceBuffer$Que
ueThread;run;com.hp.ov.mip.wsm.sn.router.server.audit.MessageTrace
Buffer;FINE;>!<Dispatched 1 traces.
```

7 Verify that the Network Services is subscribed for audit messages. Find the following message in the log file, which contains a list of the services subscribed for audit messages. Confirm that there is a `tuple` for the Network Services that is subscribed to the `http://schemas.hp.com/mip/2004/WsExecutionEnvironment/Event/MessageTraceNotification` event type.

```
Jul 5, 2005 9:58:03
AM;270;16;com.hp.wsm.sn.router.server.audit.WSMFPublisher;dispatch
;com.hp.ov.mip.wsm.sn.router.server.audit.WSMFPublisher;FINE;>!<Cu
rrent services subscribed for audit traces:

<SubscriptionTableList>
  <SubscriptionTable>
     <ManagedObject>Endpoint:id=e4f85099f4ab9246c0595be76856c2d3
     </ManagedObject>
     <SubscriptionList>
      <PushSubscriptions />
      <PullSubscriptions />
     </SubscriptionList>
  </SubscriptionTable>
<SubscriptionTable>

     <ManagedObject>SoapDispatcher:serviceId=financeServiceProxy
     </ManagedObject>
     <SubscriptionList>
       <PushSubscriptions />
       <PullSubscriptions />
     </SubscriptionList>
   </SubscriptionTable>
<SubscriptionTable>

     <ManagedObject>SmartBusinessAgent:service=WebServiceDirectory
     </ManagedObject>
     <SubscriptionList>
       <PushSubscriptions />
       <PullSubscriptions />
     </SubscriptionList>
   </SubscriptionTable>
<SubscriptionTable>
```

```
      <ManagedObject>Runtime:service=Service,id=financeServiceProxy
      </ManagedObject>
      <SubscriptionList>
        <PushSubscriptions />
        <PullSubscriptions />
      </SubscriptionList>
    </SubscriptionTable>
<SubscriptionTable>

      <ManagedObject>Runtime:service=Wsee</ManagedObject>
      <SubscriptionList>
       <PushSubscriptions>
         <EventType name="http://schemas.hp.com/mip/2004/
            WsExecutionEnvironment/Event/MessageTraceNotification">

           <Tuple>urn:subscription-push-2|Tue Jul 05 10:56:35 PDT
              2005|http://<NetworkServices_Host>:5002/
              _collectionServiceCallback
           </Tuple>
         </EventType>
       </PushSubscriptions>
       <PullSubscriptions />
     </SubscriptionList>
  </SubscriptionTable>
</SubscriptionTableList>
```

The date displayed in the `tuple` is the subscription expiration time. By default, the Network Services sets the expiration time to the current time + 1 hour. If there is not an entry for the Network Services and you are running the Network Services and the Broker on different systems, it could be that the times on the systems aren't synchronized. Either synchronize the clocks or increase the Network Services subscription expiration time in the `<install_dir>\conf\networkservices\mipServer.xml` file:

```
<entry name="com.hp.mip.event.subscriptionInterval">1440</entry>
```

8 Restart the Network Services.

Out of Memory

Receive an error that ran out of memory when running Network Services as a service.

Solution:

Increase the stack and heap sizes.

1 Modify the <*install_dir*>`\bin\win32\services\service-manager.bat` file. Add the stack and heap parameters to the system properties (`@set SYS_PROPS=`**`-Xms64m –Xmx256m`** `-Dcom.hp.mip.autopass.home...`).

2 Run the bat file to remove the Network Services service (`service-manager.bat -remove networkservices`).

3 Run the bat file again to add Network Services as a service with the new parameters (`service-manager.bat -install networkservices`).

4 Check that the new parameters are configured by looking in the registry under `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/networkservices<version num>`.

Receive an error that ran out of memory when running Network Services from the command line.

Solution:

Increase the stack and heap sizes.

1. Modify the <*install_dir*>\bin\<unix | win32>\mipserver[.bat] file. Increase the sizes for -Xms and -Xmx.
2. Restart Network Services.

Glossary

Application Channel

Application channel refers to the request/response communication between an application client, such as a browser, and an application component such as a Web service.

Auditing

Auditing is a management feature that captures trace information for all Web service requests and responses.

Availability Monitoring

Availability monitoring is a management feature that is used to monitor the availability of SOA resources such as Web services.

Broker Configurator

The Broker Configurator is the WSM Broker's administration console. It is used to create and configure brokered services as well as configure the Broker's server properties.

Brokered Services

A brokered service is a proxy to a final Web service endpoint and is used to enable the management of a Web service.

Business Services

A business service is the virtualization of some business application that is offered by a business manager to either internal or external customers.

Business Service Configuration

A business service configuration is a part of the service model that contains an IT service and provides varying levels of automation.

Business Service Explorer (BSE)

The BSE is the SOA Manager's management console. It is used to create service models and monitor SOA resources.

Content Monitoring

Content monitoring is a management feature that searches Web service request and/or response messages for specific content.

Distributed Management

Distributed management is an approach to managing resources that are deployed and distributed across an enterprise network environment.

Enterprise Management Integration

Enterprise management integration is the ability to leverage and/or customize the SOA Manger in order to create custom management solutions.

Grid

Grid computing began in high-performance technical computing as a way to share widespread computing resources. In enterprise IT environments, grid computing is now gaining adoption rapidly. In this documentation a grid is defined as the software environment for sharing loosely-coupled infrastructure and services. SOA Manager manages grid hosts that are constructed from the Globus Toolkit.

Impact Analysis

Impact analysis is the ability to discover how the performance of a service affects other related services.

Integration Points

Integration points provide the ability to either extract information from the SOA Manager or add additional management data to the SOA Manager.

Interposed Manageability

Interposed manageability means inserting management policies in the request/response path of Web services.

IT Service

An IT Service, as defined in the SOA Manager, represents the virtualization of management information or capabilities of a group of resources of a certain type that are associated with a set of stakeholders. An IT service can represent a single IT resource or can represent a collection of resources.

Logging

Logging in the SOA Manager captures the local standard output for Web service containers and Web service intermediaries so that the output can be analyzed from a remote central location.

Managed Object (MO)

An MO is a representation of a managed element such as a Web service. An MO can be related to either a logical or physical piece of the IT infrastructure. In the SOA Manager, MOs are exposed as Web services that provide attributes and operations that can be invoked.

Managed Service

A managed service is a Web service which is being managed by the SOA Manager.

Management Agents

Management agents are software components that get installed on a computer and are responsible for performing management tasks.

Management Channel

The Management channel refers to the communication between the Network Services server and one or more management agents. In the SOA manager, the management channel can be different than the application channel.

Management Information Model

The management information model is a set of Web services (based on various standards such as WSDL, WSDM, etc.) consumable on the wire, and discoverable through meta-data populated in a UDDI registry.

Management Policies

Management policies contain the management logic that is used to interpose visibility and controls on Web services. Management policies are implemented in WSM Agents or the WSM Broker.

Management Proxies

Management proxies are software components that get installed on a computer and are responsible for gathering management data for computers that do not have a native management agent available for them. The WSM Broker is an example of a management proxy.

Management Server

A Management server is a centralized software component that aggregates the data that is gathered by any number of management agents. The Network Services server is an example of a management server.

Management Web Service

A management Web service is a Web service that exposes management information using standard Web services management protocols. The WSM Agents and the WSM Broker expose their management information as management Web services.

Northbound Interfaces

Northbound interfaces are Web services-based integration interfaces that are used to extract the information contained in the SOA Manager's management model.

Performance Monitoring

Performance monitoring is a management feature that captures a set of real-time performance metrics that clearly indicate the health, availability, and performance of Web services.

Policy Handlers

Policy handlers are the actual implementation of the management policies in the WSM Agents and WSM Broker. Policy handlers are often referred to as simply handlers.

Public Key Infrastructure (PKI)

A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

Resource Management

Resource management is the act of managing the SOA resources that are being used by business applications.

Root Cause Analysis

Root cause analysis is the ability to discover which Web service is causing a group of related Web services to degrade.

Secure Sockets Layer (SSL)

SSL is a commonly-used protocol for managing the security of a message transmission over the Internet

Service

A service is a self contained collection of functionality that promotes a high degree of isolation from internal details while at the same time offering its functionality to other services.

Service Consumer

A service consumer is a participant in a service-based application that uses a service based on the functionality and value that the service provides.

Service Level Agreement (SLA)

An SLA is an agreement between a service consumer and a service provider about the expected level of availability and performance of a service.

Service Level Objective (SLO)

An SLO is a set of preferred operating limits for a Web service.

Service Oriented Architecture (SOA)

An SOA is a set of principles that define an architecture that is loosely coupled and comprised of service providers and service consumers that interact according to a negotiated contract or interface.

Service Model

A service model is the virtual representation of managed SOA resources.

Service Producer

A service producer is a participant in a service-based application that focuses on how the service provides functionality and value and which resources provide the service.

SLO Monitoring

SLO Monitoring is a management feature that evaluates a Web service's performance against an SLO to insure it is within acceptable operating limits.

Simple Object Access Protocol (SOAP)

SOAP is an XML-based protocol that is typically used over HTTP to send messages (commonly referred to as SOAP messages) between application clients and servers. SOAP is the standard for Web services messages and is one of the foundation standards of Web services.

Solution

A set of features and capabilities delivering business value to a customer through a combination of hardware, software, and services.

Southbound Interfaces

The Southbound interfaces are Web services-based integration interfaces that are used to interact with a managed WS Container/WSM Broker.

Trend Analysis

Trend analysis allows operators and administrators to analyze changes in Web service performance over time.

Universal Description, Discovery, and Integration (UDDI)

UDDI is a specification that defines a registry service for Web services that allows Web services to be discovered. UDDI is often referred to as a Yellow Pages of Web services.

Web Service

A Web service is a service that is built using the SOAP and WSDL standards.

Web Services (WS) Container

A WS container represents a SOAP container or environment that can host Web services. AXIS, IIS, and WebLogic Server are examples of WS containers.

Web Service Management (WSM)

WSM is the act of managing the Web services that are being used by business applications. WSM in the SOA Manager software goes beyond managing just Web services to include a range of SOA resources that are equally vital to the success of Web services.

Web Services Management (WSM) Agent

A WSM Agent is an enablement component that is installed in a WS Container in order to manage the Web services in the container as well as the container itself. There is a WSM Agent for both the Microsoft Internet Information Server (IIS) and for the BEA WebLogic Server (WLS).

Web Services Description Language (WSDL)

WSDL is an XML-based language that is used to describe a software component. A WSDL definition describes how to access a Web service and what operations it can perform.

Web Services Distributed Management (WSDM)

WSDM is an OASIS standard that has been formed to define web services management, including using web service architecture and technology to manage distributed resources.

Web Services Intermediary

A Web services intermediary represents a proxy to a WS Container. The WSM Broker is considered a Web service intermediary.

Web Services Management Framework (WSMF)

WSMF is a standard defined by HP and submitted to the OASIS WSDM TC. The standard defines fundamentals for the Management of Web Services (MOWS) and for Management Using Web Services (MUWS).

WSM Broker

The WSM Broker is a flexible, configurable, high performance Java-based Web services intermediary process. The WSM Broker is used to manage Web services that are hosted in containers that do not provide native management for Web services. The WSM Broker is an implementation of a Management Proxy and does not need to be co-located with the Web services being managed.

XML (Extensible Markup Language)

XML is a markup language used to describe data and does not include any presentation logic for the data.

Index

A

B

N

O

P

Q

R

S

T

U

V

W

X