



BEA AquaLogic® Service Bus

Operations Guide

Version 3.0
Revised: February 2008

Contents

Introduction

Roles in ALSB

Default Roles in ALSB	2-1
IntegrationAdmin	2-1
IntegrationDeployer	2-2
IntegrationMonitor	2-2
IntegrationOperator	2-3
Relation Between Roles in WLS and Roles in ALSB	2-4
How to Create Roles in ALSB	2-4

Monitoring ALSB at Run Time

What is Service Monitoring?	3-2
About the ALSB Monitoring Framework	3-2
Aggregation Intervals	3-4
The Refresh Rate of Monitoring Data	3-5
Sample Intervals Within Aggregation Intervals	3-5
How to Set the Aggregation Interval for Monitoring Data	3-6
What are the Consequences Of Changing Aggregation Interval Of A Service?	3-7
What are the Consequences Of Renaming Or Moving A Service?	3-7
What Statistics are Available for ALSB Services?	3-7
Accessing Statistical Information for Services	3-8
How to Access Service Statistics from the ALSB Console	3-8

How to Access Statistical Information Using the JMX Monitoring APIs	3-8
How to Access Statistics in a Cluster	3-8
How to Reset Statistics	3-9
What are the Consequences of Resetting the Statistics?	3-9
The Role of Alerts in Service Monitoring	3-10
Assigning Severity for Alerts	3-10
What are SLA Alerts?	3-11
A Sample Use Case for SLA Alerts	3-11
What are Pipeline Alerts?	3-11
A Sample Use Case for Pipeline Alerts	3-12
How to View or Delete SLA Alerts	3-12
How to View or Delete Pipeline Alerts	3-13
How to Filter a Search for Specific Alerts	3-13
How to Filter a Search for SLA Alerts	3-13
How to Filter a Search for Pipeline Alerts	3-14
What are Alert Destinations?	3-15
E-mail	3-15
SNMP Traps	3-16
Reporting	3-17
JMS	3-17
What are Operational Settings for a Service?	3-17
How to Configure the Operational Settings for a Service	3-19
How to Configure the Operational Settings at the Global Level	3-21
Updates to Operational Settings During Import of ALSB Configurations	3-23
Updates to Global Settings During the Import of ALSB Configurations	3-23
How to Preserve Operational Settings During the Import of ALSB Configuration Through APIs	3-23
SLA Alerting Functionality in ALSB	3-26

How to Configure SLA Alert rules	3-26
How to Lookup or Edit Existing Alert Rules	3-27
How to Rename Alert rules	3-27
What are the Consequences of Renaming an Alert Rule?	3-27
What Happens to Alert Rules When You Import ALSB Configurations?	3-28
The ALSB Dashboard	3-28
How to Access Service Statistics for the Current Aggregation Interval	3-29
How to Access Running Count Statistics for Services	3-32
Viewing SLA Alerts in the Dashboard	3-38
Viewing the Alert History for SLA Alerts	3-38
Viewing Pipeline Alerts in the Dashboard	3-38
Viewing the Alert History for Pipeline Alerts	3-40
Viewing Server Health in the Dashboard	3-40
Viewing Log Summary	3-40
Viewing Server Summary	3-43
Viewing Server Details	3-43

Managing Operational Settings Using Smart Search

Using Basic Search	4-2
Using Advanced Search	4-4
Finding Services Using Search Filters	4-4
Viewing and Editing Operational Settings	4-5
Managing Operational Settings for Proxy Services	4-7
Finding Proxy Services Using Search Filters	4-7
Viewing and Editing Operational Settings	4-9
Managing Operational Settings for Business Services	4-10
Finding Business Services Using Search Filters	4-10
Viewing and Editing Operational Settings	4-11

Managing Operational Settings for Alert Destinations	4-12
Finding Alert Destinations using Search Filters	4-12
Viewing and Deleting Alert Destinations	4-13
Managing Operational Settings for SLA Alert Rules	4-15
Finding SLA Alert Rules Using Search Filters	4-15
Viewing and Configuring SLA Alert Rules	4-17

Reporting

About the ALSB Reporting Framework	5-2
About the JMS Reporting Provider	5-3
How to Enable Message Reporting	5-4
How to Stop a Reporting Provider	5-6
How to Untarget a JMS Reporting Provider	5-7
How to Untarget the JMS Reporting Provider when the Server is Running	5-8
How to Untarget the JMS Reporting Provider When Server Not Running	5-9
Using the Reporting Module in the ALSB Console	5-10
Viewing the Summary of Message Reports	5-11
Viewing Message Details	5-13
How to Purge Messages from the Reporting Data Store	5-16
How to Configure a Database for the JMS Reporting Provider Store	5-17
How to Configure a Database in a Development Environment	5-17
How to Configure a Database for Production	5-18

Tracing

How to Enable or Disable Tracing	6-1
How to Access Tracing Information	6-2

Managing Endpoint URIs for Business Services

How to Configure a Business Service to Perform Retries	7-2
--	-----

How to Suppress Retries in Case of Application Errors	7-2
How to Mark a Non-Responsive URI Offline	7-3
How to Mark an Endpoint URI Offline Temporarily	7-3
How to Mark an Endpoint URI Offline Permanently	7-4
Metrics for Monitoring Endpoint URIs	7-4
Endpoint URI Status	7-5
Endpoint URI Performance Metrics	7-5
How to Mark an Offline URI as Online	7-6
How to Generate Alerts Based on Endpoint URI Status	7-7
How to Configure an Alert Rule Based on Endpoint URI Status	7-7

Throttling in ALSB

How to Enable Throttling	8-1
What are the Operational Settings for Throttling?	8-2
What Metrics are Available for Throttling ?	8-5
How to Access Throttling Metrics	8-5
How to use Throttling Metrics for Alerting	8-5
How to use Throttling for Business Services with Multiple Endpoint URIs	8-6
What Happens to Retrieved Messages During Throttling?	8-6

User Preferences

SNMP Components

Managed Resource	A-1
Management Information Base	A-1

Monitoring Statistics in ALSB

Auditing your ALSB System

Auditing the Configuration Changes	C-1
--	-----

Creating an Audit Trail for a Message Flow	C-1
Auditing Security Violations	C-1

Introduction

AquaLogic Service Bus (ALSB) is part of BEA's comprehensive business integration solutions and is part of the BEA AquaLogic family of service infrastructure products. ALSB manages the transformation and routing of messages in an enterprise system and includes administration and monitoring capabilities. ALSB is a unified product for deploying and implementing Service Oriented Architecture (SOA).

This guide describes the functional scope of the roles available in ALSB, monitoring services in ALSB, using smart search, reporting, and tracing.

This document is intended for the following audience:

- Operational Specialists: Responsible for monitoring services, servers and alerts in ALSB.
- Architects: Responsible for designing the security architecture of the enterprise system.

To best understand this guide you must be familiar with resources, proxy services, and business services in ALSB Console. For more information, see [AquaLogic Service Bus User Guide](#).

Introduction

Roles in ALSB

ALSB supports various roles. The role assigned to a user determines the tasks that a user can perform. You can assign roles to users to secure resources and services in the ALSB Console by restricting access.

This section provides information about:

- [Default Roles in ALSB](#)
- [Relation Between Roles in WLS and Roles in ALSB](#)
- [How to Create Roles in ALSB](#)

You can also restrict the user interfaces that should be made available to a given role depending on the privileges of the role.

Default Roles in ALSB

By default, `IntegrationAdmin`, `IntegrationDeployer`, `IntegrationMonitor`, `IntegrationOperator` are predefined roles in ALSB. The following section describes the various roles available in ALSB and their functionality.

IntegrationAdmin

The `IntegrationAdmin` role is an administrative security role. As an `IntegrationAdmin`, you can access ALSB Console. Users assigned to this role can access all resources and services in ALSB. This role is granted to users requiring administrator privileges in ALSB Console.

In ALSB, you can assign the `IntegrationAdmin` role by assigning the `IntegrationAdmins` parent group when you create or reconfigure a user. For more information about creating a user in ALSB, see [Adding a User](#) in Using the AquaLogic Service Bus Console.

Users who are assigned this role can perform the following tasks in ALSB Console.

- Create or commit session
- Create, edit, or delete resources and projects
- View the available users and groups in ALSB
- View and configure monitoring, reporting, and tracing for business and proxy services
- Import or export resources
- View and configure UDDI registries
- Publish and import resources from registries

IntegrationDeployer

The `IntegrationDeployer` role is assigned to users who deploy services. An `IntegrationDeployer` can access ALSB Console to create and deploy resources and services. Also in this role, you can access the existing resources and services in the ALSB.

When a user is created or reconfigured in ALSB, `IntegrationDeployer` role is granted by assigning the `IntegrationDeployers` parent group. For more information about how to create a user in the ALSB, see [Adding a User](#) in Using the AquaLogic Service Bus Console.

Users who are assigned this role can perform all tasks that can be performed by a user in the `IntegrationAdmin` role. For more information about tasks performed by an user in the `IntegrationAdmin` role, see [IntegrationAdmin](#).

IntegrationMonitor

The `IntegrationMonitor` role is granted to users who monitor resources and services in ALSB Console. Users assigned to this role can also monitor violations to Service Level Agreements (SLAs), and the alerts from the message flow pipeline.

When a user is created or reconfigured in ALSB Console, the `IntegrationMonitor` role is assigned to users by assigning the `IntegrationMonitors` parent group. For more information about how to create a user in ALSB Console, see [Adding a User](#) in Using the AquaLogic Service Bus Console.

Users who are assigned this role can perform the following tasks:

- View dashboard for SLA alerts and pipeline alerts
- Use SmartSearch to view business services, proxy services, alert destination and SLA alert rules
- View details of existing users and groups
- View details of resources

IntegrationOperator

The IntegrationOperator role is granted to users, who perform day-to-day operations in ALSB Console. IntegrationOperators can perform the day-to-day operations on the resources in ALSB Console. This role can also perform certain monitoring tasks and session management.

When a user is created or reconfigured in ALSB Console, the IntegrationOperator role is granted by assigning the IntegrationOperators parent group. For more information about how to create a user in ALSB Console, see [Adding a User](#) in Using the AquaLogic Service Bus Console.

Users who are assigned this role can perform the following tasks:

- View configuration details of all resources
- View and configure monitoring, tracing, logging, and reporting for business services and proxy services
- Edit and update dashboard settings
- Add, update, and delete alert rules
- Add, view, delete, and edit alert destinations
- View and purge SLA alerts for business services and proxy services
- View and purge pipeline alerts for proxy services
- Use SmartSearch to view and edit operational settings for business services, proxy services, alert destination, and SLA alert rules
- Use global settings to enable or disable monitoring, pipeline alerting, SLA alerting, reporting, and logging at a global level
- View the status of all the servers associated with the domain
- View and purge message reports

- View the UDDI registries that have been configured for the domain
- View, the auto-publish status and auto-import status of business services and proxy services
- View security configurations of users and groups

For more information about tasks you can perform in each of these roles, see [Role-Based Access: Configuring Administrative Security](#) in AquaLogic Service Bus Security Guide.

Relation Between Roles in WLS and Roles in ALSB

Roles in ALSB Console are related to corresponding roles in WebLogic Server Administration Console. [Table 2-1](#) gives different roles available in ALSB Console and the corresponding roles in WebLogic Server Administration Console.

Table 2-1 Relationship Between Roles in WLS and Roles in ALSB

Roles in ALSB	Roles in WLS
IntegrationAdmin	Administrator
IntegrationDeployer	Deployer
IntegrationMonitor	Monitor
IntegrationOperator	Operator

Users belonging to the Administrator role in WebLogic Server are automatically included in the IntegrationAdmin group in ALSB Console. The converse however, is not true.

Note: A user can also be associated with multiple roles. For example, a user can be associated with IntegrationAdmin role in ALSB Console must possess the Administrator role in ALSB to access the WebLogic Server Administration Console.

How to Create Roles in ALSB

You can create new roles in ALSB if you possess Administrator role in the WebLogic Server Administration Console. An administrator can create new roles from the Global Roles page and customize the role by editing the conditions for the new role in the Global Role Conditions page.

For more information about creating and customizing roles, see [Adding Roles](#) in Using the AquaLogic Service Bus Console.

Roles in ALSB

Monitoring ALSB at Run Time

ALSB enables you to monitor and collect run-time information required for system operations. ALSB aggregates run-time statistics, which you can view on the dashboard. The dashboard allows you to monitor the health of the system and notifies you when alerts are generated in your services. With this information, you can quickly and easily isolate and diagnose problems as they occur.

This section provides information on the following topics:

- [What is Service Monitoring?](#)
- [Aggregation Intervals](#)
- [What are the Consequences Of Renaming Or Moving A Service?](#)
- [What Statistics are Available for ALSB Services?](#)
- [Accessing Statistical Information for Services](#)
- [The Role of Alerts in Service Monitoring](#)
- [What are Operational Settings for a Service?](#)
- [SLA Alerting Functionality in ALSB](#)
- [The ALSB Dashboard](#)

What is Service Monitoring?

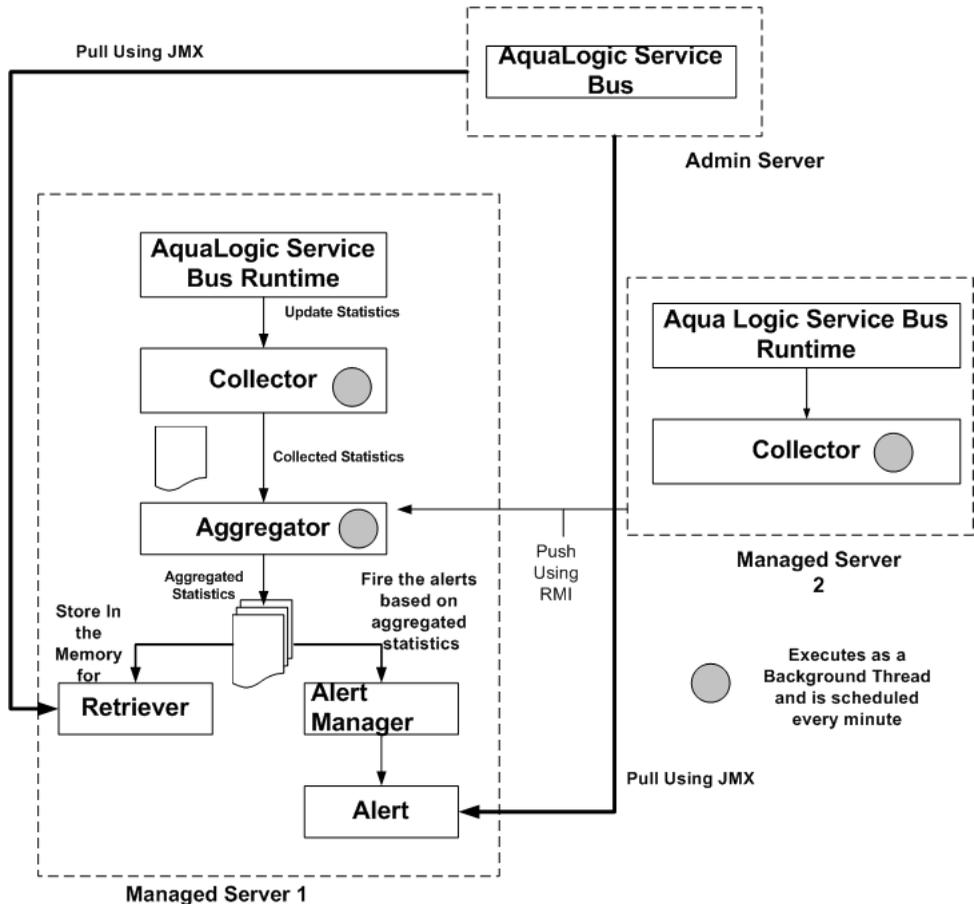
You can monitor ALSB at run time to know how many messages in a particular service have processed successfully and how many have failed.

The ALSB monitoring framework provides access to information about the number of messages that were processed successfully or failed, which project the service belongs to, the average execution time of message processing, and the number of alerts associated with the service. Using the ALSB Console you can view monitoring statistics for the period of the current aggregation interval or for the period since you last reset statistics for this service or since you last reset statistics for all services. Using the public APIs you can access only the statistics since the last reset.

About the ALSB Monitoring Framework

Monitoring in ALSB involves monitoring of the operational resources, servers, and Service Level Agreements (SLAs). [Figure 3-1](#) is an illustration of the architecture of the ALSB monitoring framework.

Figure 3-1 Monitoring Framework in ALSB



ALSB monitoring architecture consists of the following components:

- **Collector**—Each managed server in a cluster hosts a Collector. The Collector collects statistics on operational resources at regular intervals of time, which is managed in a RMI object. It also keeps samples history within the aggregation interval for the collected statistics. ALSB run time invokes a collector at the beginning of each minute. At every system-defined checkpoint interval, it stores a snapshot of current statistics into a persistent store for recovery purposes and sends the information to the Aggregator in raw format, as raw format is optimized for fast collection and small footprint.

Note: An operational resource is defined as the unit for which statistical information can be collected by the monitoring subsystem. Operational resources include proxy services, business services, service level resources such as Web Services Definition Language (WSDL) operations, flow components in a pipeline, and endpoint URIs.

- **Aggregator**–The Aggregator is present only on only one managed server. The server on which this resides is selected arbitrarily when you generate domain using the config wizard. It aggregates all the statistics that are collected from all managed servers across all managed servers in a cluster. ALSB run time invokes the aggregator twenty-five seconds past each minute, to enable collectors to collect data and send it to the aggregator. At system-defined checkpoint intervals, each managed server in the cluster sends a snapshot of its contributions to the Aggregator. Data structures in aggregator are optimized for aggregating and retrieving data.
- **Retriever**–The Retriever retrieves the statistics that are stored in the memory. This is present only in that managed server, which contains the aggregator.
- **Alert Manager**–The alert manager fires alerts based on the aggregated statistics. This is present only in that managed server, which contains the aggregator.

The Collector collects the updated statistics from ALSB run time and sends it to Aggregator. The Aggregator aggregates the statistics over the aggregation interval. The aggregated statistics are pushed to the Alert Manager. The Alert Manager triggers alerts based on these statistics. The aggregated statistics are also stored and can be retrieved by the Retriever. The following steps are executed when you monitor a service in ALSB run time:

In a cluster, all the statistics which are collected in the managed servers are pushed to the aggregator. You can access the cluster wide statistics from the Service Health tab. For more information, see [How to Access Statistics in a Cluster](#). You can also access statistics using APIs. For more information, see [How to Access Statistical Information Using the JMX Monitoring APIs](#).

The alerts are pulled from the managed server that hosts the aggregator, and they are displayed in the ALSB Console.

Aggregation Intervals

In ALSB, the monitoring subsystem collects statistics, such as message count over an aggregation interval. The aggregation interval is the time period over which statistical data is collected and displayed in the ALSB Console. Statistics which are not based on an aggregation interval are meaningless. In addition to statistics collected over well-defined aggregation interval you can also collect cumulative statistics.

The Refresh Rate of Monitoring Data

Aggregation interval is a moving window, which always refers to an interval of time in minutes, hours or days. It does not move with infinite granularity or precision, but at regular intervals of time called the sampling interval. This enables an aggregation interval to move smoothly and produce accurate statistics.

Figure 3-2 Illustration of Aggregation Interval and Sampling Interval

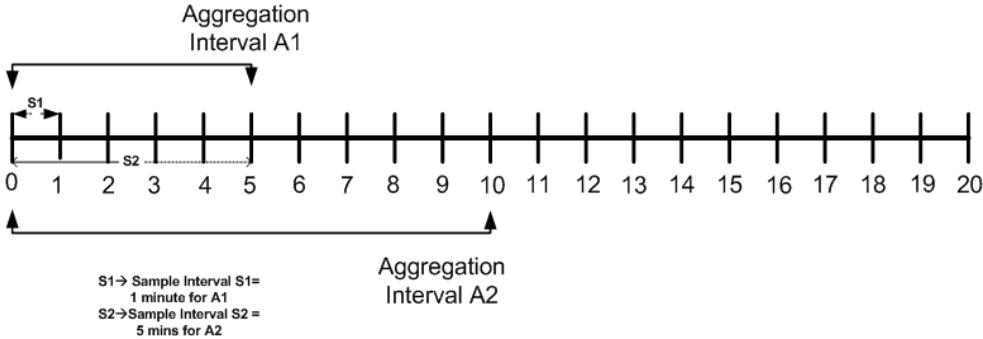


Figure 3-2 is an illustration of the of Aggregation interval. For example aggregation interval A1 is set at five minutes and aggregation interval A2 has been set at ten minutes. ALSB run time collects statistics for the service with aggregation interval A1 for every minute (S1). It aggregates the statistics at the end of the aggregation interval. Similarly for aggregation interval A2 it collects statistics for every five minutes (S2). Intervals S1 and S2 are called sampling intervals. For more information about sample interval, see [Sample Intervals Within Aggregation Intervals](#) .

Sample Intervals Within Aggregation Intervals

In ALSB run time statistics are computed at regular intervals, within every aggregation interval. These regular sub intervals are known as the sample interval. The duration of the sample interval depends on the aggregation interval. Table 3-1 gives the length of sample interval for different aggregation intervals:

Table 3-1 Sample Interval

Aggregation Interval	Sample Interval
1, 2, 3, 4, and 5 minutes	1 minute
10, 15, 20, 25, and 30 minutes	5 minutes
40, 50, and 60 minutes	10 minutes
90 and 120 minutes	30 minutes
3, 4, 5, and 6 hours	1 hour
8, 10, and 12 hours	2 hours
16, 20, and 24 hours	4 hours
2, 3, 4, 5, 6, and 7 days	1 day

How to Set the Aggregation Interval for Monitoring Data

Aggregation interval in ALSB has the following properties:

- You can track statistics for a service over only one aggregation interval.
- You cannot set an arbitrary value for an aggregation interval. You must choose from one of the values in the drop-down list.
- You can set the aggregation interval for the following:
 - A service—You must set the aggregation interval for a service in Operation tab of View a Proxy service or View a Business Service page. For more information about how to set aggregation interval for a service, see [Setting the Aggregation Interval for a Service](#) in Monitoring in Using the AquaLogic Service Bus Console.
 - An alert rule—You must set the aggregation interval for an alert rule by editing Conditions on View Alert Rule Details page. For more information about how to edit conditions for an alert rule, see [Defining Alert Rule Conditions](#) in Monitoring in Using the AquaLogic Service Bus Console.

You can only specify an aggregation interval less than or equal to seven days.

What are the Consequences Of Changing Aggregation Interval Of A Service?

When you modify the aggregation interval of a service, the statistics of the service in the current aggregation interval is reset. However, the status of the endpoint URI for the service remains unaffected by the change in the aggregation interval. A running count metrics of the service is not reset when modify the aggregation interval.

What are the Consequences Of Renaming Or Moving A Service?

When you rename or move a service within ALSB, all the monitoring statistics that have been collected in the ALSB Console are lost. All current aggregation interval and cumulative metrics are reset and the service is monitored from start. If endpoint URI for a service was marked offline before it was renamed or moved, then after you rename or move the service, the URIs are marked online again and the status of the URI is displayed as online.

What Statistics are Available for ALSB Services?

You can monitor services in ALSB and collect statistics for all services. Monitoring system in ALSB supports the following types of statistics:

- Counter—A counter simply keeps track of the count of events in ALSB run time such as number of messages received and number of failovers. This is scalar and takes on integral values.
- Interval—An interval keeps track of time elapsed between two well-defined events. This tracks the total, average, minimum, and maximum of such events in ALSB. This takes on integral and non-integral values.
- Status Type—A Status statistic keeps track of the status. Using this you can keep track of the initial status and the current status of the object.

For more information about different types of statistics, see [Appendix B "Monitoring Statistics in ALSB"](#). For more information on how to access statistics using APIs, see [How to Access Statistical Information Using the JMX Monitoring APIs](#).

Accessing Statistical Information for Services

You can access the statistical information for a service through the ALSB Console or directly by using the JMX monitoring APIs. This section describes accessing the information through the ALSB Console and the JMX monitoring APIs. For more information about accessing the statistical information through JMX monitoring APIs, see [JMX Monitoring API Programming Guide](#).

How to Access Service Statistics from the ALSB Console

You can access the service statistics from the ALSB Console for a stand alone server or a cluster. This section describes how to access statistics for a standalone server. For information on how to access service statistics for a cluster, see [How to Access Statistics in a Cluster](#).

In the you can access the statistical information for services in the current aggregation interval or for time interval since the last reset. The Service Health tab of dashboard provides the statistical information for current aggregation interval and since last reset. For more information, see [How to Access Service Statistics for the Current Aggregation Interval](#) and [How to Access Running Count Statistics for Services](#).

How to Access Statistical Information Using the JMX Monitoring APIs

You can also access statistical information directly from a program using the Java Management Extensions (JMX) monitoring APIs. Using the JMX monitoring APIs you can access only the running count statistics. The JMX monitoring APIs provide an efficient lower level support for bulk operations. For more information about using JMX monitoring APIs, see [JMX Monitoring API Programming Guide](#).

How to Access Statistics in a Cluster

In a cluster environment, statistics are available at individual managed server level and the cluster level. In Service Health tab choose Cluster or the name of a managed server from the Server drop-down list, to view statistics for the cluster or the individual managed server.

To get detailed statistics for a particular service in a cluster, access the service monitoring details page for the service from the Service Health tab. On the Service Monitoring Details page, you can access the cluster wide statistics by setting the Server drop-down list to Cluster. By setting it to the individual managed server value, statistics pertaining to that specific server can be viewed.

Set Display Statistics to Current Aggregation Interval to view cluster statistics in the current aggregation interval or Since Last Reset to view the running count statistics for the cluster.

How to Reset Statistics

You can reset the statistics of business services and proxy services from the Service Health tab of the dashboard or from the Service Monitoring Details page for a service. [Table 3-2](#) describes how to reset statistics in each case.

Table 3-2 How to Reset Statistics

To Reset Statistics from ...	Description
Service Health Tab	<p>Click the Service Health tab to go to the Service Health page. Click Reset Statistics icon to reset statistics for a service. Click Reset All Statistics link to reset statistics for all the services for which monitoring is enabled.</p> <p>Note: The reset Statistics Icon is available only when you set Display Statistics to Since Last Reset.JMS</p> <p>For more information about how to reset statistics, see Resetting Statistics for Services in Monitoring in Using the AquaLogic Service Bus Console.</p>
Service Monitoring Details Page	<p>Click the name of the service in the alert history table or on the Service Health page to go to the Service Monitoring Details page. In the Service Monitoring Details page in the Display Statistics field select Since Last Reset. Click Reset Statistics to reset the statistics for the given service.</p>

What are the Consequences of Resetting the Statistics?

When you reset statistics for a service in the ALSB Console, all the statistics collected for the service since the last reset is lost. You cannot undo this action. The status of endpoint URIs is not reset when you reset statistics.

The Role of Alerts in Service Monitoring

SLA alerts are raised in ALSB to indicate potential violation of the Service Level Agreements (SLAs). You can use alerts for:

- Monitoring and generating e-mail notification of WS-Security errors.
- Monitoring the number of messages passing through a particular pipeline.
- Detecting the violation of service level agreements with third-party products.
- Detecting a non-responsive endpoint.

Pipeline alerts can be raised in the message flow of the proxy service. You can use the alerts in a message flow for:

- Detecting errors in a message flow.
- Indicating business occurrences.

Assigning Severity for Alerts

You can configure the severity of an alert in an alert rule for SLA alerts or in the `Alert` action of a message flow of a proxy service. The severity level of alerts is user configurable and has no absolute meaning. You can configure alerts with one of the following levels of severity:

- Normal
- Warning
- Minor
- Major
- Critical
- Fatal

The alert destinations are notified when an alert is raised. If you do not configure any alert destination in an alert rule or an alert action, the notifications are sent to the ALSB Console. For more information in alert destinations, see [What are Alert Destinations?](#)

What are SLA Alerts?

SLA alerts are automated responses to violations of Service Level Agreements (SLAs). These alerts are displayed on the ALSB dashboard. They are generated when the service violates the service level agreement or a predefined condition. To raise an SLA alert, you must enable SLA alerting both at the service level and at the global level. For more information about how to configure operational settings for services, see [How to Configure the Operational Settings for a Service](#). The Alert History panel contains a customizable table displaying information about violations or occurrences of events in the system.

You must define alert rules to specify unacceptable service performance according to your business and performance requirements. Each alert rule allows you to specify the aggregation interval for that rule when configuring the alert rule. This aggregation interval is not affected by the aggregation interval set for the service. For more information about aggregation interval, see [Aggregation Intervals](#). Alert rules also allow you to send notifications to the configured alert destinations. For information on defining alert rules, see [Creating and Editing Alert Rules in Monitoring in Using the AquaLogic Service Bus Console](#).

A Sample Use Case for SLA Alerts

Consider the following use case to verify the service level agreements:

Assume that a particular proxy service is generating SLA alerts due to slow response time. To investigate this problem, you must log into the ALSB Console and review the detailed statistics for the proxy service. At this level, you can able to identify that, a third-party Web service invocation stage in the pipeline is taking a lot of time and is the actual bottleneck. You can use these alerts as the basis for negotiating SLAs. After successfully renegotiating SLAs with the third-party Web service provider, you must configure alert metrics to track the Web service provider's compliance with the new agreement terms.

What are Pipeline Alerts?

Pipeline alerts can be generated in a message flow whenever you define an `Alert` action available under the reporting category in the message flow.

You can also define conditions under which a pipeline alert is triggered using the conditional constructs available in the pipeline editor such as Xquery Editor or an if-then-else construct. The ALSB Console is the default alert destination for pipeline alerts. You can also configure the Alert Destination resource in an alert action, to define additional destinations for pipeline alerts.

You can have complete control over the alert body including the pipeline, and context variables. Also you can extract the portions of the message. For more information about how to configure `Alert` actions in a stage, see [Adding Alert Actions](#) in Proxy Service: Actions in Using the AquaLogic Service Bus Console. When the alert action is executed the alerts are notified to the appropriate alert destinations.

You can obtain an integrated view of all the pipeline alerts generated by a service on the dashboard page in the ALSB Console.

A Sample Use Case for Pipeline Alerts

Consider the following use case for pipeline alerts:

Consider a case when you want to be notified when special business conditions are encountered in a message flow. You can configure an alert action in a message flow to raise alerts when such predefined conditions are encountered. You can also configure email alert destination to receive an email notification of the alert. You can also send the details to the email recipient in the form of payload.

For example, in the case of a proxy service that routes orders to a purchase order website, and you want to be notified when an order exceeding \$10 million is routed. For this you must configure an alert action in the appropriate place in the pipeline, with the condition and configure email alert destination with the email information and use it as the target destination in the alert action. You can also include the details of the order in the form of payload.

You can also use pipeline alerting to detect errors in a message flow. For example, in the case of a proxy service that validates the input document, you want to be notified when the validation fails so that you can contact the client to fix the problem. For this you must configure an alert action within the error handler for the message flow of the proxy service. In the action you can include the actual error message in the fault variable and other details in the SOAP header, to be sent as the payload. You can also configure additional alert destinations using an alert destination resource in the alert action.

How to View or Delete SLA Alerts

In the ALSB Console the extended alert history page for the SLA alerts contains information about all the SLA alerts that have been generated in the domain. You can view all the alerts that were triggered or search for specific alerts from the table. For more information about data displayed in the extended SLA alert history page, see [Locating Alerts](#) in Monitoring in Using the AquaLogic Service Bus Console.

You can delete the alerts from the Extended Alert History page or the View Alert Details page. You can filter your search using the Extended Alert History Filters pane. For more information on how to filter your search, see [How to Filter a Search for SLA Alerts](#).

To view a pie or bar chart of the alerts, click View Bar Chart or View Pie Chart in the page. Click Purge SLA Alert History to delete all the SLA alerts. You can also purge the alerts based on the date and time they were raised.

How to View or Delete Pipeline Alerts

The extended alert history page for the pipeline alerts contains information about all the pipeline alerts that have been generated in the domain. You can view all the alerts that were triggered or search for specific alerts from the table. For more information about data displayed in the extended pipeline alert history page, see [Locating Alerts](#) in Monitoring in Using the AquaLogic Service Bus Console.

You can delete the alerts from the Extended Pipeline Alerts page or from the View Alert Details page. For more information on how to filter your search, see [How to Filter a Search for Pipeline Alerts](#). To view a pie or bar chart of the alerts, click View Bar Chart or View Pie Chart link in the page. Click Purge Pipeline Alert History to delete all the pipeline alerts. You can also purge the alerts based on the date and time they were raised.

How to Filter a Search for Specific Alerts

Use Extended Alert History to filter a search for specific alerts. The following sections describe how to search for SLA alerts and pipeline alerts using extended alert history filters.

How to Filter a Search for SLA Alerts

Use Extended Alert History Filters pane to filter a search for SLA alerts. [Table 3-3](#) describes the various criteria on which you can filter SLA alerts.

Table 3-3 Search Criteria for SLA Alerts

Search Criterion	Description
Date Range	Use this to search for pipeline alerts that were generated in the given interval of time. You can set the interval in one of the following ways: <ul style="list-style-type: none">• All• Set timestamp interval in MM/DD/YY HH:Min:SS AM/PM format.• Alerts generated during the given time interval in the format days–hours–minutes
Alert Severity	Specify the level of severity. The search result includes all the alerts that have the specified level of severity and above.
Service	Use this to search for a specific service.
Service Type	This is updated automatically when you search for a specific service.
Alert Name	Use this to search by alert name.

How to Filter a Search for Pipeline Alerts

Use Extended Alert History Filters pane to filter a search for pipeline alerts. [Table 3-4](#) describes the various criteria on which you can filter pipeline alerts.

Table 3-4 Search Criteria for Pipeline Alerts

Search Criterion	Description
Date Range	Use this to search for pipeline alerts that were generated in the given interval of time. You can set the time interval in one of the following ways: <ul style="list-style-type: none"> • All • Set timestamp interval in MM/DD/YY HH:Min:SS AM/PM format. • Alerts generated during the given time interval in the format days–hours–minutes
Alert Severity	Specify the level of severity. The search result includes all the alerts that have the specified level of severity and above.
Service	Use this to search for a specific service.
Service Type	This is updated automatically when you search for a specific service.
Alert Summary	Use this to search by alert summary.

What are Alert Destinations?

Alert destinations are resources to which alerts are sent. The ALSB Console is the default alert destination for the notification of any alert. The alerts are notified to the ALSB Console console regardless of whether you configure an alert destination or not. The console provides information about the alerts generated due to SLA violations or as a result of alert actions configured in the pipeline. The dashboard page displays the overall health of ALSB. It provides an overview of the state of the system comprising server health, services health, and alerts.

For more information about how to interpret the information on the dashboard, see [The ALSB Dashboard](#).

In ALSB you can configure Email, SNMP Traps, Reporting and JMS as alert destinations.

E-mail

E-mail alert destination, allows you to receive messages when alerts are raised in the ALSB Console. To configure this alert destination you have to use the SMTP server global resource or

a JavaMail session in the WebLogic server. For more information on configuring a default SMTP Server resource, see [Configuring a Default SMTP Server](#) in Global Resource in Using the AquaLogic Service Bus Console. For more information about configuring JavaMail sessions, see [Configure Access to JavaMail](#) in WebLogic Server Administration Console Online Help

The SMTP server global resource captures the address of the SMTP server, port number, and if required, the authentication credentials. The authentication credentials are stored inline and are not stored as a service account. The alert manager makes use of the e-mail alert destination to send the outbound e-mail messages when both pipeline alerts and SLA alerts are generated. When an alert is delivered, an e-mail metadata consisting of the details about the alert is prefixed to the details of the payload that is configured.

You can specify the e-mail ID of the recipients in the Mail Recipients field. For more information about configuring an e-mail alert destination, see [Adding E-Mail Recipients](#) in Adding E-mail and JMS Recipients in Alert Destinations in Using the AquaLogic Service Bus Console.

SNMP Traps

The Simple Network Management Protocol (SNMP) traps allow any third-party software to interface monitoring service level agreements within ALSB. By enabling the notification of alerts using SNMP, Web Services Management (WSM) and the Enterprise Service Management (ESM) tools can monitor SLA violations and pipeline alerts by monitoring alert notifications.

SNMP is an application-layer protocol which allows the exchange of information on the management of a resource across a network. It enables you to monitor a resource and, if required, take some action based on the data obtained from the resource. Both the SNMP version 1 and SNMP version 2 are supported by ALSB. SNMP includes the following components:

- Managed Resource
- Management Information Base(MIB)
- SNMP Agent
- SNMP Manager
- Network Management System (NMS)

For more information, see [Appendix A "SNMP Components"](#).

Reporting

The Reporting destination allows you to send notifications of pipeline alerts or SLA alerts to the custom reporting provider that can be developed using the reporting APIs provided with ALSB. This allows third parties to receive and process alerts in custom Java code.

JMS

Java Messaging Service (JMS) is another destination for pipeline alerts and SLA alerts. You must configure a JNDI URL for the JMS destination for alerts. When you configure an alert rule to post a message to a JMS destination, you must create a JMS connection factory and a queue or topic, and target them to the appropriate JMS server in the WebLogic Server Administration Console. For information on how to do this, see [Configuring a JMS Connection Factory and JMS Resource Naming Rules for Domain Interoperability](#) in [Configuring JMS System Resources](#) in [Configuring and Managing WebLogic JMS](#). When you define the JMS alert destination you can either use a destination queue or a destination topic. The message type can be bytes or text. For more information about how to configure JMS alert destination see [Adding JMS Recipients](#) in [Adding E-mail and JMS Recipients in Alert Destinations in Using the AquaLogic Service Bus Console](#).

What are Operational Settings for a Service?

Operational settings enable you to control the state of a service in the ALSB Console. [Table 3-5](#) describes operational settings for services in the ALSB Console.

Table 3-5 Operational Settings for Services in the ALSB Console

Operational Settings	Usage	Default Value When a Service is Created
State	Use this to enable or disable a service .	Enabled
Monitoring	Use this to enable or disable service monitoring.	Disabled
Aggregation Interval	Use this to set the aggregation interval for the service.	10 minutes
SLA Alerting	Use this to enable SLA alerting for services at a specific level of severity or above. You can also use this to disable SLA alerting for a service.	Enabled

Table 3-5 Operational Settings for Services in the ALSB Console

Operational Settings	Usage	Default Value When a Service is Created
Pipeline Alerting	Use this to enable pipeline alerting for proxy services at a specific severity level or above. You can also use this to disable pipeline alerting for proxy services.	Enabled at Normal level or higher
Message Reporting	Use this to enable or disable message reporting for proxy services.	Enabled at Normal level or higher
Logging	Use this to enable logging at a specific severity level or above. You can also use this to disable logging for proxy services.	Enabled at Debug level or higher
Tracing	Use this to enable or disable tracing for proxy services.	Disabled
Offline Endpoint URIs	Use this to enable or disable non responsive endpoints for business services. You can also specify the interval of time to wait before retrying the offline endpoint URI. You can enable or disable offline URIs for business services only.	Disabled
Throttling State	Use this to enable or disable throttling for a business service.	Disabled
Maximum Concurrency	Use this to restrict the number of messages that can be concurrently processed by a business service.	0
Throttling Queue	Use this to restrict the maximum number of messages in the throttling queue.	0
Message Expiration	The maximum time interval (in milliseconds) for which a message can be placed in throttling queue.	0

The operational settings at the service level is overridden by the global settings. For more information about configuring operational settings globally, see [How to Configure the Operational Settings at the Global Level](#).

How to Configure the Operational Settings for a Service

You can enable or disable the operational settings for an individual service from the Operation Settings view of the View a Proxy Service (see [Figure 3-3](#)) or View a Business Service page (see [Figure 3-4](#)). For more information, see [Creating and Configuring Business Services](#) in *Business Services: Creating and Managing* and [Creating and Configuring Proxy Services](#) in *Proxy Services: Creating and Managing* in *Using the AquaLogic Service Bus Console*.

Some operational settings such as service state, monitoring, SLA alerting, and pipeline alerting can be enabled or disabled through public APIs. For more information, see [Javadoc for AquaLogic Service Bus](#).

Figure 3-3 View a Proxy Service

The screenshot displays the 'View a Proxy Service' interface for 'loanGateway3'. It includes a metadata table, a navigation bar with tabs for 'Configuration Details', 'Operational Settings', 'SLA Alert Rules', 'Policies', and 'Security', and a detailed configuration section.

View a Proxy Service (MortgageBroker/ProxyServices/loanGateway3)		
Last Modified By	weblogic	Description - no description -
Last Modified On	1/21/08 12:51 PM	
References	2 Ref(s)	
Referenced By	0	

Configuration Details | **Operational Settings** | SLA Alert Rules | Policies | Security

Proxy Service Configuration (MortgageBroker/ProxyServices/loanGateway3)		Actions:   
General Configuration 		
Service Type	Web Service - SOAP 1.1 (WSDL: MortgageBroker/WSDL/normalLoan, port="helloPort")	
Content Streaming	Disabled	
Transport Configuration 		
Protocol	http	
Endpoint URI	/loan/gateway3	
Get All Headers	Yes	
HTTP Transport Configuration 		
HTTPS required	No	
Authentication	None	
Operation Selection Configuration 		
Enforce WS-I Compliance	No	
Selection Algorithm	SOAP Body Type	

Back | Edit

Figure 3-4 View a Business Service

View a Business Service (MortgageBroker/BusinessServices/loanSaleProcessor)		
Last Modified By	weblogic	Description - no description -
Last Modified On	12/12/07 2:30 PM	
References	2 Ref(s)	
Referenced By	0	

Configuration Details | **Operational Settings** | SLA Alert Rules | Policies

Business Service Configuration (MortgageBroker/BusinessServices/loanSaleProcessor)		Actions:  
General Configuration 		
Service Type	Web Service - SOAP 1.1 (WSDL: MortgageBroker/WSDL/LoanSale, binding="LargeLoanPurchasingServiceSoapBinding")	
Transport Configuration 		
Protocol	http	
Load Balancing Algorithm	none	
Endpoint URI	http://localhost:7021/jws_basic_ejb/LargeSimpleBean	
Retry Count	0	
Retry Iteration Interval	30	
Retry Application Errors	Yes	
HTTP Transport Configuration 		
Timeout	0	
HTTP Request Method	POST	
Authentication	None	
Follow HTTP redirects	ENABLED	
SOAP Binding Configuration 		
Enforce WS-I Compliance	No	

|

You can perform the following operational settings for proxy services and business services:

- State
- Aggregation Interval
- Monitoring
- SLA Alerting
- Pipeline Alerting
- Message Reporting

- Tracing
- Pipeline Logging
- URI Offline Interval
- Throttling settings

For a detailed description of the usage of each operational setting for business services, see [Configuring Operational Settings for Business Services](#) in Monitoring in Using the AquaLogic Service Bus Console. For a detailed description of the usage of each operational setting for proxy services, see [Configuring Operational Settings for Proxy Services](#) in Monitoring in Using the AquaLogic Service Bus Console.

How to Configure the Operational Settings at the Global Level

You can access the Global Settings page from the operations module. You can use the Global Settings page (see [Figure 3-5](#)) to configure the operational settings for services. [Table 3-6](#) describes the usage of the operational settings at the global level.

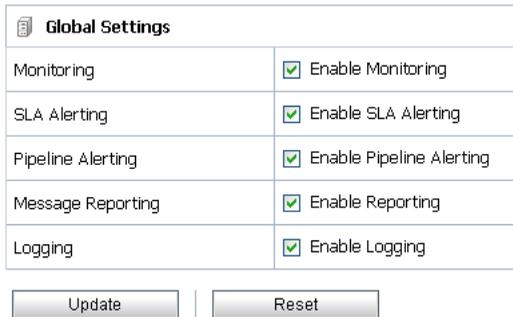
Table 3-6 Usage of Operational Settings at the Global Level

Operational Settings	Usage
Monitoring	Use this to enable monitoring for all services in a domain. Click the check box associated with Enable Monitoring to enable or disable monitoring for all the services in the domain.
SLA Alerting	Use this to enable SLA alerting for all services in a domain. Click the check box associated with Enable SLA Alerting to enable or disable monitoring for all the services in the domain.
Pipeline Alerting	Use this to enable pipeline alerting for proxy services in a domain. Click the check box associated with Enable Pipeline Alerting to enable or disable monitoring for all the services in the domain.

Table 3-6 Usage of Operational Settings at the Global Level

Operational Settings	Usage
Reporting	Use this to enable message reporting for proxy services in a domain. Click the check box associated with Enable Reporting to enable or disable monitoring for all the services in the domain.
Logging	Use this to enable logging for proxy services in a domain. Click the check box associated with Enable Logging to enable or disable monitoring for all the services in the domain.

Figure 3-5 Global Settings Page



For more information, see [Enabling Global Settings](#) in Configuration in Using the AquaLogic Service Bus Console.

Notes:

- The Enable Monitoring option allows you to enable or disable monitoring of all services that have individually been enabled for monitoring. If monitoring for a particular service has not been enabled, you must first enable it and set the aggregation interval on the Manage Monitoring page before the system starts collecting statistics for that service.
- Enable or disable these settings at the global level in conjunction with the settings at the service level to effectively enable or disable them. The operational settings at the global level supersede the operational settings at the service level.

Updates to Operational Settings During Import of ALSB Configurations

When a service is overwritten by the way of importing configuration from a config jar, the operational settings of this service can be also be overwritten. To preserve the operational settings during import, you must set the Preserve Operational Settings flag to true while importing the service. For more information, see [What Happens to Alert Rules When You Import ALSB Configurations?](#)

Updates to Global Settings During the Import of ALSB Configurations

When you import ALSB configurations, if the config jar that is being imported also contains the global settings of the domain from which it is being imported, then these domain level settings can get overwritten. In order to prevent this, set Preserve Operational Settings flag to true while importing the service.

How to Preserve Operational Settings During the Import of ALSB Configuration Through APIs

You can preserve operational settings during import of ALSB configurations using APIs. For more information, see [Importing and exporting configuration using the new API](#) in Interface ALSBConfigurationMBean. Modify the MBean as shown in [Listing 3-1](#) to preserve the during the import.

Listing 3-1 Preserve Operational Settings During the Import of ALSB Configurations Through APIs

```
/**
 *
 * // Imports a configuration jar file, applies customization, activates it
 * and exports the resources again
 *
 * // @throws Exception
 * /
 *
 * static private void simpleImportExport(String importFileName, String
 * passphrase) throws Exception {
 *
 * SessionManagementMBean sm = ... // obtain the mbean to create a session;
```

Monitoring ALSB at Run Time

```
// obtain the raw bytes that make up the configuration jar file
File importFile = new File(importFileName);
byte[] bytes = readBytes(importFile);
// create a session
String sessionName = "session." + System.currentTimeMillis();
sm.createSession(sessionName);
// obtain the ALSBConfigurationMBean that operates on the
// session that has just been created
ALSBConfigurationMBean alsbSession = getConfigMBean(sessionName);
// import configuration into the session. First we upload the
// jar file, which will stage it temporarily.
alsbSession.uploadJarFile(bytes);
// then get the default import plan and modify the plan if required
ALSBJarInfo jarInfo = getImportJarInf();
ALSBImportPlan importPlan = jarInfo.getDefaultImportPlan();
// preserve operational values
importPlan.setPreserveExistingOperationalValues(true);
// Modify the plan if required and pass it to importUploaeded method
ImportResult result = alsbSession.importUploaded(importPlan);
// Pass null to importUploaded method to mean the default import plan.
//ImportResult result = alsbSession.importUploaded(null);
// print out status
if (result.getImported().size() > 0) {
    System.out.println("The following resources have been successfully
imported.");
    for (Ref ref : result.getImported()) {
        System.out.println("\t" + ref);
    }
}
```

```

    }
    if (result.getFailed().size() > 0) {
        System.out.println("The following resources have failed to be
imported.");
        for (Map.Entry e : result.getFailed().entrySet()) {
            Ref ref = e.getKey();
            // Diagnostics object contains validation errors
            // that caused the failure to import this resource
            Diagnostics d = e.getValue();
            System.out.println("\t" + ref + ". reason: " + d);
        }
        // discard the changes to the session and exit
        System.out.println("Discarding the session.");
        sm.discardSession(sessionName);
        System.exit(1);
    }
    // perform the customization to assign/replace environment values and
    // to modify the references.
    ...
    // activate the session
    sm.activateSession(sessionName, "description");
    // export information from the core data
    ALSBConfigurationMBean alsbcore = getConfigMBean(null);
    //export the information at project level, pass only a collection of project
    refs to this method
    byte[] contentsProj =
alsbcore.exportProjects(Collections.singleton(Ref.DEFAULT_PROJECT_REF), nul
l);

```

```
// the byte contents can be saved as jar file  
}
```

SLA Alerting Functionality in ALSB

In ALSB you must define conditions based on which alerts are raised. The conditions are configured in an SLA alert rule. The alert rule also configures the severity level and an alert destination for an alert.

How to Configure SLA Alert rules

SLA alerts are automated responses to SLAs violations, which are displayed on the dashboard. You must define alert rules to specify unacceptable service performance according to your business and performance requirements. When you configure an alert rule, you must specify the aggregation interval. The alert aggregation interval is not affected by the aggregation interval set for the service. For more information about aggregation interval, see [Aggregation Intervals](#).

Creating an alert rule involves the following steps:

- **General Configuration**—defines the name, description, summary, duration, severity, frequency, state of the enabled alert rule and other general characteristics.
- **Define Condition**—defines one or more conditions that trigger the alert rule. Additionally, you must define the aggregation interval for the condition on this page.

Note: You can create alert rules even if you have not enabled for monitoring for a service.

For more information about creating an alert rule, see [Creating And Editing Alert Rules](#) in *Monitoring in Using the AquaLogic Service Bus Console*.

For a service for which monitoring is enabled, Alert rule is evaluated at discrete intervals. Once an alert rule is created it is first evaluated at the end of the aggregation interval, and after that at the end of each sample interval. For example, if the aggregation interval of an alert rule is five mins, it is evaluated five minutes after it is created, and then every minute after that (since sample interval for five mins, is one min).

If a rule evaluates to false no alert is generated. If the rule evaluates to true the alert generation is governed by the Alert Frequency. If the frequency is `Every Time`, an alert is generated every time an alert rule evaluates to true. If the frequency is `Notify Once`, an alert is generated only if no alert is generated in the previous evaluation. In other words, an alert is generated the first time the alert rule evaluates to true and no more notifications are generated until the condition resets itself and evaluates to True again.

How to Lookup or Edit Existing Alert Rules

The View Alert Rule Details page displays complete information about a specific alert rule, as shown in [Figure 3-6](#). You can view the details of the alert rule in this page. You can edit an alert rule configuration from this page. For more information about how to edit an alert rule, see [Creating and Editing Alert Rules](#) in Monitoring in Using the AquaLogic Service Bus Console.

Figure 3-6 View Alert Rule Details Page

General Configuration 	
Rule Name	newbsRule
Rule Description	
Alert Summary	
Alert Destination	default/NewalertDest
Start Time (HH:MM)	
End time (HH:MM)	
Rule Expiration Date (MM/DD/YYYY)	
Rule Enabled	true
Alert Severity	Fatal
Alert Frequency	Every Time
Stop Processing More Rules	false
Conditions 	
Condition Expression	Aggregation Interval 0 Hour(s) and 10 Minutes Success Ratio (%) = 100

How to Rename Alert rules

You can rename the alert rules from the SLA Alert Rules tab of View a Business Service or View a Proxy Service page. To rename an alert rule click Rename Alert Rule icon. Enter the new name for the alert rule in New Alert Rule Name field of the Rename Alert Rule window. Click Rename. Click Update and activate the session to complete. For more information, see [Viewing Alert Rules](#) in Monitoring in Using the AquaLogic Service Bus Console. The Rename icon for the renamed alert is now disabled.

What are the Consequences of Renaming an Alert Rule?

When alerts are triggered, they are listed on the alert history page. Click View Alert Rule Details action icon to access the alert rule page. However, when you rename an alert rule, you cannot access the alert rule by clicking the View Alert Rule Details action from the alert history page,

for the alerts that were raised before it was renamed. You can access the Alert Details page from the alert history page for the alerts that are raised before-and after renaming the alert rule. The alert name is greyed in the Alert Details page for the alerts that were raised before the alert rule was renamed. When you rename an alert details icon for the renamed alert gets disabled.

Similar limitations exist when you attempt to access the alert rule page by clicking the alert name link on the alert details page. The alert name generated by alerts rules that are later renamed refers to an outdated name. You can view the old alert rule, but the name is grayed out indicating that the alert rule has been renamed.

When you rename an alert rule, the conditions on which a rule is based are preserved. The aggregation interval of the alert rule is also preserved. The alert is raised at the end of the first aggregation interval after the alert rule is renamed. For example, consider an alert rule a1 with aggregation interval five minutes. If the alert rule is renamed to a2 after two minutes of execution the next alert under the name a2 is generated three minutes after the is renamed.

What Happens to Alert Rules When You Import ALSB Configurations?

You can preserve the alert rule configurations when you import ALSB configurations. When you import ALSB configurations, the operational settings are preserved. When services with alert rules exists in a jar that you import but does not exist in the target domain, then these services along with the alerts rules are imported as is. However, if the same service exists in the target domain as well, then the import behavior is governed by the state of the Preserve Operational Settings during the import operation. For more information on how to preserve operational settings, see [Updates to Operational Settings During Import of ALSB Configurations](#).

The ALSB Dashboard

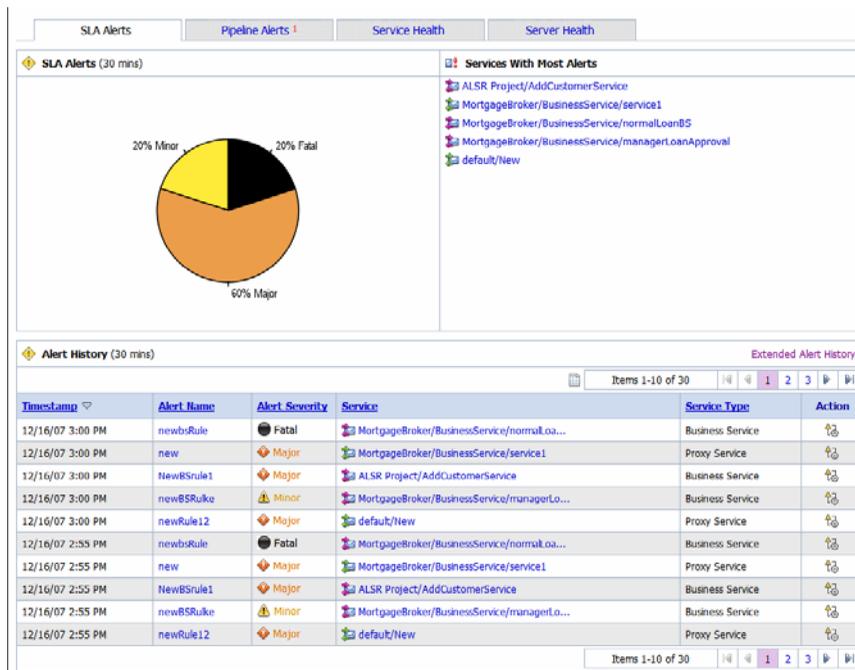
The ALSB dashboard displays service health, server health and details of all the alerts that have been triggered in ALSB run time. The dynamic refresh of this display is controlled by the Dashboard Refresh Rate setting in the User Preferences page. The default option for this setting is No Refresh. These alerts can be the result of SLA violations or pipeline alerts. Service Level Agreements(SLAs) are agreements that define the precise level of service expected from the business and proxy services in ALSB. Pipeline alerts are defined in the message flow for business purposes such as record the number of message that flow through the message pipeline, to track occurrences of certain business events, or to report errors but not for the health of the system.

Each row of the table displays the information that you have configured, such as the severity, timestamp, and associated service. Clicking the Alert Name link displays Alert Details page for more details about the SLA alert. This helps you to analyze the cause of the SLA alert. Clicking the Alert Summary link displays the Alert Details for more details about the pipeline alert. This helps you to analyze the cause of the SLA alert.

From the dashboard, you can drill-down into the system and easily find specific information, such as the average execution time of a service, the date and time an alert occurred, or the duration for which server has been running.

The following sections helps you to understand the information displayed on ALSB dashboard.

Figure 3-7 ALSB Dashboard for SLA Alerts



How to Access Service Statistics for the Current Aggregation Interval

Click the Service Health tab to access the Service Health page. The Service Health page is displayed as shown in [Figure 3-8](#).

Figure 3-8 Service Health Page—Current Aggregation Interval

The screenshot shows the Service Health page with the following data:

Name	Path	Service Type	Aggr. Interval	Avg. Resp. Time	Messages	Errors	SLA Alerts	Pipeline Alerts	Endpoint URL Status
mfProxy	default	Proxy Service	0 hr(s) 1 mins	0 msec	0	0	0	0	N/A
New	default	Proxy Service	0 hr(s) 1 mins	0 msec	0	0	0	0	N/A
normalLoanS	MortgageBroker/BusinessService	Business Service	0 hr(s) 1 mins	0 msec	0	0	0	N/A	Online
normalLoanProcessor	MortgageBroker/BusinessServices	Business Service	0 hr(s) 5 mins	0 msec	0	0	0	N/A	Online
service1	MortgageBroker/BusinessService	Proxy Service	0 hr(s) 1 mins	0 msec	0	0	0	0	N/A
service3	default	Proxy Service	0 hr(s) 1 mins	0 msec	0	0	0	0	N/A

This is a dynamic view of statistical data collected by each service. This view is available when you select Current Aggregation Interval in the Display Statistics field. The aggregation interval displayed in this view determines the statistics that are displayed. For example, if the aggregation interval of a particular service is twenty minutes, that service’s row displays the data collected in the last twenty minutes. From this page you can view all services or search for services based on the given criteria. For more information about the statistics displayed in this page, in the Current Aggregation Interval view, see [Viewing Service Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

The Service Monitoring Details page provides you with two views of detailed information about a specific service. [Figure 3-9](#) shows the Service Monitoring Details page for a business service in the current aggregation interval. [Figure 3-10](#) shows the Service Monitoring Details page for a proxy service. To access this page click the name of the service in the Service With Most Alerts section, Alert History table, or extended alert history table for SLA alerts and pipeline alerts. Also the name of the service in Service Health tab is a link to Service Monitoring Details page.

Figure 3-9 Service Monitoring Details for Business Service—Current Aggregation Interval

Service Monitoring Details Extended SLA Alert History	
Service Name	MortgageBroker/BusinessService/normalLoanBS
Service Type	Business Service
Display Statistics	Current Aggregation Interval ▾
Server	AdminServer ▾
Aggregation Interval	0 Hour(s) and 1 Minutes
<div style="display: flex; justify-content: space-around;"> Service Metrics Operations Endpoint URIs </div>	
General ⌵	
SLA Alert Count	1 Alerts ; Fatal 12/16/07 3:07 PM
Min Response Time	0 msec
Max Response Time	0 msec
Overall Avg. Response Time	0 msec
Message Count	0
Error Count	0
Failover Count	0
Success Ratio	100%
Failure Ratio	0%
WS Security Errors	0
Validation Errors	N/A
Throttling ⌵	
Min Throttling Time	0 msec
Max Throttling Time	0 msec
Average Throttling Time	0 msec
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> Back Reset Statistics Refresh </div>	

Figure 3-10 Service Monitoring Details for Proxy Services –Current Aggregation Interval

Service Monitoring Details	
Service Name	default/New
Service Type	Proxy Service
Display Statistics	Current Aggregation Interval
Server	AdminServer
Aggregation Interval	0 Hour(s) and 1 Minutes
<div style="display: flex; justify-content: space-around;"> Service Metrics Flow Components Operations </div>	
General	
SLA Alert Count	1 Alerts ; Major 12/16/07 3:11 PM
Pipeline Alert Count	0 Alerts ; Normal 12/16/07 3:11 PM
Min Response Time	0 msecs
Max Response Time	0 msecs
Overall Avg. Response Time	0 msecs
Message Count	0
Error Count	0
Success Ratio	100%
Failure Ratio	0%
WS Security Errors	0
Validation Errors	0

This is a dynamic view of statistical data collected by each service. This view is available when you select Current Aggregation Interval in the Display Statistics field. The aggregation interval displayed in this view determines the statistics that are displayed. For example, if the aggregation interval of a particular service is twenty minutes, this page displays the data collected in the last twenty minutes for that service. For more information on different tabs available for a business service, see [Service Metrics](#), [Operations](#), and [Endpoint URIs](#). For more information on different tabs available for a proxy service, see [Service Metrics](#) and [Flow Components](#) and [Operations](#).

For more information about the statistics displayed in this page, in the Current Aggregation Interval view, see [Viewing Service Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

How to Access Running Count Statistics for Services

The running count statistics for a service are statistics that are available since the last reset.

Figure 3-11 Service Health Tab—Since Last Reset

The screenshot shows the 'Service Health' tab in the dashboard. At the top, there are tabs for 'SLA Alerts 20', 'Pipeline Alerts 1', 'Service Health', and 'Server Health'. Below these, there are filters for 'Display Statistics' (set to 'Since Last Reset') and 'Server' (set to 'AdminServer'). A search section is present with fields for 'Name' and 'Path'. Below that is a 'Service Health Filters' section with a 'Search' button and a 'View All' button. The main part of the dashboard is a table with 16 items, showing the following data:

Name	Path	Service Type	Avg. Resp. Time	Messages	Errors	SLA Alerts	Pipeline Alerts	Endpoint URI Status	Action
AddCustomerService	ALSR Project	Business Service	0 msecs	0	0	13	N/A	Online	
ALSRBS	ALSR Project	Business Service	0 msecs	0	0	0	N/A	Online	
alsrBSAP	default	Business Service	0 msecs	0	0	0	N/A	Online	
binarymftest	default	Proxy Service	0 msecs	0	0	0	0	N/A	
CreditRatingService	MortgageBroker/BusinessServices	Business Service	0 msecs	0	0	0	N/A	Online	
HttpOutbound	default	Business Service	0 msecs	0	0	0	N/A	Online	
loanGateway3	MortgageBroker/ProxyServices	Proxy Service	0 msecs	0	0	0	0	N/A	
loanSaleProcessor	MortgageBroker/BusinessServices	Business Service	0 msecs	0	0	0	N/A	Online	
managerLoanApproval	MortgageBroker/BusinessService	Business Service	0 msecs	0	0	13	N/A	Online	
managerLoanReviewService	MortgageBroker/BusinessServices	Business Service	0 msecs	0	0	0	N/A	Online	

This view is a running count of the service health metrics. This view is available when you select Since Last Reset in the Display Statistics field. The statistics displayed in each row are for the period since you last reset the statistics for an individual service or since you last reset the statistics for all services. You can also reset statistics for selected services or for all services. For more information about the statistics displayed in this page, in the Since Last Reset view, see [Viewing Service Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

Figure 3-12 Service Monitoring Details Page for a Business Service—Since Last Reset

Service Monitoring Details Extended SLA Alert History	
Service Name	default/alsrBSAP
Service Type	Business Service
Display Statistics	Since Last Reset
Server	AdminServer
<div style="display: flex; justify-content: space-around;"> Service Metrics Operations Endpoint URIs </div>	
General ⌵	
SLA Alert Count	0
Min Response Time	0 msec
Max Response Time	0 msec
Overall Avg. Response Time	0 msec
Message Count	0
Error Count	0
Failover Count	0
Success Ratio	100%
Failure Ratio	0%
WS Security Errors	0
Validation Errors	N/A
Throttling ⌵	
Min Throttling Time	0 msec
Max Throttling Time	0 msec
Average Throttling Time	0 msec
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> Back Reset Statistics Refresh </div>	

Figure 3-13 Service Monitoring Details Page for a Proxy Service—Since Last Reset

Service Monitoring Details		Extended SLA Alert History Extended Pipeline Alert History
Service Name	default/binarymftest	
Service Type	Proxy Service	
Display Statistics	Since Last Reset ▼	
Server	AdminServer ▼	
<div style="display: flex; justify-content: space-around;"> Service Metrics Flow Components </div>		
General ⌵		
SLA Alert Count	0	
Pipeline Alert Count	0	
Min Response Time	0 msec	
Max Response Time	0 msec	
Overall Avg. Response Time	0 msec	
Message Count	0	
Error Count	0	
Success Ratio	100%	
Failure Ratio	0%	
WS Security Errors	0	
Validation Errors	0	
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> Back Reset Statistics Refresh </div>		

This view is a running count of the service monitoring metrics. This view is available when you select **Since Last Reset** in the **Display Statistics** field. The statistics displayed in each row are for the period since you last reset the statistics for an individual service or since you last reset the statistics for all services. From this page you can view all services or search for services based on the given criteria. You can also reset statistics for this service. For more information about the statistics displayed in this page, in the **Since Last Reset** view, see [Viewing Service Metrics](#) in *Monitoring in Using the AquaLogic Service Bus Console*.

You have the following tabs in the **Service Monitoring Details** page for each of the views:

Service Metrics

The **Service Metrics** (see [Figure 3-14](#)) view displays the metrics for a proxy service or a business service.

Figure 3-14 Service Monitoring Details Page for a Business Service-Service Metrics Tab

Service Metrics		Operations	Endpoint URIs
General			
SLA Alert Count	0		
Min Response Time	0 msec		
Max Response Time	0 msec		
Overall Avg. Response Time	0 msec		
Message Count	0		
Error Count	0		
Failover Count	0		
Success Ratio	100%		
Failure Ratio	0%		
WS Security Errors	0		

The Service Metrics tab displays the following types of metrics:

- **General**—This section enables you to quickly view the status of the alerts and service level statistics for the service in the current aggregation interval. When you view the service level statistics for the time interval since the last reset, this displays all the metrics since they were last rest. For more information about the metrics displayed in this view, see [Viewing Service Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.
- **Throttling** —This section enables to view the throttling statistics for a business service. You can also see the minimum and maximum throttling time in milliseconds. For more information on throttling statistics, see [Viewing Service Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

Operations

These metrics are displayed for WSDL based services for which you have defined operations. The Operations tab (see [Figure 3-15](#)) displays the statistics for the operation defined in a WSDL based service . For more information statistics displayed in this tab, see [Viewing Operations Metrics for WSDL Based Services](#) in Monitoring in Using the AquaLogic Service Bus Console.

Figure 3-15 Service Monitoring Details Page-Operation View

Service Metrics		Operations		Endpoint URIs	
Items 1-1 of 1					
Operation Name	Message Count	Error Count	Min Response Time	Max Response Time	Avg. Resp. Time
addCustomer	0	0	0 msecs	0 msecs	0 msecs
Items 1-1 of 1					
Back		Reset Statistics		Refresh	

Flow Components

This view (see [Figure 3-16](#)) gives information on various components of the pipeline of the service. The Flow Components tab is available only for proxy services. For more information about the statistics displayed in this tab, see [Viewing Flow Components Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

Figure 3-16 Service Monitoring Details Page-Flow Components View for Proxy Services

Service Metrics		Flow Components			
Items 1-3 of 3					
Component Name	Message Count	Error Count	Min Response Time	Max Response Time	Avg. Resp. Time
PipelinePairNode1_request	0	0	0 msecs	0 msecs	0 msecs
PipelinePairNode1_response	0	0	0 msecs	0 msecs	0 msecs
RouteNode1	0	0	0 msecs	0 msecs	0 msecs
Items 1-3 of 3					
Back		Reset Statistics		Refresh	

Endpoint URIs

The Endpoint URIs tab of the Service Monitoring page for a business service gives statistics of the various endpoint URIs configured for a business service and their status. For more information about the statistics displayed in this view, see [Viewing Business Services Endpoint URIs Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

Figure 3-17 Service Monitoring Details Page-Endpoint URI for Business Services

Service Metrics		Operations		Endpoint URIs			
Items 1-2 of 2							
Endpoint URI	Message Count	Error Count	Min Response Time	Max Response Time	Avg. Resp. Time	Status	Action
 http://company.com/cms/addCustomer	0	0	0 msecs	0 msecs	0 msecs	Online	
 http://host:7001/someService	0	0	0 msecs	0 msecs	0 msecs	Online	
Items 1-2 of 2							
Back		Reset Statistics		Refresh			

Viewing SLA Alerts in the Dashboard

You can view the details of SLA alerts in the SLA Alerts tab of the dashboard. [Table 3-7](#) describes the dashboard for SLA alerts:

Table 3-7 ALSB Dashboard for SLA Alerts

Section	Description
SLA Alerts	<p>The pie chart shows the distribution of SLA alerts based on their severity for the duration set for alert history in the dashboard settings page. The severity level of alerts is user configurable and has no absolute meaning. For more information about alert severity, see Assigning Severity for Alerts.</p> <p>Click on a specific area in the pie chart to display the Extended SLA Alert History page for alerts for the chosen level of severity and alert history duration.</p>
Services With Most SLA Alerts	This section lists all the services with most SLA alerts in the current aggregation interval.
Alert History	This section gives details for all the SLA alerts generated during the alert history duration. For more information, see Viewing the Alert History for Pipeline Alerts .

Viewing the Alert History for SLA Alerts

The Alert History ([Figure 3-7](#)) for SLA alerts table shows all the SLA alerts, which have occurred in the alert history duration you have set in the User Preferences page. For more information about alert history table, see [Viewing SLA Alerts](#) in Monitoring in Using the AquaLogic Service Bus Console.

To view a complete list of alerts, click Extended Alert History. For more information about Extended Alert History, see [How to View or Delete SLA Alerts](#).

Viewing Pipeline Alerts in the Dashboard

You can view the pipeline alerts in the Pipeline Alerts tab of the dashboard (see [Figure 3-18](#)). [Table 3-8](#) describes the dashboard for pipeline alerts.

Figure 3-18 ALSB Dashboard for Pipeline Alerts

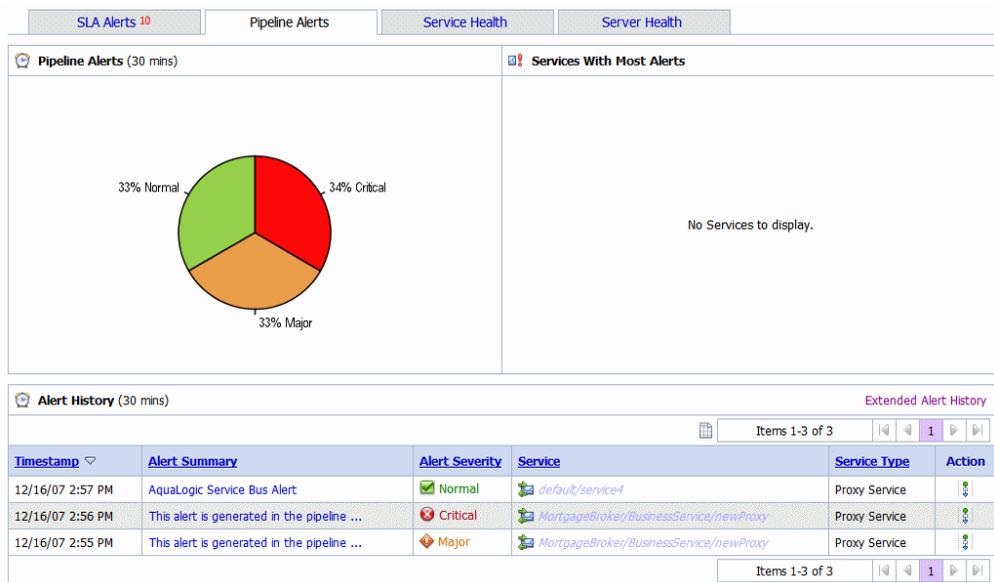


Table 3-8 Dashboard for Pipeline Alerts

Section	Description
Pipeline Alerts	<p>The pie chart shows the distribution of pipeline alerts based on their severity for the duration set for alert history in the dashboard settings page. The severity level of alerts is user configurable and has no absolute meaning. For more information about alert severity, see Assigning Severity for Alerts.</p> <p>Click on a specific area in the pie chart to display the Extended pipeline Alert History page for alerts for the chosen level of severity and alert history duration.</p>
Service With Most Alerts	This section lists all the services with most pipeline alerts in the current aggregation interval.
Alert History	This section gives details for all the pipeline alerts generated during the alert history duration. For more information, see Viewing the Alert History for Pipeline Alerts .

Viewing the Alert History for Pipeline Alerts

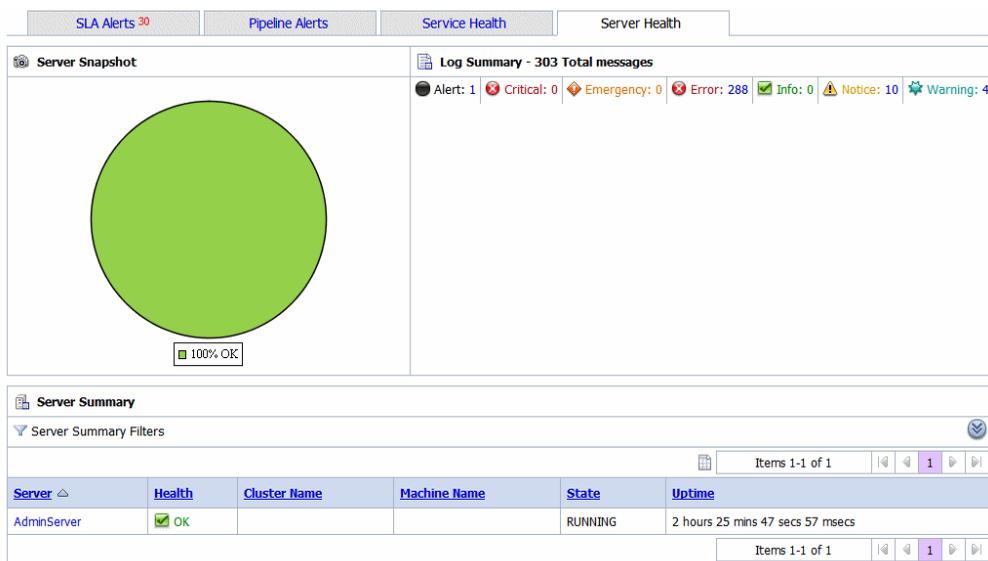
The Alert History (Figure 3-7) for pipeline alerts table shows all the pipeline alerts, which have occurred in the alert history duration you have set in the User Preferences page. For more information about Alert History table, see [Viewing Pipeline Alerts](#) in Monitoring in Using the AquaLogic Service Bus Console.

To view a complete list of alerts, click Extended Alert History. For more information about Extended Alert History, see [How to View or Delete Pipeline Alerts](#).

Viewing Server Health in the Dashboard

You can view the server summary in Server Health tab of the dashboard.

Figure 3-19 Server Health



Viewing Log Summary

The Log Summary section in the Server Health tab displays the summary log for the servers associated with the domain. The domain log file provides a central location from which to view the overall status of the domain. Each server instance forwards a subset of its messages to a domain-wide log file. By default, servers forward only messages of severity level Notice or higher. You can modify the set of messages that are forwarded. For more information, see

[Understanding WebLogic Logging Services](#) in Configuring Log Files and Filtering Log Messages.

If you configure the logging action in a pipeline, the log is forwarded to the admin server log. You can view the logging messages in the Server Health tab of the ALSB Console. In a cluster it is forwarded to the managed server. You cannot view the logging messages in the ALSB Console. Unless you configure WebLogic Server to forward these messages to the domain log, you cannot view this log from the ALSB Console. For information on how to do this, see [Create Log Filters](#) in the WebLogic Server Administration Console Online Help.

To see the number of messages currently raised by the system, click the View Log Summary link in the Server Summary panel. A table is displayed that contains the number of messages grouped by severity, as shown in [Figure 3-19](#).

You can view the log summary only if you possess administrator privileges in the WebLogic Server Console.

[Table 3-9](#) describes the status messages in the log summary.

Table 3-9 Log Summary Messages

Message	Description
Alert	This indicates that a particular service is in an unusable state while other parts of the system continue to function. Automatic recovery is not possible; immediate attention of the administrator is required to resolve the problem.
Critical	This indicates that a system or service error has occurred. The system can recover but there might be a momentary loss or permanent degradation of service.
Emergency	This indicates that the server is in an unusable state. This severity indicates a severe system failure.
Error	This indicates that a user error has occurred. The system or application can handle the error with no interruption. Limited degradation of service may occur.
Info	This reports normal operations; a low-level informational message.

Table 3-9 Log Summary Messages

Message	Description
Notice	This is an informational message with a higher level of importance than Info messages.
Warning	This indicates that a suspicious operation or configuration has occurred. However, normal operations may not be affected.

This display is based on the health state of the running servers, as defined by the WebLogic Diagnostic Service. For more information about the WebLogic Diagnostic Service, see [Configuring and Using the WebLogic Diagnostics Framework](#).

To view the domain log for a particular status of alert message, click the number corresponding with the status of alert message. shows an example of a domain log file displayed in the ALSB Console.

Figure 3-20 Domain Log File Entries

This page shows you the latest contents of the domain log file.

[Customize this table](#)

Domain Log File Entries

[Previous](#) | [Next](#)

View

	Date	Subsystem	Severity	Machine	Message ID	Message
<input type="radio"/>	Nov 23, 2006 9:50:29	WebLogicServer	Notice	svaidyan02	BEA-000365	Server state changed to RUNNING
<input type="radio"/>	Nov 23, 2006 9:50:29 AM IST	WebLogicServer	Notice	svaidyan02	BEA-000360	Server started in RUNNING mode

View

For more information about domain log file, see [Viewing Domain Log Files](#) in Monitoring in Using the AquaLogic Service Bus Console.

For more information, see Message Attributes in [Understanding WebLogic Logging Services](#) in Configuring Log Files and Filtering Log Messages.

To display details of a single log file on the page, select the appropriate log, then click the View. You can also customize the Domain Log File Entries table to view the following additional information:

- Machine
- Server
- Thread
- User ID
- Transaction ID
- Context ID
- Timestamp

For additional description of these information, see [Viewing Details of Server Log Files](#) in Monitoring in Using the AquaLogic Service Bus Console. For more information about how to customize the Domain Log File Entries table, see [Customizing Your View of Domain Log File Entries](#) in Monitoring in Using the AquaLogic Service Bus Console.

Viewing Server Summary

You can view the Server Summary in the Server Health tab of the dashboard. In a single node domain, the Server Summary displays the summary of the admin server. In a cluster domain, it displays the health of all the servers in a cluster, in case of a cluster environment. For more information on Server Summary, see [Viewing Server Information](#) in Monitoring in Using the AquaLogic Service Bus Console.

Viewing Server Details

You can access this page by clicking the name of a server under server summary or by clicking the name of a server in the Servers Summary page.

This page enables you to view more server monitoring details, as shown in [Figure 3-21](#).

Figure 3-21 Server Details Page—General

Settings for AdminServer		
General Channels Performance Threads Timers Workload Security JMS Control		
This page provides general runtime information about this server.		
State:	RUNNING	The current life cycle state of this server. More Info...
ActivationTime:	Thu May 31 09:17:39 IST 2007	The time when the server was started. More Info...
Weblogic Version:	WebLogic Server 10.0 Thu May 10 12:15:30 EDT 2007 933139	The version of this WebLogic Server instance (server). More Info...
Java Vendor:	Sun Microsystems Inc.	Returns the vendor of the JVM. More Info...
Java Version:	1.5.0_06	The Java version of the JVM. More Info...
OSName:	Windows XP	Returns the operating system on which the JVM is running. More Info...
OSVersion:	5.1	The version of the operating system on which the JVM is running. More Info...
JACC Enabled:	false	Indicates whether JACC (Java Authorization Contract for Containers) was enabled on the commandline for the jvm hosting this server More Info...

[Top](#)

The information displayed on this page is a subset of the Monitoring tab in the ALSB Console Server Settings page. [Table 3-10](#) describes the available information.

Table 3-10 Server Information

Information	Description
General	This provides general run-time information about the server. Click Advanced to view more information, such as WebLogic Server version or operating system name.
Channels	This provides monitoring information about each channel.
Performance	This provides information about the performance of the server.
Threads	This provides current run-time characteristics and statistics for the server’s active executable queues.
Timers	This provides information about the timer used by the server.
Workload	This provides statistics for work managers, constraints, and policies configured on the server.

Table 3-10 Server Information

Information	Description
Security	This statistics for work managers, constraints, and policies configured on the server.
JMS	This allows you to monitor JMS information about the server.
JTA	This provides the summary of all transaction information for all resource types on the server.

For more information, see [WebLogic Server Administration Console Online Help](#).

Monitoring ALSB at Run Time

Managing Operational Settings Using Smart Search

You can use the ALSB Smart Search utility for searching and managing resources such as proxy services, business services, alert rules for Service Level Agreements(SLA) violations, and alert destinations. You can use this utility to search for resources based on the various criteria regardless of your role in ALSB. For more information about tasks , which can be performed by each role ALSB, see [Roles in ALSB](#).

You can also use results of a search to change the operational settings at the service level. For effectively enabling or disabling any operational setting, you must enable or disable the setting both at the global level and the service level. For more information, see [How to Configure the Operational Settings for a Service](#).

You can access Smart Search from the Configuration module on the Operations navigator bar (see [Figure 4-1](#)).

Figure 4-1 Accessing Smart Search



There are the two levels of smart search available in ALSB—basic search and advanced search. Using basic search you can search using the following basic criteria—Type, Name, and Path. Using advanced search, you can use additional filters to customize your search for each type. The following sections describe:

- [Using Basic Search](#)
- [Using Advanced Search](#)
- [Managing Operational Settings for Proxy Services](#)
- [Managing Operational Settings for Business Services](#)
- [Managing Operational Settings for Alert Destinations](#)
- [Managing Operational Settings for SLA Alert Rules](#)

Using Basic Search

Basic Search helps you to search for resources using basic criteria such as resource type or the name of a resource. [Table 4-1](#) describes the basic criteria you can use with the search functionality.

Table 4-1 Criteria for Basic Search

Criteria	Usage
Type	<p>This search criterion is mandatory. Use the Type drop-down list (see Figure 4-2) to specify the type of resource. The drop-down list has the following options:</p> <ul style="list-style-type: none"> • All Services: Choose this type when you search for both proxy services and business services. • Proxy Services: Choose this type when you search for proxy services only. • Business Services: Choose this type when you search for business services only. • Alert Destinations: Choose this type when you search for alert destinations. • SLA Alert Rules: Choose this type when you search for SLA alert rules. <p>Note: To view all the resources of a given type, choose the resource type in the Type drop-down list and click View All.</p>
Name	Optional. Enter the name of specific resource you want to find.
Path	Optional. Enter a path in the Path field to specify a location (path) of the resource.

You can use any one or a combination of these criteria (see [Figure 4-2](#)).

Figure 4-2 Basic Smart Search

The screenshot shows a 'Smart Search' interface. At the top left is a magnifying glass icon and the text 'Smart Search'. Below this is a form with three rows: 'Type' with a dropdown menu set to 'All Services', 'Name' with an empty text input field, and 'Path' with an empty text input field. Below the form is a section for 'Type-based Filters: All Services' with a checkmark icon. At the bottom are two buttons: 'Search' and 'View All'.

Using Advanced Search

Use the advanced search if you want to configure your search with additional criteria. To use these filters, click Open Advanced Search Filters icon. The following sections describe the usage of advanced search filters in smart search functionality to manage operational settings.

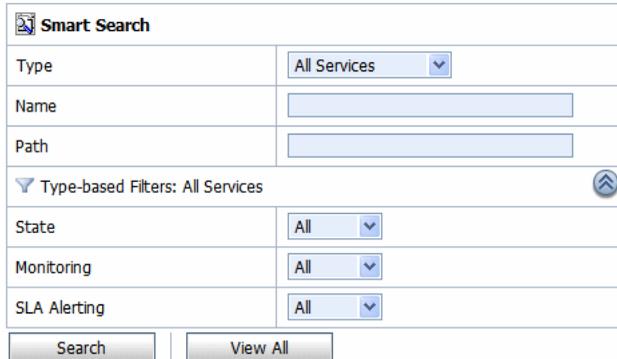
Managing Operational Settings for All Services

You can search for proxy services and business services in the ALSB Console using filters in Smart Search. This section describes finding, viewing, and editing proxy services and business services.

Finding Services Using Search Filters

Figure 4-3 shows the filters you can use to search for All Services.

Figure 4-3 Type Based Filters: All Services



The screenshot shows the 'Smart Search' interface. At the top, there is a search icon and the text 'Smart Search'. Below this, there are three input fields: 'Type' with a dropdown menu set to 'All Services', 'Name' with an empty text box, and 'Path' with an empty text box. Underneath these is a section titled 'Type-based Filters: All Services' with a collapse icon on the right. This section contains three dropdown menus: 'State' set to 'All', 'Monitoring' set to 'All', and 'SLA Alerting' set to 'All'. At the bottom of the form, there are two buttons: 'Search' and 'View All'.

Table 4-2 describes the usage advanced filters to customize your search for both proxy services and business services.

Table 4-2 Using Advanced Filters to Find Proxy Services and Business Services

Filter	Usage
Service State	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
Service Monitoring	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter
Service SLA Alerting	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.

Click Search to find all services using the set criteria or click View All to view all the services.

Viewing and Editing Operational Settings

You can view results of the search for proxy service and business service in the Summary of All Services table (see [Figure 4-4](#)).

Use this table to enable or disable services, monitoring, and SLA alerting functionality for both business service and proxy services. You can also use this to enable or disable pipeline alerting functionality, message reporting, tracing, and pipeline logging for proxy services. To enable or disable select the check box in the appropriate field and click Update. The run-time effects of these settings also depend on corresponding settings at the global level. For more information about Global Settings, see [How to Configure the Operational Settings at the Global Level](#). You can update the information for one or more services concurrently using this table.

Figure 4-4 Summary of All Services

Summary of All Services										
Name	Path	Type	State	Monitoring	SLA Alerting	Pipeline Alerting	Reporting	Logging	Tracing	Actions
AddCustomerService	ALSR Project	Business Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled (0)					
ALSRBS	ALSR Project	Business Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled (0)					
alvProxy	ALSR Project	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled	
DS2	ALSR Project	Business Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled (0)					
CustomerNotificationService	ALSR Project	Business Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled (0)					
foo	ALSR Project	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled (0)	<input type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled	
foo1	ALSR Project	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled (0)	<input type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (0)	<input checked="" type="checkbox"/> Enabled	

Items 1-7 of 7

Update Reset

The following information is displayed for all services:

Table 4-3 Understanding Summary of All Services

Property	Description
Name	The name assigned to the service. The name is a link to the View Proxy Service page for proxy services or View Business Services page for business services.
Path	The project associated with the service. If the service resides in a project folder, this folder is also listed. The path is displayed in the format: project-name/root-folder/ . . ./parent-folder The path is a link to the corresponding path in the Project Explorer.
Type	The type of the parent service: proxy service or business service.
State	The state of the service—Enabled or Disabled.
Monitoring	The monitoring status of the service—Enabled or Disabled.
SLA Alerting	The SLA alerting status. Enabled or Disabled, and the level enabled at and above: <ul style="list-style-type: none"> • Normal (N) • Warning (W) • Minor (Mn) • Major (Mj) • Critical (C) • Fatal (F)
Pipeline Alerting	For proxy services only. The pipeline alerting status—Enabled or Disabled, and the level enabled at and above: <ul style="list-style-type: none"> • Normal (N) • Warning (W) • Minor (Mn) • Major (Mj) • Critical (C) • Fatal (F)

Table 4-3 Understanding Summary of All Services

Property	Description
Reporting	For proxy services only. The message reporting status of the service: Enabled or Disabled.
Logging	For proxy services only. The logging status—Enabled or Disabled, and the severity level at which it is enabled—Debug (D), Info (I), Warning (W), or Error (E).
Tracing	For proxy services only. The tracing status—Enabled or Disabled
Actions	For proxy services: The View Message Flow icon is a link to the pipeline for that proxy service.

Click Reset to discard any changes in the summary table and refresh the page with currently stored settings.

Note: You can edit the operational settings depending on the privileges of your role. For more information about roles, see [Chapter 2, “Roles in ALSB.”](#)

Managing Operational Settings for Proxy Services

You can search for proxy services in the ALSB Console using filters in Smart Search. This section describes finding, viewing, and editing proxy services.

Finding Proxy Services Using Search Filters

[Figure 4-5](#) shows the different types of filters you can use for Proxy Services.

Figure 4-5 Type Based Filters: Proxy Services

The screenshot shows a 'Smart Search' interface. At the top, there's a search bar with a magnifying glass icon and the text 'Smart Search'. Below this are three input fields: 'Type' (a dropdown menu currently showing 'Proxy Services'), 'Name' (a text input field), and 'Path' (a text input field). Underneath these is a section titled 'Type-based Filters: Proxy Services' with a collapse icon on the right. This section contains seven rows, each with a filter name and a dropdown menu: 'State' (All), 'Monitoring' (All), 'SLA Alerting' (All), 'Pipeline Alerting' (All), 'Reporting' (All), 'Logging' (All), and 'Tracing' (All). At the bottom of the form are two buttons: 'Search' and 'View All'.

Table 4-4 describes advanced filters to customize your search for proxy services.

Table 4-4 Using Advanced Filters to Search for Proxy Services

Filter	Usage
State	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
Monitoring	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
SLA Alerting	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
Pipeline Alerting	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
Reporting	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.

Table 4-4 Using Advanced Filters to Search for Proxy Services

Filter	Usage
Logging	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
Tracing	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.

Click Search to find all proxy services using the set criteria or click View All to view all the services.

Viewing and Editing Operational Settings

You can view results of the search for proxy service in the Summary of Proxy Services table (see [Figure 4-6](#))

Figure 4-6 Summary of Proxy Services

Name	Path	Type	State	Monitoring	SLA Alerting	Pipeline Alerting	Reporting	Logging	Tracing	Actions
newP	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	
sampleWSDLProxy	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	
xqueryProxyService	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	
xyz	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	

The Summary of Proxy Services view displays State, Monitoring, SLA Alerting, Pipeline Alerting, Reporting, Logging, Tracing, Path, Type, Name, and Actions. For more information about the fields displayed in the summary of proxy services, see [Viewing and Editing Operational Settings](#).

Use this table to enable or disable proxy services, monitoring, and SLA alerting, pipeline alerting, message reporting, tracing, and pipeline logging. To enable or disable click the check box in the appropriate field and click Update. The run time effects of these settings also depend on corresponding settings at the global level. For more information about Global Settings, see [How to Configure the Operational Settings at the Global Level](#). You can update the information for one or more proxy services concurrently using this table.

Click Reset to discard any changes in the summary table and refresh the page with currently stored settings.

Note: You can edit the pipeline message flow depending on the privileges of your role. For more information about roles, see [Chapter 2, “Roles in ALSB.”](#)

Managing Operational Settings for Business Services

You can search for business services in the ALSB Console using filters in Smart Search. This section describes finding, viewing, and editing business services.

Finding Business Services Using Search Filters

[Figure 4-7](#) shows the different types of filters you can use for Business Services.

Figure 4-7 Type Based Filters: Business Services

Smart Search	
Type	Business Services
Name	<input type="text"/>
Path	<input type="text"/>
Type-based Filters: Business Services	
State	All
Monitoring	All
SLA Alerting	All
<input type="button" value="Search"/> <input type="button" value="View All"/>	

[Table 4-5](#) describes the filters you can use to customize your search for business services.

Table 4-5 Using Advanced filters to Search for Business Services

Filters	Usage
Service State	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.

Table 4-5 Using Advanced filters to Search for Business Services

Filters	Usage
Service Monitoring	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.
Service SLA Alerting	Choose Enabled or Disabled from the drop-down list. Choose All to ignore this filter.

Click Search to find all services using the set criteria or click View All to view all the services.

Viewing and Editing Operational Settings

You can view results of the search for business service in the Summary of Business Services table (see [Figure 4-8](#)).

Figure 4-8 Summary of Business Services

Summary of Business Services					
Name	Path	Type	<input checked="" type="checkbox"/> State	<input type="checkbox"/> Monitoring	<input checked="" type="checkbox"/> SLA Alerting
alsrBSAP	default	Business Service	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)
B	default	Business Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)
HttpOutbound	default	Business Service	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)

Items 1-3 of 3

Update | Reset

The Summary of Business Services view displays State, Monitoring, SLA Alerting, Name, Path, and Type. For more information about the fields displayed in the summary of business services, see [Viewing and Editing Operational Settings](#).

Use this table to enable or disable services, monitoring, and SLA alerting. To enable or disable, select the check box in the appropriate field and click Update. The run time effects of these settings also depend on corresponding settings at the global level. For more information about Global Settings, see [How to Configure the Operational Settings at the Global Level](#). You can update the information for one or more business services concurrently using this table.

Click Reset to discard any changes in the summary table and refresh the page with currently stored settings.

Note: You can edit the operational settings for a business service depending on the privileges of your role. For more information about roles, see [Chapter 2, “Roles in ALSB”](#).

Managing Operational Settings for Alert Destinations

You can search for alert destinations in the ALSB Console using advanced filters in Smart Search. You can view and delete alert destinations using smart search.

Finding Alert Destinations using Search Filters

[Figure 4-9](#) shows the different types of filters you can use to search for Alert Destinations.

Figure 4-9 Type Based Filters: Alert Destinations

Smart Search	
Type	Alert Destinations ▾
Name	<input type="text"/>
Path	<input type="text"/>
Type-based Filters: Alert Destinations ⌵	
Target	<div style="border: 1px solid gray; padding: 2px;">SNMP Trap Reporting e-mail JMS</div>
Search Pattern (Any String)	<input type="text"/>
<input type="button" value="Search"/> <input type="button" value="View All"/>	

[Table 4-6](#) describes the filters you can use to customize your search for alert destinations.

Table 4-6 Using Advanced Filters to Search for Alert destinations

Filter	Usage
Target	<p>You can choose from one of the following options:</p> <ul style="list-style-type: none"> • SNMP Trap • Reporting • E-mail • JMS <p>Only alert destinations with at least one of the selected targets are displayed. By default Target filter is not applied.</p>
Search Pattern	<p>The system uses the string to search all the Description fields of the Alert Destinations, as well as the specific detailed fields of the e-mail and JMS destinations. If the string appears in any of the Alert Destination fields, the Alert Destinations matching the search criteria are displayed.</p> <p>Click Search to find all alert destinations using the set criteria or click View All to view all the alert destinations. For more information about alert destinations, see What are Alert Destinations?</p>

Viewing and Deleting Alert Destinations

You can view results of the search for alert destinations in the Summary of Alert Destinations table (see [Figure 4-10](#)).

Figure 4-10 Summary of Alert Destinations

<input type="checkbox"/>	Name <small>▲</small>	Path	Options
<input type="checkbox"/>	! NewalertDest	default	
<input type="checkbox"/>	! newAlertDestination	default	
<input type="checkbox"/>	! TestAlert	default	
<input type="checkbox"/>	! testdestination	MortgageBroker/BusinessService	
<input type="checkbox"/>	! Unassigned	default	

Items 1-5 of 5 | Page 1

Delete

Table 4-7 describes the information is provided in the Summary of Alert Destination table.

Table 4-7 Summary of Alert Destination

Column Name	Description
Name	This displays the names of the alert destinations that satisfy the search criteria.
Path	This displays the location of the resource in the ALSB domain.
Options	This displays the actions that can be performed on the alert destination. You can delete an alert destination from this field.

You can delete one or more alert destination concurrently using this table. To delete an alert destination click the check box associated with the alert destination and click Delete.

Notes:

- To create an alert destination click the path to view the corresponding project folder. Select Alert Destination in Create Resource to create a new alert destination.
- To reconfigure or view the details of an alert destination click the alert destination to go to the Alert destination configuration page.

Managing Operational Settings for SLA Alert Rules

You can search for SLA alert rules in the ALSB Console using additional filters in Smart Search. This section describes finding, viewing, and configuring alert rules using smart search.

Finding SLA Alert Rules Using Search Filters

Figure 4-11 shows the different types of filters you can use when you search for SLA alert rules.

Figure 4-11 Type based Filters: SLA Alerts

Smart Search	
Type	SLA Alerts
Name	<input type="text"/>
Path	<input type="text"/>
Type-based Filters: SLA Alerts	
Parent Service	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Clear"/>
Service Type	All Services
Rule State	All
Severity	Normal <input checked="" type="checkbox"/> or above
<input type="button" value="Search"/> <input type="button" value="View All"/>	

Table 4-8 describes the filters you can use to customize your search for SLA ALert Rules:

Table 4-8 Using Advanced Filters to Search for SLA Alert Rules

Filters	Usage
Parent Service	You can base the search for SLA alert rules on the proxy service or business service associated with the SLA alert rule. Use this filter to override the path specified in the basic search.
Service Type	<p>You can specify the type of the parent service criterion. The parent service can be one of the following options:</p> <ul style="list-style-type: none"> • All Services: The parent service is either a proxy service or a business service. • Proxy Services • Business Service <p>Note: When you specify the value for Service Type, Parent Service is reset.</p>
Rule State	<p>You can customize the search based on the state of the SLA alert rule. The SLA alert rule can be in either of the following states:</p> <ul style="list-style-type: none"> • Enabled: Use this to search for all the SLA alert rules that are enabled. • Disabled: Use this to search for all the SLA alert rules that are disabled. <p>Choose All to ignore this filter.</p>
Severity	You can customize the search based on the severity of the SLA alerts. To do so, set the level of severity in the Severity drop-down list.

Click Search to find all services using the set criteria or click View All to view all the services.

Note: Select the **or above** check box to restrict your search to the specified severity level or above (listed from the most inclusive to the most restrictive level): Normal, Warning, Minor, Major, Critical, and Fatal. For example, to search for alert rules with severity levels equal to Major, Critical, and Fatal set severity equal to Major and click the check box associated with **or above**.

Viewing and Configuring SLA Alert Rules

You can view results of the search for SLA alert rules in the SLA Alert Rules table (see [Figure 4-12](#)). You can update the information for one or more alert rule concurrently using this table. To enable or disable the alert rule select the associated check box and click Update.

Click Reset to discard any changes in the summary table and refresh the page with currently stored settings.

Figure 4-12 SLA Alert Rules

Name	SLA State	Service Name	Path	Severity	Aggr. Interval	Expiration Date	Frequency
binaryAlertRule	<input checked="" type="checkbox"/> Enabled	binarymfttest	default	Critical	0 hr(s) 10 mins	Never Expires	Every Time
LSR	<input checked="" type="checkbox"/> Enabled	loanSaleProcessor	MortgageBroker/BusinessServices	Warning	0 hr(s) 1 mins	Never Expires	Every Time
newbsRule	<input checked="" type="checkbox"/> Enabled	normalLoanBS	MortgageBroker/BusinessService	Fatal	0 hr(s) 10 mins	Never Expires	Every Time
NewBSRule1	<input checked="" type="checkbox"/> Enabled	AddCustomerService	ALSR Project	Major	0 hr(s) 10 mins	Never Expires	Every Time
newBSRule	<input checked="" type="checkbox"/> Enabled	managerLoanApproval	MortgageBroker/BusinessService	Minor	0 hr(s) 10 mins	Never Expires	Every Time
newrule10	<input checked="" type="checkbox"/> Enabled	mftProxy	default	Warning	0 hr(s) 1 mins	Never Expires	Every Time
newRule12	<input checked="" type="checkbox"/> Enabled	New	default	Major	0 hr(s) 10 mins	Never Expires	Every Time
rule	<input checked="" type="checkbox"/> Enabled	service4	default	Minor	0 hr(s) 1 mins	Never Expires	Every Time

The following information is displayed in the SLA Alert Rules Summary table:

Table 4-9 SLA Alert Summary Table

Property	Description
Name	The name of the alert rule. Click the name to go to the View Alert Rule Details page. For more information, see How to Lookup or Edit Existing Alert Rules .
SLA State	The status of the alert rule: Enabled or Disabled.
Description	Note: This field is hidden by default. A description of the alert rule.
Service Name	The name of the parent service. The name is a link to the Operational Settings page.

Table 4-9 SLA Alert Summary Table

Property	Description
Path	<p>The project associated with the parent service of the alert rule. If the parent service of the alert rule resides in a project folder, this folder is also listed. The path is displayed in the format:</p> <p>project-name/root-folder/ . . ./parent-folder</p> <p>The path is a link to the corresponding path in the Project Explorer.</p>
Severity	<p>The severity of the alert that is triggered by this rule: Normal, Warning, Minor, Major, Critical, or Fatal.</p>
Aggr Interval	<p>The aggregation interval in terms of hours and minutes.</p>
Expiration Date	<p>The date when this alert rule is no longer in effect.</p>
Stop Processing	<p>Displays Yes or No.</p> <p>Note: This field is hidden by default.</p>
Frequency	<p>The frequency of this alert:</p> <ul style="list-style-type: none"> • Every Time • Notify Once

Note: You can enable or disable an alert rule depending on the privileges of your role. For more information about roles, see [Chapter 2, “Roles in ALSB.”](#) For more information about enabling and disabling alert rules, see [How to Configure the Operational Settings for a Service.](#)

Reporting

ALSB delivers message data and alerts to one or more reporting providers. Message data can be captured from the body of the message and from other variables associated with the message, such as header or inbound variables. Alert data contains information about Service Level Agreement (SLA) violations that you can configure to monitor proxy services. You can use the message or alert data delivered to the reporting provider for functions such as tracking messages or regulatory auditing.

ALSB includes a JMS reporting provider for message reporting. The Reporting module in the ALSB Console displays the information captured from this reporting provider. If you do not wish to use the JMS Reporting Provider that is provided with your ALSB installation, you can untarget it and create your own reporting provider using the Reporting Service Provider Interface (SPI). If you configure your own reporting provider for messages, no information is displayed in the ALSB Console. You must create your own user interface. To capture SLA data, you must create a reporting provider for alerts.

This chapter contains information about following topics

- [About the ALSB Reporting Framework](#)
- [About the JMS Reporting Provider](#)
- [How to Enable Message Reporting](#)
- [How to Stop a Reporting Provider](#)
- [How to Untarget a JMS Reporting Provider](#)
- [Using the Reporting Module in the ALSB Console](#)

About the ALSB Reporting Framework

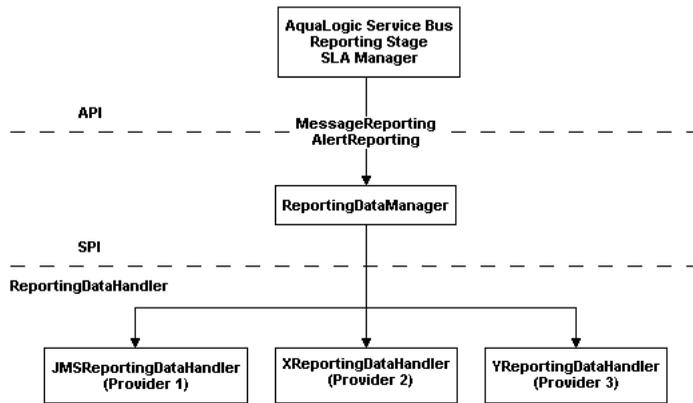
ALSB contains an extensible framework for creating one or more reporting providers for messages or alerts.

To enable message reporting you must first create a Report action in the message flow for the proxy service. The Report action allows you to extract information from each message and write it to the ALSB Reporting Data Stream. You do not need to configure a report action for alert reporting. Alert data is always available in the Reporting Data Stream. For more information, see [How to Enable Message Reporting](#).

Information you need for creating your own reporting provider is located in `com.bea.wli.reporting` in the [Javadoc for AquaLogic Service Bus](#). The Javadoc provides information about what you need to do for implementing a reporting provider, including how to package it, where it goes, how to deploy it, and the order of deployment. The reporting schema is `MessageReporting.xsd`, located in `ALSB_HOME/lib/common/reporting-api.jar`.

Figure 5-1 shows the reporting framework.

Figure 5-1 Reporting Framework



As shown in the [Figure 5-1](#), both report messages and alerts are exported to reporting data streams. In the Report stage, information is extracted by the Report action from each message and written to the Reporting Data Stream with metadata that adheres to `MessageReporting.xsd`. Similarly, the SLA Manager uses Reporting Data Manager APIs to write to the Alert Reporting Stream with metadata that adheres to the `AlertReporting.xsd`. To develop a reporting provider for alerts or your own message reporting provider, you need to implement `ReportingDataHandler` interface and use the `ReportingDataManager` class.

The `ReportingDataHandler` interface takes the reporting or alert data stream and processes it. It can either process or store a stream, or do both in a relational database, file, JMS queue, and so on. Depending on which stream you want to use, you need to implement the appropriate handle methods to process the data stream:

- Message Reporting Stream—the Report action of ALSB run time uses the following two handle methods to write to the Message Reporting Stream:

```
handle(com.bea.xml.XmlObject metadata, String s)
```

```
handle(com.bea.xml.XmlObject metadata, com.bea.xml.XmlObject data)
```

- Alert Reporting Stream—the Alert Manager uses the following `handle` method to write to the Alert Reporting Stream:

```
handle(com.bea.xml.XmlObject metadata, com.bea.xml.XmlObject data)
```

The `ReportingDataManager` is a local server object that keeps a registry of reporting providers. Reporting providers implement the `ReportingDataHandler` interface. The `ReportingDataManager` provides operations to:

- Add and remove reporting data handlers.
- Export reporting data stream using various handle operations.

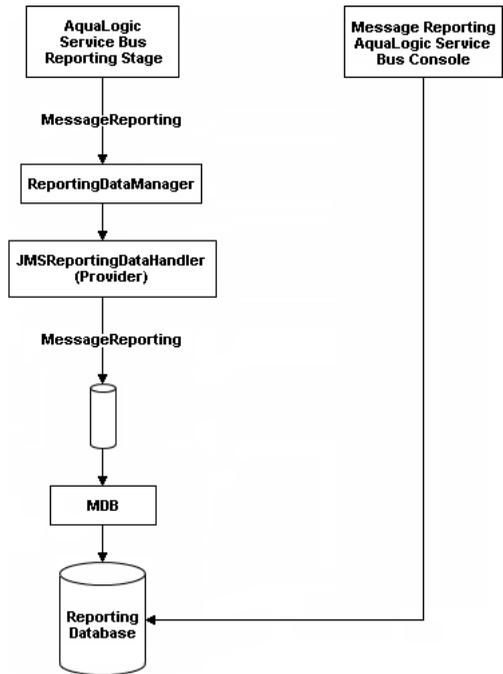
About the JMS Reporting Provider

The JMS Reporting Provider provides a pluggable architecture to capture the reporting information from each message using a Report action. The default JMS Reporting Provider is automatically configured when you create an ALSB domain. All messages across the cluster are aggregated and stored in a JMS Reporting Provider Data Store in a database specific format. This provider displays information from the JMS Reporting Provider Data Store.

Note: If you do not wish to use this reporting provider, you must untarget it. For more information, see [How to Untarget a JMS Reporting Provider](#).

The JMS Reporting Provider consists of a producer and a consumer, which are decoupled to improve scalability. The producer is a JMS producer and the Message Driven Bean (MDB) acts as the JMS consumer, as shown in [Figure 5-2](#).

Figure 5-2 JMS Reporting Provider



The Reporting stage contains the Report actions that collect the reporting information and dispatch the reporting stream to JMS Reporting Provider through various handle operations in the ReportingDataManager. The JMSReportingDataHandler is the JMS producer of the reporting provider. The JMSReportingDataHandler takes the reporting stream and logs the information to a JMS queue. The MDB listens to the JMS reporting queue, which processes the message asynchronously and stores the data in the JMS Reporting Provider Data Store.

How to Enable Message Reporting

To receive report messages from either the JMS Reporting Provider, which is provided with ALSB installation, or your reporting provider, you must first create a Report action in the message flow for the proxy service. The Report action allows you to extract information from each message and write it to the ALSB Reporting Data Stream. In the Report action, you must specify the information you want to extract from the message and add to the ALSB Reporting Data Stream.

You need not to configure a Report action for alert reporting. Alert data are always available in the Reporting Data Stream.

When configuring a Report action, use key values to extract key identifiers from the message. You can configure multiple keys. Information can be captured not only from the body of the message but any other variable associated with the message, such as header or inbound variables. For more information about message variables, see [Message Context](#) in AquaLogic Service Bus User Guide.

You can use any XML elements as a key:

```
<?xml version="1.0" encoding="utf-8"?>
  <poIncoming>
    <areacode>408</areacode>
    <item-quantity>100</item-quantity>
    <item-code>ABC</item-code>
    <item-description>Medicine</item-description>
  </poIncoming>
```

For example, you can specify the key as the itemcode, the value as `./item-code` (an XPath expression), and the variable as message body (body), as shown in [Figure 5-3](#).

Figure 5-3 Key Name and Value

 Report `$body` with search keys:

Key Name	Key Value	Options
 itemCode	<code>./itemCode</code> in variable <code>body</code>	

If you are using the default JMS Reporting Provider, the keys and associated values are displayed in the Report Index column of the Summary of Messages table. If you configure multiple keys, the key-value pairs are displayed in the Report Index column with each key-value separated by a comma, as shown in [Figure 5-4](#).

Figure 5-4 Keys and Associated Values Display

Report Index	DB TimeStamp	Inbound Service	Error Code
errorCode= BEA-382505	12/14/07 9:09 AM	default/service3	BEA-380525
errorCode= BEA-382505	12/14/07 9:09 AM	default/service3	BEA-380525

For information about creating a Report action or on how to view the Summary of Messages page, see the following in Using the AquaLogic Service Bus Console:

- Report in [Proxy Services: Actions](#).
- Listing and Locating Messages in [Reporting](#).

How to Stop a Reporting Provider

If you wish to stop a reporting provider when the server is running in the ALSB domain, do the following:

1. Start the WebLogic Server Administration Console. For more information, see Starting the Administration Console in [Overview of the Administration Console](#) in Introduction to WebLogic Server and WebLogic Express.
2. After logging into the WebLogic Server Administration Console, in the Domain Structure, click Deployments. The Summary of Deployments page is displayed.
3. In the Deployments table, select the check box next to the reporting provider you wish to stop.

Figure 5-5 Stopping a Reporting Provider

Summary of Deployments

Control **Monitoring**

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

[Customize this table](#)

Deployments

Install Update Delete Start Stop

Showing 31 - 40 of 81 Previous Next

<input type="checkbox"/>	Name	State	Type	Deployment Order
<input type="checkbox"/>	emailtransport-I10n(2.5,2.5)	Active	Library	152
<input type="checkbox"/>	File Transport Provider	Active	Enterprise Application	155
<input type="checkbox"/>	filetransport-I10n(2.5,2.5)	Active	Library	154
<input type="checkbox"/>	FLOW Transport Provider	Active	Enterprise Application	175
<input type="checkbox"/>	Ftp Transport Provider	Active	Enterprise Application	151
<input type="checkbox"/>	ftpttransport-I10n(2.5,2.5)	Active	Library	150
<input checked="" type="checkbox"/>	JMS Reporting Provider	Active	Enterprise Application	125
<input type="checkbox"/>	JPD Transport Provider	Active	Enterprise Application	168
<input type="checkbox"/>	jpgdtransport-I10n(1.0,1.0)	Active	Library	167
<input type="checkbox"/>	jsf-myfaces(1.1,1.1.1)	Active	Library	1

Install Update Delete Start Stop

Showing 31 - 40 of 81 Previous Next

- Click Stop and after the list is displayed, choose the appropriate command.
- After the Stop Application Assistant page is displayed, click Yes. The Deployments table shows that the state of the reporting provider is now Prepared.

How to Untarget a JMS Reporting Provider

If you do not wish to use the default JMS reporting provider or any reporting provider, you must untarget it.

Note: If no reporting provider exists, you can still define a Report action. However, no data is be written.

How to Untarget the JMS Reporting Provider when the Server is Running

To untarget a reporting provider when the server is running in the ALSB domain, do the following:

1. Start the WebLogic Server Administration Console. For more information, see Starting the Administration Console in [Overview of the Administration Console](#) in Introduction to WebLogic Server and WebLogic Express.
2. After logging into the WebLogic Server Administration Console, in the Change Center, click Lock & Edit.
3. From the left panel, under Domain Structure, click Deployments. The Summary of Deployments page is displayed.
4. In the Deployments table, click the reporting provider you wish to untarget. The Settings page for the Reporting Provider is displayed.
5. Click the Targets tab.
6. Clear the appropriate check box.

Figure 5-6 Untargeting a Reporting Provider



7. Click Save. A message is displayed indicating that the settings have been successfully updated.
8. After you untarget the reporting provider, untarget the data source used by the reporting provider, as follows:

Note: This step is only required for reporting providers that use their own data sources. To untarget the default JMS reporting provider in ALSB installation you must perform the following steps.

- a. In the left panel, under Domain Structure, select Services > JDBC > Data Sources.
- b. In the Summary of JDBC Data Source page, click the name of the data source you wish to untarget. The Settings page for the data source is displayed.
- c. Click the Targets tab.
- d. Clear the appropriate check box.
- e. Click Save. A message is displayed indicating that the settings have been successfully updated.
- f. To activate the changes, in the Change Center, click Activate Changes.

How to Untarget the JMS Reporting Provider When Server Not Running

If the server is not running in the ALSB domain, you can use the WebLogic Scripting Tool (WLST) to remove the JMS Reporting Provider from the ALSB domain. For more information about WLST, see [WebLogic Scripting Tool](#) in the WebLogic Server documentation.

To untarget a reporting provider, complete the following steps:

1. If you have not already set up your environment to use WLST, see “Main Steps for Using WLST” in [Using the WebLogic Scripting Tool](#) in WebLogic Scripting Tool.

2. Invoke WLST Offline.

```
C:>java com.bea.plateng.domain.script.jython.WLST_offline
```

3. To read the domain that was created using the Configuration Wizard execute:

```
wls:/offline>readDomain("C:/bea/user_projects/domains/base_domain")
```

4. To untarget the reporting provider data source execute:

```
wls:/offline/base_domain>unassign("JdbcSystemResource",
"wlslbjmsrpdDataSource", "Target", "AdminServer")
```

5. To the reporting provider application execute:

```
wls:/offline/base_domain>unassign("AppDeployment", "JMS Reporting
Provider", "Target", "AdminServer")
```

- To update the domain execute:

```
wls:/offline/base_domain>updateDomain()
```

- To close the domain execute:

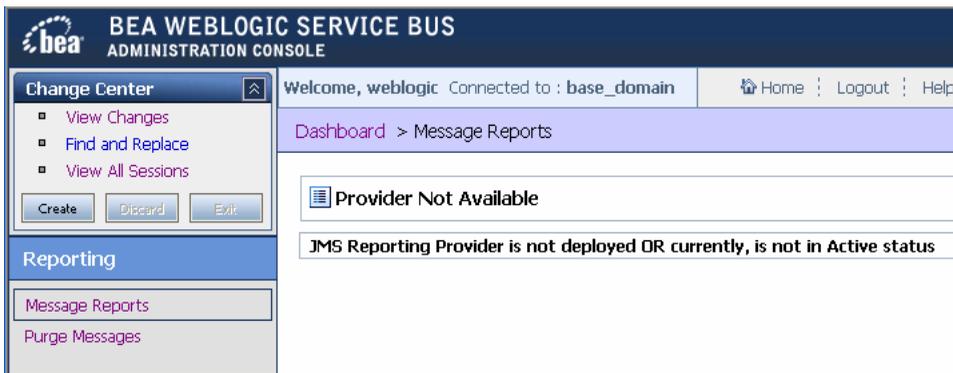
```
wls:/offline/base_domain>closeDomain()
```

- Exit from the WLST command prompt execute:

```
wls:/offline>exit()
```

After the ALSB JMS reporting provider is untargeted, the Reporting module in the ALSB Console indicates that the reporting provider is not deployed, as shown [Figure 5-7](#).

Figure 5-7 Reporting Provider Not Deployed



Note: In a cluster, the JMS Reporting Provider is targeted to Cluster. Therefore in a cluster, to view and purge messages, you must configure at least one managed server to run with the Administration server. If no managed servers are running, the ALSB Console displays the message shown in [Figure 5-7](#).

Using the Reporting Module in the ALSB Console

The reporting module in the ALSB Console displays the information collected by the JMS Reporting Provider Data Store. The first page of the Reporting module, called the Summary of Messages, displays a table containing the extracted information and other information, such as the time the message was written to the database and the service with which the message is associated. You can customize the display of information on this page by filtering and sorting the data. You can also drill down to view detailed information about specific messages, including error information.

The Reporting module provides a purge function to help you manage your message data. You can purge all of the messages from the reporting datastore or base the purge on a time-range.

The JMS Reporting Provider Data Store requires a database. An evaluation version of the PointBase database is installed with WebLogic Server. You can use PointBase for a development environment but not for production. ALSB also supports databases from other vendors. Be sure to apply standard database administration practices to the database hosting the JMS Reporting Provider Data Store. For more information, see [How to Configure a Database for the JMS Reporting Provider Store](#).

For more information about the reporting module, see [Reporting](#) in *Using the AquaLogic Service Bus Console*.

Viewing the Summary of Message Reports

When you click Message Reports in the Reporting module of the Operations navigation bar, the Summary of Messages page is displayed. This page contains a table that provides a list of report messages sorted by the database timestamp.

Figure 5-8 Summary of Messages

Report Index	DB TimeStamp	Inbound Service	Error Code
errorCode= BEA-382505	12/13/07 3:48 PM	default/service3	BEA-380525
errorCode= BEA-382505	12/13/07 3:32 PM	default/service3	BEA-380525
errorCode= BEA-382505	12/13/07 3:30 PM	default/service3	BEA-380525

If the messages are not filtered, the Summary of Messages table displays up to 100 of the latest messages based on the database timestamp. If you filter the messages, up to 1000 messages are displayed.

Note: The filter is not reset automatically. The filter remains in effect until you update it or reset it.

[Table 5-1](#) describes the information in the Summary of Message Reports.

Table 5-1 Summary of Message Reports

Column Name	Description
Report Index	Displays the key-value pairs extracted from the message context variables or the message payload. For more information, see About the JMS Reporting Provider
DB TimeStamp	Displays the time when the message was written to the database.
Inbound Service	Displays the inbound service associated with the message. Click the name of the service to go to View a Proxy Service page.
Error Code	Displays the error code associated with this message, if it exists. For more information about error codes, see Error Messages and Handling in Proxy Services: Error Handlers in Using the AquaLogic Service Bus Console.

To search for specific messages, click Filter in the Summary of Messages Table to filter the display of messages. The available filtering is shown in [Figure 5-9](#).

Figure 5-9 Summary of Messages Search

The screenshot shows a web interface titled "Summary of Message Reports" with a "Purge Messages" link in the top right. Below the title is a "Message Reports Filters" section with a collapse icon. The "Date Range" section has three radio button options: "All", "Message From" (with date and time pickers), and "for the last" (with input fields for days, hours, and minutes). Below this are three text input fields for "Inbound Service Name", "Error Code", and "Report Index" (with a note to separate multiple indexes with commas). At the bottom are "Search" and "View All" buttons.

As shown in [Figure 5-9](#), you can filter report messages for a specified period of time, by the name of a service, by error code, and by report index. After you filter the messages, the title of the page changes to Summary of Filtered Messages. For information about using the Summary of Messages filter, see [Listing and Locating Messages in Reporting](#) in Using the AquaLogic Service Bus Console.

To view more information about a report message, click the name of the message in the Report Index column. The View Message Details page is displayed.

Viewing Message Details

The View Message Details page displays complete information about the report messages, as shown in [Figure 5-10](#).

Figure 5-10 Report Message Detail Page

View Message Details	
General Configuration	
Message ID	uuid:e5ef14028f46333b:512cc00a:116d18f26dc-7aa3
Database Timestamp	Thursday, December 13, 2007 3:48:16 PM IST
Time at point of Logging	Thursday, December 13, 2007 3:48:16 PM IST
Server Name	AdminServer
State	ERROR
Node Name	
Pipeline Name	
Stage Name	
Inbound Service	
Name	default/service3
URI	/service3
Operation	
Outbound Service	
Name	
URI	
Operation	
Report Index	
Report Index Text	errorCode=
Fault	
Error Code	BEA-380525
Reason	There is a error
Detail	
Report Body	
Detail	Detail

[Table 5-2](#) describes the information displayed in Report Message Detail Page.

Table 5-2 Message Information

Category	Message Information	Description
General Configuration		
	Message ID	An unique identifier for this message.
	Database Timestamp	The time when the message was written to the database.
	Time at point of Logging	The date and time, on the server machine, that the message was reported.
	Server name	The name of the server from which this message was generated.
	State	<p>The state of the pipeline from which this message was generated. The pipeline can be in one of the following states:</p> <ul style="list-style-type: none"> • REQUEST: indicates that the reporting action was executed in a request pipeline. • RESPONSE: indicates that the reporting action was executed in a response pipeline. • ERROR: the action was running in the service-level error handler.
	Node Name	The pipeline node from which this message was generated.
	Pipeline Name	The pipeline from which this message was generated.
	Stage Name	The stage from which this message was generated.
Inbound Service		

Table 5-2 Message Information

Category	Message Information	Description
	Name	The inbound proxy service associated with this message. An inbound proxy service exchanges messages with client applications. The name is a link to the View a Proxy Service page. For more information about this page, see “Viewing and Changing Proxy Services” in Proxy Services in Using the AquaLogic Service Bus Console.
	URI	The URI associated with the proxy service.
	Operation	The inbound operation associated with this message. Operations are the tasks performed by a pipeline or route node in the message flow associated with the service.
Outbound Service		
	Name	The outbound business service associated with this message. An outbound business service exchanges messages with an ALSB proxy service. Click on the link to go to View Business Service Details page. For more information about this page, see “Viewing and Changing Business Services” in Business Services in Using the AquaLogic Service Bus Console.
	URI	The URI to the outbound business service end point.
	Operation	The name of the operation invoked on the outbound service. Operations are the tasks performed by a pipeline or route node in the message flow associated with the service.
Report Index		
	Report Text Index	Displays the key-value pairs extracted by a Report Action from the message context variables or the message payload. For more information, see About the JMS Reporting Provider .
Fault		

Table 5-2 Message Information

Category	Message Information	Description
	Error Code	The code associated with the error, if any. For more information, see Error Messages and Handling in Proxy Services: Error Handlers in Using the AquaLogic Service Bus Console.
	Reason	The code associated with the error, if any. For more information, see Error Messages and Handling in Proxy Services: Error Handlers in Using the AquaLogic Service Bus Console.
	Detail	The fault details associated with the error. These details, if present, are typically a stack trace of where a particular fault occurred. The stack trace may be truncated due to a size limitation in the database. The limit is 2048 characters.
Report Body		
	Detail	Opens a new browser window that displays the report body in a browser. You can use an XQuery expression in a Report action to capture the report body text. For more information, see Report in Proxy Services: Actions and Using the Inline XQuery Expression Editor in Proxy Services:XQuery Editors in Using the AquaLogic Service Bus Console.

- Detail: opens a browser window that displays the report body in a browser. You can use an XQuery expression in a Report Action to capture the report body text.

How to Purge Messages from the Reporting Data Store

You can purge all of the messages from the reporting datastore or base the purge on a range of time. Message purging is an asynchronous process that occurs in the ALSB Console. This feature enables you to work with the Summary of Messages page in the ALSB Console while the purge occurs in the background.

Figure 5-11 Purging Messages Page

The duration of time it takes a purge to complete depends on how many messages are in the purge queue. The deletion of messages is slowed if you search for reporting messages during the purge process. Moreover, the Summary of Messages page may display incorrect data as some data may not yet be purged.

Because the purge process is asynchronous and occurs in the background, the ALSB Console does not display any messages to indicate that a purge is in progress. However, if another user attempts to start a purge when a purge is in progress, the following message is displayed:

A Purge job is already running. Please try later.

How to Configure a Database for the JMS Reporting Provider Store

ALSB requires a database for the JMS Reporting Provider Data Store. The PointBase database that is installed with WebLogic Server is for evaluation purposes only and not intended for a production environment. Non-evaluation development or other use of the PointBase Server requires that you obtain a separate PointBase license.

In a production environment you must use one of the supported databases. For the latest information about supported databases, see Supported Databases and Drivers in [Supported Configurations for ALSB](#).

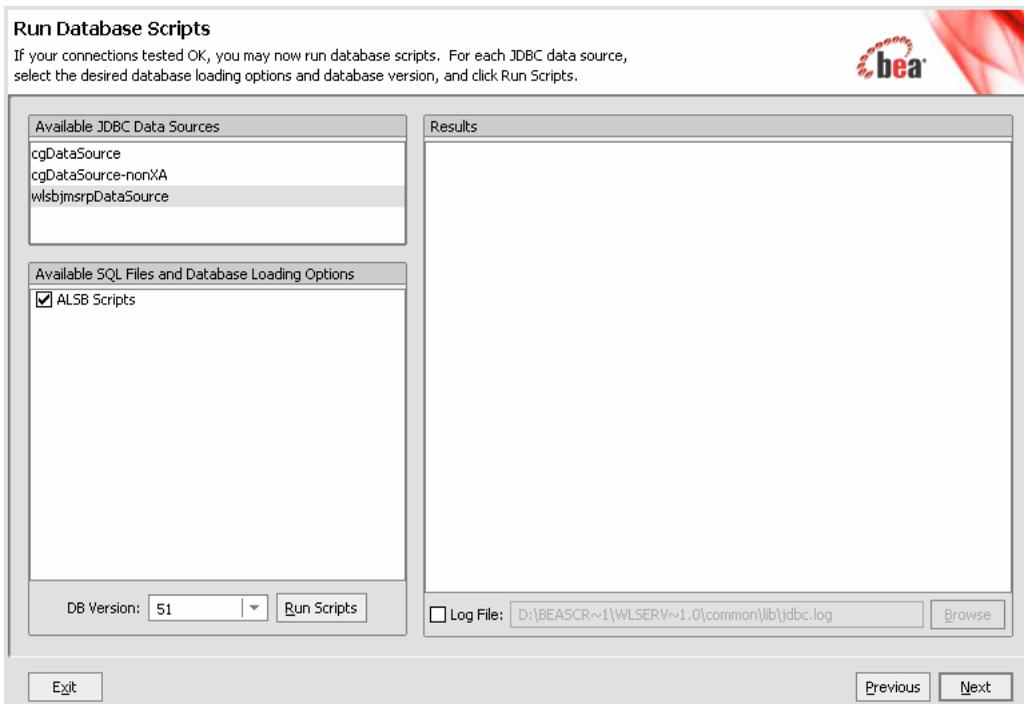
How to Configure a Database in a Development Environment

When you create an ALSB domain, the Configuration Wizard does not create database tables automatically. In a development environment, the default JMS Reporting Provider checks whether tables exist for the specified database at run time. If tables do not exist, the Reporting Provider creates them; if they do exist, the Reporting Provider uses them.

Note: If you are using Pointbase, you need not specify a database in the Configuration Wizard. You can specify which database is used by the JMS Reporting Provider in one of the following ways:

- Run the reporting SQL scripts in your ALSB domain. The scripts are located in `<BEA_HOME>/alsb_3.0/dbscripts>ls` where BEA_HOME represents the location in which you installed WebLogic products.
- When you create a domain in the Configuration Wizard, customize the JDBC Settings on the Run Database Scripts page (see [Figure 5-12](#)). For more information, see [Creating WebLogic Domains Using the Configuration Wizard](#).

Figure 5-12 Run Database Scripts in the Configuration Wizard



How to Configure a Database for Production

For complete information about configuring a database for production, see *AquaLogic Service Bus Deployment Guide* in the following chapters:

- [Configuring a Single-Server Deployment](#)
- [Configuring a Cluster Deployment](#)

Tracing

ALSB enables you to trace messages without having to shut down the server. This feature is useful in both a development and production environments. Tracing allows administrators, support engineers, and systems engineers to troubleshoot and diagnose a message flow in one or more proxy services.

For example, if one of your proxy services is failing and you want to find out at which stage the problem exists, you can enable tracing for that proxy service. After tracing is enabled, the system logs various details extracted from the message flow such as stage name, name of the pipeline, and route node name. The entire message context is also printed, including headers and message body. When a fault occurs in the message flow, additional details such as error code and reason are logged. Tracing occurs at the beginning and end of each component in the message flow, which includes stages, pipelines, and nodes. Actions are not traced individually.

How to Enable or Disable Tracing

You can enable tracing from View a Proxy Service page of the ALSB Console, as shown in [Figure 6-1](#). to configure tracing:

1. Using smart search find the required proxy service. For more information on how to find a proxy service, see [Finding Proxy Services Using Search Filters](#) and [Finding Proxy Services in Using the AquaLogic Service Bus Console](#).
2. In Summary of Proxy Services table click the check box next to Enable in Tracing field for the proxy service.

Note: To enable tracing for all proxy services, search for all proxy services and click the check box next to Tracing.

3. Click Update and activate the session.

Figure 6-1 Tracing Configuration

Name	Path	Type	State	Monitoring	SLA Alerting	Pipeline Alerting	Reporting	Logging	Tracing	Actions
newP	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	
sampleWSDLProxy	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	
xqueryProxyService	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	
xyz	default	Proxy Service	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (N)	<input type="checkbox"/> Enabled (N)	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled (D)	<input type="checkbox"/> Enabled	

You can view the tracing status for a proxy service in the Operation Settings tab of the View a Proxy Service page, Summary of All Services table, and Summary of Proxy Services table. For more information about Summary of All Services, see [Managing Operational Settings for All Services](#), and for more information about Summary of Proxy Services, see [Managing Operational Settings for Proxy Services](#).

How to Access Tracing Information

The tracing information is stored in the server directory logs. For example, in the ALSB examples domain, which is created when you install the product, if you enable tracing for the proxy services before they are tested, the tracing information is logged in the following log file.

```
<BEA_HOME>\weblogic92\samples\domains\servicebus\servers\xbusServer\logs\servicebus.log
```

where, BEA_HOME is the directory in which you installed your BEA product.

Figure 6-2 shows a sample of the tracing log.

Figure 6-2 Tracing Log Example

```

weblogic.application.utils.StateMachineDriver.nextState(StateMachineDriver.java:26)
>
####<Dec 29, 2006 2:14:24 PM IST> <Notice> <Log Management> <svaidyan02> <xbusServer>
<[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'\> <<WLS
kernel>> <> <> <1167381864275> <BEA-170027> <The server initialized the domain log
broadcaster successfully. Log messages will now be broadcasted to the domain log.>
####<Dec 29, 2006 2:14:24 PM IST> <Notice> <webLogicServer> <svaidyan02> <xbusServer> <Main
Thread> <<WLS kernel>> <> <> <1167381864976> <BEA-000365> <Server state changed to ADMIN>
####<Dec 29, 2006 2:14:24 PM IST> <Notice> <webLogicServer> <svaidyan02> <xbusServer> <Main
Thread> <<WLS kernel>> <> <> <1167381864996> <BEA-000365> <Server state changed to RESUMING>
####<Dec 29, 2006 2:14:28 PM IST> <Notice> <Security> <svaidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)'\> <<WLS kernel>> <> <>
<1167381868541> <BEA-090171> <Loading the identity certificate and private key stored under
the alias demoIdentity from the jks keystore file
C:\bea2613a\WEBLOG-1\server\lib\demoIdentity.jks.>
####<Dec 29, 2006 2:14:29 PM IST> <Notice> <Security> <svaidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)'\> <<WLS kernel>> <> <>
<1167381869643> <BEA-090169> <Loading trusted certificates from the jks keystore file
C:\bea2613a\WEBLOG-1\server\lib\demoTrust.jks.>
####<Dec 29, 2006 2:14:29 PM IST> <Notice> <Security> <svaidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)'\> <<WLS kernel>> <> <>
<1167381869713> <BEA-090169> <Loading trusted certificates from the jks keystore file
C:\bea2613a\JROCKI-1\jre\lib\security\cacerts.>
####<Dec 29, 2006 2:15:32 PM IST> <Warning> <Server> <svaidyan02> <xbusServer>
<dynamicSSLListenThread[DefaultSecure[1]]> <<WLS kernel>> <> <> <1167381932743> <BEA-002611>
<Hostname "svaidyan02.apac.bea.com", maps to multiple IP addresses: 192.168.1.5,
172.22.56.120>
####<Dec 29, 2006 2:15:32 PM IST> <Notice> <Server> <svaidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)'\> <<WLS kernel>> <> <>
<1167381932753> <BEA-002613> <Channel "Default[2]" is now listening on 127.0.0.1:7021 for

```

Note: The tracing pattern in the server log is identical to the tracing in the test console. For more on tracing in the test console, see [Tracing Proxy services—Test Console](#) in *Using the AquaLogic Service Bus Console*.

Tracing

Managing Endpoint URIs for Business Services

An endpoint URI is the URL of an external service that is accessed by a business service. In ALSB you must define at least one endpoint URI for a business service. When you define multiple endpoint URIs for a business service you must define one of the following load balancing algorithm:

- Round robin
- Random
- Random-weighted
- None

The load balancing algorithm controls the manner in which business service tries to access the endpoint URI. The status of the endpoint URI can be online or offline. For more information, see [Configuring Operational Settings for Business Services](#) in Monitoring in Using the AquaLogic Service Bus Console.

This section contains the following topics:

- [How to Configure a Business Service to Perform Retries](#)
- [How to Mark a Non-Responsive URI Offline](#)
- [Metrics for Monitoring Endpoint URIs](#)
- [How to Mark an Offline URI as Online](#)
- [How to Generate Alerts Based on Endpoint URI Status](#)

How to Configure a Business Service to Perform Retries

You can define the retry option for business services. The retry option specifies the maximum number of times a business service can attempt to access endpoint URIs after an initial failure. For example, consider the behavior of a business service B with endpoint URIs `eu1`, `eu2`, and `eu3`, when the retry count is set to 1, 2, and 4.

When Retry Count = 1

If business service B fails to process a request or is unable to access the endpoint URI `eu1`, it tries to process the request with `eu2` (retry 1). If the retry fails then the business service returns failure. The business service does not retry the third endpoint URI `eu3`.

When Retry Count = 2

If business service B fails to process a request or is unable to access the endpoint URI `eu1`, it tries to process the request with `eu2` (retry 1). If the retry fails then the business service tries to process the request with `eu3` (retry 2). If the retry fails then the business service returns failure.

When Retry Count = 4

If business service B fails to process a request or is unable to access the endpoint URI `eu1`, it tries to process the request with `eu2` (retry 1). If the retry fails then the business service tries to process the request with `eu3` (retry 2). Then the business service waits for a interval you have configured for retry iteration interval (in seconds) before trying `eu1` (retry 3). If this fails the business service retries `eu2` (retry 4). If the retry fails then the business service returns failure.

If the retry count is set to 0, then the business service does not retry after the failure.

Note: The order in which a business service retries the endpoints is controlled by the load balancing algorithm.

How to Suppress Retries in Case of Application Errors

A business service fails to process a request due to communication or application errors.

Communication errors occur due to random network problems. Retrying such requests with another endpoint URI can be successful. Application errors occur when a request is malformed or due to errors, and cannot be processed by any of the endpoints. You can turn off retry behavior for the application errors by setting Retry Application Errors to No in the Transport Configuration page for a business service.

The option of suppressing the retries is available for the following transports:

- HTTP
- DSP
- JMS
- JPD
- Tuxedo
- SB
- WS
- EJB

How to Mark a Non-Responsive URI Offline

A communication error occurs each time a business service tries to access a non-responsive URI. You can configure a business service to mark non-responsive URIs offline. Doing so prevents a business service from repeatedly attempting to access a non-responsive URI and therefore avoids these communication errors.

To do so, you must enable the Offline Endpoint URIs operational setting for the business service. You can mark an endpoint URI offline temporarily or permanently as described in the following sections.

Mark an endpoint URI offline temporarily if you want the business service to automatically retry the same endpoint after a short interval of time; mark it offline permanently if you want the business service to treat the endpoint URI as offline until it is reset manually.

How to Mark an Endpoint URI Offline Temporarily

Mark an endpoint URI offline temporarily if you want the business service to automatically retry the same endpoint after a specified interval of time.

To mark an endpoint URI offline temporarily, you can specify a Retry Interval value in the Offline Endpoint URI operational setting for the business service. On encountering a communication error, the endpoint URI status is changed to Offline. When the retry interval has passed and this business service attempts to process a new request, it tries to access this endpoint URI. If this attempt is successful, then the endpoint URI is marked online again. If the attempt to access the endpoint URI fails, then the URI is marked offline again for the duration of the retry interval, and the cycle is repeated.

This configuration can be useful for the case in which a communication error is temporary and corrects itself. For example, when an endpoint becomes temporarily overloaded communication errors occur, but reverts to normal operation without requiring manual intervention.

How to Mark an Endpoint URI Offline Permanently

Mark an endpoint URI offline permanently if you want a business service to treat the endpoint URI as offline until you reset it manually.

To mark an endpoint URI offline permanently, you specify a Retry Interval value of 0 hours 0 min 0 sec in the Offline Endpoint URI operational setting for the business service. On encountering a communication error, the endpoint URI status is changed to Offline and remains offline until you mark the endpoint URI online again.

For more information, see [Configuring Operational Settings for Business Services](#) in Monitoring in Using the AquaLogic Service Bus Console and [Monitoring ALSB at Run Time](#).

This configuration is useful for a case in which a communication error is caused by a problem with the endpoint URI that must be resolved by manual intervention.

Metrics for Monitoring Endpoint URIs

You can monitor the metrics using the ALSB Console or the JMX monitoring APIs. For information on using the ALSB Console, see [How to Access Service Statistics from the ALSB Console](#). For information on using the JMX monitoring APIs, see [JMX Monitoring API Programming Guide](#).

In the ALSB Console, the endpoint URI metrics are available on the Endpoint URIs tab within the Service Monitoring Details page for a service. This includes count, response time, and endpoint URI status metrics.

For more information about the statistics displayed in this view, see [Viewing Business Services Endpoint URIs Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

You can monitor the endpoint URIs using URI status statistics and URI level statistics. The following items describe the expected behavior when you monitor endpoint URIs:

- You can obtain the statistics only when you enable monitoring for a business service.
- When you rename or move a service, the URI level statistics is reset.
- When you change the aggregation interval, all the URI level statistics except the URI status are reset.

- When you reset statistics for the service (or reset all statistics), all the URI level statistics except the URI status are reset.
- When you add a new URI to an existing business service, the metrics for the new URI are collected automatically.

Endpoint URI Status

The Status statistic on the ALSB Console indicates whether the endpoint URI is online or offline. You can also obtain the status of an endpoint URI using the JMX monitoring APIs. [Table 7-1](#) describes the possible states of an endpoint URI.

Table 7-1 Status of Endpoint URIs

Status	Description
Online	Implies the URI is online on a given server. In a cluster it implies that the URI is online for all servers.
Offline	Implies the URI is offline on a given server. In a cluster it implies that the URI is offline for all servers.
Partial	Implies that at least one server in the cluster reports a problem for that URI. This metric is available for clusters only.

Note: When a URI is associated with more than one business service, the same endpoint URI can have a different status for each of the business services.

Endpoint URI Performance Metrics

The endpoint URI performance metrics provide information on how many messages have been processed by a given endpoint and how many failed and their response times. You can use the following metrics for monitoring the endpoint URIs:

- Message Count
- Error Count
- Average Response Time
- Min Response Time
- Max Response Time

For more information about these statistics, see [Viewing Business Services Endpoint URIs Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

The following are the important properties of the endpoint URI statistics:

- You can obtain the statistics only when you enable monitoring for a business service.
- When you rename or move a service or change the aggregation interval, the URI level statistics is reset.
- When you add a new URI to an existing business service, the metrics for the new URI are collected automatically.

How to Mark an Offline URI as Online

You can mark an endpoint URI that is offline as online using the ALSB Console or by using the public APIs.

In the ALSB Console, you can mark an offline endpoint URI as online from the Service Monitoring Details page. Click the **Click to mark this endpoint URI online** icon in the Actions column of the Endpoint URIs tab. For more information, see [Viewing Business Services Endpoint URIs Metrics](#) in Monitoring in Using the AquaLogic Service Bus Console.

All the endpoint URIs are marked online when:

- You add them to a business service
- You restart a server
- You enable a disabled service
- You rename or move a service
- A business service is able to successfully access the URI after the retry interval you have configured is past.

You can also use APIs to mark an offline endpoint URI as online. This is useful when the you have not enabled monitoring for a business service but you require to mark its endpoint URIs online. For more information, see `com.bea.wli.monitoring.ServiceDomainMBean` in [Javadoc](#).

When you mark an endpoint URI online in a cluster domain, it is marked online on all the managed servers.

How to Generate Alerts Based on Endpoint URI Status

If an endpoint URI is not accessible, the business service trying to access it receives a communication error.

In addition to configuring a business service to take a non responsive URI offline, as described in, [How to Mark a Non-Responsive URI Offline](#) you can raise an alert when a system encounters non-responsive URIs. You do this by configuring SLA alert rules based on endpoint URI status.

How to Configure an Alert Rule Based on Endpoint URI Status

You can configure the alert rule for a business service, based on the status of the Endpoint URI. Complete the tasks as described in [Configuring General Information for Alert Rules](#) in Monitoring in Using the AquaLogic Service Bus Console.

Then complete the following tasks in the Alert Rule Conditions Configuration page:

1. In the Simple Expression section of the Alert Rule Conditions Configuration page (see [Figure 7-1](#)), choose Status in the first drop-down list.

Figure 7-1 Alert Rule Condition Configuring page

Alert Rule Conditions Configuration

Select Aggregation Interval for the condition : 0 hours and 10 mins

Simple Expression

▶ Status All URIs offline = True Evaluate on all servers Add Clear

The endpoint URI status based alert rule condition is comprised of:

2. A state transition clause—The state transition clause supports notification when any endpoint URI or all endpoint URIs change state from online to offline, or from offline to online. Choose one of the following options to identify the status for which you want to create a notification:
 - All URIs offline
 - All URIs online
 - Any URI offline
 - Any URI online

For example, consider a business service for which two alert rules are configured, one based on `All URIs offline = True` condition and another on `Any URI offline = True` condition. If an alert based on `All URIs offline = True` condition is generated then it signifies a severe problem because all requests to this service are likely to fail until the situation is resolved. However, if an alert based on `Any URI offline = True` is generated, it implies that the other endpoint URIs are responsive and subsequent requests may not fail.

Note: All alert rules are independently evaluated. If alerts based on both (any or all URI) clauses have been configured for the same business service, it is likely that both alerts are generated simultaneously when the last endpoint URI is marked offline.

If a business service has only one URI, the `All URIs offline = True` and `Any URI offline = True` clauses mean the same thing and so they behave in an identical manner.

The evaluation of an alert rule condition based on a transition from offline to online behaves in a similar fashion except that it tracks any or all endpoint URIs being marked back to online state.

3. A server clause—The server clause allows you to specify an alert trigger when a state transition occurs on any or all servers. The server clause is significant only in a cluster domain with multiple managed servers. Choose one of the following options to create the expression:
 - Evaluate on all servers
 - Evaluate on any server

A communication error can occur due to network problem on a machine hosting a managed server. Such an event is interpreted by the business service as the endpoint URI being non-responsive (although the remote endpoint being accessed is responsive). A communication error can also occur because the endpoint URI is not responding.

In the first case, the URIs are marked offline on only one server (on the machine with network problems) and online on all the other servers in the cluster. An alert condition based on `Evaluate on any server` clause generates an alert, but an alert condition based on the `Evaluate on all servers` clause does not generate an alert.

For the second case, the URI is marked offline on all the managed servers (one by one as each server tries to access that endpoint). As each managed server marks the endpoint URI offline, the alert rule condition based on `Evaluate on any servers` is met and an alert is generated. When the endpoint URI is marked offline on the last of the servers in the cluster domain, the alert rule condition based on `Evaluate on all servers` is also met and this alert is also generated.

Notes:

- All alert rules are independently evaluated. If you have configured alerts based on both (any or all server) clauses for the same business service, it is likely that both alerts are generated simultaneously when the endpoint URI is marked offline on the last server in the cluster.
- In a single server domain, the `Evaluate on any server` and `Evaluate on all servers` clauses mean the same thing and behave in an identical manner.

When designing the alert rules for your system, you must choose one or more combinations of the clauses in accordance with your requirements.

You must set any one of the conditions to be True or False. These conditions can be evaluated on all servers or any server in a cluster.

Note: To ensure that you do not miss any alert that is triggered due to frequent changes in the status of the URI, BEA recommends that you set the aggregation interval for alert rules based on the status of the URI to one minute. For more information on aggregation interval, see [Aggregation Intervals](#).

Managing Endpoint URIs for Business Services

Throttling in ALSB

In ALSB, you can restrict the message flow to a business service. This technique of restricting a message flow to a business service is known as throttling. This section contains the following topics:

- [How to Enable Throttling](#)
- [What are the Operational Settings for Throttling?](#)
- [What Metrics are Available for Throttling ?](#)
- [How to Access Throttling Metrics](#)
- [How to use Throttling Metrics for Alerting](#)
- [How to use Throttling for Business Services with Multiple Endpoint URIs](#)

How to Enable Throttling

You must enable throttling for a business service from the **Operational Settings** tab of the **View a Business Service** page. In this tab, under **Throttling** select the **Enable** check box for the **Throttling State**. When you enable throttling for a business service you must specify values for **Maximum Concurrency**. You can also specify the **Throttling Queue** and **Message Expiration** for the business service. For more information, see [What are the Operational Settings for Throttling?](#) and [Configuring Operational Settings for Business Services](#) in Monitoring in Using the AquaLogic Service Bus Console.

[Table 8-1](#) provides some important definitions in throttling.

Table 8-1 Important Definitions

What is ...	Definition
Throttling queue	<p>The priority queue in which the messages are enqueued when business services reach their maximum concurrency. Messages with higher priority are processed first. Messages are processed on a first-in first-out basis, if they have the same priority. You can assign priority to messages using the routing options.</p> <p>Note:</p> <ul style="list-style-type: none">• The greater the integer for priority, the higher is the priority of the message.• You can configure only one queue for a business service <p>A throttling queue is an in-memory queue. Messages that are placed in this queue are not recoverable when a server fails or when you restart a server.</p> <p>When you delete or rename a business service, all the messages in the throttling queue are discarded.</p>
Message priority	The priority of a message in the throttling queue.
Expired message	A message that has been in the throttling queue for an interval greater than the value of message expiration. For more information on message expiration, see Table 8-2 .

What are the Operational Settings for Throttling?

[Table 8-2](#) describes the operational settings for throttling.

Table 8-2 Operational Settings for Throttling

Operation Setting	Use this to ...
Throttling State	<p data-bbox="565 427 1042 453">Enable or disable throttling for a business service.</p> <p data-bbox="565 475 1233 557">Note: When you disable throttling for a business service at run time, all messages in the throttling queue are processed without throttling.</p>
Maximum Concurrency	<p data-bbox="565 588 1233 730">Restrict the number of messages that can be concurrently processed by a business service. This must be a positive integer. When this threshold is reached for a business service, all the incoming messages for the business service are placed in a throttling queue until the business service can accept more messages.</p> <p data-bbox="565 748 1233 973">Any change to this setting affects both new messages and those already in the queue. When you increase the value, the ALSB run time allows more messages to be sent to the business service after processing those in the queue first. When you decrease the value, the ALSB run time places any new messages in a throttling queue until the concurrency setting goes below the new threshold, if you have defined a throttling queue. If you have not defined a throttling queue, the messages are discarded.</p> <p data-bbox="565 991 1233 1078">In a cluster environment, the number of messages that can be concurrently processed by a business service is equally divided among the managed servers.</p> <p data-bbox="565 1095 1163 1150">Note: You can set this operational setting only if you enable throttling for the business service.</p>

Table 8-2 Operational Settings for Throttling

Operation Setting	Use this to ...
Throttling Queue (operational setting)	<p>Restrict the number of messages in the throttling queue. The length of the throttling queue must be positive integer. All the incoming messages beyond the maximum concurrency limit for the business service are placed in the throttling queue. When the queue is full, the message in the queue with the lowest priority will be removed from the queue if a new incoming message has a higher priority.</p> <p>If you set this length to be equal to zero, it implies that a throttling queue does not exist for the business service.</p> <p>Any change to this setting is dynamically implemented. When you decrease the value for this setting, all the messages beyond the new length are discarded.</p> <p>Note: You can set this operational setting only if you enable throttling for the business service.</p> <p>In a cluster environment, this is equally divided among the managed servers.</p>
Message Expiration	<p>Restrict the maximum time (in milliseconds) spent by a message in the throttling queue of a business service. This must be a positive integer. When this time has elapsed, the message is removed from the queue. These messages are referred to as expired messages.</p> <p>If the message expiration is set to zero for a service, the messages in throttling queue for this service will never expire.</p> <p>When you increase the value for this setting, the expiration time for the new messages and the messages that are already present in the queue is increased. When you decrease the value, all the messages that have exceeded the new value are immediately discarded.</p> <p>Note: You can set this operational setting only if you enable throttling for the business service.</p>

What Metrics are Available for Throttling ?

[Table 8-3](#) describes the metrics that are available for throttling.

Table 8-3 Throttling Metrics

Metrics	Description
Max Throttling time	The maximum time spent by all messages in the throttling queue in milli seconds. If this value is greater than zero for a business service, it indicates that messages are placed in the queue for the business service.
Min Throttling time	The minimum time spent by all messages in the throttling queue in milli seconds. If this value is equal to zero some messages are not placed in the throttling queue.
Average Throttling time	The average the time spent by all messages in the throttling queue in milli seconds.

For more information about throttling metrics, see [How to Access Throttling Metrics](#).

How to Access Throttling Metrics

You can access the throttling metrics from the **Service** tab of the **Service Monitoring Details** page in the ALSB Console. You can obtain the metrics for the current aggregation interval and for the interval since the last reset. For more information, see [How to Access Service Statistics from the ALSB Console](#).

You can also access the metrics using JMX Monitoring APIs. For more information, see [Viewing SLA Alerts in the Dashboard](#).

How to use Throttling Metrics for Alerting

You can define an SLA alert rule based on throttling metrics. You can define the alert rule based on Average Throttling Time. For more information, see [Creating and Editing Alert Rules in Monitoring in Using the AquaLogic Service Bus Console](#).

How to use Throttling for Business Services with Multiple Endpoint URIs

This topic provides information on using throttling for business services with multiple endpoint URIs.

In ALSB, a business service can be associated with multiple endpoint URIs. For more information on endpoint URIs, see [Managing Endpoint URIs for Business Services](#). When you associate a business service with multiple URIs, you must configure the maximum concurrency for the business service and not the individual URI. The maximum concurrency for each URI is set internally depending on the overall maximum concurrency and the load balancing weight, based on the following equation:

$$\text{URI-specific max_concurrency} = [\text{User configured max_concurrency}] \times [\text{weight}]$$

For example, consider a business service *B* with three endpoint URIs *eu1*, *eu2*, and *eu3*. The load balancing algorithm is defined as random-weighted. The weights of the URIs are 1, 2, and 3 respectively. Assuming that you have defined a maximum concurrency of 10 for the business service, the URI specific maximum concurrency is 10, 20, and 30. The effective maximum concurrency of the business service *B* is 60. If the last endpoint URI that has a weight of 3 is offline, the effective maximum concurrency of the business service is 30.

Notes:

- The weights for the URI when the load balancing is `round robin` or `random` is 1. When the load balancing is `None` the weight of the primary URI is 1 and the weight of the backup URI is 0. The weight of the backup URI becomes 1 when the primary URI goes offline.
- Messages, for which endpoint URI is overridden in routing options are not throttled.

What Happens to Retried Messages During Throttling?

When failover is enabled on a service, retried messages are not throttled. The message is sent to the next URI regardless of the operational settings for throttling.

Messages that are expired or that are discarded, because the throttling queue is full or because the service reached its maximum concurrency, are not retried.

User Preferences

ALSB allows you to customize your home page and other settings in the ALSB Console. The home page is the page you wish to access first when you log into the ALSB Console. To set your preferences for the home page, click User Preferences in the Configuration module of the Operations navigator bar. Your user preferences are preserved across different sessions.

[Table 9-1](#) describes the preferences you can set from the User Preferences page.

Table 9-1 User Preferences

User Preference	Description
Home Page	<p>You can set the home page to one of the following options:</p> <ul style="list-style-type: none">• Operations: Choose this option to set one of the following pages as your home page:<ul style="list-style-type: none">– Dashboard– Smart Search– Global Settings– User Preferences– Message Reports

Table 9-1 User Preferences

User Preference	Description
Home Page	<ul style="list-style-type: none">• Resource Browser: Choose this option to set one of the following pages as your home page:<ul style="list-style-type: none">– Proxy Services– Business Services– WSDLs– XML Schemas– WS-Policies– XQueries– XSLTs– MFLs– Service Account– Service Key Providers– Jars– Alert Destinations

Table 9-1 User Preferences

User Preference	Description
Home Page	<ul style="list-style-type: none">• Project Explorer: Choose this option to view the list of projects in the ALSB Console.• Security Configuration: Choose this option to set one of the following pages as your home page:<ul style="list-style-type: none">– Users– Groups– Roles• System Administration: Choose this option to set one of the following pages as your home page:<ul style="list-style-type: none">– Import Resources– Export Resources– UDDI Registries– Import From UDDI– Auto Import Status– Publish to UDDI– Auto-Publish Status– JNDI Providers– SMTP Servers– Find and Replace– Create Customization File– Execute Customization File <p>Note: The pages that can be set for these options and the default setting for these options vary depending on the role assigned to the user.</p>
Display Search Filters	Select Yes to display all search filters in the ALSB Console. The default setting is No.
Display Stage Annotations	Set this to display stage annotations or not. The default setting is No.
Display Resource Metadata	Set this to display resource metadata or not. The default setting is Yes.

Table 9-1 User Preferences

User Preference	Description
Dashboard Refresh Rate	Use this to set the refresh rate of the dashboard. You can set this to No refresh, 1, 2, 3, 4, 5, 10, 20, 30, or 60 minutes. The default value for this is No refresh. For more information about Refresh Rate of the Dashboard, see The Refresh Rate of Monitoring Data .
Alert History Duration	You can set the alert history duration to 30 minutes, 1, 2, 3, or 6 hours. The default value is 30 minutes. For more information about Alert History, see Viewing the Alert History for SLA Alerts and Viewing the Alert History for Pipeline Alerts .

SNMP Components

Simple Network Management Protocol (SNMP) is an application-layer protocol that allows the exchange of information on the management of a resource across a network. It enables you to monitor a resource and if required, take some action based on the data obtained from the resource. Both the SNMP version 1 and SNMP version 2 are supported by ALSB. SNMP is made up of the following components:

- [Managed Resource](#)
- [Management Information Base](#)

Managed Resource

This is the resource that is being monitored. The resource and its attributes are added to the Management Information Base (MIB).

Management Information Base

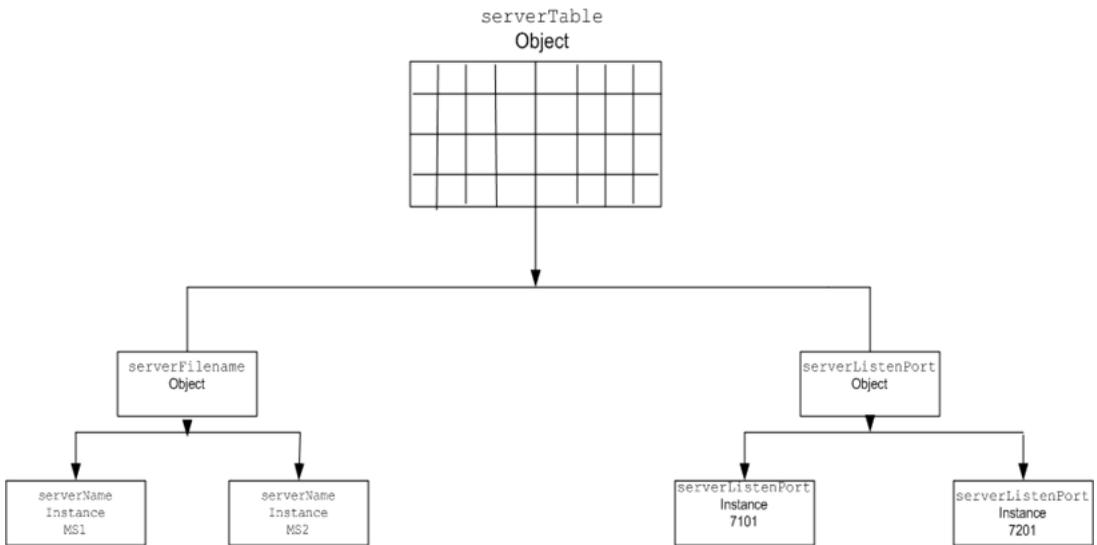
The MIB is a data structure that stores all the resources to be monitored in an hierarchical manner. It also stores the attributes of the resources. Each resource is given a unique identifier called the Object Identifier (OID). You can use the SNMP commands to retrieve the information on the management of a resource. The following section gives an illustration of the WebLogic Server MIB.

The Weblogic Server installer creates a copy of the MIB in the following location:

```
<BEA_HOME>/wlserver_10.0/server/lib/BEA-WEBLOGIC-MIB.asn1
```

where <BEA_HOME> is the directory in which you installed WebLogic Server. WebLogic Server exposes thousands of data points in its management system. To organize this data it provides a hierarchical data model that reflects the collection of services and resources that are available in a domain. [Figure A-1](#) illustrates the hierarchy of objects in the MIB.

Figure A-1 Hierarchy of Objects in MIB



For example, if you created two managed servers, MS1 and MS2, in a domain, then MIB contains one object serverTable, which in turn contains one serverName object. The serverName object in turn contains two instances containing values MS1 and MS2. The MIB assigns a unique number called an object identifier (OID) to each managed object. Once assigned you cannot change the OID. Each OID consists of a sequence of integers. This sequence defines the location of the object in the MIB tree. Each node in the path has both a number and a name associated with it.

For more information about WebLogic Server MIBs, see WebLogic Server documentation at [WebLogic Server® 10.0 MIB Reference](#).

SNMP Agent

Each managed resource uses an SNMP agent to update the relevant information in the MIB. For this you should configure the SNMP agent to detect certain conditions within a managed resource and send trap notifications (reports) to the SNMP manager. You can configure the SNMP agent to generate traps in one of the following ways:

- Automatically: Configure the SNMP agent to generate traps for events such as server startup or server shut down.
- Using log messages: Using filters, configure the SNMP agent to detect specific log messages and generate traps.
- Monitoring traps: Create JMX API clients to monitor the changes in the attributes and notify SNMP agent to generate traps. You can also configure the SNMP agents to monitor the changes in the attribute. For more information about JMX API clients, see [JMX Monitoring API Programming Guide](#).

SNMP Manager

The SNMP manager controls the SNMP agents. It is also the primary interface to the Network Management System.

Network Management System (NMS)

The Network Management System forms the interface with the user. It gathers data using the SNMP manager and presents it to the user.

SNMP Components

Monitoring Statistics in ALSB

In ALSB, you can collect many types of statistics when you monitor business services or proxy services. The name of statistics are linked to component of the service for which they are collected using ‘.’.

[Table B-1](#) lists the different statistics available in ALSB:

Table B-1 Different Statistics in ALSB

Name	Type of Associated Service	Type
Transport.error-count	Business Service and Proxy Service	count
Transport.message-count	Business Service and Proxy Service	count
Transport.response-time	Business Service and Proxy Service	interval
Transport.failover-count	Business Service	count
Security.WebService Security.wss-error	Business Service and Proxy Service	count
Alert.sla-all	Business Service and Proxy Service	count

Table B-1 Different Statistics in ALSB

Name	Type of Associated Service	Type
Alert.sla-normal	Business Service and Proxy Service	count
Alert.sla-warning	Business Service and Proxy Service	count
Alert.sla-minor	Business Service and Proxy Service	count
Alert.sla-major	Business Service and Proxy Service	count
Alert.sla-critical	Business Service and Proxy Service	count
Alert.sla-fatal	Business Service and Proxy Service	count
Alert.pipeline-all	Proxy Service	count
Alert.pipeline-warning	Proxy Service	count
Alert.pipeline-minor	Proxy Service	count
Alert.pipeline-major	Proxy Service	count
Alert.pipeline-critical	Proxy Service	count
Alert.pipeline-fatal	Proxy Service	count
Router.error-count	Proxy Service	count
Router.message-count	Proxy Service	count
Router.validation-errors	Proxy Service	count
Router.Pipeline.pipeline_name.error-count	Proxy Service	count
Router.Pipeline.pipeline_name.message-count	Proxy Service	count
Router.Pipeline.pipeline_name.elapsed-time	Proxy Service	count

Table B-1 Different Statistics in ALSB

Name	Type of Associated Service	Type
Router.Route Node.route_node_name.error-count	Proxy Service	count
Router.Route Node.route_node_name.message-count	Proxy Service	count
Router.Operation Node.route_node_name.elapsed-time	Proxy Service	count
Router.Operation.operation_name.error-count	Proxy Service	count
Router.Operation Node.operation_name.message-count	Proxy Service	count
Router.Operation.operation_name.elapsed-time	Proxy Service	count
Transport.url.url_name.status	Business Service	status
Transport.url.url_name.error-count	Business Service	count
Transport.url.url_name.message-count	Business Service	count
Transport.url.url_name.response-time	Business Service	interval
Transport.uri-offline_count-status	Business Service	status
Transport.throttling-time	Business Service	interval

For more information about statistics, see [Statistics Details–Concepts](#) in JMX Monitoring API Programming Guide.

Notes:

- Only the name of the statistics are displayed in the console.
- Statistics `Router.error-count`, `Router.message-count`, and `Router.elapsed-time` are not displayed. Instead, `Transport.error-count`, `Transport.message-count`, and `Transport.elapsed-time` are displayed.
- `Success Ratio` and `Failure Ratio` are also displayed in the console. `Success ratio` is the percentage ratio of, succesful messages to total number of messages. `Failure ratio` is the percentage ratio of failed messages to total number of messages.

Monitoring Statistics in ALSB

- You cannot obtain any statistic of the type status for a cluster using the JMX Monitoring APIs.

Auditing your ALSB System

In addition to monitoring the services in your ALSB system, you can audit your system to determine the history of configuration changes to the system, log the status of messages as they flow through the ALSB pipeline at run time, and log any security violations for messages in the pipeline.

Auditing the Configuration Changes

When you perform configurational changes in the ALSB console, a track record of the changes is generated and a record of all the configurational changes is maintained. Only the previous image of the object is maintained. You can view or access the history of configurational changes and the list of resources that have been changed during the session only through the console. However, to access all the information on configuration you have to activate the session.

Creating an Audit Trail for a Message Flow

Auditing the entire message flow pipeline during is time consuming. However, you can use the reporting action to perform selective auditing of the message flow pipeline during run time. You insert the reporting action at required points in the message flow pipeline and extract the required information. The extracted information may be then stored in a database or sent to the reporting stream to write the auditing report.

Auditing Security Violations

When a message is sent to the proxy service and there is a breach in the transport level authentication or the security of the Web Services, WebLogic server generates an audit trail. You

Auditing your ALSB System

must configure the WebLogic server to generate this audit trail. Using this you can audit all security violations that occur in the message flow pipeline. It also generates an audit trail whenever it authenticates a user. For more information about security auditing, see [Configuring the WebLogic Security Framework–Main Steps](#) in AquaLogic Service Bus Security Guide.