# BEA AquaLogic Service Bus™

## Operations Guide

Version: 2.6
Document Revised: January 2007

# Contents

## Introduction



## Roles in AquaLogic Service Bus



## Monitoring

# Using Smart Search

# Reporting

# Tracing

CHAPTER 1

# Introduction

BEA AquaLogic Service Bus is part of BEA's comprehensive business integration solutions. AquaLogic Service Bus is part of the BEA AquaLogic™ family of Service Infrastructure Products. AquaLogic Service Bus manages the transformation and routing of messages in an enterprise system and includes administration and monitoring capabilities. AquaLogic Service Bus is unified product for deploying and implementing Service Oriented Architecture.

The following sections provide an overview of:



## Document Scope and Audience

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

This document is intended for the following audience:

- Operational Specialists: Operational specialists are responsible for monitoring services, servers and alerts in AquaLogic Service Bus.
- Architects who design the security architecture of the enterprise system.

In order to understand the AquaLogic Service Bus Operations Guide you must be familiar with resources, proxy services, and business services in the AquaLogic Service Bus Console. For more

information on resources, proxy services, and business services in the AquaLogic Service Bus Console, see AquaLogic Service Bus User Guide.

# Roles in AquaLogic Service Bus

AquaLogic Service Bus Console offers restricted access by assigning roles to users. Each role in AquaLogic Service Bus has a limited functionality. Users in a given role can perform only those functions that are assigned to that role. The user interfaces that are available to the user in a particular role is limited and depends on the functionality of the role. AquaLogic Service Bus supports the following roles:

- Administrator
- Deployer
- Monitor
- Operator

For more information on scope and functions of each role see Chapter 2, "Roles in AquaLogic Service Bus."

# Document Organization

This document contains the following topics:

- Roles in AquaLogic Service Bus: This section describes the different roles available AquaLogic Service Bus Console, the user interfaces that are available for each role, and the scope of each role.
- Monitoring: This section describes how to monitor the health of services in AquaLogic Service Bus and collect the run-time information for system operations and business auditing purposes. It also describes how monitor System Level Agreements (SLA) violations and pipeline alerts.
- Using Smart Search: This section describes how to use Smart Search functionality as operations management tool in AquaLogic Service Bus.
- Reporting: This section describes how to capture message data for tracking messages or regulatory auditing. This section also contains information about setting up your own reporting provider, using the JMS reporting provider included with AquaLogic Service Bus, using the Reporting module in AquaLogic Service Bus Console, and configuring a reporting provider for data on alerts.

- Tracing: This section describes how to trace messages without shutting down the server. This feature is useful in both a development and production environment. This feature allows you to troubleshoot and diagnose a message flow in one or more proxy services.

CHAPTER 2

# Roles in AquaLogic Service Bus

BEA AquaLogic Service Bus offers improved security by assigning roles to users, depending on the tasks they perform. You can secure the resources and the services in the AquaLogic Service Bus Console by restricting the access by assigning roles to users.

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

**Note:** If you belong to a role in the WebLogic Server, you automatically belong to the corresponding role in the AquaLogic Service Bus Console. For example if you belong to the `Operator` in the WebLogic Server Administration Console, then by default you posses all the privileges of `IntegrationOperator` in AquaLogic Service Bus Console.

By default there are some predefined roles in the AquaLogic Service Bus Console. You can also create new roles or customize an existing role.This chapter describes various roles available in the AquaLogic Service Bus console and their functionality. The following are the default roles in the AquaLogic Service Bus console:

# IntegrationAdmin

The `IntegrationAdmin` role is an administrative security role in the AquaLogic Service Bus. As an `IntegrationAdmin` you can access the AquaLogic Service Bus Console only. By default the `IntegrationAdmin` role will grant you the access to all resources and services in the AquaLogic Service Bus Console. You must grant this role only to users requiring administrator privileges in the AquaLogic Service Bus Console.

In the AquaLogic Service Bus Console you can assign the `IntegrationAdmin` role by assigning the `IntegrationAdmin` Parent Group when you create or reconfigure a user. For more information on how to create a user in the AquaLogic Service Bus Console, see Adding a User in *Using the AquaLogic Service Bus Console*.

As an `IntegrationAdmin` you can create or commit a session. When you are assigned this role you can perform the following tasks:

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

# IntegrationDeployer

The `IntegrationDeployer` is an administrative security role in the AquaLogic Service Bus. An `IntegrationDeployer` can access the AquaLogic Service Bus Console to create and deploy resources and services. You will also be able to access the existing resources and services in the AquaLogic Service Bus. You must grant this role to users, who deploy services in the AquaLogic Service Bus.

In the AquaLogic Service Bus Console you can assign the `IntegrationDeployer` role by assigning the `IntegrationDeployer` Parent Group, when you create or reconfigure a user. For more information on how to create a user in the AquaLogic Service Bus, see Adding a User in *Using the AquaLogic Service Bus Console*.

Users in the `IntegrationDeployer` can perform all tasks that can be performed by user in the `IntegrationAdmin` role. For more information on tasks performed by an user in the `IntegrationAdmin` role, see "IntegrationAdmin" on page 2-2.

# IntegrationMonitor

The `IntegrationMonitor` role enables you to monitor resources and services in the AquaLogic Service Bus Console. You can also monitor the violations of the Service Level Agreements, and the alerts from the message flow pipeline.

In the AquaLogic Service Bus Console you can assign the `IntegrationMonitor` role by assigning the `IntegrationMonitor` parent group, when you create or reconfigure a user. For more information on how to create a user in the AquaLogic Service Bus Console, see Adding a User in *Using the AquaLogic Service Bus Console*.

Users in the `IntegrationMonitor` role can perform the following tasks:

- View Dashboard for SLA alerts and pipeline alerts.
- Use smart search to view business services, proxy services, alert destination and SLA alert rules.
- View details of existing users and groups.
- View details of resources.

# IntegrationOperator

As an `IntegrationOperator` you can perform the day-to-day operations on the resources in the AquaLogic Service Bus Console.You can also perform certain monitoring tasks and session management. You must grant this role to users, who perform day to day operations in the AquaLogic Service Bus Console.

In the AquaLogic Service Bus Console you can assign the `IntegrationOperator` by assigning the `IntegrationOperator` in the Parent Group when you create or reconfigure a user. For more information on how to create a user in the AquaLogic Service Bus Console, see Adding a User in *Using the AquaLogic Service Bus Console*.

Users in the `IntegrationOperator` 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 and alert rules.
- View SLA alerts and pipeline alerts for business services and proxy services.
- Use smart search to view business services, proxy services, alert destination and SLA alert rules.
- Use global settings to enable or disable monitoring, tracing, reporting, and logging on a global level.
- View the server status for all the servers associated with the domain.
- View and purge message reports.
- View the UDDI that have been configured with the domain.
- View, the auto-publish and auto-import status of business services and proxy services.
- View security configurations for users and groups.

For more information on tasks you can perform in each of the preceding roles, see Role-Based Access: Configuring Administrative Security in *AquaLogic Service Bus Security Guide*.

CHAPTER 3

# Monitoring

BEA AquaLogic Service Bus provides the capability to monitor and collect run-time information required for system operations. AquaLogic Service Bus aggregates run-time statistics, which you can view on a 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 includes the following topics:



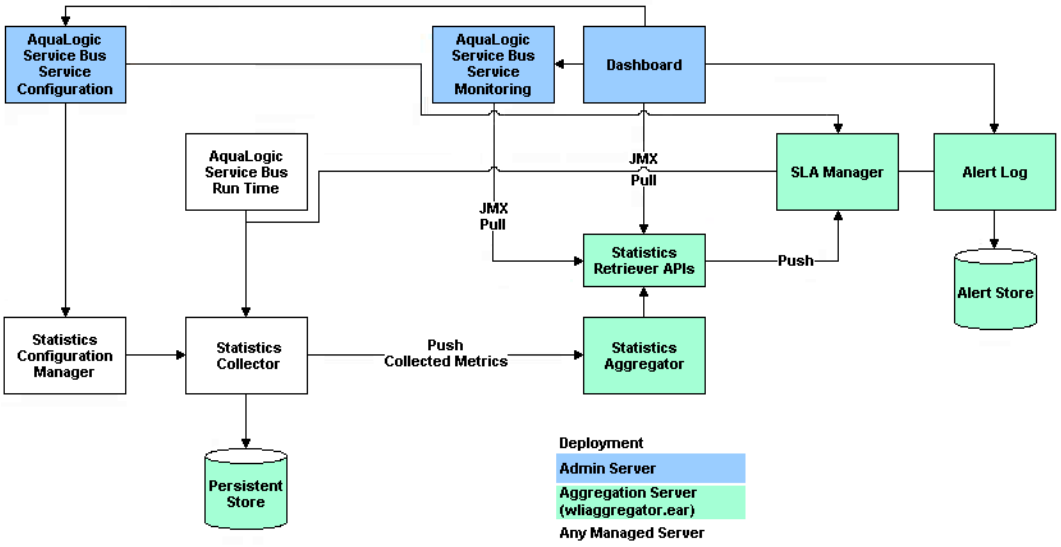
## About Monitoring

This section contains information on the following topics:

# Understanding Monitoring Architecture

Monitoring in AquaLogic Service Bus involves monitoring of the operational resources, server, and service level agreements. Figure 3-1 shows the architecture of AquaLogic Service Bus monitoring.

**Figure 3-1 Monitoring Architecture**




The Statistics Configuration Manager stores and manages the statistics configuration for each operational resource. 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 and flow components in a pipeline. The Statistics Configuration Manager is notified about changes in the service definition, such as adding, updating, or deleting a pipeline.

Each managed server in a cluster hosts a Statistics Collector. The Statistics Collector collects statistics on operational resources as directed by the Statistics Configuration Manager. The

Statistics Collector also keeps samples history within the aggregation interval for the collected statistics. At every system-defined checkpoint interval, the Statistics Collector stores a snapshot of current statistics into a persistent store for recovery purposes and sends the information to the Statistics Aggregator.

One of the managed servers in a cluster, called the *Aggregating Server* or *Aggregator*, is designated as the aggregator for cluster-wide statistics. At system-defined checkpoint intervals, each managed server in the cluster sends a snapshot of its contributions to the Aggregator. The Aggregator then combines this information to offer cluster-wide statistics to its clients through Retriever APIs. The clients of Aggregator are the Dashboard, SLA Manager, and Service Monitoring modules.

To contribute a data point to the system, an operational resource in the system, such as a run-time proxy service pipeline, calls a method on the Statistics Collector, and identifies itself, the statistic, and the data point.

# Understanding Alerts

Alerts are raised in AquaLogic Service Bus to indicate potential violation of the service level agreements. You can use alerts for:

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

Alerts can also 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.

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. 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, the notifications are sent to AquaLogic Service Bus Console. For more information in alert destinations, see "Understanding Alert Destination" on page 3-5.

This section contains information on:



## SLA Alerts

SLA alerts are automated responses to violations of Service Level Agreements (SLAs). These alerts are displayed on the AquaLogic Service Bus `Dashboard`. They are generated when the service violates the service level agreement or a predefined condition. To raise an SLA alert you have to raise an enable `SLA Alerting` both at the service level and at the global level. For more information on how to enable or disable monitoring for services, see "Monitoring Services" on page 3-43. 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 on aggregation interval, see "Aggregation Intervals" on page 3-15. Alert rules also allow you to send notifications to the configured alert destinations. For information on defining alert rules, see Creating Alert Rules in the *Using the AquaLogic Service Bus Console.*

### Using 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 AquaLogic Service Bus Console and a review at the detailed statistics for the proxy service. At this level, you will be 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 Service Level Agreements. After successfully renegotiating service level agreements 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.

### 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. You must configure the `Alert Destination` resource in an alert rule, to define the destination for the alert.

You will 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 on how to configure `Alert` actions in a stage, see Alert— Proxy Service: Actions in *Using the AquaLogic Service Bus Console*. The alerts are notified to alert destinations.

You can obtain an integrated view of all the alerts generated by a service on the Dashboard page in AquaLogic Service Bus Console.

## Understanding Alert Destination

Alert destinations are resources to which alerts are dispatched.

AquaLogic Service Bus Console is the default alert destination for notification of any alert. The alerts are notified to the AquaLogic Service Bus console regardless of whether you configure an alert destination or not. It 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 AquaLogic Service Bus. It provides an overview of the state of the system comprised of server, services, and alerts.

For more information on how to interpret the information on the dashboard, see “The AquaLogic Service Bus Dashboard” on page 3-17.

In AquaLogic Service Bus you can configure one or more of the following alert destinations:

- “E-mail” on page 3-6
- “SNMP Traps” on page 3-6
- “JMS” on page 3-8
- “Reporting” on page 3-9

## E-mail

This is one of the destinations for the alerts.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 SMTP Server resource, see Overview of SMTP Servers in *Using the AquaLogic Service Bus Console*. For more information on 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 payload configured.

You can specify the e-mail id of the recipients in the Mail Recipients field. for more information on configuring an e-mail alert destination, see Adding an E-Mail Recipient: 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 (SLAs) within AquaLogic Service Bus. 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.

Simple Network Management Protocol (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 AquaLogic Service Bus. SNMP is made up of the following components:


- "Managed Resource" on page 3-7
- "Management Information Base(MIB)" on page 3-7
- "SNMP Agent" on page 3-8
- "SNMP Manager" on page 3-8
- "Network Management System (NMS)" on page 3-8

## 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(MIB)

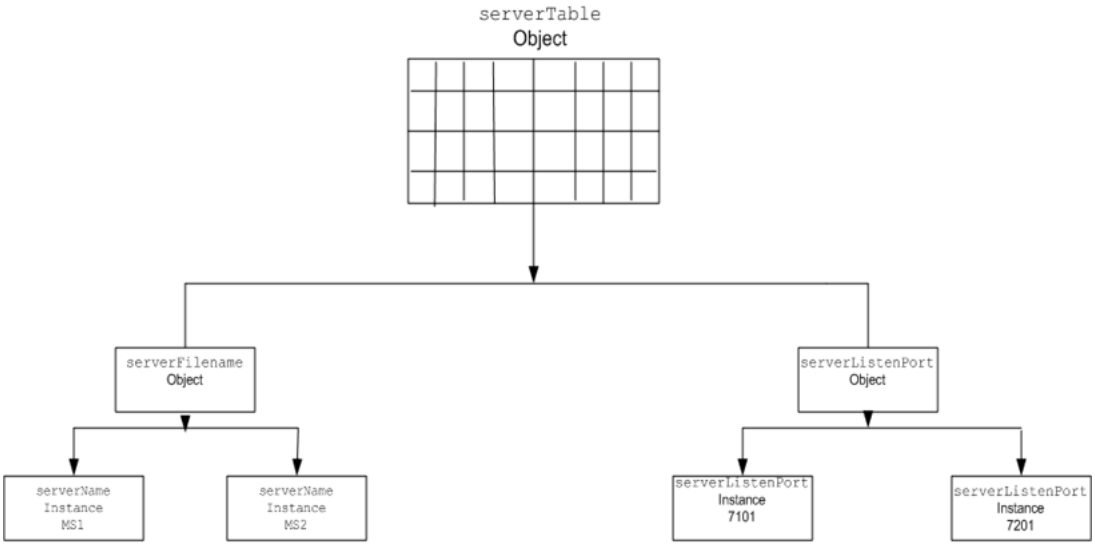
The Management Information Base (MIB) is a data structure that stores all the resources to be monitored in an hierarchical manner. It also stores the attributes of the resources. Each resource is given a unique identifier called the Object Identifier (OID).You can use the SNMP commands to retrieve the 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>/weblogic92/server/lib/BEA-WEBLOGIC-MIB.asn1`

where `<BEA_HOME>` is the directory in which you installed the 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 3-2 illustrates the hierarchy of objects in the MIB.

**Figure 3-2 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 on WebLogic Server MIBs see WebLogic Server documentation at WebLogic Server® 9.2 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: You can configure the SNMP agent to generate traps for events such as server startup or server shut down.
- Using log messages: Using filters, you can configure the SNMP agent to detect specific log messages and generate traps.
- Monitoring traps: You can 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 on JMX API clients, see JMX Monitoring API Programming Guide.

### SNMP Manager

The SNMP manager manages the SNMP agents. SNMP is also it is 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.

## JMS

Java Messaging Service (JMS) is another destination for pipeline alerts and SLA alerts. You will have to 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 on how to configure JMS alert destination see Alert Destinations in *Using the AquaLogic Service Bus Console*.

### Reporting

The Reporting destination allows you to send notifications of pipeline alerts or SLA alerts to the default AquaLogic Service Bus JMS reporting provider or custom reporting provider that can be developed using the reporting APIs provided by AquaLogic Service Bus. This allows third parties to receive and process alerts in custom Java code.For more information on reporting, see Chapter 5, "Reporting '.

## Understanding Alert Rules

In AquaLogic Service Bus you must define conditions based on which alerts are raised. The conditions are called the alert rule. The alert rule also configures the severity level and an alert destination for an alert.

This section provides information on the following topics:



### Alert Rules

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 can specify the aggregation interval. The alert aggregation interval is not affected by the aggregation interval set for the service. For more information on aggregation interval, see "Aggregation Intervals" on page 3-15.

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 can 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 is located in "Create an Alert Rule" in Monitoring in the *Using the AquaLogic Service Bus Console*.

On the Alert Rule page, if you set the Alert Frequency to `Every Time`, the notifications are issued to the dashboard every time the alert rule evaluates to `True`. If you set the Alert Frequency to `Notify Once` the notifications are issued the first time the rule evaluates to `True`, and no more notifications are generated until the condition resets itself and evaluates to `True` again.

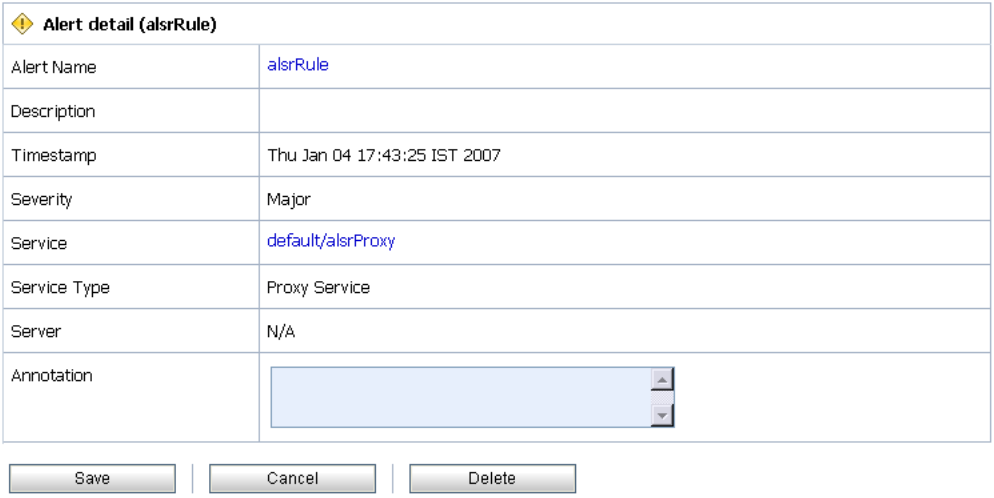
In the case where the Alert Frequency is set to `Every Time`, the number of times an alert rule is fired depends on the aggregation interval associated with that rule. For example, if the aggregation interval is set to five minutes, the sample interval is one minute. Rules are evaluated each time five samples of data are available. Therefore, the rule is evaluated for the first time approximately five minutes after it is created and every minute thereafter.

In the case where the Alert Frequency is set to `Notify Once`, after an alert is fired the first time in an aggregation interval, it is not fired again in the same aggregation interval.

## Viewing Alert Details

You can access this page when you click the name of the alert rule (or alert summary) in the Alert History table. The Alert Details page displays complete information about the alert and allows you to add an annotation to the alert, as shown in the Figure 3-3. Click on the name of the alert rule to go to the View Alert Rules Details Page. Click on the name of the service to go to the Service Monitoring Details page of the proxy service or the business service. Click on Delete to delete the alert rule. For more information on viewing alert details, Alert Details—Monitoring see in *Using the AquaLogic Service Bus Console*.

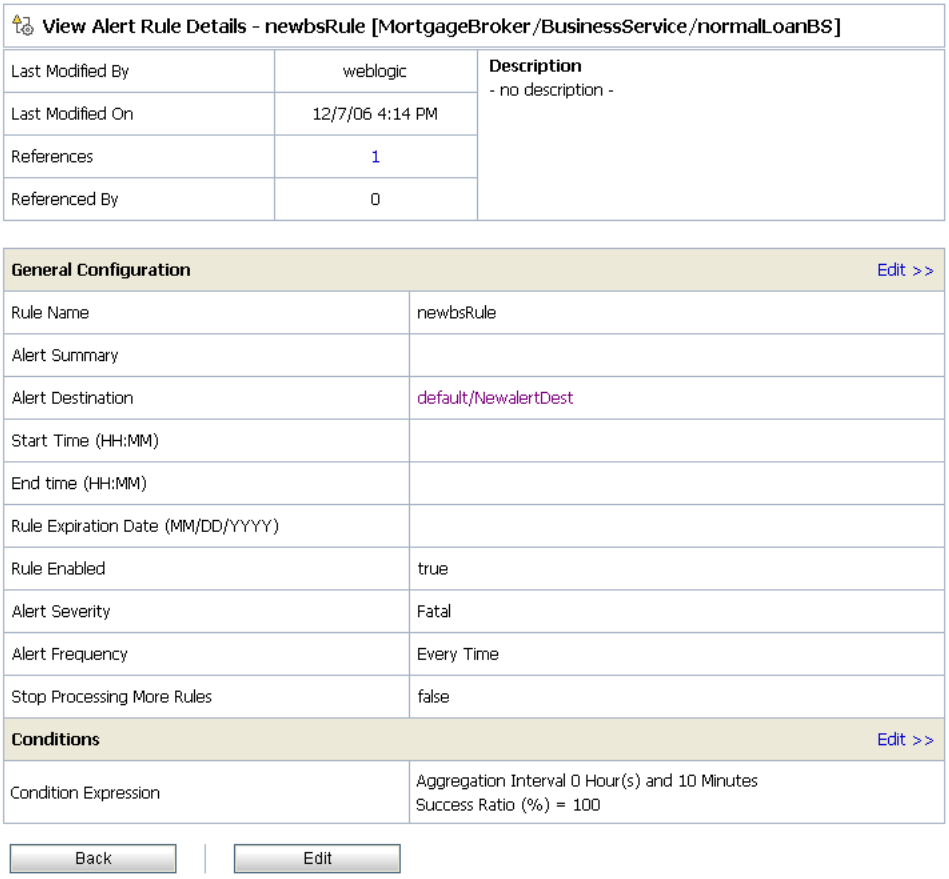
**Figure 3-3 Alert Details Page for SLA Alerts**




## Understanding Alert Rule Details

The View Alert Rule Details page displays complete information about a specific alert rule, as shown in Figure 3-4. 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 on how to edit an alert rule, see To Review Configuration: Creating an Alert Rule—Monitoring in *Using the AquaLogic Service Bus Console*.

**Figure 3-4 View Alert Rule Details Page**



View Alert Rule Details - newbsRule [MortgageBroker/BusinessService/normalLoanBS]

| | | |
|---|---|---|
| Last Modified By | weblogic | **Description** - no description - |
| Last Modified On | 12/7/06 4:14 PM | |
| References | 1 | |
| Referenced By | 0 | |

| **General Configuration** | Edit >> |
|---|---|
| Rule Name | newbsRule |
| 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** | Edit >> |
| Condition Expression | Aggregation Interval 0 Hour(s) and 10 Minutes<br>Success Ratio (%) = 100 |

Back | Edit

## Frequently Asked Questions

The information in this section is presented in question-answer format. The following are some of the most frequently asked questions:

- "I have restarted the server and none of my services have processed any requests. Why are alerts being generated?" on page 3-13
- "I have created an alert rule where I have defined the condition so as to raise an error if the success ratio drops below given percentage. But why are alerts raised even when the condition is not true?" on page 3-13

**I have restarted the server and none of my services have processed any requests. Why are alerts being generated?**

Answer: Once the Monitoring subsystem has started collecting data for services, stopping and restarting a server does not abort the collection process. The data collected is persisted and statistic collection picks up from where it left off.

**I have created an alert rule where I have defined the condition so as to raise an error if the success ratio drops below given percentage. But why are alerts raised even when the condition is not true?**

Example: You have an alert rule with the following definition:

```
Aggregation Interval:0 Hours(s) and 5 Minutes
Success Rate < 80%
```

The Service Monitoring Summary page shows the following values:

```
Message Count: 4
Error Count: 1
```

Why are you being alerted in this case? Shouldn't the success rate be 80% in this case?

Answer: No, the message count value displayed is the total of all messages processed by the service, including the ones that generated an error. Subsequently, in this case, the success rate is 75%.

**I have created a service with an aggregation interval of ten minutes that sends a JMS message. I could see the message on the Service Monitoring Summary page, but some time later why does the message count for my service shows as zero?**

Answer: The Service Monitoring Summary page displays dynamic statistics. In this case, it shows the message count in the last ten minutes. Because no messages were processed by the system in the last ten minutes, the message count is displayed as zero.

**I changed the aggregation interval of a service. Why does the Service Monitoring Summary page for Current Aggregation Interval not display any statistics for this service?**

Answer: Changing the aggregation interval for a service removes the statistical information for all the services and alerts associated with that service. The alert initializes again and triggers an alert at the end of aggregation interval expiry.

**I have defined an alert rule for a business service with multiple endpoints. When one of the endpoints goes down, the alert is triggered. Why is an error is generated, when a service has only one endpoint?**

Example: You have a business service with multiple endpoints with an alert rule defined as `Failover-count > 0`. When one of the endpoints goes down, the alert is triggered. However, when a service has only one endpoint, the `Failover-count` is not incremented for this service. Instead, why is an error is generated.

Answer: Set the Retry count to a number greater than zero. For information about setting the Retry count, see "Adding a Business Service" in Business Services in *Using the AquaLogic Service Bus Console*.

**I see that an alert is generated on the Dashboard but why is this not being reflected on the** Service Monitoring Details page for `Current Aggregation Interval`?

Answer: Alert rules are evaluated after the completion of the interval, which occurs after a checkpoint completion. If a rule evaluates to true, the rule's actions are triggered, a log is generated, and the interval-count statistic attribute (Alerts for Current Aggregation Interval) is incremented. The updated value of this counter is processed in the next checkpoint, 60 seconds later. The Monitoring Details page displays the updated count approximately one minute after the alert is generated.

**How does the active time for rules that span midnight work?**

Answer: Consider the case where the active time for a rule is specified as 22:00 to 09:00.

On a given date, say June 7, the rule will be active and inactive as follows:

```
June 6, 10:00 P.M. to June 7, 9:00 A.M. – Active
```

```
June 7, 9:01 A.M. to June 7, 9:59 P.M. – Inactive
June 7, 10:00 P.M. to June 8, 9:00 A.M. – Active
```

The monitoring system aggregates the data received every minute makes it available for the retriever sub system. The aggregator thread is behind by twenty five seconds with respect to the Statistics Collector checkpoint thread.

If you disable monitoring for the domain, you disable the collection of statistics for that domain. The monitoring data is no longer collected from the next minute, which means there is no data returned if you attempt to retrieve it. The same applies when you enable monitoring for the domain. The system initially does not show any data. However, after a maximum of two minutes, the Service Summary page displays the results of monitoring.

# Aggregation Intervals

In AquaLogic Service Bus, the monitoring subsystem collects statistical information, such as message count and statistics over an aggregation interval. The aggregation interval is the time period over which statistical data is collected and displayed in AquaLogic Service Bus Console. In an statistics are recomputed at regular intervals known as the sample interval. Thus aggregation interval is composed of many sample intervals. The duration of the sample interval depends on the aggregation interval.The following is an illustration of how the aggregation interval works:

Consider a proxy service you have configured for processing a purchase order, for which you have configured an aggregation interval of ten minutes. Until the first ten minutes elapse, the Service Summary page displays the partially computed data because the system has not yet collected a full ten minutes worth of data. After the first ten minutes of data aggregation, the system always displays the last ten minutes of data. For example, at the fourteenth minute, the Dashboard displays minutes four through fourteen. If no messages are processed after the fifteenth minute, on the twenty fifth minute, no data is displayed for the service.

Under certain conditions an alert rule may fire if the expiration of a sample interval completes an aggregation interval. If you update an alert rule aggregation interval or create an alert rule with new aggregation interval, then the new aggregation interval is set for the service and the conditions specified in the alert rule that has statistical metrics associated with the service. Also if the statistics from the aggregation interval associated with the previous alert rule is a part of the new or the updated alert rule, then the new alert rule will inherit the statistics and the alert rule is fired when the sample interval of the aggregation interval expires.

For example you have a service `s1` for which you have defined an alert rule `a1` with aggregation interval equal to ten minutes and condition `message count>10`. The sample interval for this

aggregation interval would be five minutes. Statistics for the service will be collected during each sample interval and aggregated over the aggregation interval. Now when you create a new alert rule `a2` with an aggregation interval of fifteen minutes and the condition being the same. that is an alert should be raised when the `message count >10.` The alert for the new aggregation interval should fire after time interval of `t+15` minutes, where `t` is the time when the new aggregation interval was set. However, as the statistics for alert rule `a1` are already being collected the alert rule may fire when a sample interval for the alert rule `a2` completes.

For more information about how aggregation interval affects the display of monitored information, see "Statistics Associated With Different Resources" on page 3-49.

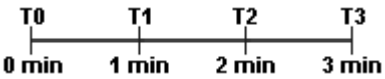
You must explicitly enable monitoring for any business or proxy service that you create; monitoring is disabled by default. After you have enabled monitoring and set the aggregation interval for your individual services, you can enable or disable monitoring for all those services from the Global Settings page in the System Administration module. For more information, see "Configuring Operational Settings at a Global Level" on page 3-47.

# The Refresh Rate of Monitored Information

At run time, the default refresh rate for the Dashboard page is one minute. However, it may take up to three minutes for the information to be displayed on the Dashboard. This delay occurs because of the time gaps between when the messages are processed by the proxy service, when the metrics are collected, and the refresh rate of the Dashboard. The system works as follows:

1. Every minute the Statistics Collector sends the current snapshot to the aggregator.
2. Every minute, the aggregator merges all the documents it has received from the managed servers within the last minute.
3. AquaLogic Service Bus Console refreshes every minute; that is, it runs a query on the aggregated document and then displays the results.

**Figure 3-5 Aggregation Time Line**




For example, a proxy service starts sending data in T1, as shown in Figure 3-5. At T2—that is, the second minute—the Statistics Collector sends the data to the aggregator. However, if an aggregation cycle has just occurred, the aggregator does not merge this data until the next aggregation cycle, which occurs after one minute, or a maximum of two minutes from the previous aggregation cycle. When the data is merged, it is now available for AquaLogic Service

Bus Console. Since the console refreshes every minute, if the refresh cycle has just passed, but the console displays the alerts after a maximum time of three minutes.

By default refresh rate of the dashboard is set to `1` minute. But you can set it to `2`,`3`,`4`,`5`,`10`,`20`, or `30` minutes. You can view the alert history data by default for `30` minutes. But you can also view this data for `1`, `2`, `3`, or `6` hours.

You can change the Dashboard polling interval in the Global Settings in Operations module in the AquaLogic Service Bus Console. For information on how to do this, see Changing the Dashboard Settings: Monitoring in *Using the AquaLogic Service Bus Console*.

# The AquaLogic Service Bus Dashboard

The dashboard displays all the alerts that have been fired. This display is dynamically refreshed. These alerts could 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 AquaLogic Service Bus business and proxy services, while pipeline alerts are defined in the message flow for business purposes such as record the number of message that flow through the message pipeline, 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 severity link will display more details about the alert to help analyze the cause of the alert.

This section helps you to understand the information displayed on AquaLogic Service Bus dashboard. The dashboard displays separate views for SLA alerts and pipeline alerts.

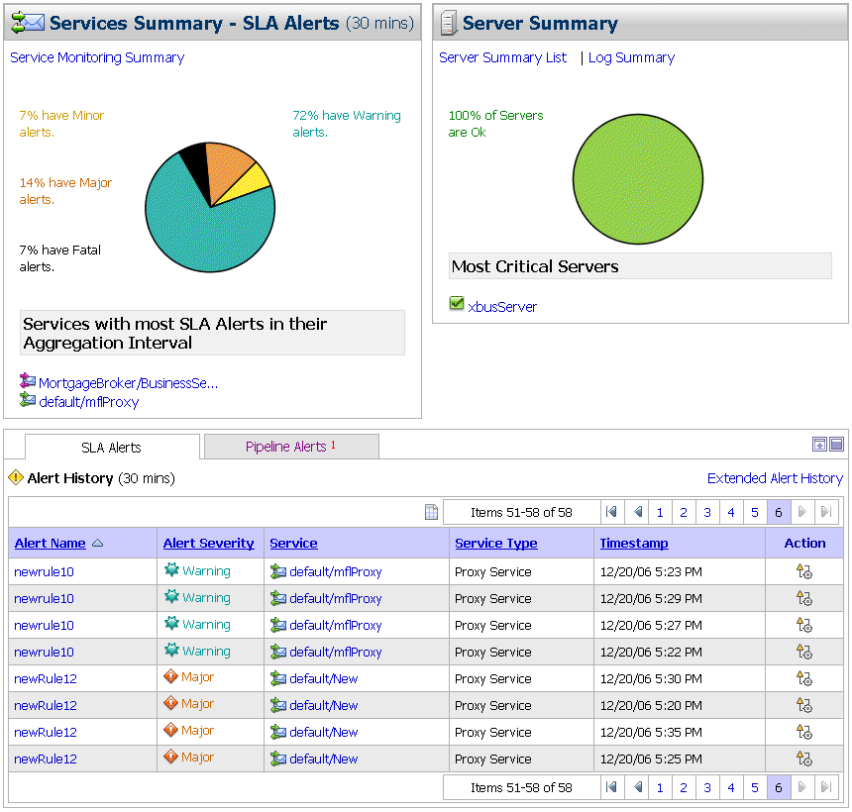
The following sections contain information for:


- "Understanding the Dashboard for SLA Alerts" on page 3-17
- "Understanding the Dashboard for Pipeline Alerts" on page 3-29
- "Understanding the Server Summary" on page 3-34


## Understanding the Dashboard for SLA Alerts

When you log onto the AquaLogic Service Bus Console, by default the dashboard for SLA alerts Figure 3-6 is displayed. The dashboard shows the monitoring information for the alert history duration set in the dashboard settings page. It provides an overview of the state of the system—comprised of services, server, and alerts.

**Figure 3-6 AquaLogic Service Bus Dashboard-SLA Alerts**




The following sections provide information for:

- “Understanding Services Summary Panel for SLA Alerts” on page 3-19
- “Understanding the Service Monitoring Summary” on page 3-20
- “Viewing Service Monitoring Details” on page 3-22
- “Understanding the Alert History for SLA Alerts” on page 3-26
- “Viewing the Extended Alert History for SLA Alerts” on page 3-27

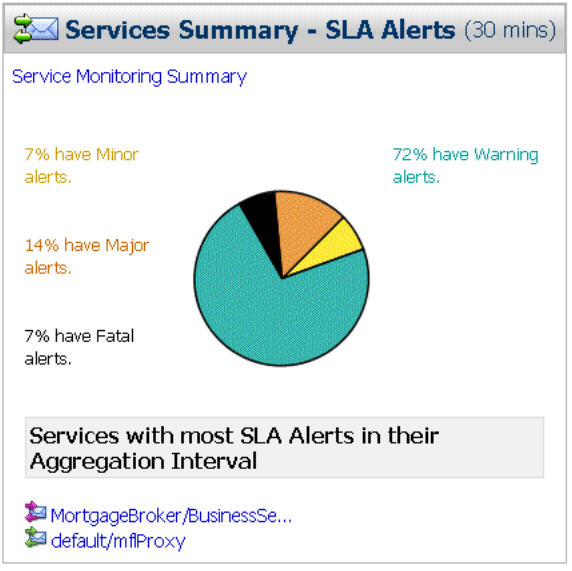
## Understanding Services Summary Panel for SLA Alerts

The Service Summary panel provides an overview of the state of the services. The Service Summary 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. Severity types include

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

The services having the most number of alerts are listed beneath the pie chart, as shown in Figure 3-7. Up to ten services are listed in descending order of services with the most alerts in their respective current aggregation interval.

**Figure 3-7 Services Summary Panel for SLA Alerts**



From the Service Summary panel, you can access more information about alerts by clicking the following:

- A specific area on a pie chart: displays the Extended SLA Alert History page for alerts for the given level of severity.
- The name of a service under Services With Most Alerts In Their Aggregation Interval: displays the Service Monitoring Details page for that service. For more information on Service Monitoring Details page, see "Viewing Service Monitoring Details" on page 3-22.
- Service Monitoring Summary: displays the Service Monitoring Summary page. To help you locate specific services, you can filter the services by different criteria. For more information on Service Monitoring Summary page, see "Understanding the Service Monitoring Summary" on page 3-20.

**WARNING:** When a service (or its component; for example, a pipeline node) is renamed or relocated, its statistical data is lost.

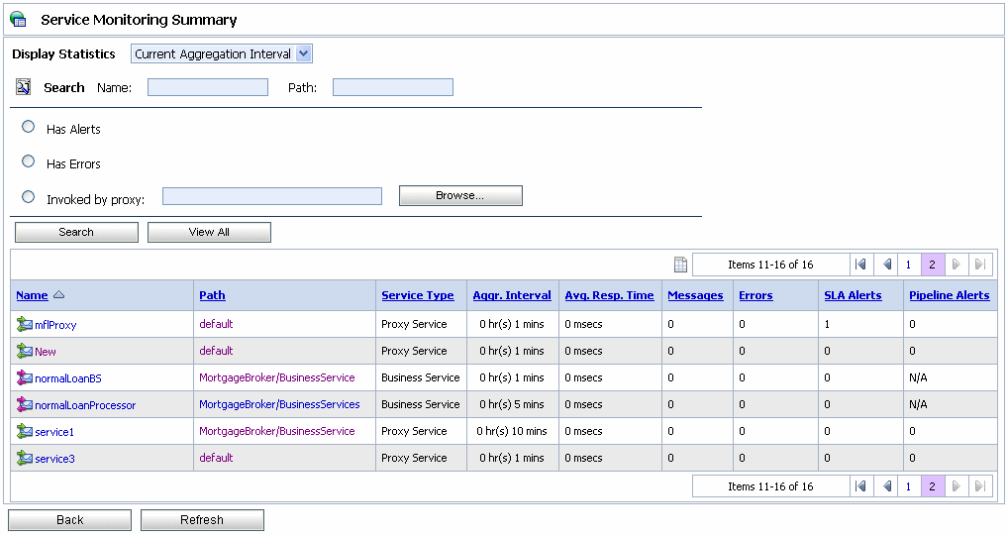
For information on how to access detailed alert information, see "Viewing the Dashboard Statistics" in Monitoring in the *Using the AquaLogic Service Bus Console*.

## Understanding the Service Monitoring Summary

The Service Monitoring Summary page provides two views of service monitoring statistics, as shown in Figure 3-8 and Figure 3-9.

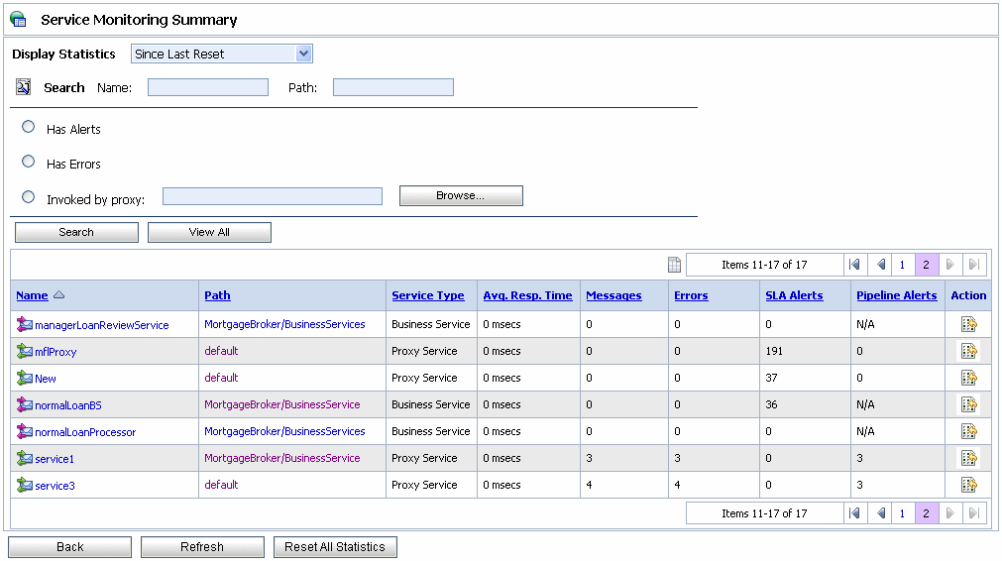
The first is a dynamic view of statistical data collected by each service. This view is available when you select Current Aggregation Interval in the Display Statistics field. The aggregation interval displayed in this view determines the statistics that are displayed. For example, if the aggregation 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 on the statistics displayed in this page, in the Current Aggregation Interval view, see Listing and Locating Service Metrics—Monitoring in *Using the AquaLogic Service Bus Console*.

**Figure 3-8 Service Monitoring Summary Page—Current Aggregation Interval**




The second view is a running count of the 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 selected services or for all services. For more information on the statistics displayed in this page, in the Since Last Reset view, see Listing and Locating Service Metrics—Monitoring in *Using the AquaLogic Service Bus Console*.

**Figure 3-9 Service Monitoring Summary Page—Since Last Reset**




## Viewing Service Monitoring Details

The Service Monitoring Details page provides you with two views of detailed information about a specific service, as shown in Figure 3-10 and Figure 3-11.

The first 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 on the statistics displayed in this page, in the Current Aggregation Interval view, see Listing and Locating Service Metrics—Monitoring in *Using the AquaLogic Service Bus Console*.

## Figure 3-10 Service Monitoring Details Page—Current Aggregation Interval

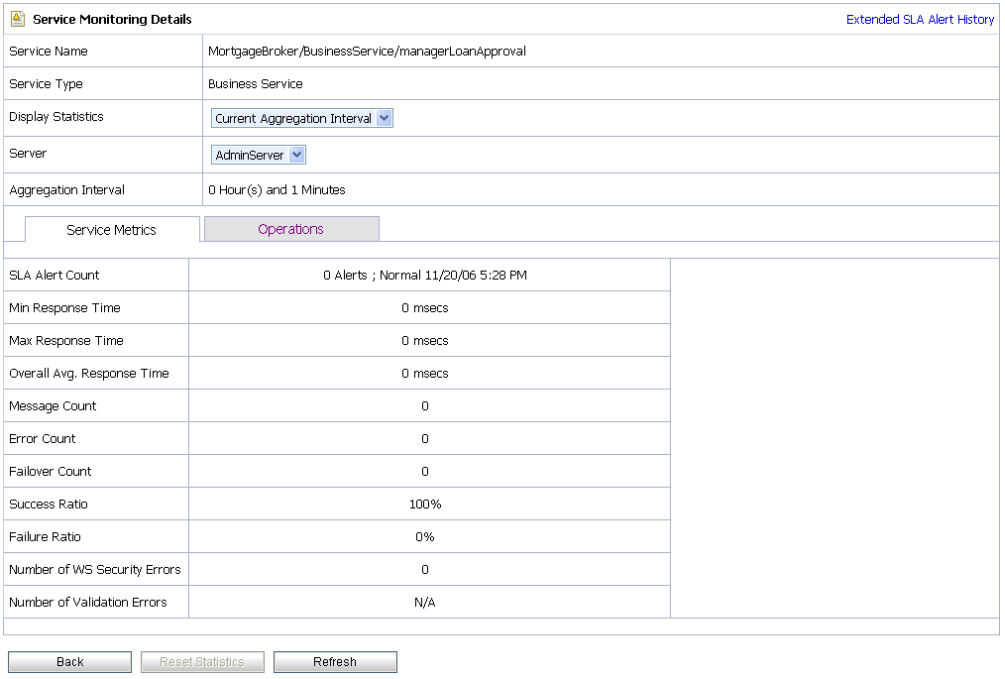
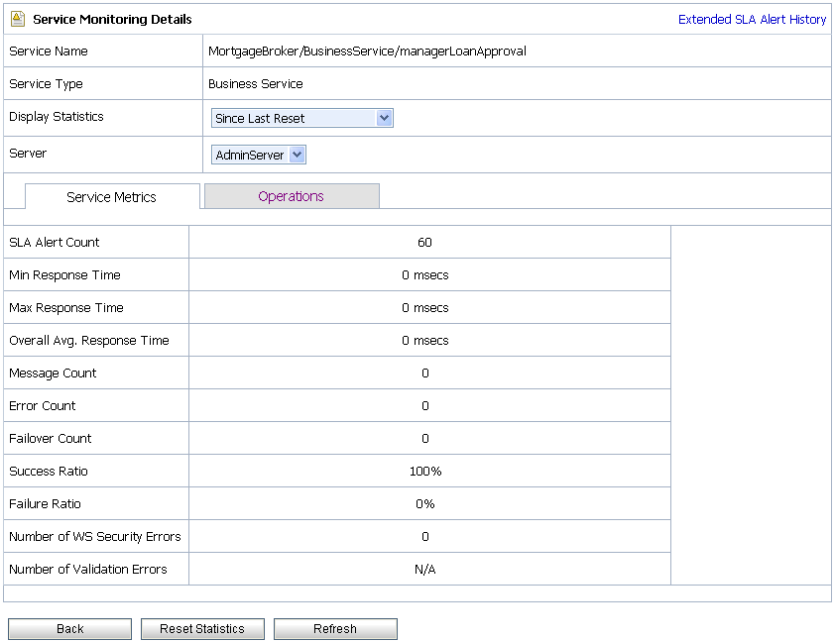


**Figure 3-11 Service Monitoring Details Page—Since Last Reset**

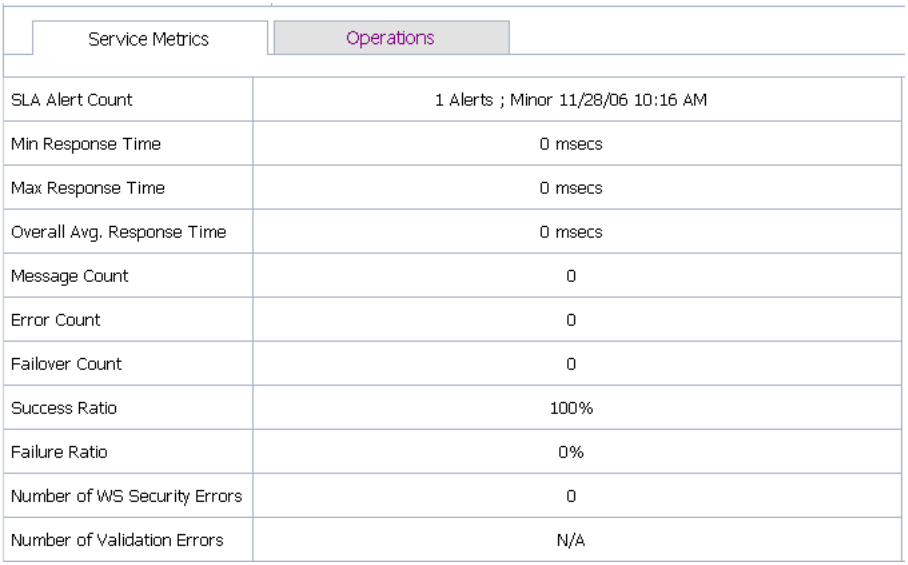



The second view is a running count of the metrics. This view is available when you select Since Last Reset in the Display Statistics field. The statistics displayed in each row are for the period since you last reset the statistics for an individual service or since you last reset the statistics for 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 on the statistics displayed in this page, in the Since Last Reset view, see Listing and Locating Service Metrics—Monitoring in *Using the AquaLogic Service Bus Console*.

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

- Service Metrics: The Service Metrics (see Figure 3-12) view displays the metrics for a proxy service or a business service.

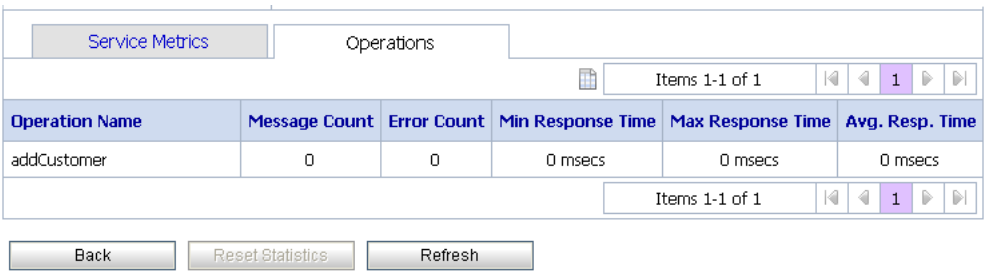
**Figure 3-12 Service Monitoring Details Page for a Business Service-Service Metrics View**




This panel 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 the total number of alerts since last reset. For more information on the metrics displayed in this view, see Viewing Service Monitoring Details—Monitoring in *Using the AquaLogic Service Bus Console*

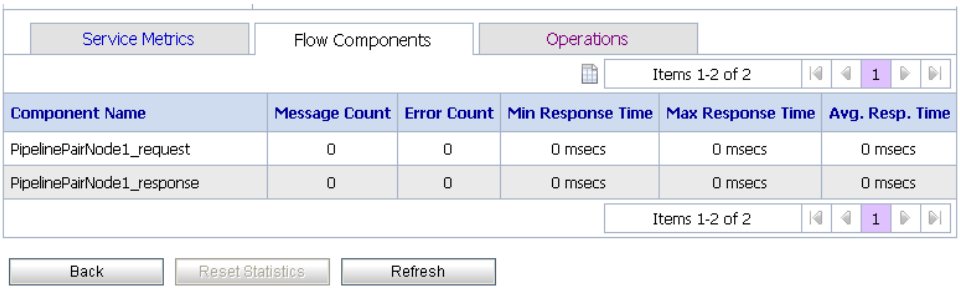
- Operations: This is displayed for WSDL based services for which you have defined operations. The Operations view (see Figure 3-13) displays the statistics for the operation defined in a service. For more information statistics displayed in this view, see Viewing Service Monitoring Details—Monitoring in *Using the AquaLogic Service Bus Console*.

**Figure 3-13 Service Monitoring Details Page-Operation View**



- Flow Components: This view gives information on various components of the pipeline of the service. The Flow Components view is available only for proxy services. For more information on the statistics displayed in this view, see Viewing Service Monitoring Details—Monitoring in *Using the AquaLogic Service Bus Console*.

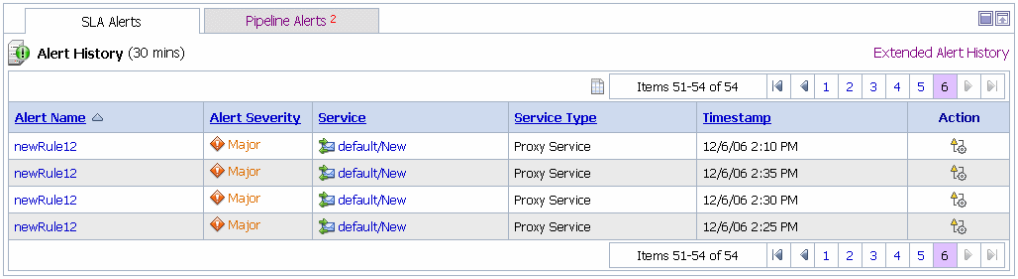
**Figure 3-14 Service Monitoring Details Page-Flow Components View for Proxy Services**




## Understanding the Alert History for SLA Alerts

The Alert History (Figure 3-15) for SLA alerts table shows all the SLA alerts, which have occurred in the alert history duration you have set in the dashboard settings page. It contains the following details:

**Figure 3-15 Alert History for SLA Alerts**




- Alert Name—the name of the alert rule. The name is a link to the Alert Details page, which contains the details of the alert. For more information on Alert Details page, see "Viewing Alert Details" on page 3-10.
- Alert Severity—the user-defined severity of the alert. The Severity is a link to the Alert Details page.

- Service—the name of the service and project associated with the alert. The name is a link to the Service Monitoring Details page. See "Viewing Service Monitoring Details" on page 3-22.
- Service Type—whether the service is a proxy service or a business service.
- Timestamp—the time when the alert occurred in the pipeline in the format MM/DD/YY HH:MM AM/PM.
- Action—click the view alert rules details  icon to go to the View Alert Rules Details page. For more information on View Alert Rules Details page, see "Viewing Alert Details" on page 3-10.

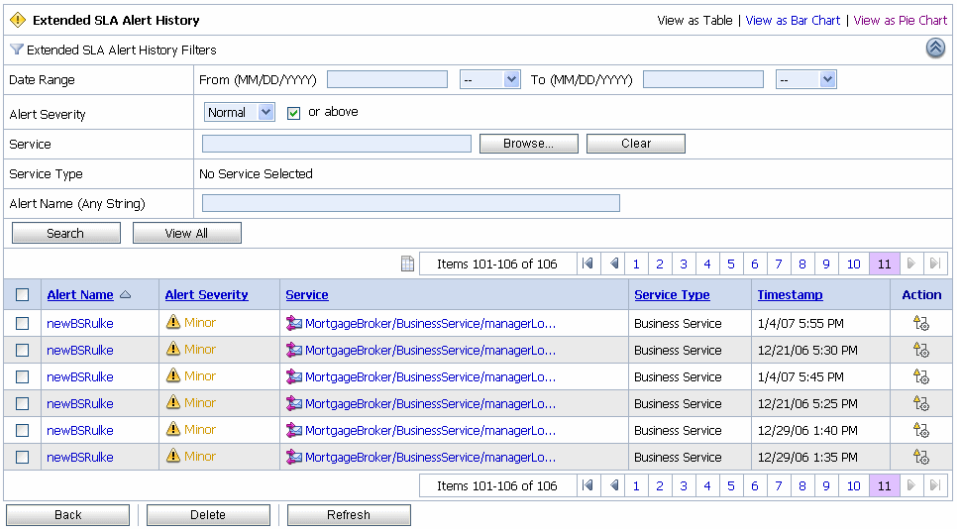
To customize the information displayed in the **Alert History** table, click customize table  icon above the table. The available filtering is shown in the Figure 3-21. For more information on customizing the alert history table, see Customizing Table Views—Monitoring in *Using the AquaLogic Service Bus Console*

To view a complete list of alerts, click Extended Alert History. For more information on Extended Alert History, see "Viewing the Extended Alert History for SLA Alerts" on page 3-27.

## Viewing the Extended Alert History for SLA Alerts

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 on data displayed in the extended SLA alert history page, see Listing and Locating Alerts—Monitoring in *Using the AquaLogic Service Bus Console*.

**Figure 3-16 Extended SLA Alert History**



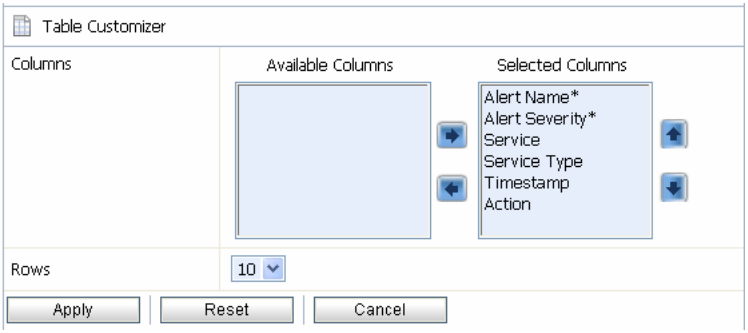

You can delete the alerts from this page or go to the View Alert Rules Page. You can filter your search using the Extended Alert History Filters pane. You can filter using the following criteria:

- Date
- Alert Severity
- Service
- Service Type
- Alert Name

To view a pie or bar chart of the alerts, click View Bar Chart or View Pie Chart in the page.

You can also customize the table depending on information you require. To customize the information displayed in the table click on the table customizer icon. You must use the Table Customizer (see Figure 3-17) to customize the information displayed in the Extended SLA Alert History table.

**Figure 3-17 Table Customizer**

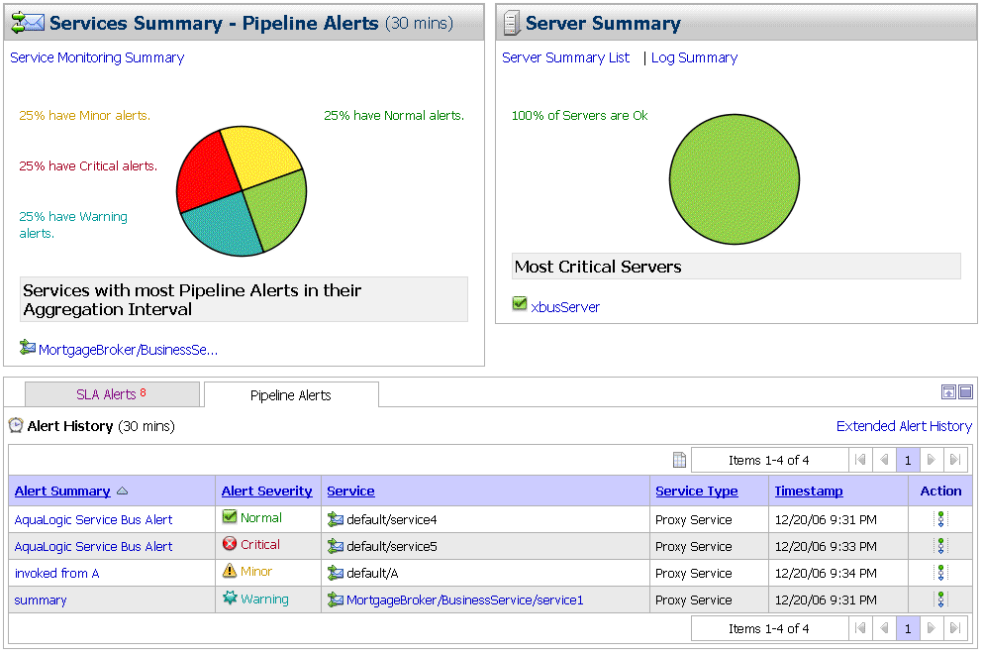



For information about how to use the customizing your search, see "Customizing Your View of Alerts" in Monitoring in the *Using the AquaLogic Service Bus Console*.

## Understanding the Dashboard for Pipeline Alerts

When you log onto AquaLogic Service Bus Console, by default the dashboard for SLA alerts is displayed. Click on Pipeline Alerts to view the dashboard for the pipeline alerts.The dashboard shows the monitoring information for the last thirty minutes. It provides an overview of the state of the system—organized by server, services, and pipeline alerts, as shown in Figure 3-18.

**Figure 3-18 AquaLogic Service Bus Dashboard for Pipeline Alerts**



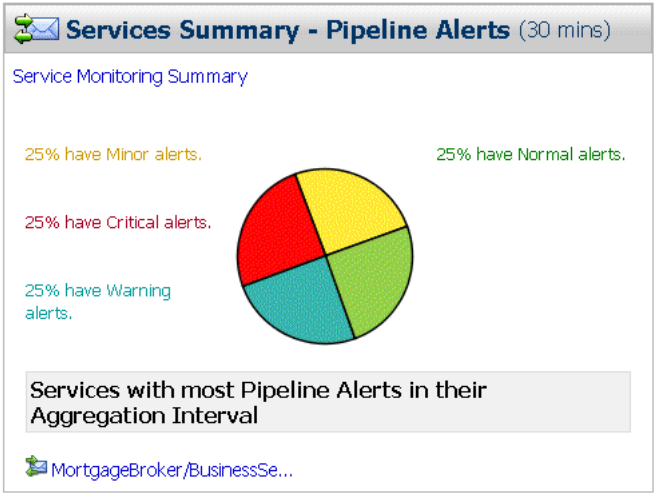

This section contains information for:

- "Understanding the Services Summary Panel for Pipeline Alerts" on page 3-30
- "Understanding Alert History for Pipeline Alerts" on page 3-32
- "Extended the Alert History for Pipeline Alerts" on page 3-33

## Understanding the Services Summary Panel for Pipeline Alerts

The services summary panel (see Figure 3-19) shows the distribution of alerts based on their severity.

**Figure 3-19 Service Summary Panel for Pipeline Alerts**




It provides an overview of the state of the services. The Service Summary pie chart shows the percentage of pipeline alerts according to their severity for all services for the alert history duration set in the dashboard settings page. The severity level of alerts is user configurable and has no absolute meaning. Severity types include

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

The services having the most number of alerts are listed beneath the pie chart, as shown in Figure 3-19. Up to ten services are listed in descending order of services with the most alerts.

From the Service Summary panel, you can access more information about alerts by clicking the following:

- A specific area on a pie chart: displays the Extended Pipeline Alert History page for alerts for the given level of severity.

- The name of a service under Services With Most Alerts In Their Aggregation Interval: displays the Service Monitoring Details page for that service. For more information on Service Monitoring Details page, see "Viewing Service Monitoring Details" on page 3-22.
- Service Monitoring Summary: displays the Service Monitoring Summary page. To help you locate specific services, you can filter the services by different criteria. For more information on Service Monitoring Summary page, see "Understanding the Service Monitoring Summary" on page 3-20.

**WARNING:** When a service (or its component; for example, a pipeline node) is renamed or relocated, its statistical data is lost.

For information on how to access detailed alert information, see "Viewing the Dashboard Statistics" in Monitoring in the *Using the AquaLogic Service Bus Console*.

## Understanding Alert History for Pipeline Alerts

The Alert History (see Figure 3-20) for pipeline alerts displays the details of all the pipeline alerts that have been triggered in the last alert history duration set in the dashboard settings page. It contains the following details:

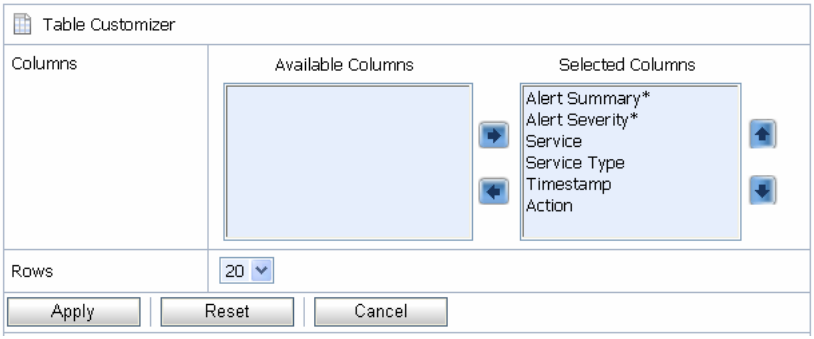
- Alert Summary—the alert summary message you have supplied in the alert action configured in the pipeline. The summary is a link to the Alert Details page, which contains the details of the alert. For more information on Alert Details page, see "Viewing Alert Details" on page 3-10.
- Alert Severity—the severity of the pipeline alert.
- Service—the name of the service with full path.
- Service Type—type of the service.
- Timestamp—the time when the alert occurred in the pipeline in the format MM/DD/YY HH:MM AM/PM.
- Action—click on the  edit pipeline icon to edit the message flow.

**Figure 3-20 Alert History for Pipeline Alerts**


To view a complete list of alerts, click Extended Alert History. For more information on Extended Alert History, see "Extended the Alert History for Pipeline Alerts" on page 3-33.

To customize the information displayed in the Alert History table, click customize table  icon above the table. The available filtering is shown in the Figure 3-21.

**Figure 3-21 Table Customizer**

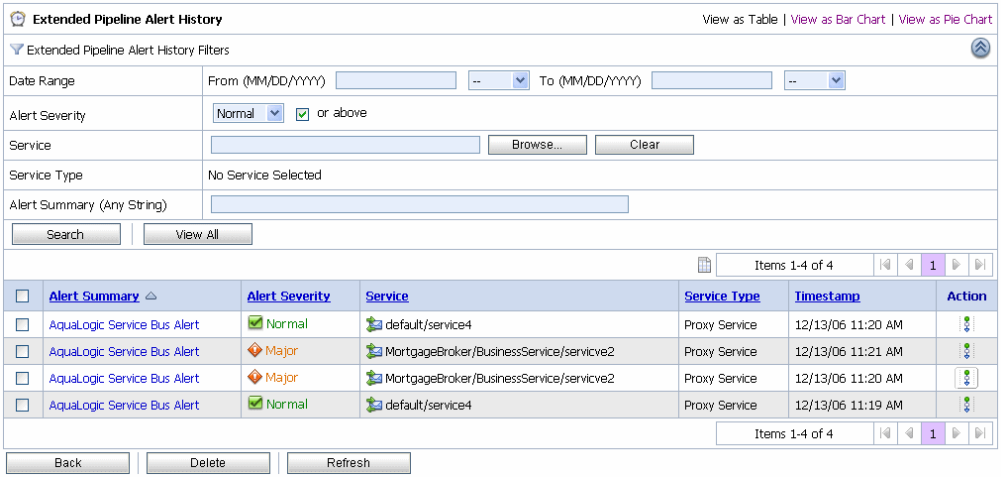



To customize the sort order of the displayed alerts, click the sort icons beside the column headers.

## Extended the Alert History for 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, see Listing and Locating Alerts—Monitoring in *Using the AquaLogic Service Bus Console*.

**Figure 3-22 Extended Pipeline Alert History**




You can filter your search using the Extended Alert History Filters pane. You can filter using the following criteria:

- Date
- Alert Severity
- Service
- Service Type
- Alert Summary

To view a pie or bar chart of the alerts, click View Bar Chart or View Pie Chart in the page.

You can also customize the table depending on information you require. To customize the information displayed in the table click on the table customizer icon. You must use the Table Customizer (see Figure 3-17) to customize the information displayed in the Extended Pipeline Alert History table. For more information, see

## Understanding the Server Summary

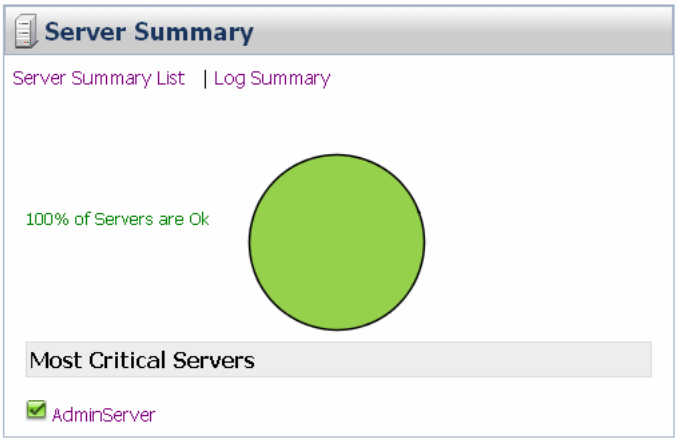
The Server Summary panel displays the status of all the servers associated with the domain. It provides an overview of the state of the servers. The pie chart shows the status of each server in

the domain. The status for each server is derived from the WebLogic Diagnostic Service. The five most critical servers are displayed, as shown in Figure 3-23.

**Note:** The Server Summary panel is common for both SLA alert view and pipeline alert view of the dashboard.

For more information about the WebLogic Diagnostic Service, see *Configuring and Using the WebLogic Diagnostics Framework*.

**Figure 3-23 Server Summary panel**




The displayed status has the following meanings:

- `Fatal`—the server has failed and must be restarted.
- `Critical`—server failure likely; something must be done immediately to prevent failure. For more details, check the server logs and the corresponding `RuntimeMBean`.
- `Warning`—the server could have problems in the future. For more details, check the server logs and the corresponding `RuntimeMBean`.
- `OK`—the server is functioning without any problems.
- `Overloaded`—the server has more work assigned to it than the configured threshold; it might refuse more load.

This section contains the following information for:

- "Understanding the Log Summary" on page 3-36

- "Viewing Server Summary List" on page 3-39
- "Viewing Server Details" on page 3-41

## Understanding the Log Summary

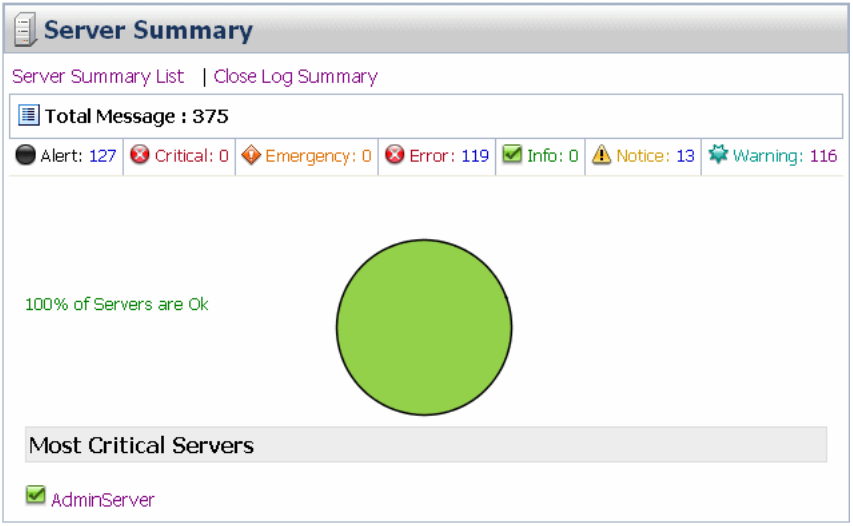
The Log Summary page displays the summary log for the servers associated with the domain. The domain log file provides a central location from which to view the overall status of the domain. Each server instance forwards a subset of its messages to a domain-wide log file. By default, servers forward 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 server log. Unless you configure WebLogic Server to forward these messages to the domain log, you cannot view this log from AquaLogic Service Bus Console. For information in 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 3-24.

**Note:** You can view the log summary only if you posses administrator privileges in the WebLogic Server Console.

**Figure 3-24 Log Summary**



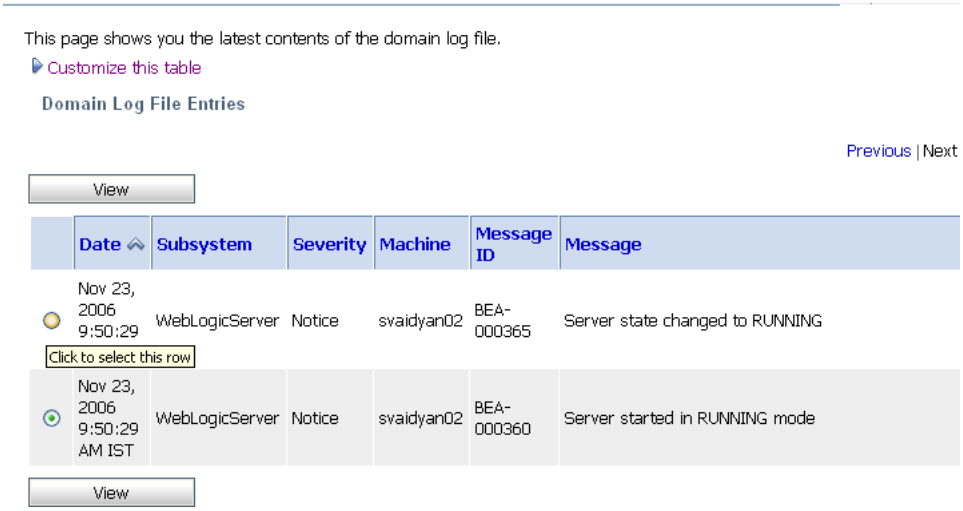

The displayed message statuses have the following meanings:

- Alert—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—a system or service error has occurred. The system can recover but there might be a momentary loss or permanent degradation of service.
- Emergency—the server is in an unusable state. This severity indicates a severe system failure.
- Error—a user error has occurred. The system or application can handle the error with no interruption. Limited degradation of service may occur.
- Info—reports normal operations; a low-level informational message.
- Notice—an informational message with a higher level of importance than Info messages.
- Warning—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 type of message, click the number corresponding with the type of message. Figure 3-25 shows an example of a domain log file displayed in the AquaLogic Service Bus Console.

**Figure 3-25 Domain Log File Entries**




The following information is displayed:

- Date—the date and time the entry was logged in a format that is specific to the local time zone and format.
- Subsystem—the WebLogic Server subsystem that was the source of the message, such as the EJB container or Java Messaging Service (JMS).
- Severity—indicates the degree of impact or seriousness of the event.
- Message ID—the unique six-digit identification for the message.
- Message—a description of the event or condition.

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:

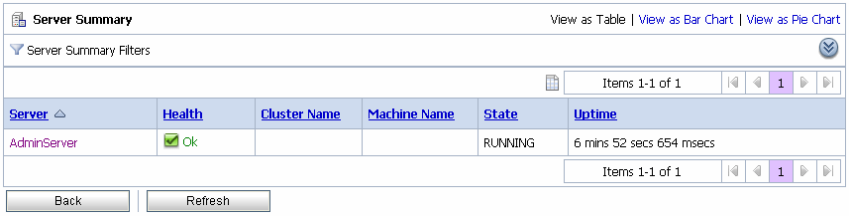
- Machine
- Server
- Thread
- User ID
- Transaction ID
- Context ID
- Timestamp

For additional description of these information, see Viewing Details of Server Log Files—Monitoring in *Using the AquaLogic Service Bus Console*. For more information on how to customize the Domain Log File Entries table, see Customizing Your View of Domain Log File Entries—Monitoring in *Using the AquaLogic Service Bus Console*.

## Viewing Server Summary List

The Server Summary page provides a customizable table of servers, as shown in Figure 3-26.

**Figure 3-26 Server Summary Page**




As shown in the upper section of the Figure 3-26, the Server Summary Page displays the number of messages currently raised by the system. For information about the meaning of each type of status message, see "Understanding the Log Summary" on page 3-36.

The server table displays the following information:

- `Health`—the health of the server:
  - `Fatal`—the server has failed and must be restarted.
  - `Critical`—server failure likely; something must be done immediately to prevent failure. For more details, check the server logs and the corresponding `RuntimeMBean`.

  - `Warning`—the server could have problems in the future. For more details, check the server logs and the corresponding `RuntimeMBean`.
  - `OK`—the server is functioning without any problems.
  - `Overloaded`—the server has more work assigned to it than its configured threshold; it cannot take on more load.

    **Note:** Click the check box associated with the status to filter the results based on more than one status value.

- Server—the name of the server. The name is a link to the View Server Details page. See "Viewing Server Details" on page 3-41.
- Cluster Name—if the server is part of a cluster, the name of the cluster.
- Machine Name—the name of the computer associated with the server.
- State—the state of the server:
  - `RUNNING`
  - `FAILED`
  - `SHUTDOWN`
- Uptime—the duration for which this server has been running.

To view this information in the table as a pie or bar chart, click View as a Bar Chart or View as a Pie Chart.

To filter the display of servers, click Customize Table above the server table. The available filtering is shown in Figure 3-27.

**Figure 3-27 Server Summary Table Filter**

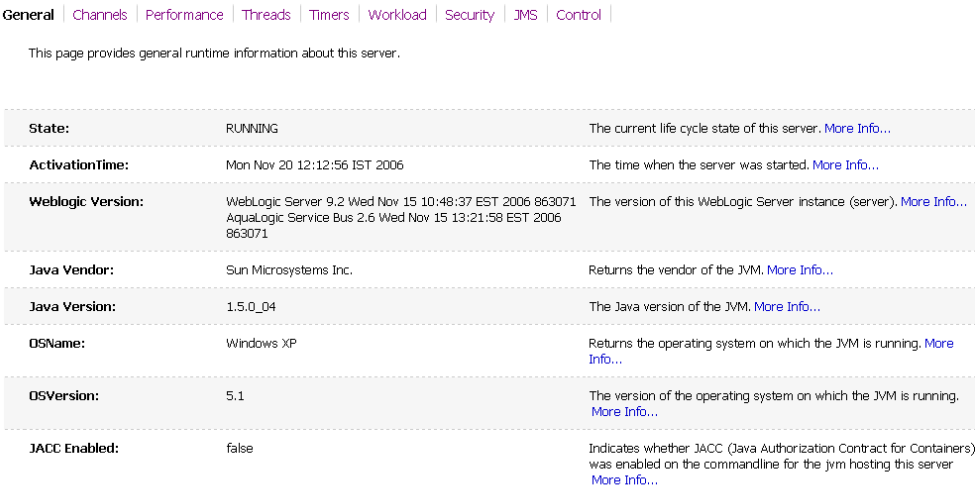

For information about how to use the Server Summary Table Filter, see "Customize Your View of the Server Summary" in Monitoring in the *Using the AquaLogic Service Bus Console*.

## Viewing Server Details

You can access the View Server Details page by clicking the name of a server under Most Critical Servers or by clicking the name of a server in the Servers Summary page.

The View Server Details page enables you to view more server monitoring details, as shown in Figure 3-28.

**Figure 3-28 Server Details Page—General Tab**




The information displayed on this page is a subset of the Monitoring tab in the AquaLogic Service Bus Console Server Settings page. The details available are:

- General—provides general run-time information about the server. Click Advanced to view more information, such as WebLogic Server version or operating system name.
- Channels—displays monitoring information about each channel.
- Performance—displays performance information about the server.
- Threads—displays current run-time characteristics and statistics for the server's active executable queues.
- Timers—displays information about the timer used by the server.
- Workload—displays statistics for work managers, constraints, and policies configured on the server.
- Security—allows you to monitor user-lockout management statistics for the server.
- JMS—allows you to monitor JMS information about the server.
- JTA—displays the summary of all transaction information for all resource types on the server.

For more information, see *WebLogic Server Administration Console Online Help*.

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.

You configure the dashboard and monitoring in the AquaLogic Service Bus Console, which is described in the Monitoring section of *Using the AquaLogic Service Bus Console*.

# Monitoring Operations

The following sections describe some of the tools and functionality available in the AquaLogic Service Bus Console to monitor messages and system operations. It includes:



## Monitoring Services

When you create a business service or a proxy service, monitoring is disabled by default for that service. This section describes:



### Configuring Operational Settings for Individual Services

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 3-29) or View a Business Service page (see Figure 3-30).

**Figure 3-29 View a Proxy Service**

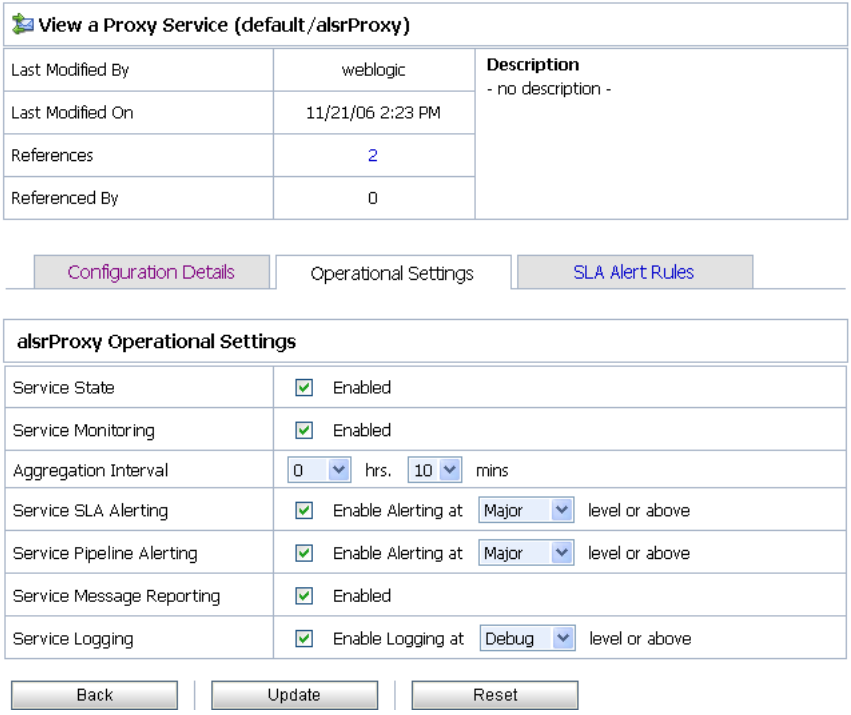
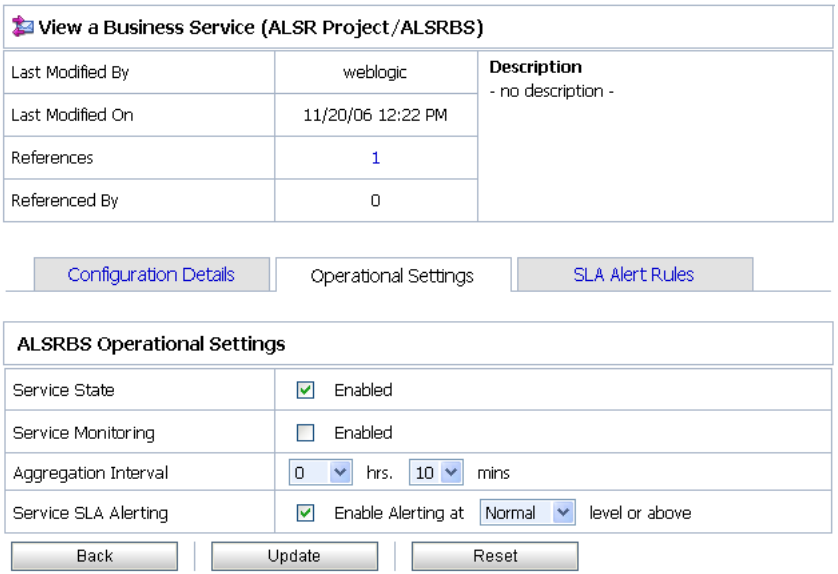


**Figure 3-30 View a Business Service**




The View a Proxy Service or View a Business Service pages contain the following information about a proxy service or a business service:

- Configurational Details: This view contain all the configurational details of a service.
- SLA Alert Rules: This view contains the summary of alert rules.
- Operational Settings: You must use the Operational Settings view to enable or disable the following for individual services:
  - Service State: You must use this setting to enable or disable a service.
  - Service Monitoring: You must use this setting to enable or disable monitoring for a service.
  - Aggregation Interval: You must use this to set the aggregation interval in terms of hours and minutes. For more information on Aggregation interval, see "Aggregation Intervals" on page 3-15.
  - Service SLA Alerting: You must use this setting to enable or disable SLA Alerting. You can also set the level at which SLA alerting is enabled for the service. The supported levels of severity are:
    - `Normal` (default)

- `Warning`
- `Minor`
- `Major`
- `Critical`
- `Fatal`

All alerts that are of same or higher severity will then be raised whenever the rule condition is met.

You can enable or disable the following settings for proxy services only.

– Service Pipeline Alerting: You must use this setting enable or disable pipeline alerting. You can also set the level at which pipeline alerting is enabled for this service. All alert actions that are of same or higher severity will then be raised whenever those actions are executed during message processing. The supported levels of severity are:

- `Normal` (default)
- `Warning`
- `Minor`
- `Major`
- `Critical`
- `Fatal`

– Service Message Reporting: You must use this setting to enable or disable message reporting actions in a pipeline.

– Service Pipeline Logging: You must use this setting to enable or disable logging actions in a pipeline. You can also set the level at which pipeline logging is enabled for this service. For all log actions of same or higher level the output will be written to the server log whenever those actions are executed during message processing. The supported levels of severity are:

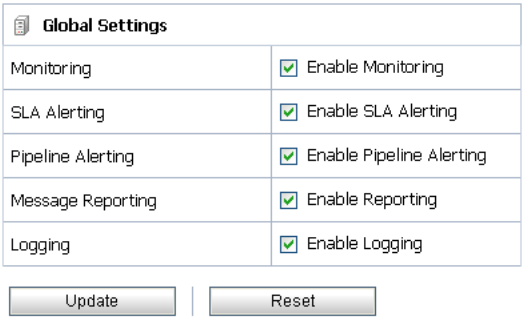
- `Debug`
- `Info`
- `Warning`
- `Error`

## Configuring Operational Settings at a Global Level

You can access the Global Settings page from the operations module. You can use the Global Settings page (see Figure 3-31) to configure the following operational settings for services:

- Monitoring: To enable monitoring for all services, select the Enable Monitoring checkbox on the Global Settings page.
- SLA Alerting: To enable SLA alerting for all services, select the Enable SLA Alerting checkbox on the Global Settings page.
- Pipeline Alerting: To enable pipeline alerting for proxy services, select the Enable Pipeline Alerting checkbox on the Global Settings page.
- Message Reporting: To enable message reporting for proxy services, select the Enable Message Reporting checkbox on the Global Settings page.
- Logging: To enable logging for proxy services, select the Enable Logging checkbox on the Global Settings page.

**Figure 3-31 Global Settings Page**




**Notes:**

- The Enable Monitoring option permits 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.

# Monitoring Service Statistics

Monitoring Statistics helps you know how many messages in a particular service have processed successfully and how many have failed. To access this information, from the Dashboard, you access the Service Monitoring Summary page and filter the display for the relevant service. Besides displaying the number of messages that have been processed successfully or failed, you can also see which project the service belongs to, the average execution time of message processing, and the number of alerts associated with the service. 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.

You use the Service Monitoring Summary page or the Service Monitoring Details page with Display Statistics set to Since Last Reset to reset statistics.

**Caution:** When you reset the statistics, make sure you are not in a WebLogic session on the WebLogic Server Administration Console.

Clicking the name of the service brings you to that service's Service Monitoring Details page. This page provides additional information such as the minimum and maximum response times and the overall average time it takes for the service to execute a message, the success-failure ratio, the number of messages that have failed because of security or validation errors, and the number of messages associated with proxy service components (pipelines and route nodes). You can view this information for specific operations associated with the service. Again, you can view these statistics for the period of the current aggregation interval or you can display the statistics for the period since you last reset statistics for this service or since you last reset statistics for all services.

To view the statistical information for business service operations in the Service Monitoring Details page, you must mention the name of the operation that is being invoked in the route node of the proxy service that routes messages to the business service. For example, say proxy service A routes messages to business service B, for operation C. The Service Monitoring Details page for the business service B increments the message count for operation C in conjunction with the Service Monitoring Summary page only if the binding and the transport layers of the AquaLogic Service Bus recognize the operation that is invoked. You can achieve this in one of the following ways:

- Configure the name of the operation in the route node of the proxy service.
- Use a request action in the route node to modify the value of the operation element in variable `$outbound`, for example

  ```
  insert "<ctx:operation>foo</ctx:operation>"
  ```

as last child element in "./ctx:service", where `foo` is the name of the operation that is invoked.

- Click the check box associated with " Use inbound operation for outbound " in the Edit Stage Configuration page of a route node in a pipeline of the proxy service.

If you do not mention name of the operation in the route node of the proxy service, the binding and transport layers of the AquaLogic Service Bus fail to recognize the operation that is invoked. Hence the metrics for operation C will not be incremented in the Service Monitoring Details page (for business service B) in conjunction with the Service Monitoring Summary page, which will be incremented to reflect the number of messages sent to the business service B.

# Statistics Associated With Different Resources

The following section provides more information on different statistics associated with:


- "SERVICE" on page 3-49
- "FLOW_COMPONENT" on page 3-50
- "WEBSERVICE_OPERATION" on page 3-51


## SERVICE

A service has an inbound endpoint or an outbound endpoint that is registered with the Service Directory of AquaLogic Service Bus. Such services are associated with other resources such as WSDLs, and security settings. The statistics reported for this resource type is listed in Table 3-1. It also give you the type of the statistics.

**Table 3-1 Statistics Reported for SERVICE**

| Statistic | Type |
|---|---|
| `message-count` | count |
| `error-count` | count |
| `failover-count` | count |
| `response-time` | interval |
| `validation-errors` | count |
| `sla-severity-warning` | count |

**Table 3-1 Statistics Reported for SERVICE**

| Statistic | Type |
|---|---|
| sla-severity-major | count |
| sla-severity-minor | count |
| sla-severity-normal | count |
| sla-severity-fatal | count |
| sla-severity-critical | count |
| sla-severity-all | count |
| pipeline-severity-warning | count |
| pipeline-severity-major | count |
| pipeline-severity-minor | count |
| pipeline-severity-normal | count |
| pipeline-severity-fatal | count |
| pipeline-severity-critical | count |
| pipeline-severity-all | count |
| failure-rate | count |
| wss-error | count |
| success-rate | count |

# FLOW_COMPONENT

Statistics are collected for two FLOW_COMPONENT types, namely, Pipeline-pair nodes and Route notes. For more information on Pipeline-pair node and route node, see Building Message Flow —Modeling Message Flow in *AquaLogic Service Bus User Guide*. The statistics reported for FLOW_COMPONENT are listed in Table 3-2.

**Table 3-2 Statistics Reported For FLOW_COMPONENT**

| Statistic | Type |
|---|---|
| `elapsed-time` | interval |
| `message-count` | count |
| `error-count` | count |

## WEBSERVICE_OPERATION

The statistics pertaining to the WEBSERVICE_OPERATION resources such as WSDLs, are collected and stored in a runtime XML file. The statistics reported for this type of resource are listed in Table 3-3.

**Table 3-3 Statistics Reported for WEBSERVICE_OPERATION**

| Statistics | Type |
|---|---|
| `elapsed-time` | interval |
| `message-count` | count |
| `error-count` | count |

# Auditing

Auditing helps you to keep track of changes in the configuration of the AquaLogic Service Bus. The three types of auditing you can perform are briefly described in:

- "Configuration Change Auditing" on page 3-51
- "Auditing of Messages at Runtime" on page 3-52
- "Auditing Security" on page 3-52

## Configuration Change Auditing

When you perform configurational changes in AquaLogic Service Bus console a track record of the changes is generated and history 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, in order to access all the information on configuration you have to activate the session.

## Auditing of Messages at Runtime

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 in order to write the auditing report.

## Auditing Security

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 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 on security auditing, see Configuring the WebLogic Security Framework: Main Steps in *AquaLogic Service Bus Security Guide*.

CHAPTER 4

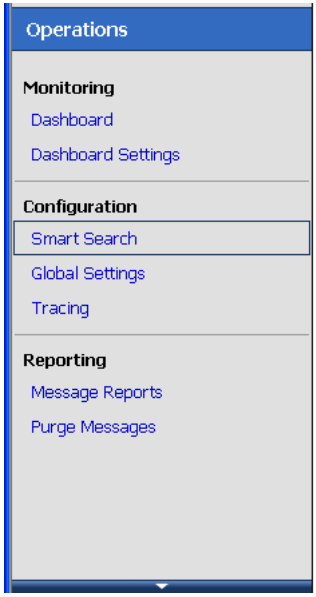
# Using Smart Search

BEA AquaLogic Service Bus provides a Smart Search feature, which is a powerful utility you can use for searching 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 administrative privileges. For more information on the privileges of roles in AquaLogic Service Bus, see Chapter 2, "Roles in AquaLogic Service Bus."

You can also use results of a search to change the operational settings at the service level. But note 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 "Monitoring Services" on page 3-43.

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

**Figure 4-1 Accessing Smart Search**




The following sections describe:

- "Using Basic Search" on page 4-2
- "Using Advanced Search" on page 4-3

# Using Basic Search

Basic Search helps you to search for resources using basic criteria such as resource type or the name of a resource. You can use the basic search functionality to find resources using the following basic criteria:

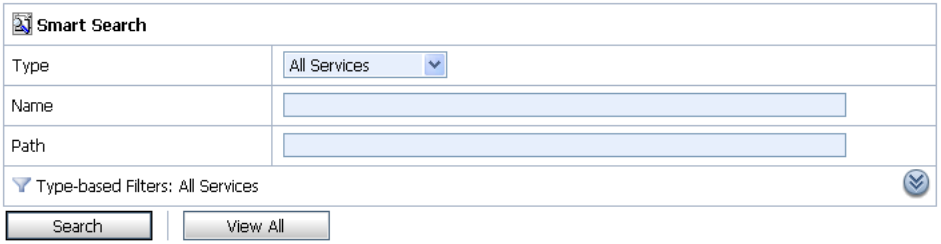
Type: This search criterion is optional. Use the Type drop-down list (see Figure 4-2) to specify the type of resource. You can search for the following types of resource:

- 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 Service Level Agreement (SLA) alert rules.

**Note:** To view all the resources of a given type, choose the resource type in the Type drop-down list and click View All.

**Figure 4-2 Basic Smart Search**




- Name: This search criterion is optional to search for a specific resource.
- Path: This search criterion is optional. Enter a path in the Path field (see Figure 4-2) to specify a location (path) of the resource.

  You can use any one or a combination of these criteria.

# Using Advanced Search

Use the advanced search if you want to configure your search with additional criteria. To use these filters, click  .

This section describes the following:

# Managing Operational Settings for All Services

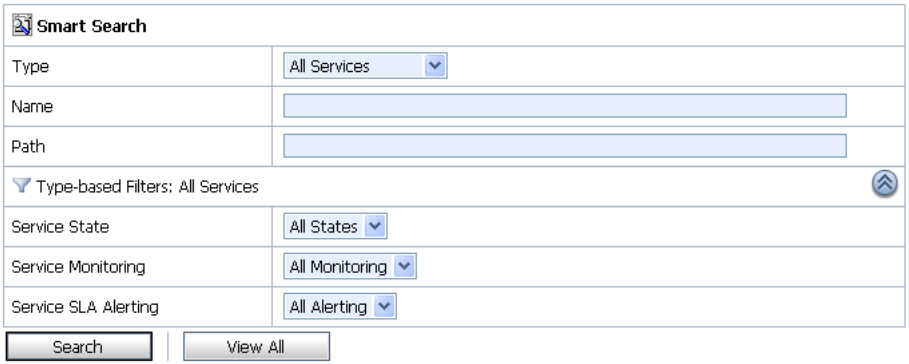
You can search for proxy services and business services in the AquaLogic Service Bus Console using filters in Smart Search. This section describes the following:


- "Finding Services Using Search Filters" on page 4-4
- "View and Edit Operational Settings" on page 4-5


## 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**




You can use the following filters to customize your search for both proxy services and business services:

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

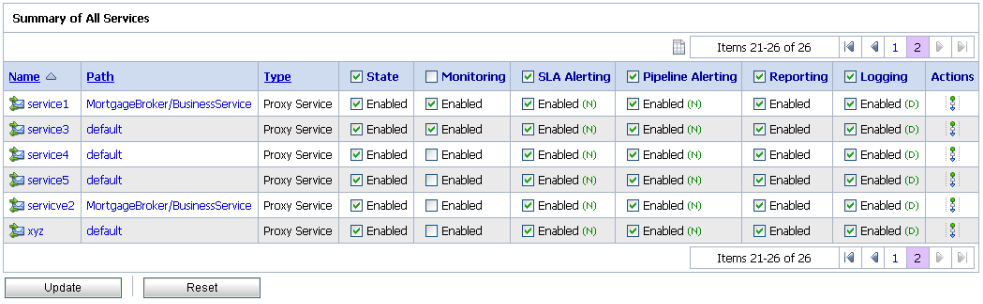
  Click Search to search all services using the set criteria or View All to view all the services.

## View and Edit 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 for both business service and proxy services. You can also use this to enable or disable pipeline alerting, message reporting, and pipeline logging for proxy services. To enable or disable select the check box in the appropriate field and click Update. The runtime effects of these settings also depend on corresponding settings at the global level. For more information on Global Settings, see "Configuring Operational Settings at a Global Level" on page 3-47. You can update the information for one or more services concurrently using this table.

**Figure 4-4 Summary of All Services**




The following information is displayed for all services:

**Table 4-1 Understanding Summary of All Services**

| Property | Description |
|---|---|
| Name | The name assigned to the service. The name is a link to the Operational Settings page. |
| 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:<br>`project-name/root-folder/ . . ./parent-folder`<br>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. |

**Table 4-1 Understanding Summary of All Services**

| Property | Description |
|---|---|
| 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:<br>Normal (N), Warning (W), Minor (Mn), Major (Mj), Critical (C), or Fatal (F). |
| Pipeline Alerting | For proxy services only:<br>The pipeline alerting status: Enabled or Disabled, and the level enabled at and above: Normal (N), Warning (W), Minor (Mn), Major (Mj), Critical (C), or Fatal (F). |
| Reporting | For proxy services only:<br>The message reporting status of the service: Enabled or Disabled. |
| Logging | For proxy services only:<br>The logging status: Enabled or Disabled, and the severity level at which it is enabled:<br>Debug (D), Info (I), Warning (W), or Error (E). |
| 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 on roles, see Chapter 2, “Roles in AquaLogic Service Bus.”

# Managing Operational Settings for Proxy Services

You can search for proxy services in the AquaLogic Service Bus Console using additional filters in Smart Search. This section describes the following:

## 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**


You can use the following filters to customize your search for proxy services:

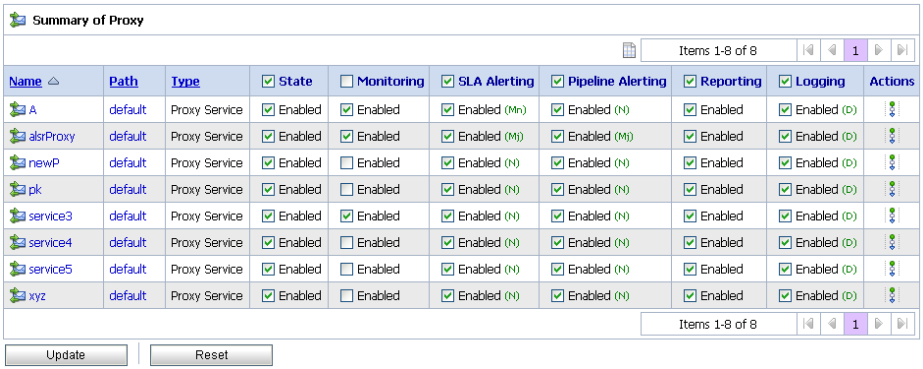
- Service State: Choose Enabled or Disabled from the dropdown list. Choose All States to ignore this filter.
- Service Monitoring: Choose Enabled or Disabled from the dropdown list. Choose All Monitoring to ignore this filter.
- Service SLA Alerting: Choose Enabled or Disabled from the dropdown list. Choose All Alerting to ignore this filter.
- Service Pipeline Alerting: Choose Enabled or Disabled from the dropdown list. Choose All Alerting to ignore this filter.
- Service Message Reporting: Choose Enabled or Disabled from the dropdown list. Choose All Reporting to ignore this filter.
- Service Logging: Choose Enabled or Disabled from the dropdown list. Choose All Logging to ignore this filter.

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

## View and Edit 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**




The Summary of Proxy Services view displays State, Monitoring, SLA Alerting, Pipeline Alerting, Reporting, Logging, Path, Type, Name, and Actions. For more information on the fields displayed in the summary of proxy services, see "View and Edit Operational Settings" on page 4-5.

Use this table to enable or disable proxy services, monitoring, and SLA alerting, pipeline alerting, message reporting, and pipeline logging. To enable or disable select the check box in the appropriate field and click Update. The runtime effects of these settings also depend on corresponding settings at the global level. For more information on Global Settings, see "Configuring Operational Settings at a Global Level" on page 3-47. 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 on roles, see Chapter 2, "Roles in AquaLogic Service Bus."

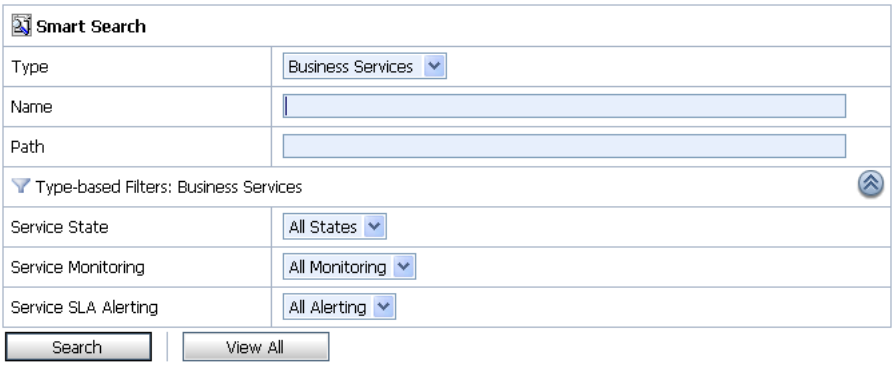
# Managing Operational Settings for Business Services

You can search for business services in the AquaLogic Service Bus Console using additional filters in Smart Search. This section describes the following:

## Finding Business Services Using Search Filters

Figure 4-7 shows the shows the different types of filters you can use for Business Services.

**Figure 4-7 Type Based Filters: Business Services**




You can use the following filters to customize your search for business services:

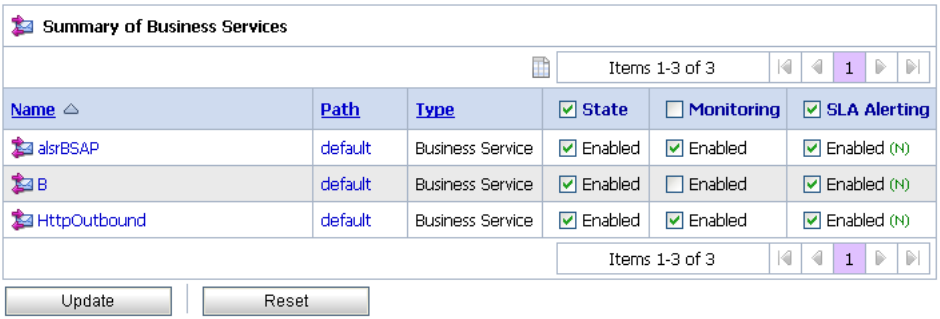
- Service State: Choose Enabled or Disabled from the dropdown list. Choose All States to ignore this filter.
- Service Monitoring: Choose Enabled or Disabled from the dropdown list. Choose All Monitoring to ignore this filter.
- Service SLA Alerting: Choose Enabled or Disabled from the dropdown list. Choose All Alerting to ignore this filter.

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

## View and Edit 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**




The Summary of Business Services view displays State, Monitoring, SLA Alerting, Name, Path, and Type. For more information on the fields displayed in the summary of business services, see "View and Edit Operational Settings" on page 4-5.

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 runtime effects of these settings also depend on corresponding settings at the global level. For more information on Global Settings, see "Configuring Operational Settings at a Global Level" on page 3-47. 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 on roles, see Chapter 2, "Roles in AquaLogic Service Bus."

# Managing Operational Settings for Alert Destinations

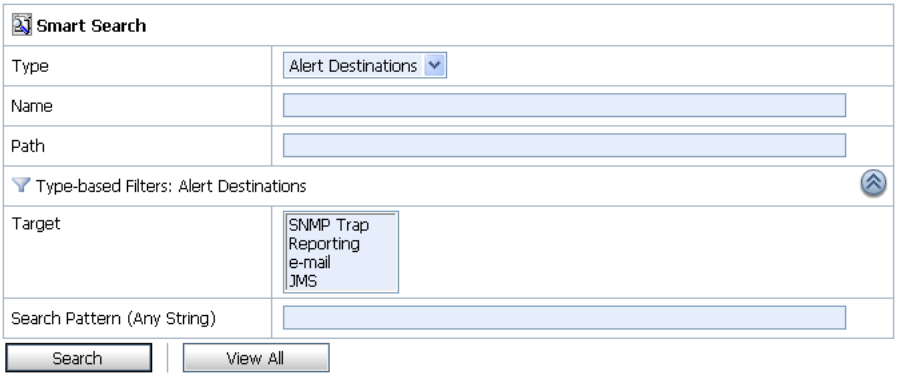
You can search for alert destinations in the AquaLogic Service Bus Console using additional filters in Smart Search. This section describes the following:

- "Finding Alert Destinations using Search Filters" on page 4-10
- "View and Delete Alert Destinations" on page 4-11

## Finding Alert Destinations using Search Filters

Figure 4-9 shows the shows the different types of filters you can use to search for Alert Destinations.

**Figure 4-9 Type Based Filters: Alert Destinations**




You can use the following filters to customize your search for alert destinations:

- Target: You can choose from one of the following options:
  - SNMP Trap
  - Reporting
  - E-mail
  - JMS

  Only alert destinations with at least one of the selected targets will be displayed. By default the Target filter is not applied.

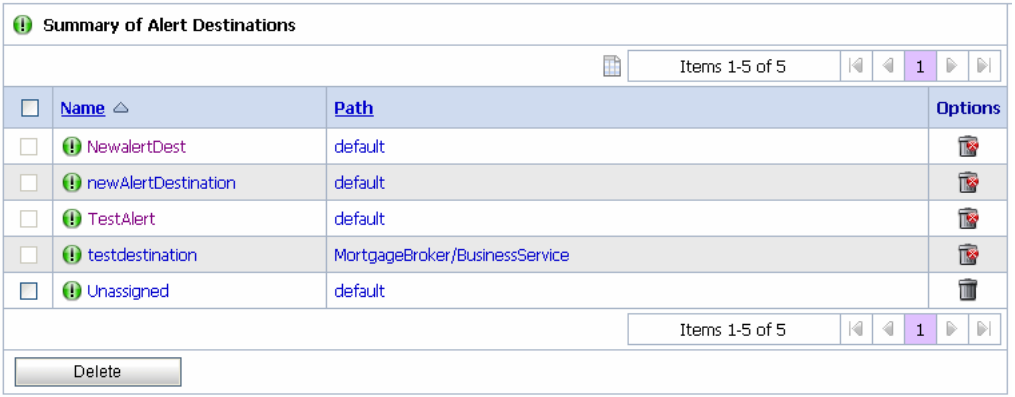
- Search Pattern: The system uses the string to search all the Description fields of the Alert Destinations, as well as the specific detailed fields of the e-mail and JMS destinations. If the string appears in any of the Alert Destination fields, the Alert Destinations matching the search criteria are displayed.

  Click Search to search all alert destinations using the set criteria or View All to view all the alert destinations. For more information on alert destinations, see "Understanding Alert Destination" on page 3-5.

## View and Delete 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**




The following information is provided in the Summary of Alert Destination table:

- Name: This displays the names of the alert destinations that satisfy the search criteria.
- Path: This displays the location of the resource in the AquaLogic Service Bus 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

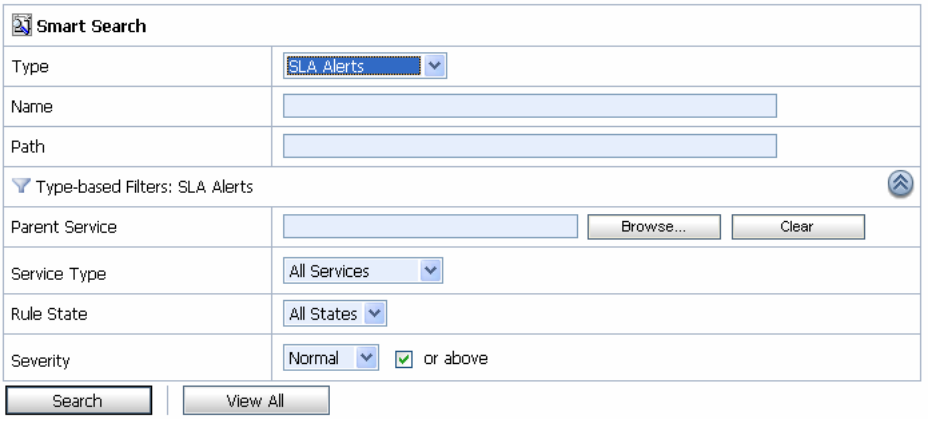
You can search for SLA Alert Rules in the AquaLogic Service Bus Console using additional filters in Smart Search. This section describes the following:

- "Finding SLA Alert Rules Using Search Filters" on page 4-13
- "View and Configure SLA Alert Rules" on page 4-14

## Finding SLA Alert Rules Using Search Filters

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

**Figure 4-11 Type based Filters: SLA Alerts**




You can use the following filters to customize your search for SLA ALert Rules:

- 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: You can specify the type of the parent service criterion. The parent service can be one of the following options:
  - All Services: The parent service is either a proxy service or a business service.
  - Proxy Services
  - Business Service

  **Note:** When you specify the value for Service Type, Parent Service is reset.
- Rule State: 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:
  - 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.

- 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 search all services using the set criteria or 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".

## View and Configure 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**

Summary of SLA Alert Rules

Items 1-8 of 8 | 1

| Name | SLA State | Service Name | Path | Severity | Aggr. Interval | Expiration Date | Frequency |
|---|---|---|---|---|---|---|---|
| binaryAlertRule | Enabled | binarymfltest | default | Critical | 0 hr(s) 10 mins | Never Expires | Every Time |
| LSR | Enabled | loanSaleProcessor | MortgageBroker/BusinessServices | Warning | 0 hr(s) 1 mins | Never Expires | Every Time |
| newbsRule | Enabled | normalLoanBS | MortgageBroker/BusinessService | Fatal | 0 hr(s) 10 mins | Never Expires | Every Time |
| NewBSrule1 | Enabled | AddCustomerService | ALSR Project | Major | 0 hr(s) 10 mins | Never Expires | Every Time |
| newBSRulke | Enabled | managerLoanApproval | MortgageBroker/BusinessService | Minor | 0 hr(s) 10 mins | Never Expires | Every Time |
| newrule10 | Enabled | mflProxy | default | Warning | 0 hr(s) 1 mins | Never Expires | Every Time |
| newRule12 | Enabled | New | default | Major | 0 hr(s) 10 mins | Never Expires | Every Time |
| ruLe | Enabled | service4 | default | Minor | 0 hr(s) 1 mins | Never Expires | Every Time |

Items 1-8 of 8 | 1

Update | Reset

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

**Table 4-2 SLA Alert Summary Table**

| Property | Description |
|---|---|
| Name | The name assigned to this alert rule. The name is a link to the View Alert Rule Details page. For more information, see "Understanding Alert Rule Details" on page 3-11. |
| SLA State | The status of the alert rule: Enabled or Disabled. |
| Description | **Note:** This field is hidden by default.<br>A description of the alert rule. |
| Service Name | The name of the parent service. The name is a link to the Operational Settings page. |
| Path | 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:<br>`project-name/root-folder/ . . ./parent-folder`<br>The path is a link to the corresponding path in the Project Explorer. |
| Severity | The severity of the alert that is triggered by this rule: Normal, Warning, Minor, Major, Critical, or Fatal. |
| Aggr Interval | The length of the aggregation interval in terms of hours and minutes. |
| Expiration Date | The date when this alert rule is no longer in effect. |
| Stop Processing | **Note:** This field is hidden by default.<br>Displays Yes or No. |
| Frequency | The frequency of this alert:<br>• Every Time<br>• Notify Once |

**Note:** You can enable or disable an alert rule depending on the privileges of your role.For more information on roles, see Chapter 2, "Roles in AquaLogic Service Bus." For more information on enabling and disabling alert rules, see "Monitoring Services" on page 3-43.

CHAPTER 5

# Reporting

BEA AquaLogic Service Bus 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.

AquaLogic Service Bus includes a JMS Reporting Provider for message reporting. The Reporting module in the AquaLogic Service Bus 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 AquaLogic Service Bus 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 AquaLogic Service Bus Console and you will need to create your own user interface. If you wish to capture SLA data, you will need to create a reporting provider for alerts.

This chapter contains information on the following topics

# Reporting Framework

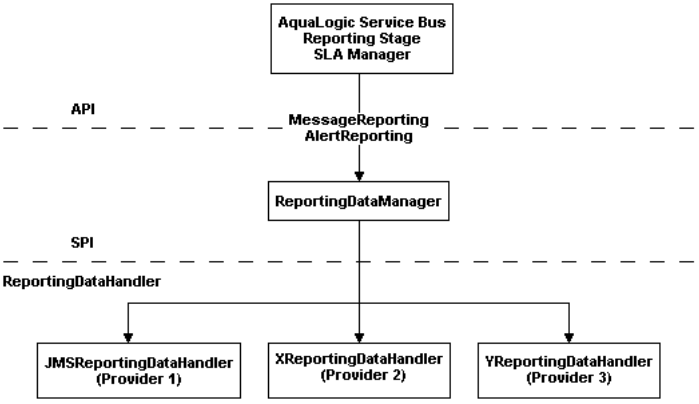
AquaLogic Service Bus contains an extensible framework for creating one or more reporting providers for messages or alerts.

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 AquaLogic Service Bus 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" on page 5-5.

All the information you need in order to create 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 to implement a reporting provider, including how to package it, where it goes, how to deploy it, and the order of deployment. The location of the reporting schema (`MessageReporting.xsd`) is `<BEA_HOME>/weblogic92/servicebus/lib/sb-schemas.jar`, where *BEA_HOME* is the directory in which you installed BEA products.

The 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`. If you want to develop a

reporting provider for alerts or your own message reporting provider, you need to implement an interface called `ReportingDataHandler` and use `ReportingDataManager` class.

The `ReportingDataHandler` interface takes the reporting or alert data stream and processes it. It can either process or store, or both this stream 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 AquaLogic Service Bus 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 server-local object that keeps a registry of reporting providers. Reporting providers implement the `ReportingDataHandler` interface. The `ReportingDataManager` provides operations to do the following:

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

# JMS Reporting Provider

The JMS Reporting Provider provides a pluggable architecture to capture the reporting information from each message via a Report action. All messages across the cluster are aggregated and stored in the JMS Reporting Provider Data Store in a database specific format. When you use the JMS Reporting Provider, which is provided with AquaLogic Service Bus installation the Reporting module in the AquaLogic Service Bus Console displays information from the JMS Reporting Provider Data Store.

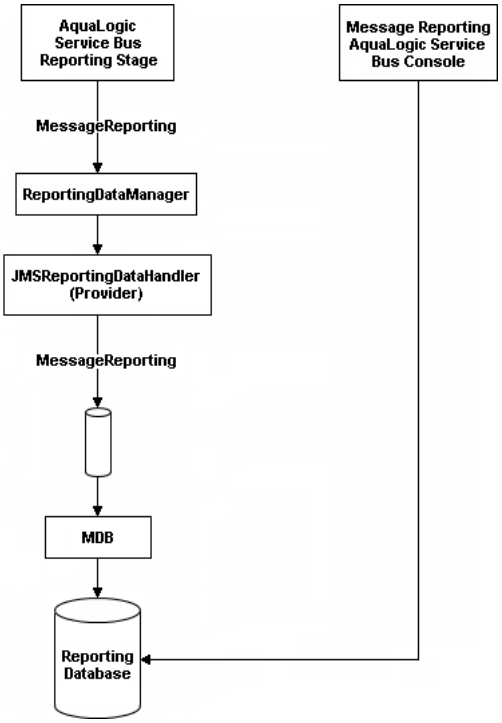
**Note:** The JMS Reporting Provider is automatically configured when you create an AquaLogic Service Bus domain. If you do not wish to use this reporting provider, you must untarget it. For more information, see "Removing, Stopping, or Untargeting a Reporting Provider" on page 5-14.

This section contains information on the following topics:

# About the 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 the following diagram.

**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 AquaLogic Service Bus 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 AquaLogic Service Bus Reporting Data Stream. In the `Report` action, you must specify the information you want to extract from the message and add to the AquaLogic Service Bus Reporting Data Stream.

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

When configuring a Report action, you 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*.

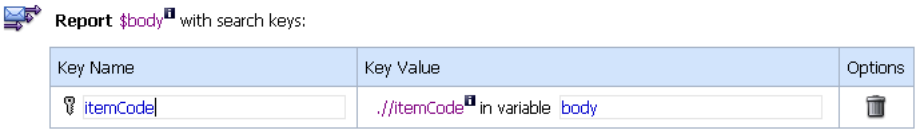
You can use any XML elements as a key:

```
<?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>
```

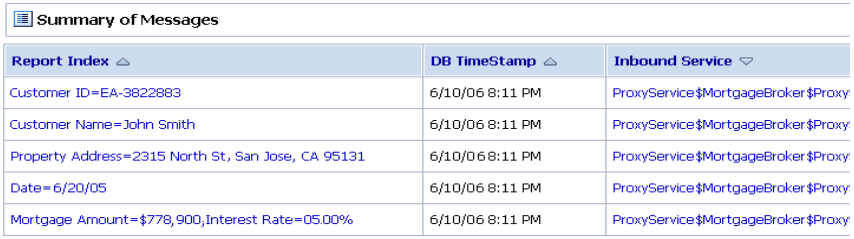
For example, you can specify the key as the `itemcode`, the value as `.//item-code` (an XPath expression), and the variable as message body (`body`), as shown in the Figure 5-3.

**Figure 5-3 Key Name and Value**




If you are using the JMS Reporting Provider, which is provided with AquaLogic Service Bus installation, 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 Report Index Column with each key-value separated by a semicolon, as shown in Figure 5-4.

**Figure 5-4 Keys and Associated Values Display**


Summary of Messages

| Report Index | DB TimeStamp | Inbound Service |
|---|---|---|
| Customer ID=EA-3822883 | 6/10/06 8:11 PM | ProxyService$MortgageBroker$Proxy |
| Customer Name=John Smith | 6/10/06 8:11 PM | ProxyService$MortgageBroker$Proxy |
| Property Address=2315 North St, San Jose, CA 95131 | 6/10/06 8:11 PM | ProxyService$MortgageBroker$Proxy |
| Date=6/20/05 | 6/10/06 8:11 PM | ProxyService$MortgageBroker$Proxy |
| Mortgage Amount=$778,900,Interest Rate=05.00% | 6/10/06 8:11 PM | ProxyService$MortgageBroker$Proxy |

For information on how to create 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.

# Using the Reporting Module

The reporting module in the AquaLogic Service Bus 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. AquaLogic Service Bus 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 “Configuring a Database for the JMS Reporting Provider Store” on page 5-12.

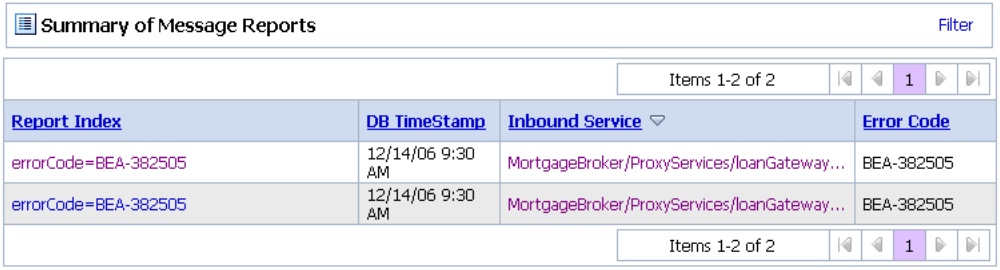
For more information on how to use the reporting module, see Reporting in *Using the AquaLogic Service Bus Console*.

This section includes information on the following topics:

# Understanding Summary of Messages

When you click Reporting in the navigation panel, 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 5-5 Summary of Messages**




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.

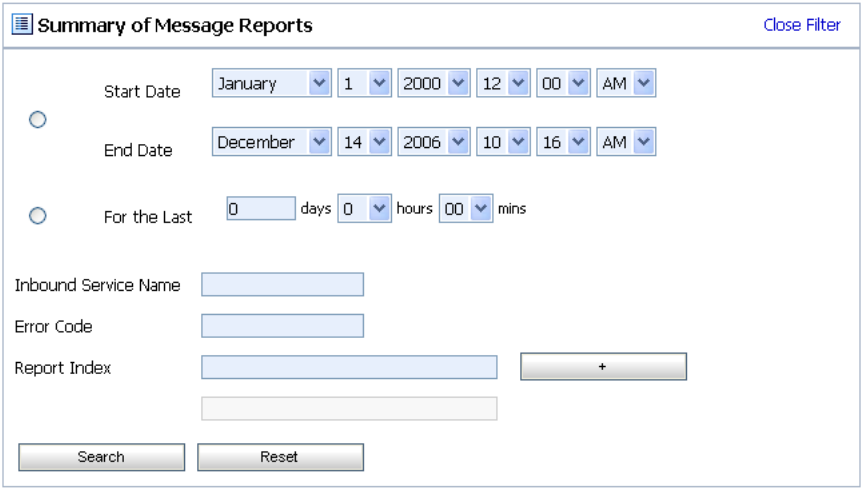
**Note:** After you filter the message, the filter remains in effect until you update it or reset it.

The table shown in Figure 5-5 provides the following information:

- 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" on page 5-4.
- DB TimeStamp: the time when the message was written to the database.
- Inbound Service: the inbound service associated with the message. The service is a link to the View a Proxy Service page.
- Error Code: 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, you can filter the display of messages by clicking Filter in the Summary of Messages Table. The available filtering is shown in Figure 5-6.

**Figure 5-6 Summary of Messages Search**



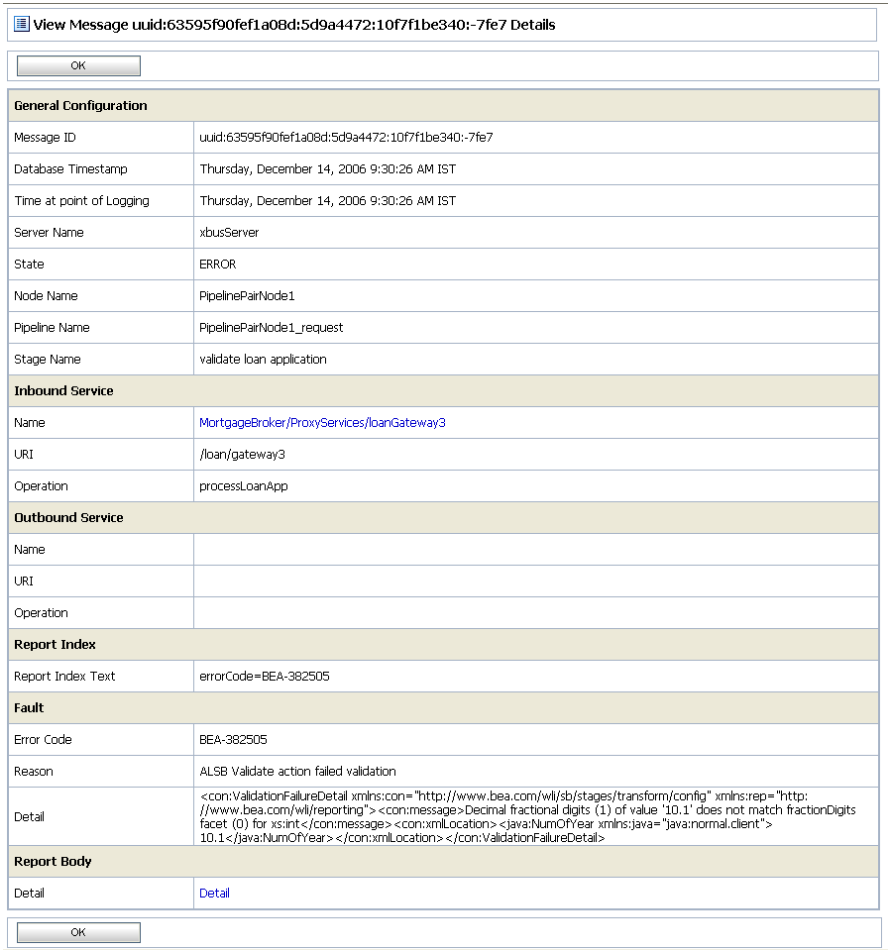

As shown in the Figure 5-6, you can filter report messages for a specified period of time, by the name of a service, by error code, and by report index. After you filter the messages, the title of the page changes to Summary of Filtered Messages. For information on how to use the Summary of Messages 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 5-7.

**Figure 5-7 Report Message Detail Page**



View Message uuid:63595f90fef1a08d:5d9a4472:10f7f1be340:-7fe7 Details

OK

| General Configuration | |
|---|---|
| Message ID | uuid:63595f90fef1a08d:5d9a4472:10f7f1be340:-7fe7 |
| Database Timestamp | Thursday, December 14, 2006 9:30:26 AM IST |
| Time at point of Logging | Thursday, December 14, 2006 9:30:26 AM IST |
| Server Name | xbusServer |
| State | ERROR |
| Node Name | PipelinePairNode1 |
| Pipeline Name | PipelinePairNode1_request |
| Stage Name | validate loan application |
| **Inbound Service** | |
| Name | MortgageBroker/ProxyServices/loanGateway3 |
| URI | /loan/gateway3 |
| Operation | processLoanApp |
| **Outbound Service** | |
| Name | |
| URI | |
| Operation | |
| **Report Index** | |
| Report Index Text | errorCode=BEA-382505 |
| **Fault** | |
| Error Code | BEA-382505 |
| Reason | ALSB Validate action failed validation |
| Detail | <con:ValidationFailureDetail xmlns:con="http://www.bea.com/wli/sb/stages/transform/config" xmlns:rep="http://www.bea.com/wli/reporting"><con:message>Decimal fractional digits (1) of value '10.1' does not match fractionDigits facet (0) for xs:int</con:message><con:xmlLocation><java:NumOfYear xmlns:java="java:normal.client">10.1</java:NumOfYear></con:xmlLocation></con:ValidationFailureDetail> |
| **Report Body** | |
| Detail | Detail |

OK

The page shows the following information:

- General Configuration
  - Message ID: the unique identification 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: state of the pipeline from which this message was generated, as follows:

    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.

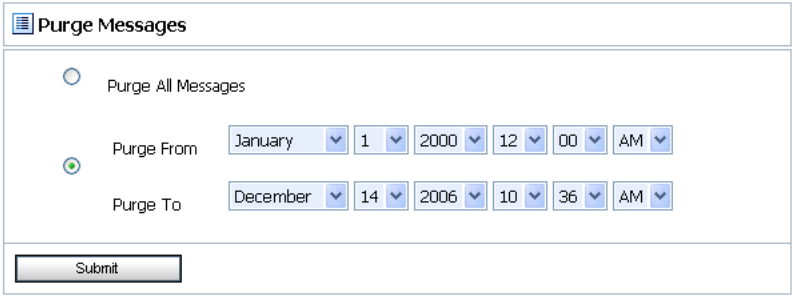
- Inbound Service
  - Name: the inbound proxy service associated with this message. An inbound proxy service exchanges messages with client applications. The name is a link to the View a Proxy Service page. For more information about this page, see "Viewing and Changing Proxy Services" in Proxy Services 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 AquaLogic Service Bus proxy service. The name is a link to the 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: 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" on page 5-4.

- Fault
  - 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 reason for the error.
  - 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 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*.

# Purging Messages

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 AquaLogic Service Bus Console. This feature enables you to work with the Summary of Messages page in the AquaLogic Service Bus Console while the purge occurs in the background.

**Figure 5-8 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 AquaLogic Service Bus Console does not display any messages to indicate that a purge is in process. 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.
```

# Configuring a Database for the JMS Reporting Provider Store

AquaLogic Service Bus 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.

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 WebLogic Platform in *Supported Configurations for AquaLogic Service Bus*.

This section provides information on the following topics:


- "Configuring a Database in a Development Environment" on page 5-12
- "Configuring a Database for Production" on page 5-13


## Configuring a Database in a Development Environment

When you create an AquaLogic Service Bus domain, the Configuration Wizard does not create database tables automatically. In a development environment, the JMS Reporting Provider, which is provided with AquaLogic Service Bus installation 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.

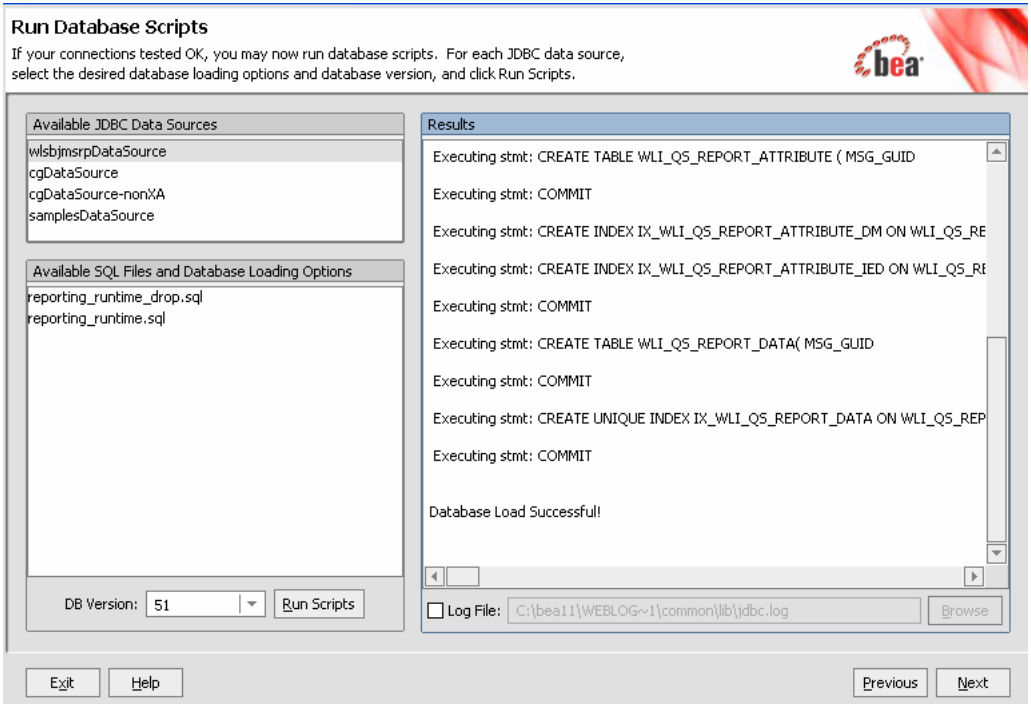
**Note:** If you are using Pointbase, you do not need to specify a database in the Configuration Wizard.

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 AquaLogic Service Bus domain. The scripts are located in `<BEA_HOME>/weblogic92/integration/common/dbscripts`, 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 5-9). For more information, see *Creating WebLogic Domains Using the Configuration Wizard*.

**Figure 5-9 Run Database Scripts in the Configuration Wizard**




## Configuring a Database for Production

Complete information about configuring a database for production is located in the *AquaLogic Service Bus Deployment Guide* in the following chapters:

- Configuring a Single-Server Deployment
- Configuring a Cluster Deployment

# Removing, Stopping, or Untargeting a Reporting Provider

As previously mentioned, the JMS Reporting Provider, which is provided with AquaLogic Service Bus installation is automatically configured when you create an AquaLogic Service Bus domain. If you do not wish to use this 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 will be written.

The following sections provide information on how to stop or untarget any reporting provider:

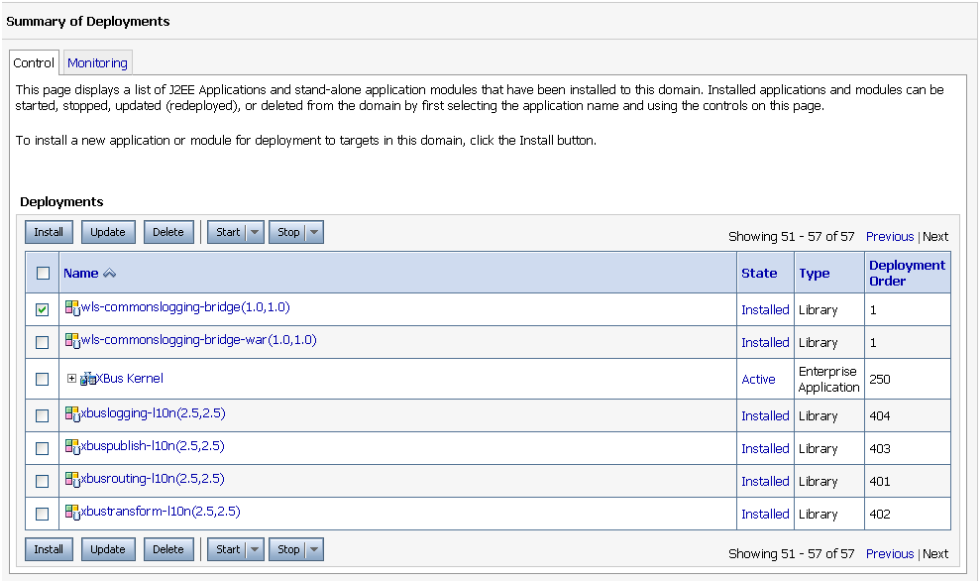

- "Stopping a Reporting Provider when the Server is Running" on page 5-14
- "Untargeting a Reporting Provider when the Server is Running" on page 5-15
- "Untargeting the JMS Reporting Provider—Server Not Running" on page 5-17


## Stopping a Reporting Provider when the Server is Running

If you wish to stop a reporting provider when the server is running in the AquaLogic Service Bus domain, do the following steps:

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 checkbox beside the reporting provider you wish to stop.

**Figure 5-10 Stopping a Reporting Provider**




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

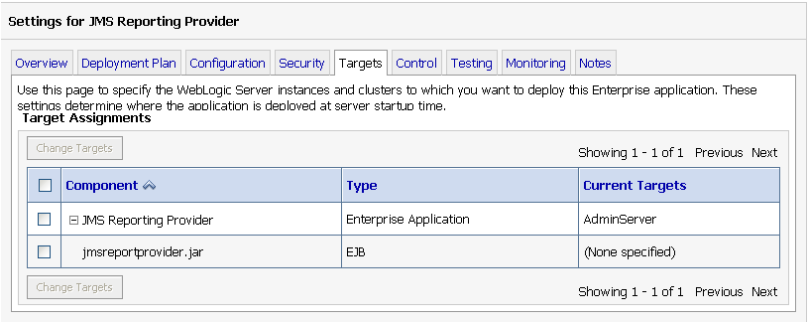
# Untargeting a Reporting Provider when the Server is Running

If you wish to untarget a reporting provider when the server is running in the AquaLogic Service Bus 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 checkbox.

**Figure 5-11 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. If you are untargeting the JMS Reporting Provider, which is provided with AquaLogic Service Bus 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 checkbox.
   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.

# Untargeting the JMS Reporting Provider—Server Not Running

If the server is not running in the AquaLogic Service Bus domain, you can use the WebLogic Scripting Tool (WLST) to remove the JMS Reporting Provider from the AquaLogic Service Bus 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. Open a UNIX shell or terminal window.
3. Invoke WLST Offline.

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

4. Read the domain that was created using the Configuration Wizard. For example:

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

5. Untarget the reporting provider data source. For example:

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

6. Untarget the reporting provider application. For example:

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

7. Update the domain:

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

8. Close the domain:

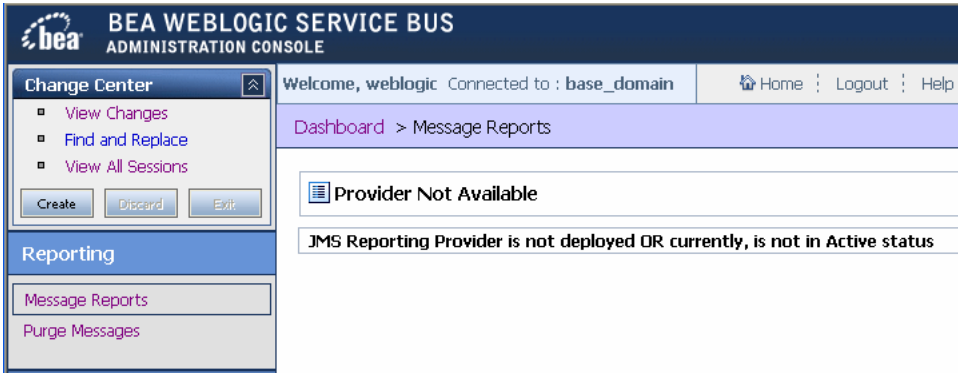
   ```
   wls:/offline/base_domain>closeDomain()
   ```

9. Exit from the WLST command prompt:

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

After the AquaLogic Service Bus JMS reporting provider is untargeted, the Reporting module in the AquaLogic Service Bus Console will indicate that the reporting provider is not deployed, as shown Figure 5-12.

**Figure 5-12 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, AquaLogic Service Bus Console displays the message shown in the previous figure.

# Reporting Scenarios

The following scenarios describe some of the ways in which you can use AquaLogic Service Bus to track messages:

- "Message Tracking" on page 5-18
- "Search for a Particular Message" on page 5-19
- "Logging for Regulatory Auditing" on page 5-19
- "Alert Reporting Provider" on page 5-19

## Message Tracking

In the AquaLogic Service Bus Console, you can track the messages Processing proxy service. When you drill down into some of the messages, you discover that the pipeline errors are due to message transformation errors and that the mangled messages are coming out of the portal associated with the proxy service. To solve the problem, you can add a new transformation to the pipeline for all messages originating from that portal site.

## Search for a Particular Message

You can log into the AquaLogic Service Bus Console and search for the trade number. The search shows that two messages were processed in the request pipelines, but no response messages. You can ask Customer Service to contact the customer and assure the customer that the trade was successfully processed.

## Logging for Regulatory Auditing

You can configure the Log action in the pipeline of a proxy service to capture the relevant message information. Using the logging action you can extract specific data from the messages

## Alert Reporting Provider

By configuring a reporting provider for alerts, you can receive an alert notification outside of the AquaLogic Service Bus Console and process the alert according to your business needs. For example, you could develop an alert reporting provider that utilizes the reporting stream for alerts and then display the alerts on a custom console, such as HP OpenView, or Tivoli.

# Tracing

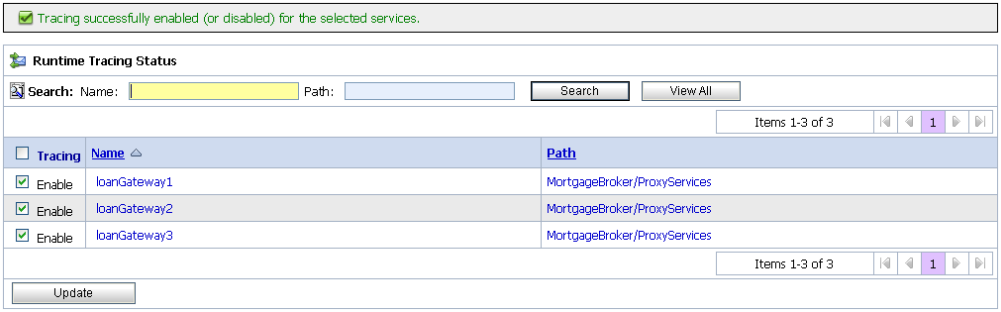
BEA AquaLogic Service Bus supports to trace messages without having to shut down the server. This feature is useful in both a development and production environment. Tracing allows administrators, support engineers, and systems engineers to troubleshoot and diagnose a message flow in one or more proxy 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.

## To Enable or Disable Tracing

You can enable tracing from the Operations module of the AquaLogic Service Bus Console, as shown in Figure 6-1.

**Figure 6-1 Tracing Configuration**




As shown in the Figure 6-1, the Tracing Configuration page displays the tracing status of the proxy services. If the checkbox adjacent to the name of the proxy service is selected, tracing is enabled for that service. The Runtime Tracing Status table displays the following information:

- Tracing: the tracing status for the service.
- Name: the name of the proxy service. The name is a link to the View a Proxy Service page.
- Path: the project name and the name of the folder in which the proxy service resides. It is a link to the Project Details or Folder Details page.

To enable or disable the tracing settings click the check box in the Tracing field and click Update. Activate the session to start logging. Once the session is activated, the trace setting is persisted along with the other details of the proxy service configuration.

Information about the pages referenced from the Runtime Tracing Status table is available in the *Using the AquaLogic Service Bus Console*, as follows:

- View a Proxy Service page: “Viewing and Changing Proxy Services” in Proxy Services.
- Project Details: “Viewing Project Details” in Project Explorer.
- Folder Details: “Viewing Folder Details” in Project Explorer.

For information on how to use the AquaLogic Service Bus Console to enable tracing, see “Enabling Runtime Tracing Status of Proxy Services” in Configuration in *Using the AquaLogic Service Bus Console*.

The tracing information is stored in the server directory logs. For example, in the AquaLogic Service Bus Examples, if tracing is enabled for the 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*.