2.2.1 Introduction to Service Monitoring and Management

Service Bus includes a powerful set of runtime tools for monitoring, alerting, reporting, configuration, and management. The Service Bus monitoring framework provides access to server statistics, such as the number of messages that were processed successfully or that failed, the average execution time of message processing, the number of errors and alerts generated, and the average response time. Using Fusion Middleware Control, you can view monitoring statistics for the period of the current aggregation interval or for the period since you last reset statistics for this service or since you last reset statistics for all services. Using the public APIs you can access only the statistics since the last reset.

2.2.1.1 Administration Consoles

Service Bus is fully integrated with Fusion Middleware Control for SOA-wide management. Most monitoring and management tasks for Service Bus services are performed using Fusion Middleware Control, though certain administration tasks require the Oracle Service Bus Console.

14

In Fusion Middleware Control, Service Bus provides operational functions and settings that allow you to monitor SLA alerts, pipeline alerts, logs, reports, and policy usage by providing a cluster-wide view of service status and statistics. The framework monitors business services, proxy services, pipelines, and split-joins, including response times, message counts, error counts, and security policy usage and violations. Using Fusion Middleware Control, you can also turn tracing on and off, enable and disable services, update logging and alert levels, and recover from resequencing faults. Service-level flags and global flags help control monitoring, alerting, reporting, and logging.

The Oracle Service Bus Console provides configuration tools for creating service level agreement alerts, pipeline alerts, messaging reporting actions, alert destinations, and throttling groups for business service endpoints. Using the console, you can also update environmental values, either individually or in bulk.

2.2.1.2 Auditing Capabilities

Service Bus provides the following capabilities for auditing and monitoring services:

- Gathers statistics about message invocations, errors, performance characteristics, messages passed and SLA violations.
- Sends SLA-based alerts as SNMP traps, enabling integration with third-party ESM solutions.
- Logs selected parts of messages for both systems operations and business auditing purposes.
- Provides search capabilities by extracting key information from a message and use as it as a search index.

2.2.2 Introduction to the Oracle Service Bus Monitoring Framework

The monitoring framework monitors the operational resources, servers, and service level agreements (SLAs) for Service Bus.Figure 2-1 illustrates of the architecture of the monitoring framework.

2.3.1 Service Health Monitoring

Information about system operational health can be viewed at the server, project, and individual service level. The Service Bus domain and Service Bus Project Service Health pages display statistics aggregated for each service in either the domain or project. Individual service dashboards also display performance statistics at an operational level for more granular analysis. For pipelines and split-joins, performance statistics can be gathered for components in the message flow.

Statistics are collected for all Service Bus services. The monitoring system supports the following types of statistics:

14

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

For more information about different types of statistics collected, see Using the JMX Monitoring API. For information about monitoring service health, see Monitoring Oracle Service Bus Service Health.

2.3.1.1 Metric Aggregation

The displayed health statistics are based on an asynchronous aggregation of data collected during system operation. In a production cluster domain, the data aggregator runs as a singleton service on one of the Managed Servers in the cluster. Server-specific data aggregation is performed on each of the Managed Servers in the domain. The aggregator is responsible for the collection and aggregation of data from all the Managed Servers at regular, configurable intervals. These metrics are aggregated across the cluster for the configured aggregation interval and displayed on the Service Bus pages in Fusion Middleware Control.

2.3.1.2 Monitoring a Service that was Renamed or Moved

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

2.3.2 SLA and Pipeline Alert Monitoring

14

Service level agreement (SLA) alerts and pipeline alerts are configured for specific services in order to generate information about how messages are being processed through those services. SLA alerts are raised to indicate potential violations of service level agreements. The following are some common uses for SLA alerts:

- Monitoring and generating e-mail notification of WS-Security errors.
- Monitoring the number of messages passing through a particular pipeline.

- Detecting the violation of service level agreements with third-party products.
- Detecting a non-responsive endpoint.

Pipeline alerts are defined directly in a pipeline using an alert action. Pipeline alerts are generally used to detect errors in a message flow or to indicate a business event. For more information about creating and monitoring alerts, see Monitoring Oracle Service Bus Alerts.

2.3.2.1 SLA Alerts Overview

Service Level Agreements (SLAs) define the precise level of service expected from the services in Service Bus. SLA alerts are automated responses to violations of SLA rules and conditions. Service Bus runs SLA rules against aggregated monitoring statistics and raises alerts when rule violations are found. After monitoring those alerts, you can enable or disable services as needed. Administrators can set service level agreements (SLAs) on the following conditions:

14

- Message processing times.
- Message processing volume.
- Number of errors, security violations, and validation errors.
- Failure and success ratios.
- For business services only, endpoint URI status.

The Service Bus Dashboard and Alert History page in Fusion Middleware Control both display SLA alerts. When an SLA alert is raised, Service Bus also sends a notification to the alert destinations defined for that alert rule. In order for Service Bus to raise SLA alerts, SLA alerting must be enabled at both the service level and the global level.

The Oracle Service Bus Console provides editors to create SLA alert rules and to define the conditions under which an alert is raised. Alert rules specify unacceptable service performance according to your business and performance requirements. Each alert rule allows you to specify the aggregation interval for that rule. This interval is not affected by the aggregation interval set for the service.

2.3.2.2 Pipeline Alerts Overview

In addition to SLA alerts, Service Bus also provides alert actions that can be configured within the message flow of a pipeline. Pipeline alerts are generally used for business purposes such as recording the number of messages that flow through the message pipeline, tracking occurrences of certain business events, or reporting errors (though not for the health of the system). Pipeline alert actions generate alerts based on the message context in a pipeline, and can be configured to include an alert name, description (which can include message elements), alert destination, and alert severity.

Service Bus generates a pipeline alert when it reaches an alert reporting action in a pipeline and the conditions defined for the action are met. You define the conditions under which a pipeline alert is triggered using the conditional constructs available in the pipeline editor, such as an XQuery expression or an if-then-else construct. When a pipeline alert is raised, Service Bus sends a notification to the alert destinations defined for that alert action.

4
Monitoring Oracle Service Bus Alerts

This chapter describes how to monitor and manage Service Bus service level agreement (SLA) and pipeline alerts. You create and configure SLA alert rules in the Oracle Service Bus Console, defining the conditions that trigger alerts that you can monitor at runtime. You define pipeline alerts when defining the message flow in a pipeline through an alert action.
This chapter includes the following topics:

4.1 Introduction to Oracle Service Bus Alerts

14

Oracle Service Bus lets you define two different types of alerts for service components: service level agreement (SLA) alerts and pipeline alerts. For both types of alerts, you can specify alert destinations, such as email addresses and JMS queues.

You define SLA alert rules in the Oracle Service Bus Console, and you define pipeline alert rules in either the Oracle Service Bus Console or JDeveloper. The following figure shows the Service Bus Service Health page, with a list of services that have generated alerts.

4.1.1 Alerts on the Service Bus Dashboard

In Fusion Middleware Control, you can monitor domain-wide SLA and pipeline alerts on the Service Bus Dashboard page. This page displays information about all alerts that occurred on the domain within the specified interval or since the last time the statistics were reset. The Dashboard includes the following information:

- A pie chart illustrating the breakdown of alerts by severity for the specified period.
- The top 10 services with the specified type of alert in the current aggregation interval, listed in descending order.
- A table that lists and describes the alerts represented by the pie chart.
- A table that lists the services with the most errors.

The alerts listed on the page are the alerts that are represented in the pie chart. You can click on the name of an alert or service in any of the tables on this page to view more information, or click on a section of the pie chart to view additional information about alerts of the specified severity.