WebSphere software

IBM

IBM WebSphere DataPower SOA Appliances

Part IV: Management and Governance

- Monitor DataPower with IBM Tivoli Composite Application Manager for SOA
- Integrate WebSphere Registry and Repository with DataPower
- Manage configurations on multiple DataPower devices

Juan R. Rodriguez
Somesh Adiraju
Robert Bunn
Markus Grohmann
Marcel Kinard
Tamika Moody
Srinivasan Muralidharan
Christian Ramirez
Adolfo Rodriguez

Redpaper

ibm.com/redbooks

International Technical Support Organization

IBM WebSphere DataPower SOA Appliances Part IV: Management and Governance

April 2008

REDP-4366-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (April 2008)

This edition applies to Version 3, Release 6, Modification 0 of IBM WebSphere DataPower Integration Appliance.

This document was created or updated on April 22, 2008.

© Copyright International Business Machines Corporation 2008. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices v
Trademarks vi

Preface vii
The team that wrote this paper vii
Become a published author ix
Comments welcome. ix

Chapter 1. IBM Tivoli Composite Application Manager for SOA in the DataPower environment 1
1.1 ITCAM for SOA overview 2
1.1.1 Product features 2
1.1.2 Product components 3
1.1.3 ITCAM for SOA management resources 6
1.2 ITCAM for SOA installation 10
1.2.1 Planning the implementation. 10
1.2.2 Installing ITCAM for SOA application support. 12
1.2.3 Installing the ITCAM for SOA monitoring agent 20
1.2.4 Enabling the monitoring agent in the DataPower environment. 20
1.2.5 Configuring the warehouse proxy 21
1.2.6 Installing IBM Web Services Navigator. 25
1.3 ITCAM for SOA in the DataPower environment 27
1.3.1 The DataPower data collector as a proxy 27
1.3.2 Planning for deployment 28
1.3.3 Deploying the DataPower data collector. 29
1.3.4 Troubleshooting 33
1.4 ITCAM for SOA usage scenarios 35
1.4.1 Monitoring Web services calls. 36
1.4.2 Using historical reporting. 39
1.5 Summary. 43

Chapter 2. IBM Tivoli Composite Application Manager System Edition for WebSphere DataPower 45
2.1 Installation overview 46
2.1.1 Planning for installation 46
2.1.2 Supported platforms 46
2.1.3 Hardware requirements. 46
2.1.4 Software requirements 47
2.1.5 Required firmware version 47
2.1.6 Firewall considerations 47
2.1.7 Obtaining the installation images 47
2.1.8 Installing ITCAM SE for WebSphere DataPower 48
2.1.9 Verifying the installation and starting ITCAM SE 52
2.1.10 Enabling the XML Management Interface on the DataPower appliance. 53
2.2 Managing DataPower with ITCAM SE 54
2.2.1 Example overview. 54
2.2.2 Downloading the firmware. 55
2.2.3 Managing the firmware 55
2.2.4 Creating a managed set 57

© Copyright IBM Corp. 2008. All rights reserved.

2.2.5 Creating a device 59
2.2.6 Adding a master device to a managed set 61
2.2.7 Adding domains to a managed set 63
2.2.8 Adding a slave device to the managed set (ITSO_managedSet) 64
2.3 Summary 65

Chapter 3. Service level monitoring 67
3.1 Overview of the SLM concepts in the DataPower device 68
3.2 Types of monitors in the DataPower device 68
3.2.1 Message monitors 69
3.2.2 Web service monitors 71
3.2.3 SLM policy actions 71
3.3 SLM policy configuration example in a multiprotocol gateway 72
3.3.1 Configuring the multiprotocol gateway service in the DataPower device 75
3.4 SLM policy configuration example in a Web service proxy 88
3.5 Summary 98

Chapter 4. Web service proxy with WebSphere Registry and Repository 99
4.1 SOA governance 100
4.2 WebSphere Service Registry and Repository 101
4.3 A sample scenario 102
4.3.1 Registering the WSDL file 103
4.3.2 Configuring a Web service proxy 113
4.3.3 Creating a host alias 118
4.3.4 Verifying the connectivity 119
4.3.5 Verifying a transaction result by using the Probe section 120
4.3.6 Executing the scenario 121
4.4 Summary 129

Appendix A. Additional material 131
Locating the Web material 131
Using the Web material 131
System requirements for downloading the Web material 131
How to use the Web material 132

Related publications 133
IBM Redbooks 133
Other publications 133
Online resources 134
How to get Redbooks 134
Help from IBM 134

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

© Copyright IBM Corp. 2008. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX 5L™
AIX®
Candle®
CICS®
DataPower device®
DataPower®
DB2 Universal Database™
DB2®
IBM®
IMS™
Lotus Notes®
Lotus®
Notes®
OMEGAMON®
Rational®
Redbooks (logo) ®
Redbooks®
Tivoli®
WebSphere®
z/OS®

The following terms are trademarks of other companies:

SAP NetWeaver, SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Java, J2EE, Solaris, Sun, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

IBM® WebSphere® DataPower® SOA Appliances represent an important element in the holistic approach of IBM to service-oriented architecture (SOA). IBM SOA appliances are purpose-built, easy-to-deploy network devices that simplify, secure, and accelerate your XML and Web services deployments while extending your SOA infrastructure. These appliances offer an innovative, pragmatic approach to harness the power of SOA. By using them, you can simultaneously use the value of your existing application, security, and networking infrastructure investments.

This series of IBM Redpaper publications is written for architects and administrators who need to understand the implemented architecture in WebSphere DataPower appliances to successfully deploy it as a secure and efficient enterprise service bus (ESB) product. These papers give a broad understanding of the new architecture and traditional deployment scenarios. They cover details about the implementation to help you identify the circumstances under which you should deploy DataPower appliances. They also provide a sample implementation and architectural best practices for an SOA message-oriented architecture in an existing production ESB environment.

Part 4 of the series, this part, provides ways to integrate the DataPower appliance with other products such as WebSphere Registry and Repository (WSRR), IBM Tivoli® Composite Application Manager for SOA (ITCAM SOA) and Tivoli Composite Application Manager System Edition (ITCAM SE). The entire IBM WebSphere DataPower SOA Appliances series includes the following papers:

- *IBM WebSphere DataPower SOA Appliances Part I: Overview and Getting Started*, REDP-4327
- *IBM WebSphere DataPower SOA Appliances Part II: Authentication and Authorization*, REDP-4364
- *IBM WebSphere DataPower SOA Appliances Part III: XML Security Guide*, REDP-4365
- *IBM WebSphere DataPower SOA Appliances Part IV: Management and Governance*, REDP-4366

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Juan R. Rodriguez is a Consulting IT professional and Project Leader at the IBM ITSO Center, Raleigh. He has a Master of Science (MS) degree in Computer Science from Iowa State University. He writes extensively and teaches IBM classes worldwide on Web technologies and information security. Before joining the IBM ITSO, Juan worked at the IBM laboratory in Research Triangle Park, North Carolina, as a designer and developer of networking products.

Somesh Adiraju is an Integration Architect with Ultramatics Inc., in Florida. He has nine years of experience in working with Enterprise Application Integration in areas of banking, finance, and telecommunications. His interests are in design, architecture, and developing enterprise scale applications. He specializes in the use of WebSphere MQ, Message Broker

© Copyright IBM Corp. 2008. All rights reserved.

and IBM Tivoli Monitoring. Somesh holds a Bachelor of Technology degree from Andhra University, India.

Robert Bunn is a Senior Software Engineer with 26 years of experience working on IBM support teams. He is currently assigned as a team lead for WebSphere DataPower Level 2 Support. He has worked in various support roles on a wide range of products operating on IBM mainframes, personal computers and now IBM WebSphere SOA DataPower appliances. He has a Bachelor of Science (BS) degree in Computer Science from North Carolina State University.

Markus Grohmann is an IT Specialist working as an IBM Business Partner in Austria. He has five years of experience with a broad range of IBM products and their implementation in customer environments. Markus graduated from Salzburg University of Applied Sciences and Technologies in 2002.

Marcel Kinard is a Software Engineer within the IBM WebSphere Technology Institute. He has over 16 years of experience at IBM, with a focus on networking and Web-based technologies, and the creation of new prototypes. He is currently working on DataPower-related projects.

Tamika Moody is a WebSphere Business Integration Message Broker/WebSphere DataPower Consultant and IT Specialist for IBM. She has over seven years of experience in the IT integration area. Tamika has broad experience in leading middleware engagements ranging from electronic data interchange (EDI) and business-to-business (B2B) implementations to design, implementation, and problem determination of DataPower and IBM middleware solutions.

Srinivasan Muralidharan is an Advisory Engineer with 15 years of industrial experience and nine years with IBM. He is currently working on DataPower related projects at the IBM WebSphere Technology Institute. He is widely experienced in SOA-related technologies in all tiers of the software development stack. He has studied SOA performance with DataPower appliances. Srinivasan has also investigated integrating DataPower with other mid-tier and back-end traditional components, such as WebSphere Application Server, MQ, CICS®, and IMS™, in the SOA context of reusing existing systems and enterprise modernization.

Christian Ramirez is an IBM Software Solutions Architect working for GBM Corporation, an IBM Alliance Company, located in San José, Costa Rica. He has ten years of experience with IBM products and five years experience as an Integration Solution Architect. He has worked with Lotus® Notes®, WebSphere MQ, and WebSphere BI Message Broker. In addition, he has been part a WebSphere Pre-Sales team and has implemented several integration projects.

Adolfo Rodriguez is a Software Architect within the IBM WebSphere Technology Institute (WSTI). He leads a team of engineers who focus on emerging technologies in WebSphere products and, more recently, DataPower SOA appliances. His recent contributions include projects in the areas of Web services enablement, XML processing, SOA management, and application-aware networking. His primary interests are networking and distributed systems, application middleware, overlays, and J2EE™ architecture. Adolfo is also an Assistant Adjunct Professor of Computer Science at Duke University, where he teaches networking courses. He has written 12 books and numerous research articles. He holds four degrees from Duke University: a BS in Computer Science, a Bachelor of Arts in Mathematics, MS in Computer Science, and a Ph.D. in Computer Science (Systems).

Thanks to the following people for their contributions to this project:

Robert Callaway
John Graham
IBM Research Triangle Park, North Carolina, USA

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

IBM Tivoli Composite Application Manager for SOA in the DataPower environment

In this chapter, we describe the concepts, installation, and usage of IBM Tivoli Composite Application Manager for SOA (ITCAM for SOA) V6.1 in the DataPower environment. We discuss the following topics:

- “ITCAM for SOA overview” on page 2
- “ITCAM for SOA installation” on page 10
- “ITCAM for SOA in the DataPower environment” on page 27
- “ITCAM for SOA usage scenarios” on page 35

© Copyright IBM Corp. 2008. All rights reserved.

1.1 ITCAM for SOA overview

In this section, we discuss the following topics in regard to ITCAM for SOA V6.1:

- Product features
- Product components
- ITCAM for SOA management resources

1.1.1 Product features

ITCAM for SOA manages a service-oriented architecture (SOA). It can monitor, manage, and control the Web services layer of IT architectures while drilling down to the application or resource layer to identify the source of bottlenecks or failures and to pinpoint services that consume the most time or the most resources. ITCAM for SOA offers the following support:

- Provides service monitoring views in Tivoli Enterprise Portal

  ITCAM for SOA workspaces consist of data collector-based workspaces:

  - *Performance Summary* shows the response time information for Web service calls as viewed from the client or server.
  - *Message Summary* shows the message statistics, including the volume and size of message information.
  - *Fault Summary* shows failure analysis for Web service calls.

  Other workspaces for each agent are:

  - *Service Management Agent Environment* provides a summary of the Web service metrics for all data collectors.
  - *Service Management Agent* shows the agent configuration summary, data collectors, monitoring profiles, and filters.
  - *Mediation Configuration* shows configuration entries for mediation on a Service Component Architecture (SCA).
  - *Message arrival* shows the message arrival rate and events based on the message arrival critical situation.

- Uses Tivoli Enterprise Portal situations to check thresholds

  The predefined situations address the following items:

  - Number of messages received by a service within a time window
  - Size of the messages

- Provides basic mediation support with the ability to filter or reject Web services call messages from a particular client or service

  It can log request and response messages for analysis.

- Offers heterogeneous platform coverage:

  - Supports IBM WebSphere Application Server, CICS Transaction Server, Microsoft® .NET, JBoss, BEA WebLogic, and other SOA clients and servers
  - Targets IBM Enterprise Service Bus platforms including WebSphere Application Server Versions 5.x and 6.x and WebSphere Business Integration Server Foundation V5.1.1

- Displays a list of services and operations that are monitored in the environment
- Uses Tivoli Enterprise Portal workflow and policy editor for threshold-triggered action sequences
- Offers the ability to include services-layer views in Tivoli Enterprise Portal

The context-rich views and inter-workspace linkages in Tivoli Enterprise Portal enable users to drill down to IT resources to identify Web service bottlenecks and failures. With the built-in and extensible alerts, situations, and workflows, users can create powerful automated mediation scenarios by using the Tivoli Enterprise Portal.

The service metrics, alerts, and automation workflows provided by ITCAM for SOA and other Tivoli products can be displayed in Tivoli Enterprise Portal with the cross-workspace linkages. In doing so, Tivoli Enterprise Portal provides a rich and multilayered source of information that can help to reduce the time and skills required for problem root-cause analysis and resolution.

ITCAM for SOA includes the Web Services Navigator, which is a plug-in to IBM Rational® Application Development and other Eclipse-based tools. It provides a deep understanding of the service flow, patterns, and relationships for developers and architects. The Web Services Navigator uses data from the IBM Tivoli Monitoring V6.1 Tivoli Data Warehouse or from the ITCAM for SOA log files by using the Log Assembler tool.

In Version 6.1, ITCAM for SOA contains a new component for mediation service management based on SCA. With this component, you can modify some of the mediation service settings on the fly. Mediation is a facility that sits between the Web service requester and Web service provider that allows manipulation of Web service messages, including format translation, filtering, and enrichment.

1.1.2 Product components

ITCAM for SOA manages Web services. Web services can be viewed as a remote processing facility that is defined through the use of the Web Services Definition Language (WSDL). Usual access uses SOAP over HTTP. Internally, Web services are implemented by using the Java™ application programming interface (API) for Extensible Markup Language (XML)-based Remote Procedure Call (JAX-RPC). ITCAM for SOA installs itself as the JAX-RPC handler to capture and manage Web services calls.

ITCAM for SOA consists of the following logical components:

- Web services data collector that acts as the JAX-RPC handler and intercepts Web services calls to collect statistical information and write to a log file
- Tivoli Enterprise Monitoring Agent that collects information from all of the data collectors on a machine and forwards them to Tivoli Enterprise Monitoring Server

  We discuss the data collectors and Tivoli Enterprise Monitoring Agent in “Monitoring agent data collector” on page 3.
- An Eclipsed-based viewer that processes log files that are generated by the Web services data collector

  It generates visual representations of various characteristics of monitored Web services. See “IBM Web Services Navigator” on page 5.
- Mediation SCA tools that enable partial monitoring of SCA within the WebSphere Enterprise Service Bus. See “Managing SCA mediation” on page 6.

Monitoring agent data collector

ITCAM for SOA works with several application server environments:

- IBM WebSphere Application Server V5.1.0.5 with PQ89492, V6.0, and V6.1
- IBM WebSphere Business Integration V5.1.1.1
- IBM WebSphere Process Server V6.0.1
- IBM WebSphere Enterprise Service Bus V6.0.1
- IBM CICS Transaction Server V3.1 and later

- BEA WebLogic Server V8.1.4
- Microsoft .NET V1.1 with Service Pack 1 and V2.0
- JBoss V4.03
- WebSphere Community Edition V1.0 and its service packs
- SAP® NetWeaver V6.40 with Service Pack 9 or later service packs
- IBM WebSphere DataPower SOA Appliance Firmware V3.5.0.5 or later

Figure 1-1 shows the ITCAM for SOA data collection conceptual architecture.

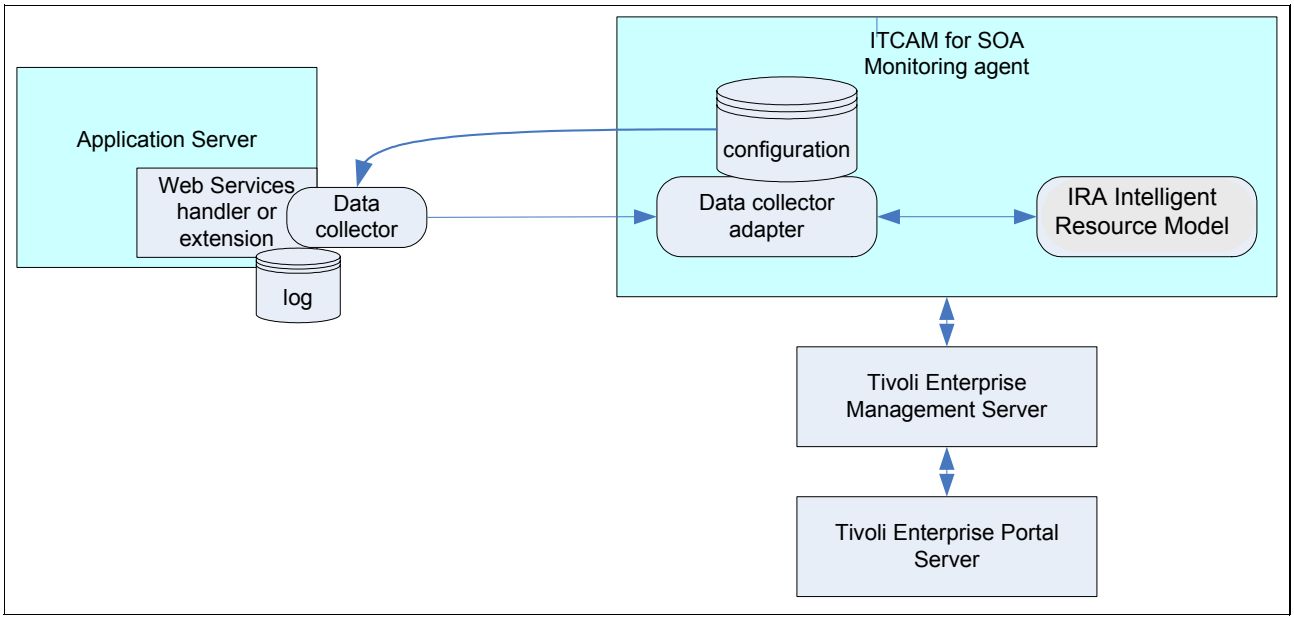


Figure 1-1 ITCAM for SOA structure

The monitoring agent data collector is implemented as a JAX-RPC handler or service extension that is installed into the application servers that are hosting the monitored Web services. The handler is given control when either of the following events occurs:

- A client application invokes a Web service, which is referred to as a *client-side interception*
- The Web service request is received by the hosting application server, which is referred to as a *server-side interception*

The monitoring agent records and collects monitored information into one or more local log files. The information is then transferred to Tivoli Enterprise Monitoring Server and can be archived into a historical database for later retrieval with IBM Web Services Navigator.

ITCAM for SOA V6.1 focuses on the SOAP engine of IBM WebSphere Application Server, WebSphere Service Integration Bus, Microsoft .NET Framework, and BEA WebLogic.

The Web services data collector supports both J2EE application client and server container environments because JAX-RPC handlers are supported only by these environments. The Web services must be compliant with JSR-109 specifications.

To ensure proper operation of the JAX-RPC handler, verify that the client applications are written according to the conventions of “Java Specification Request-000109 Implementing Enterprise Web Services” at the following Web address:

`http://www.jcp.org/aboutJava/communityprocess/final/jsr109/`

IBM Web Services Navigator

IBM Web Services Navigator is an Eclipsed-based tool that is used to visualize Web services in an SOA environment. It provides a graphical display of the following information:

- Service topology
- Web services transaction flows
- Flow patterns

Figure 1-2 illustrates the concepts of Web Services Navigator.

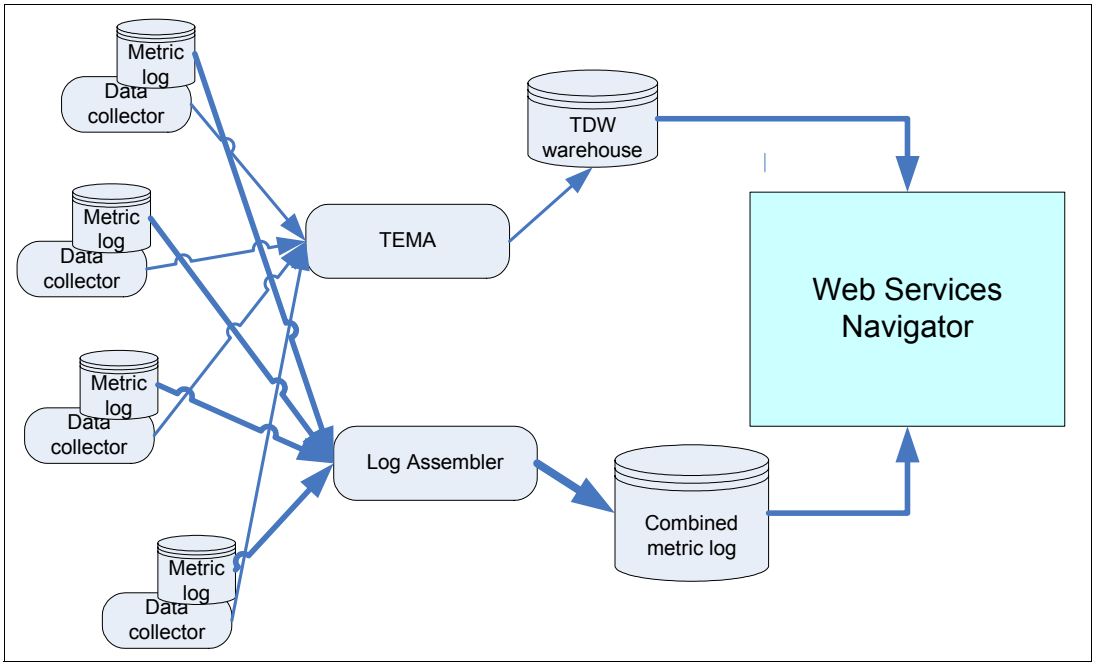


Figure 1-2 Web Services Navigator

The Web Services Navigator is a log-browsing tool that is intended for offline analysis of SOA Web services. The Web Services Navigator provides four primary views:

- Statistic tables
  - Message statistics

    Per-message statistics including requestor, provider, send/receive time, and message size
  - Invocation statistics

    Response time, network delay, message size, and more for each Web service invocation
  - Transaction statistics

    Statistics for aggregated transactions, including elapsed time, number of faults, number of machines this transaction involves, and number of invocations for this transaction

– Pattern invocation statistics

  Statistics for discovered patterns, including operation names, number of occurrences, response times, and message sizes

> **Message content:** To see the message content from the ITCAM for SOA metric log:
>
> 1. Set a monitor control higher than “none” for any or all of the Web services that are being monitored.
> 2. Include the subsequent xxxx.content.log when running Log Assembler.

- Service topology view

  This graphical representation of the monitored Web services displays aggregated information and information about the relationships between Web services.

- Transaction flows view

  The transaction flows view displays Universal Markup Language (UML) style sequence diagrams. The transaction flow shows a chronological view of each transaction, the flow between the various Web services over time, and the topology and statistics for each transaction. You can zoom in on the view to see the details of individual transactions.

- Flow pattern view

  The flow pattern view is a visual representation of the aggregated pattern of transactions represented in the log file. The view also represents each pattern as a distinct sequence of Web service calls and displays the frequency of each pattern.

Managing SCA mediation

WebSphere Process Server and WebSphere Enterprise Service Bus introduce a new way to model services in an SOA, called the *Service Component Architecture*. The SCA is designed to separate business logic from its implementation, so that you can focus on assembling an integrated application without knowing implementation details.

Mediation is a special type of SCA component. In an SOA, where services are loosely coupled rather than being connected directly to each other, mediations can be inserted between the services, where they can intercept and process messages that are being passed between the services. Mediations can process these messages and take appropriate actions, such as to reroute, log, or transform a message or to create a notification or an event.

ITCAM for SOA provides the ability to dynamically enable and disable the deployed mediation functions. This facility is available for applications in the WebSphere Enterprise Service Bus or WebSphere Process Server runtime environment. The invocation is provided in a new workspace in Tivoli Enterprise Portal called the *Mediation Configuration workspace*. The actions are ConfigureMediation_610 and DeletePrimitiveProperty_610.

1.1.3 ITCAM for SOA management resources

In the following sections, we discuss the following management resources for ITCAM for SOA:

- Workspaces
- Attributes
- Situations
- Actions

Workspaces

ITCAM for SOA delivers a set of predefined workspaces, which you can select from the Tivoli Enterprise Portal navigator view. Each workspace has its own set of views that display Web services data and metrics in various levels of detail. Figure 1-3 shows the workspace navigator area.

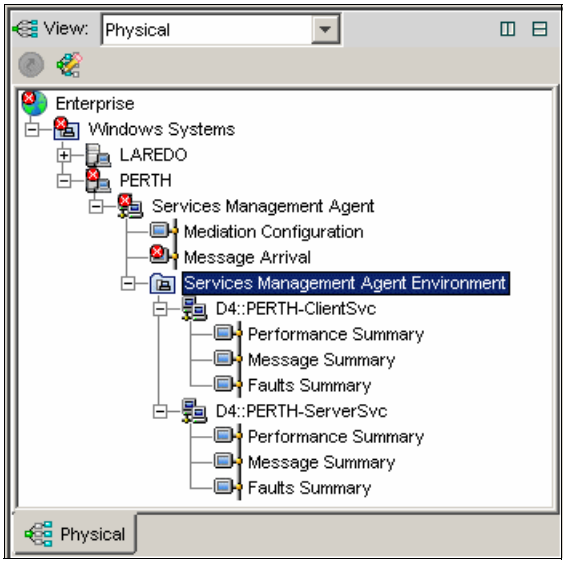


Figure 1-3 Navigator in the workspace

The following workspaces are available:

- The *Service Management Agent workspace* displays the current configuration details for the monitoring agent data collectors that are configured in different application server instances. This workspace contains the following views:
  - Data Collector Global Configuration
  - Data Collector Monitor Control Configuration
  - Data Collector Filter Control Configuration
- The *Mediation Configuration workspace* contains the SCA mediation configuration. This workspace can be used to launch the SCA mediation actions.
- The *Message Arrival Summary workspace* provides a summary of the number of messages that arrive at the data collector for each combination of service name, operation name, and remote IP address that has been configured as a situation. This workspace contains the following views:
  - Message Arrival Details
  - Message Arrival by Service
  - Message Arrival by Operation
- The *Services Management Agent Environment workspace* represents the agent monitoring applications for all of the application servers on that system. The Services Management Agent Environment workspace provides a set of views that summarize the performance, message activity, and fault occurrences associated with the Web services traffic through this monitoring agent. This workspace contains the following views:
  - Average Response Time by Operation
  - Number of Messages by Operation
  - Average Message Size by Operation

- The *Performance Summary workspace* provides the inventory of currently active and monitored services, as well as the response time of the services. This workspace contains the following views:
  - Average Response Time by Operation
  - Services Inventory
- The *Messages Summary workspace* provides details about the number and size of messages received for services and service/operation combinations. This workspace contains the following views:
  - Number of Messages by Service - Operation - Type
  - Average size of Messages by Service - Operation - Type
- The *Faults Summary workspace* provides a general faults summary. This workspace contains the following views:
  - Faults Summary by Operation
  - Fault Details

Attributes

Attributes are measurements that are collected by the IBM Tivoli Monitoring V6.1 family of products. ITCAM for SOA stores specific measurements or attributes that are relevant to its needs and function.

The tables that are available for long-term historical data collection are indicated in the description of the table. In addition, they show the historical reference information that identifies each attribute within each table. Each table identifies the column name, attribute name, and a description of the data provided. These attributes are used in ITCAM for SOA situations. Refer to *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492.

Situations

In the IBM Tivoli Monitoring V6.1 context, a *situation* is a condition where a set of attributes is tested against a threshold within any filtering rules (if necessary). The situation evaluates these conditions at predefined intervals and invokes the necessary automated responses and notification methods when needed.

ITCAM for SOA provides a set of predefined situations that are designed to help monitor critical activities and serve as templates for creating customized situations for your own use. Predefined situations are started automatically when the product is installed. After the situations have been configured, the situation alerts provided with ITCAM for SOA trigger event notification.

Table 1-1 lists the predefined situations that are provided with ITCAM for SOA.

Table 1-1 ITCAM for SOA situations

Situation name	Description
Fault	Monitors the messages in the Web services flow to determine whether a Web services fault has occurred.
Message arrival critical	Alerts you to excessive amounts of Web services traffic (the number of messages received from one or more remote clients exceeds a threshold that you specify).
Message arrival clearing	Clears a previously triggered Message Arrival Critical situation. This situation can also be used to alert for a message that falls below a specified threshold (lack of activity alert).

Situation name	Description
Message size	Monitors the length, in bytes, of each message during the Web services flow. If the length of the message is more than the threshold value, this situation is triggered.
Response time critical	Monitors elapsed round-trip response time, in milliseconds, for the completion of a Web services request.
Response time warning	Monitors elapsed round-trip response time, in milliseconds, for the completion of a Web services request.

Monitoring thresholds: Each implementation provides its own set of thresholds, because the product's default does *not* fit your environment. You must tune your monitoring thresholds.

The default situations are based on individual service calls that are stored in the Services_Metric table. Analyzing summarized information in the Services_Inventory table can reduce some of the monitoring processor usage.

Actions

In ITCAM for SOA V6.1, different sets of actions exist for different contexts. Although the available action types are the same, now four actions are available for each type. The existing 6.0 actions are still kept for compatibility and coexistence with ITCAM for SOA V6.0 agents and data collectors. New generic ITCAM for SOA actions are labeled with the suffix _610. These actions contain new parameters and functionality to be used with the new ITCAM for SOA V6.1 data collectors. When invoked from the workspaces with Service Metric or Service Inventory data, the data is inserted automatically as the arguments for the actions. The action name is prefixed with SM_* or SI_* respectively.

The following take-action methods are available for ITCAM for SOA:

AddFltrCntrl Creates new filter control settings to reject messages.

AddMntrCntrl Creates new monitor control settings. These monitor settings affect the data logging for use with IBM Web Service Navigator.

DelFltrCntrl Deletes existing filter control settings.

DelMntrCntrl Deletes existing monitor control settings.

DisableDC Disables data collection and the ability to reject messages.

EnableDC Enables data collection and the ability to reject messages.

updateLogging Defines the level of logging information.

UpdMntrCntrl Updates existing message logging levels for monitor control.

updateTracing Enables or disables tracing.

These actions can be invoked manually or triggered by a situation. They can also be triggered by workflows, which are predefined automations that you can build on the IBM Tivoli Monitoring platform.

1.2 ITCAM for SOA installation

When installing ITCAM for SOA, use the following overall implementation procedure:

1. Plan for the configuration.

   It is important to have a good understanding of the managed environment and the capability of the product. We discuss planning considerations in “1.2.1, “Planning the implementation” on page 10.

2. Install and operate ITCAM for SOA within the management infrastructure of the Tivoli Enterprise Monitoring Server services platform.

   Perform the installation of IBM Tivoli Monitoring V6.1 and its support pack 004 before any other ITCAM for SOA component. For Tivoli Monitoring installation information, see *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407.

3. Install the application support component for ITCAM for SOA on your Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal systems.

   See 1.2.2, “Installing ITCAM for SOA application support” on page 12.

4. Install and configure the monitoring agents of ITCAM for SOA.

   See 1.2.3, “Installing the ITCAM for SOA monitoring agent” on page 20.

5. Store metrics that are collected by the ITCAM for SOA data collector (DC) in Tivoli Data Warehouse.

   The Data Warehouse Proxy must be configured on the Tivoli Enterprise Monitoring Server in order to enable historical data collection for ITCAM for SOA. We discuss this in 1.2.5, “Configuring the warehouse proxy” on page 21, and 1.2.6, “Installing IBM Web Services Navigator” on page 25.

> **More information:** In this chapter, we intend to give an overview of the main components and installation process of ITCAM for SOA. Refer to *IBM Tivoli Composite Application Manager for SOA Installation and User’s Guide*, GC32-9492, for more detailed information.

1.2.1 Planning the implementation

When planning the implementation of ITCAM for SOA, you must make considerations for the following components:

- IBM Tivoli Monitoring services
- ITCAM for SOA application support
- ITCAM for SOA monitoring agent
- IBM Web Service Navigator

IBM Tivoli Monitoring services

IBM Tivoli Monitoring services, which include Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server, must be already installed and configured in your environment. Refer to *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407, to understand the available options for deploying the various components on one or more systems in your enterprise.

> **More information:** This chapter does not list the detailed steps to install, set up, or implement Tivoli Monitoring Services. See *Getting Started with IBM Tivoli Monitoring 6.1 on Distributed Environments*, SG24-7143.

Familiarize yourself with the Tivoli Enterprise Monitoring Server management infrastructure that is installed in your enterprise environment, including its various facilities to manage the system such as workflows and situations. Use Tivoli Enterprise Portal Server and Tivoli Enterprise Portal to understand workspaces and views for operators and their implication in the overall monitoring.

ITCAM for SOA application support

To view the ITCAM for SOA monitored agents through Tivoli Enterprise Portal, you must install application support for the agent on Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal. The Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server services are restarted during the ITCAM for SOA application support installation process.

The application support files include the following information:

- Data structure definition for Tivoli Enterprise Monitoring Server attributes and attribute groups (tables)

  ITCAM for SOA contains two tables: Services_Metrics and Services_Inventory.
- Situation definitions that allow proactive monitoring to be performed in the IBM Tivoli Monitoring environment
- Presentation information to be installed in the Tivoli Enterprise Portal Server, including help resources and workspace definitions
- Additional resources such as sample workflow and historical collection information

ITCAM for SOA monitoring agent

In a typical distributed environment, Tivoli Enterprise Monitoring Server is installed on one system, and Tivoli Enterprise Portal Server is installed on another system. Tivoli Enterprise Monitoring Agent is installed on additional multiple application server systems where Web services traffic is to be monitored.

You must install ITCAM for SOA agents on each system that has one or more application server environments that run Web services, such as IBM WebSphere Application Server, Microsoft .NET, and BEA WebLogic. Review *IBM Tivoli Composite Application Manager for SOA Release Notes*, GI11-4096, which contains the most current information.

When you install ITCAM for SOA on the application server, select to install the agent support component. This includes the data collector component that intercepts request and response messages for the Web services that you want to monitor. You must configure the appropriate data collector after installing the agent component.

The IBM Tivoli Monitoring environment requires installation and configuration to be performed on both distributed and z/OS®-managed systems where some of the platform components are installed and run. For more information about installing ITCAM for SOA on a supported z/OS operating system, refer to *Configuring IBM Tivoli Composite Application Manager for SOA z/OS*, SN32-9493.

When the ITCAM for SOA monitoring agent is installed and the application server is enabled, the data collector is the monitoring component of the ITCAM for SOA. It is implemented as a SOAP message handler and is used to monitor Web services that flow across an interception point. The interception point is a JAX-RPC handler in IBM WebSphere Application Server and BEA WebLogic server environments and service extensions in the Microsoft .NET environment.

IBM Web Service Navigator

IBM Web Services Navigator has the following features in the Eclipse environment:

- An import wizard to import Web services log files or retrieve data from ITCAM for SOA historical data into the IBM Web Services Navigator
- Web Services Profiling perspectives with a set of views of Web services transactions
- A separate Log Assembler tool that can be used to manually combine locally stored metric and content log files from the multiple application servers in your Web services environment into a single log file that can be imported to the IBM Web Services Navigator for viewing

1.2.2 Installing ITCAM for SOA application support

In this section, we explain the installation procedures for application support of the ITCAM for SOA monitoring agent on the Tivoli Enterprise Monitoring Server. You install the ITCAM for SOA application support from the CD, which includes multiple-platform support (Microsoft Windows®, IBM AIX® 5L™, and Sun™ Solaris™ binaries). The wizard copies the files from the CD-ROM to the disk. If you install the files from disk, copy the CD content into the *same* path. Otherwise, the installation wizard fails.

Perform the following steps:

1. Navigate to the \KD4\ITM_ASI directory on the ITCAM for SOA product CD. The installer is provided to support the IBM Tivoli Monitoring V6.1 installation. Select the appropriate operating system platform. For Windows, we invoke **`setup.exe`**.

2. In the Install Prerequisites window (Figure 1-4), for Choose common installation drive for both:, we type `C:`. The wizard can discover the IBM Tivoli Monitoring or Candle® platform installation. It checks for the appropriate GSKit and Java environment. Click **Next**.

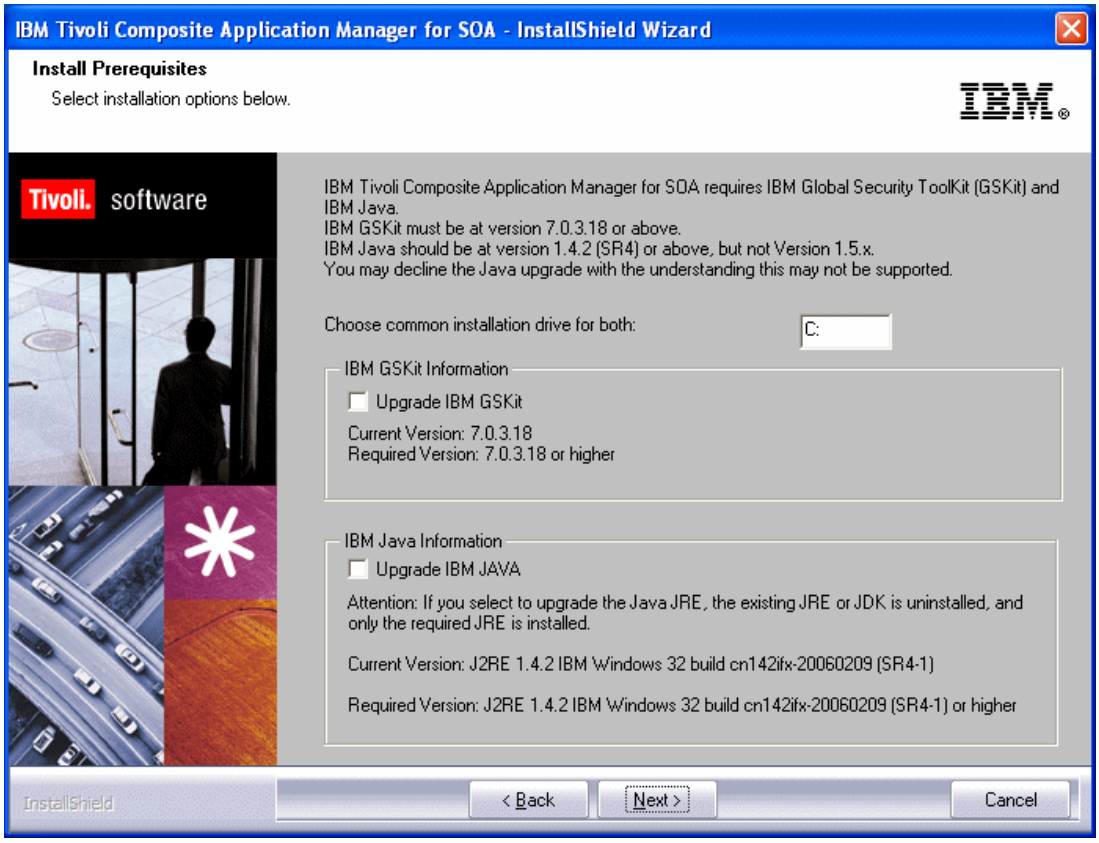


Figure 1-4 Installation Prerequisites window

3. In the Select Features window (Figure 1-5), you see that all of the components are selected to install to the local machine. They are all selected because Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal are installed on one system. Click **Next**.

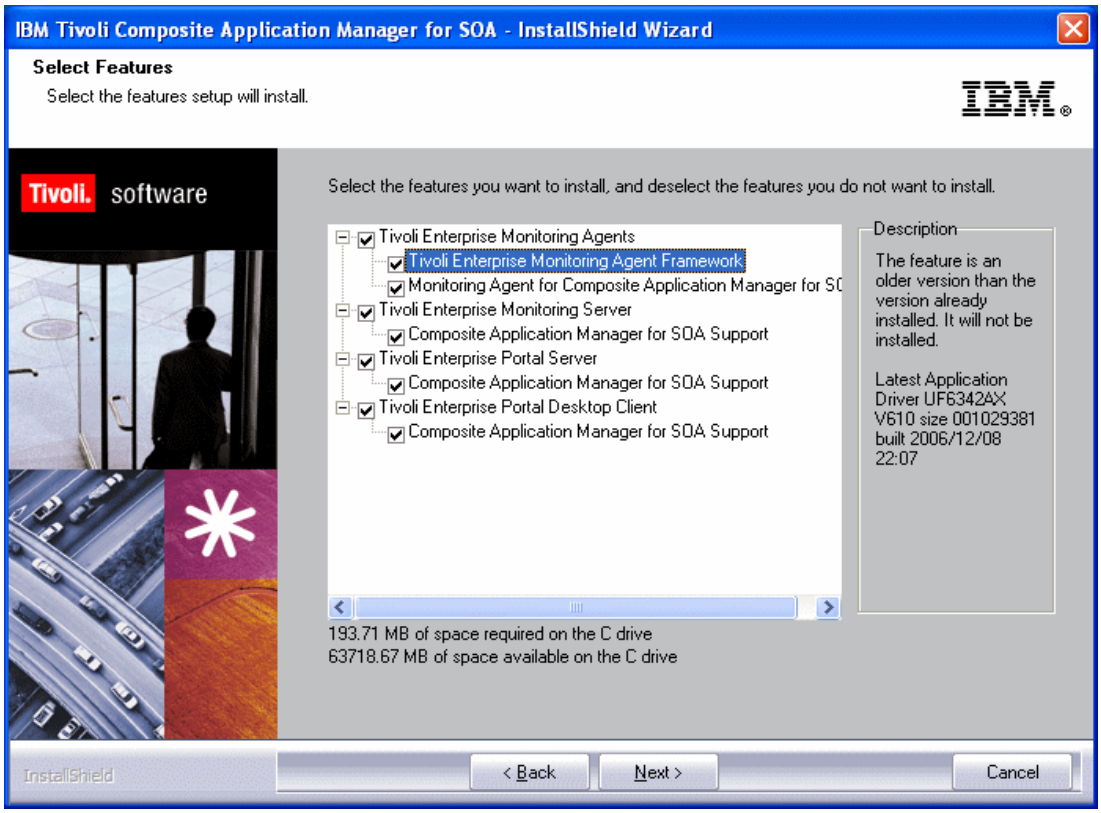


Figure 1-5 Select Features window

Application support components: If you select any of the application support components that are already installed, a window opens that shows a warning message. You can either overwrite the existing installation files or deselect the desired component to avoid overwriting the files.

4. In the Agent Deployment window (Figure 1-6), you see that ITCAM for SOA supports packaging of the agent for remote deployment. This is primarily used for monitoring the DataPower device®. We select **Monitoring Agent for Composite Application Manager for SOA**. Click **Next**.

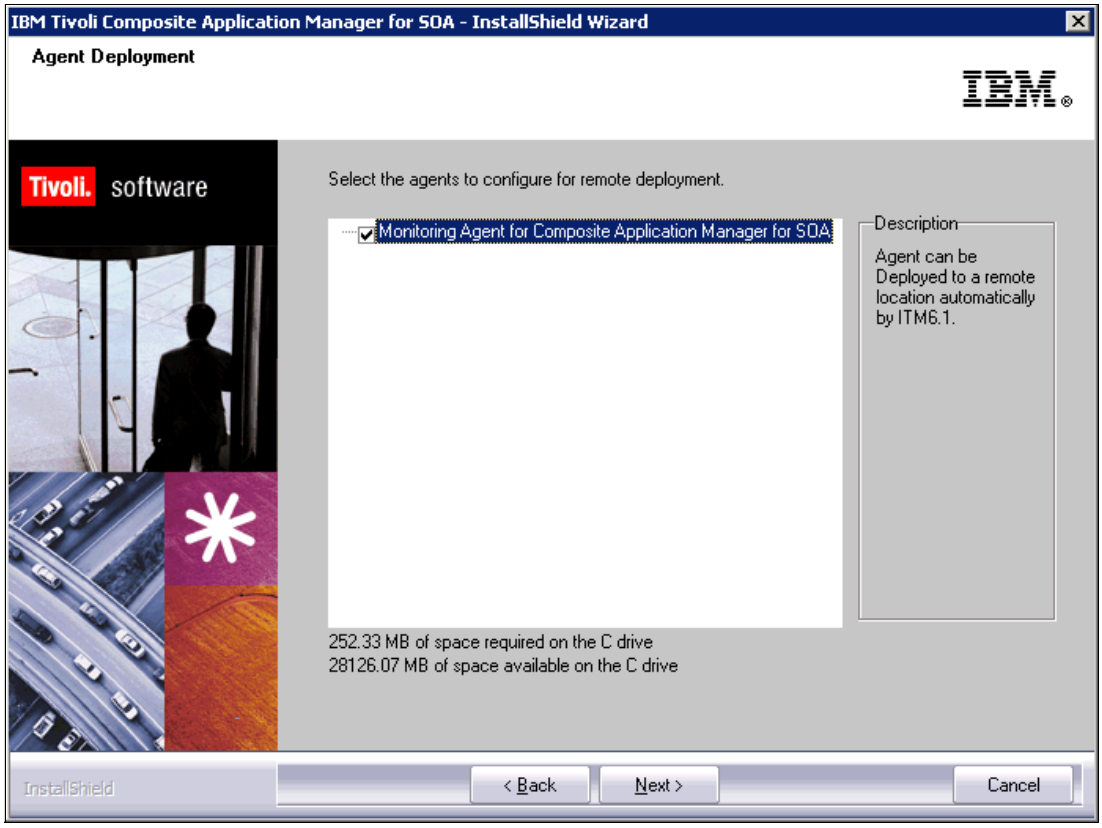


Figure 1-6 Agent Deployment window

5. In the Start Copying Files window (Figure 1-7), review the installation summary and click **Next**.

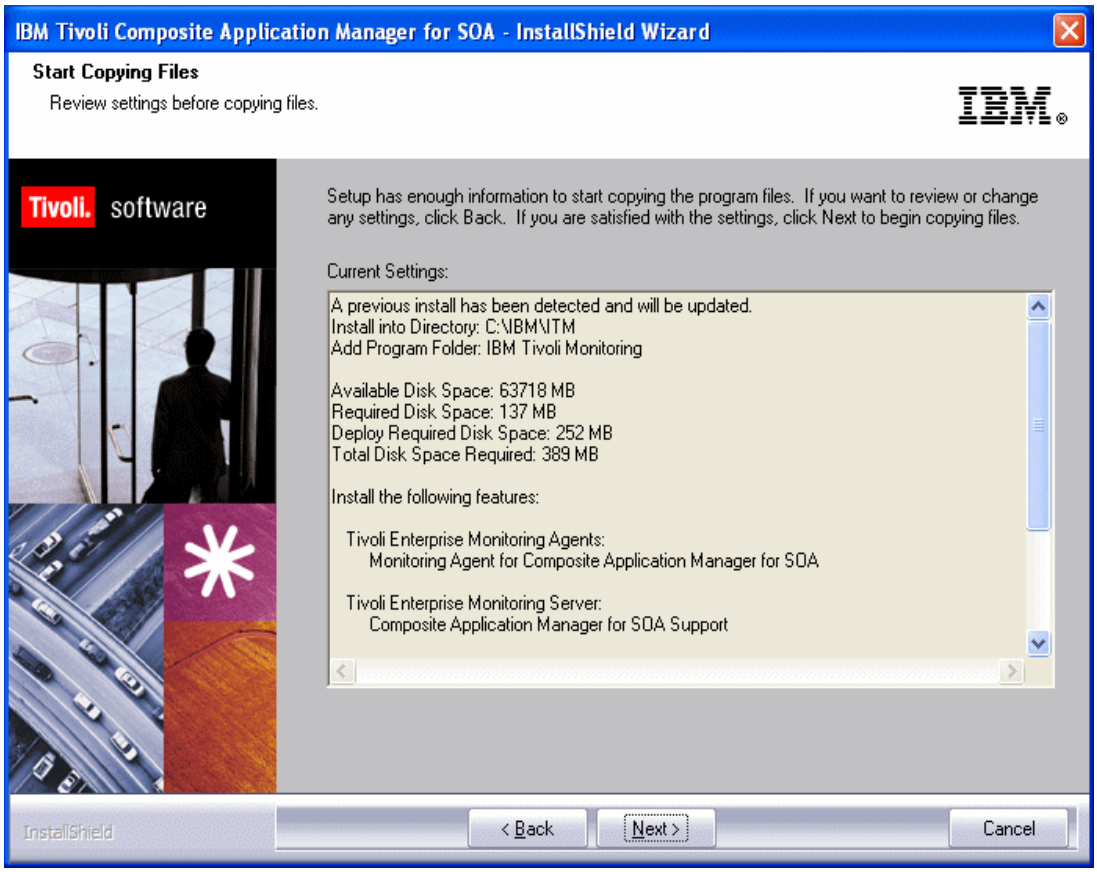


Figure 1-7 Start Copying Files (Summary) window

6. In the Setup Type window (Figure 1-8), select the components that you want to configure and click **Next**.

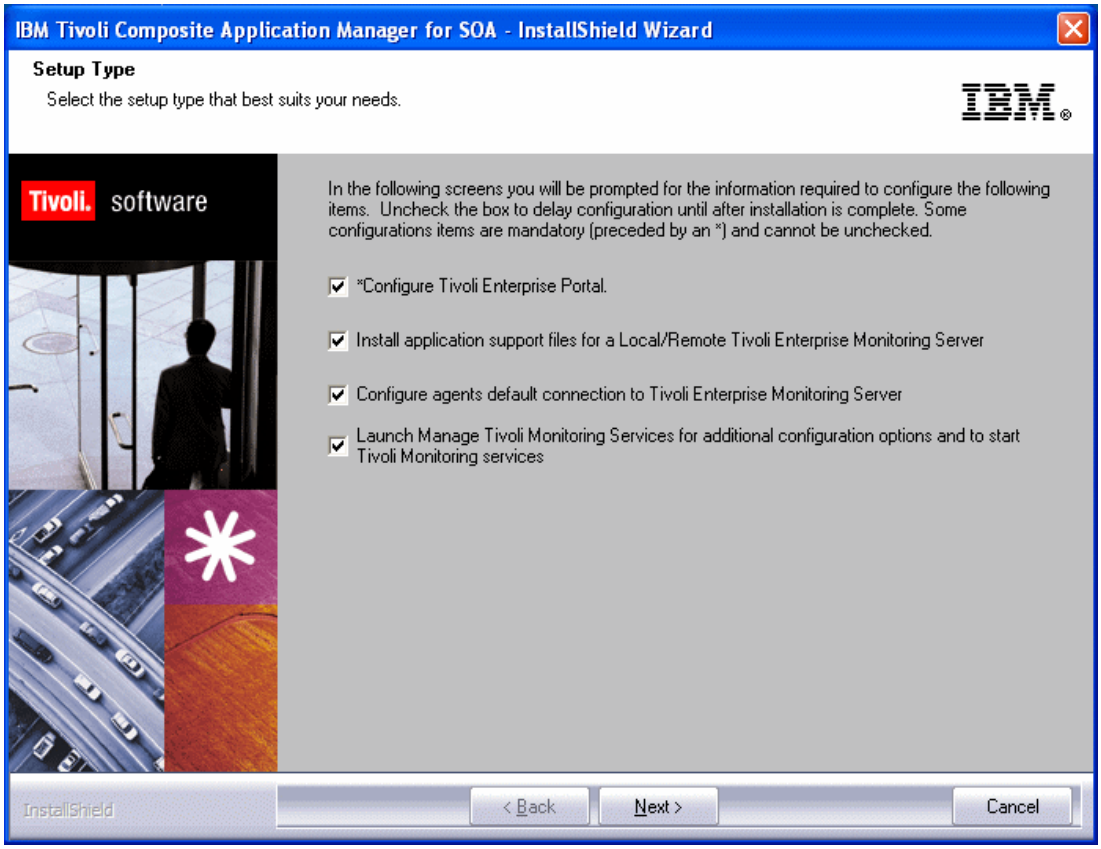


Figure 1-8 Setup Type window with configuration options

7. In the next window, enter the host name of the machine where Tivoli Enterprise Portal Server is installed. In our case, we enter `Lima`.
8. Enter the information for the Tivoli Enterprise Monitoring Server management hub or remote server, as shown in Figure 1-9.

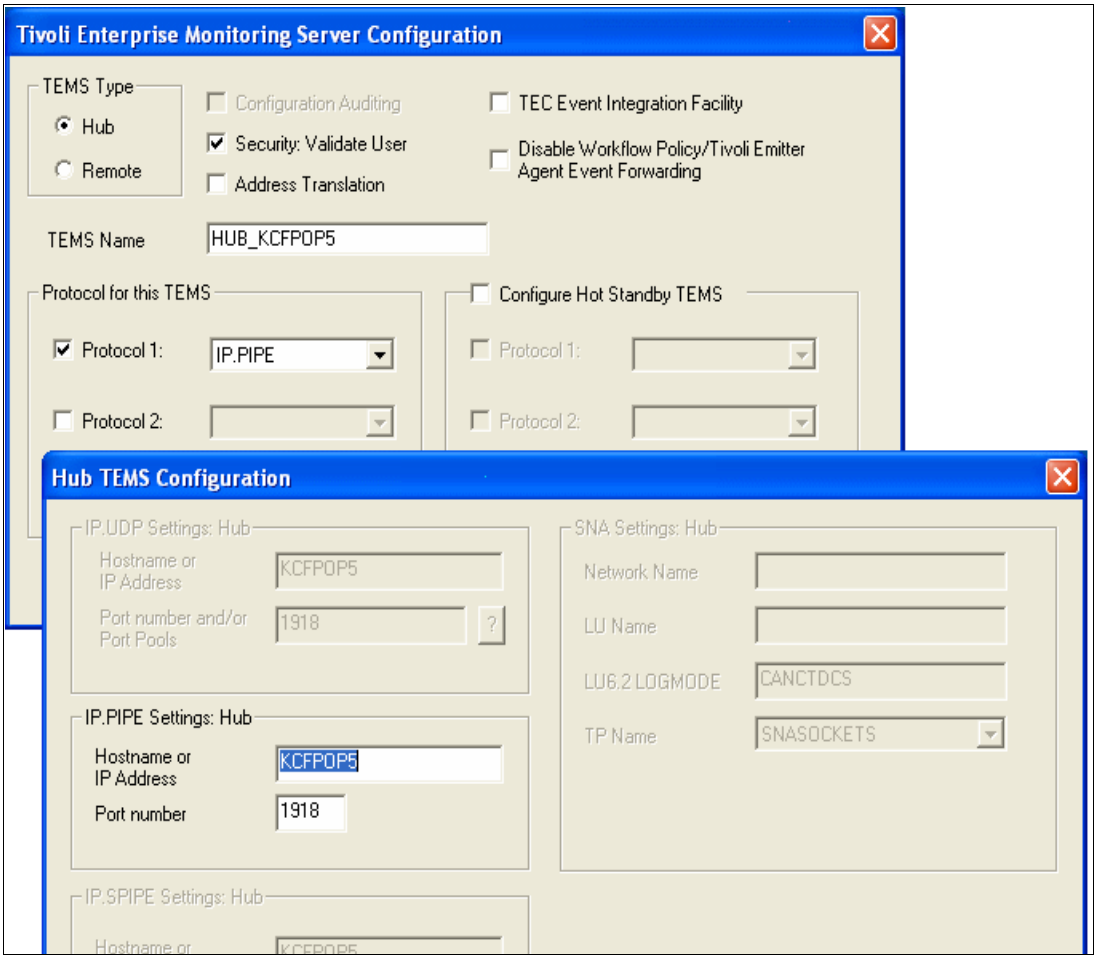


Figure 1-9 Tivoli Enterprise Monitoring Agent hub configuration

9. In the ITCAM for SOA: Agent Advanced Configuration window, select whether Tivoli Enterprise Monitoring Server is located on the same system. In our installation, we select **Protocol 1:** and **IP.PIPE** as shown in Figure 1-10. Then click **OK**.

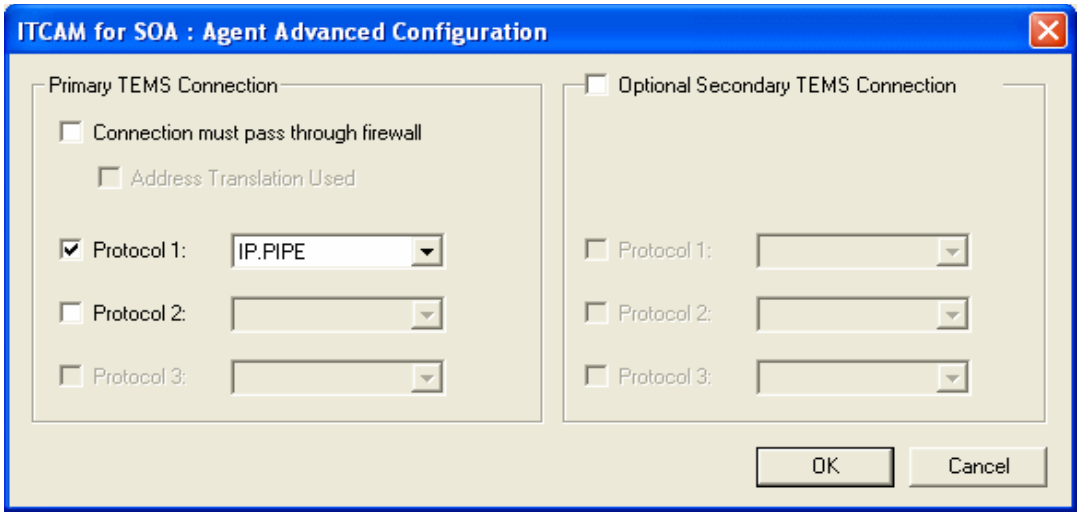


Figure 1-10 Tivoli Enterprise Monitoring Agent configuration (part 1)

10. In the next window, enter the default configuration for the Tivoli Enterprise Monitoring Server connection as shown in Figure 1-11. Then click **OK**.

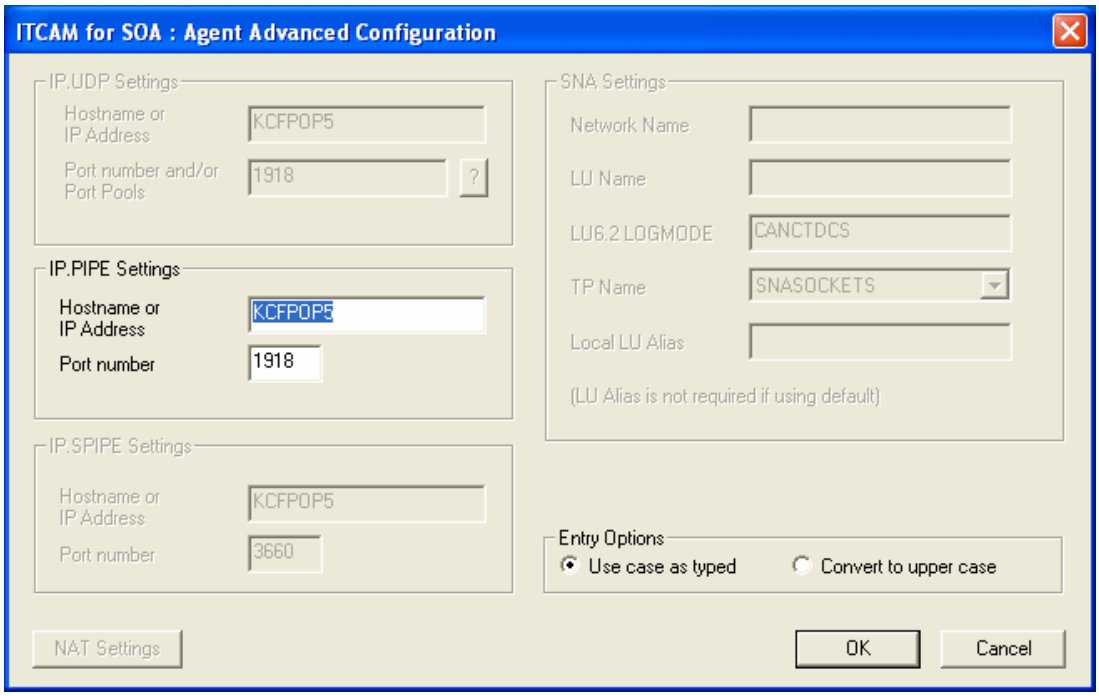


Figure 1-11 Tivoli Enterprise Monitoring Agent configuration (part 2)

1.2.3 Installing the ITCAM for SOA monitoring agent

The monitoring agent installation differs by environment. In this section, we give an overview of the monitoring agent installation. The ITCAM for SOA monitoring agent installation includes the data collector, which is installed into each application server environment where Web services traffic is to be monitored.

Prerequisites: If you are installing the ITCAM for SOA monitoring agent on an application server where Tivoli Enterprise Portal is running, close the Tivoli Enterprise Portal client or browser.

If you are installing ITCAM for SOA monitoring agent on an application server where Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are installed and running, open the Manage Tivoli Enterprise Monitoring Services utility and stop these services. If these Tivoli Monitoring services are running on other application servers in your enterprise, you do not have to stop them.

To launch the ITCAM for SOA monitoring agent Welcome window, you can use either of the following methods:

- For a Windows installation, navigate to the /WINDOWS directory and select **`setup.exe`** from the ITCAM for SOA product CD.
- For a UNIX® installation, refer to *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492.

Starting the agent: Start the agent with the same user ID that you used to start WebSphere, because the agent must be able to start and stop WebSphere with the default startServer and stopServer scripts.

You do not have to start the ITCAM for SOA monitoring agent until the monitoring agent is enabled for the application server. If you start the monitoring agent prior to enabling the application server, the agent starts but must be stopped and restarted after enabling the application server. Tivoli Enterprise Monitoring Server does not collect data from the ITCAM for SOA monitoring agent if you enable the application server after initially starting the ITCAM for SOA service.

1.2.4 Enabling the monitoring agent in the DataPower environment

Next you enable the ITCAM for SOA monitoring agent data collector handler in the DataPower environment. After you install ITCAM for SOA monitoring agent on the application server, the data collector directory structure is created in the Tivoli Enterprise Monitoring Agent base directory as follows:

- In %TEMA_HOME%\TMAITM6\KD4 for Windows
- In $TEMA_HOME/<OS_INTERP>/d4/KD4 for UNIX
- In <TEMA_HOME> for z/OS

These directories contain all the files that are required to run the data collectors.

Installation script: An installation script, called *KD4configDC*, configures the data collector for all application server platforms. However, each platform requires its own additional parameters and steps that must be performed to enable the monitoring of Web services.

Depending on your operating system platform, run the **KD4configDC.sh** or **KD4configDC.bat** commands. The arguments for these commands vary depending on the application server environment. Refer to *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492, for more detailed information about the **KD4configDC** options.

We only enable the data collection in our WebSphere DataPower environment. For the DataPower device, enter the following command to enable the DataPower device to use the KD4 data collector as a JAX-RPC handler:

```
KD4configDC -enable -env 8 <host> <user> <pswd>
```

This command creates a KD4.dpdcConfig.properties file in the %TEMA_HOME%\TMAITM6\KD4 directory.

After the ITCAM for SOA monitoring agent data collector is configured, start the data collector by entering the **startDPDC** command.

1.2.5 Configuring the warehouse proxy

You can configure the warehouse proxy to start retrieving data into Tivoli Data Warehouse from the Manage Tivoli Enterprise Monitoring Services windows as explained in the following steps:

1. In the TEMS Mode window (Figure 1-12), right-click **Warehouse Proxy** and select **Reconfigure**.

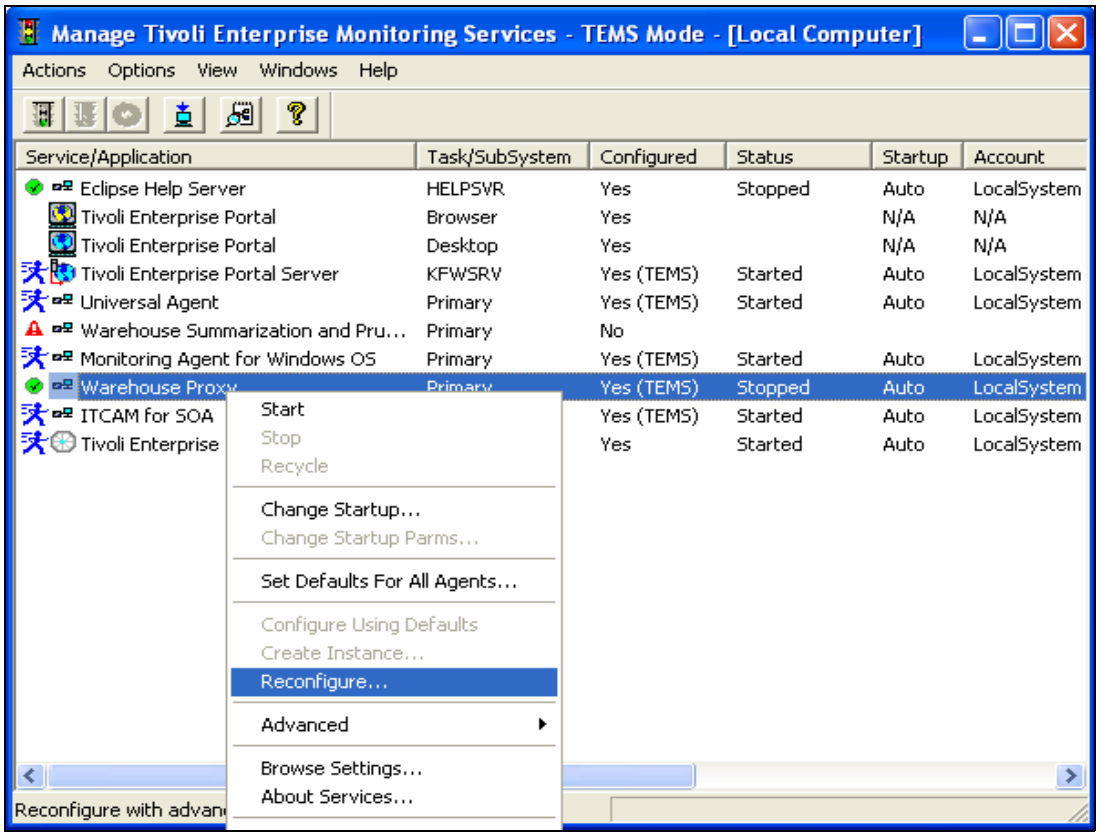


Figure 1-12 Manage Tivoli Enterprise Monitoring Services - TEMS Mode window

2. As shown in the windows in Figure 1-13, specify the Tivoli Enterprise Monitoring Server settings.

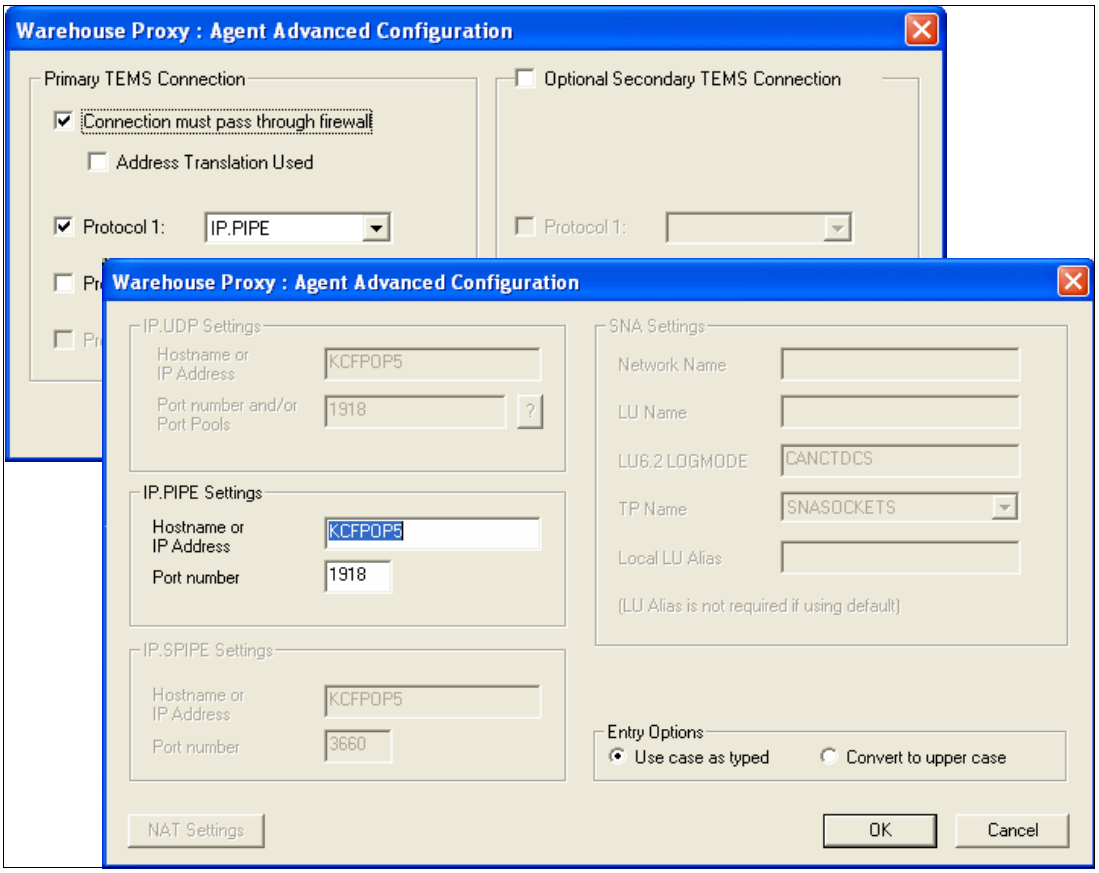


Figure 1-13 Warehouse Proxy configuration: Tivoli Enterprise Monitoring Server settings

3. Provide the database settings (Figure 1-14). We use the `Warehous` database in our DB2® Universal Database™ database.

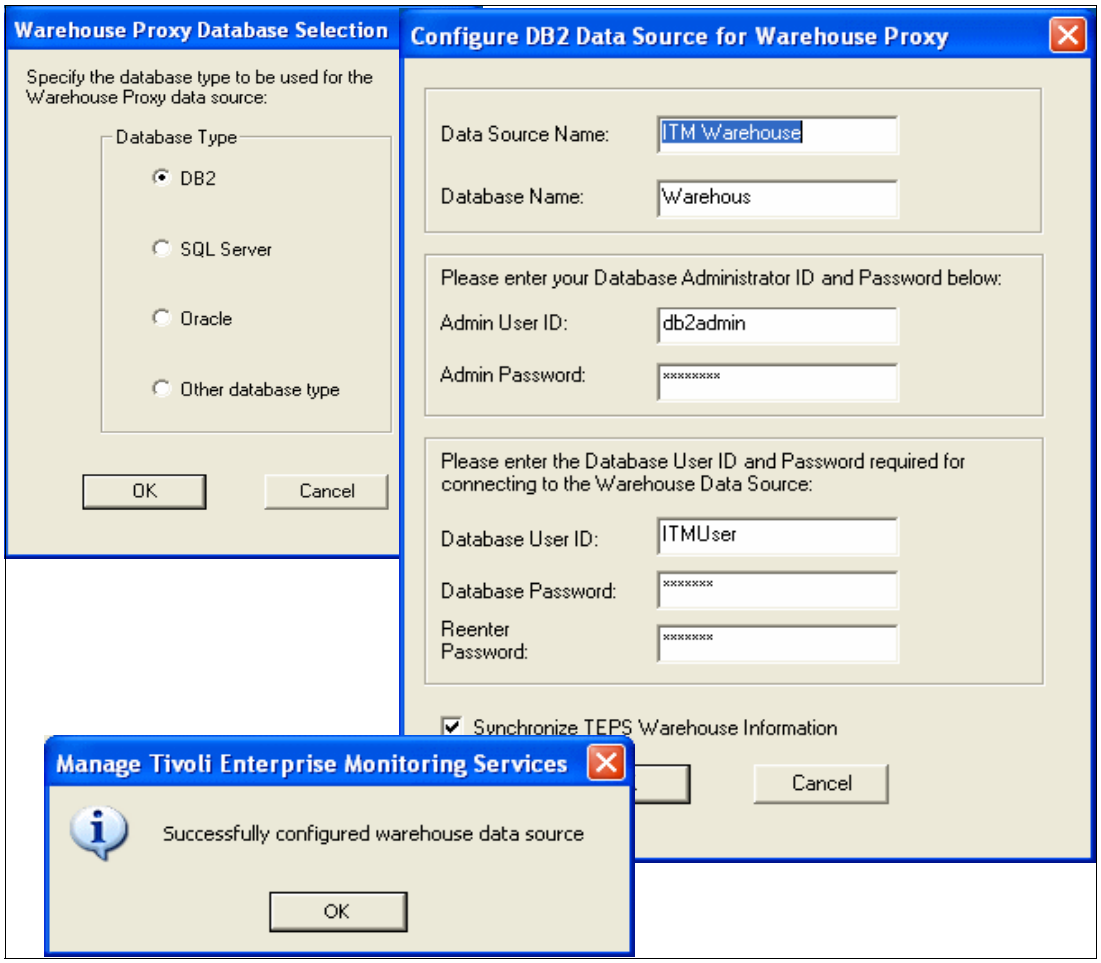


Figure 1-14 Warehouse Proxy configuration: Database settings

Now the warehouse proxy has been configured and started. You can configure data collection for the IBM Tivoli Monitoring Agents. To enable ITCAM for SOA collection:

1. Click the **Historical data configuration** button ( ) in Tivoli Enterprise Portal.
2. In the History Collection Configuration window (Figure 1-15), specify that the ITCAM for SOA information is to be collected.

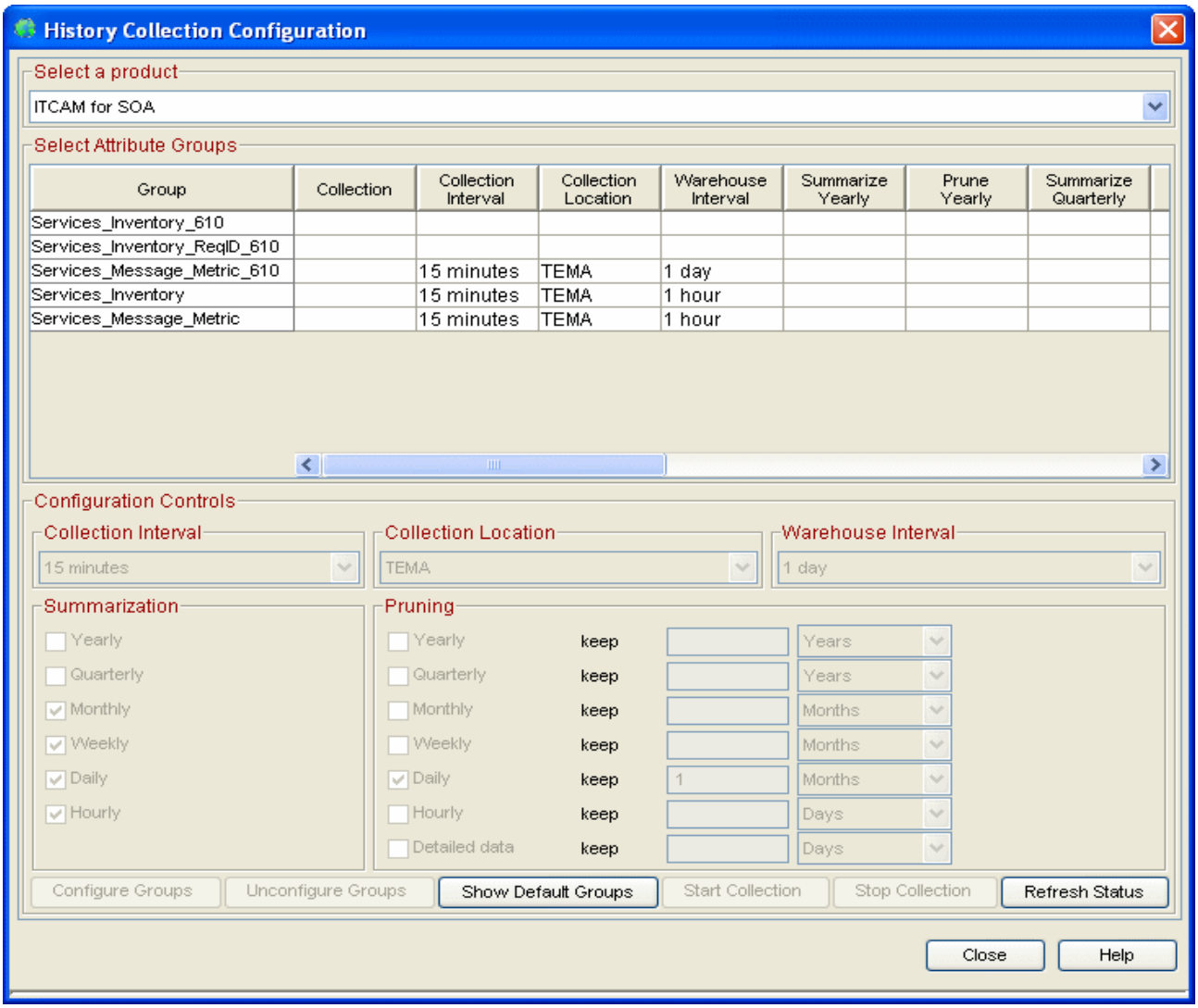


Figure 1-15 History Collection Configuration for ITCAM for SOA

ITCAM for SOA then collects a large amount of data. You might want to limit the collection to a particular shorter time. The data from ITCAM for SOA in the metric table is used by IBM Web Services Navigator.

1.2.6 Installing IBM Web Services Navigator

IBM Web Services Navigator runs in the Eclipse environment. ITCAM for SOA V6.1 is packaged with its own Eclipse V3.0.2 environment. You can install IBM Web Services Navigator into IBM Rational Application Developer V6.1 and IBM Rational Software Architect V6.1, which are built on the Eclipse platform. Refer to *IBM Tivoli Composite Application Manager for SOA Tools version 6.1.0*, GC32-9494, for more information.

IBM Web Services Navigator can be installed with a new Eclipse environment or to an existing Eclipse environment as an Eclipse plug-in. Currently, IBM Web Services Navigator is supported only on Windows and Linux®-based operating systems. Figure 1-16 shows the installation path and option that we use.

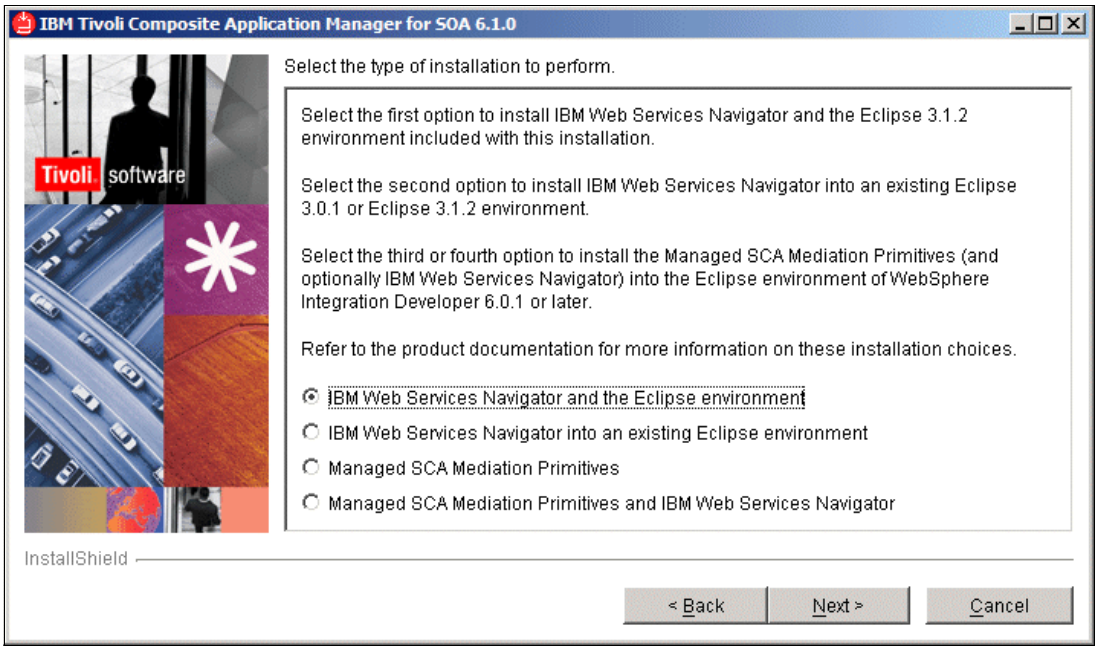


Figure 1-16 IBM Web Services Navigator installation

When the installation is completed, you can launch IBM Web Services Navigator from **Programs** → **IBM Tivoli Composite Application Manager for SOA 6.1.0** → **IBM Web Services Navigator**, or by executing `runNavigator`.

IBM Web Services Navigator uses a perspective in Eclipse called the *Web Services Profiling perspective*. For more information about Eclipse and perspective usage in Eclipse, refer to the Eclipse Web site at the following address:

http://www.eclipse.org

When starting IBM Web Services Navigator, the task assistant page (Figure 1-17) opens to guide you through the use of the navigator.

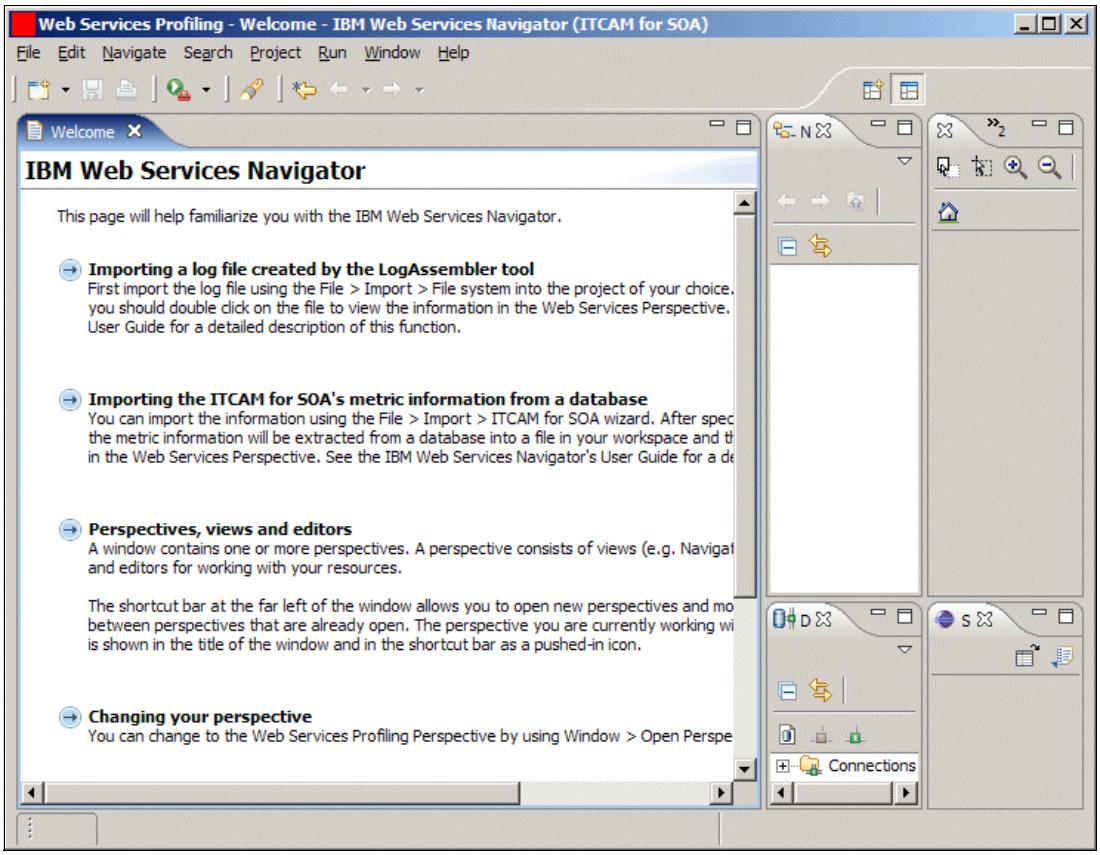


Figure 1-17 Initial help window for IBM Web Services Navigator

You can exit the help window by using the restore tool and resizing the help window. Figure 1-18 shows an empty Eclipse workspace with the Web Services Profiling perspective.

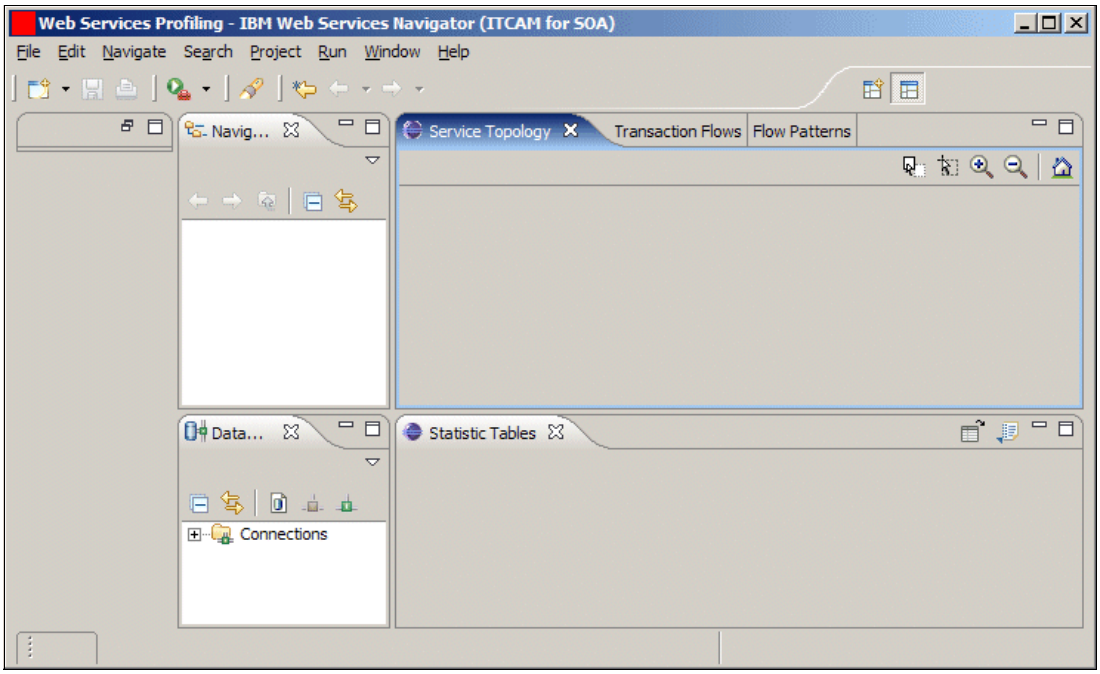


Figure 1-18 Empty IBM Web Services Navigator workspace

1.3 ITCAM for SOA in the DataPower environment

The monitoring of Web services flows is supported through a DataPower SOA appliance that acts as a proxy between the Web services client and server. You use a DataPower SOA appliance to improve security and performance by offloading such functions as authentication and authorization, XML schema validation, and Web services encryption and decryption.

IBM Tivoli Composite Application Manager for SOA v6.1 includes a DataPower data collector that monitors Web services flows through a DataPower SOA appliance. It provides similar services management and availability information that IBM Tivoli Composite Application Manager for SOA currently provides for application server runtime environments. This information is displayed in the Tivoli Enterprise Portal by using the usual predefined or user-defined workspaces and views.

Upgrading your firmware

Before you use the DataPower data collector, you must upgrade the firmware on the DataPower SOA appliances that you want to monitor, to include the necessary monitoring and data transformation capabilities. Be sure to upgrade your firmware to version 3.5.0.5 or later.

1.3.1 The DataPower data collector as a proxy

Data collectors provided with IBM Tivoli Composite Application Manager for SOA are usually installed directly into the application server runtime environment that hosts the services that are being monitored. The DataPower SOA appliance, however, does not support the installation of additional software, such as a data collector. Instead, the DataPower SOA

appliance provides a communication mechanism that allows external software applications to receive data from its internal transaction log.

The DataPower data collector is installed on a separate machine. It uses this communication mechanism to retrieve monitoring data about Web services requests flowing through one or more DataPower SOA appliances, and converts the data into a format that IBM Tivoli Composite Application Manager for SOA can process. In this way, the DataPower data collector acts as a proxy between the DataPower SOA appliances and the IBM Tivoli Composite Application Manager for SOA intelligent remote agent (IRA).

Note: IBM supports running only one instance of the DataPower data collector on any given system.

When the DataPower data collector starts, it subscribes to each monitored DataPower SOA appliance and then polls (at an interval that you can configure) the appliance for monitoring data. The data that is retrieved from the DataPower SOA appliance is written to metric log files in the format used by IBM Tivoli Composite Application Manager for SOA. When this data is displayed later in the Tivoli Enterprise Portal, nodes are displayed in the Tivoli Enterprise Portal Navigator view that represent the DataPower SOA appliances being monitored. You can select workspaces under these nodes and view the service management data for the Web services requests that flow through the monitored DataPower SOA appliances.

The DataPower data collector can subscribe to multiple DataPower SOA appliances, and retrieve and manage data from multiple domains. This data can then be separated by a DataPower domain or aggregated across multiple domains and appliances, depending on how you configure the data collector. We discuss the various configurations in the next section “Planning for deployment”.

1.3.2 Planning for deployment

DataPower Web services proxies are defined within application domains, and DataPower users can be restricted to access some or all domains. When configuring the DataPower data collector, you must understand how the domains and users are defined on the monitored DataPower SOA appliances to ensure that the data collector uses valid authentication credentials. In addition, you must decide how you want to aggregate or separate the data collected from those domains for display in the Tivoli Enterprise Portal.

You can use the DataPower SOA appliance in several typical configurations:

- Single appliance, single domain
- Single appliance, multiple domains
- Multiple appliances with different configurations
- Multiple appliances with identical configurations

Given these typical configurations, the DataPower data collector provides a great deal of flexibility in defining how the collected monitoring data should be separated or aggregated, across a single appliance or multiple appliances, for display in the Tivoli Enterprise Portal.

The following examples illustrate how data can be separated or aggregated for managing the data from various domains and appliances:

- Separation of data at the domain

  You can view the services management data for the resources in a single domain, separate from the data for resources in other domains.

- Aggregation of data across domains

  You can view the services management data for the resources in several domains (for example, all of the domains on a given DataPower SOA appliance) in an aggregated form, with no regard for the domain in which individual resources are defined.

- Separation of data at the appliance

  You can view the services management data for resources on a single DataPower SOA appliance, separate from the data for resources on other appliances.

- Aggregation of data across appliances

  You can view the services management data for the resources on several DataPower SOA appliances (for example, all of the appliances in a load-balancing cluster) in an aggregated form, with no regard for the activity that occurs on each individual appliance.

By default, the DataPower data collector aggregates data for all of the monitored domains on a single DataPower SOA appliance, even if the domains are accessed by using different credentials. The data collector also keeps the data from each DataPower SOA appliance separated.

A single instance of the DataPower data collector can monitor any number of DataPower SOA appliances, limited only by the memory, processor power, and other resources available to it.

> **Note:** IBM supports running only a single instance of the DataPower data collector on any given system.

1.3.3 Deploying the DataPower data collector

The deployment of the DataPower data collector in your environment requires the following actions:

1. Configuring the DataPower SOA appliance for monitoring
2. Enabling the DataPower data collector
3. Starting the DataPower data collector

Configuring the DataPower SOA appliance for monitoring

Before a DataPower SOA appliance can be monitored by the DataPower data collector, configure the DataPower SOA appliance by performing the following tasks:

1. Enable the XML Management Interface on the appliance as explained in the following section.
2. Check the additional optional settings for each domain to be monitored.
3. Configure a user account on the DataPower SOA appliance for use with the DataPower data collector.

Enabling the XML Management Interface on the appliance

The XML Management Interface on the appliance must be enabled by using the DataPower administration console. To enable this service:

1. Start the DataPower administration console in a Web browser:

   `https:// datapower.itso.ral.ibm.com:9090/login.xml`

2. Log in to the administration console as admin in the *default* domain.
3. In the navigation area on the left, navigate to **Objects** → **Management** → **XML Management Interface**.

4. On the main tab, select the **WS-Management Endpoint** and enable the interface. Click **Apply** to activate the changes.

Optionally you can navigate to **Services** → **Miscellaneous** → **Web Service Agent** where you enable the options as shown in Figure 1-19.

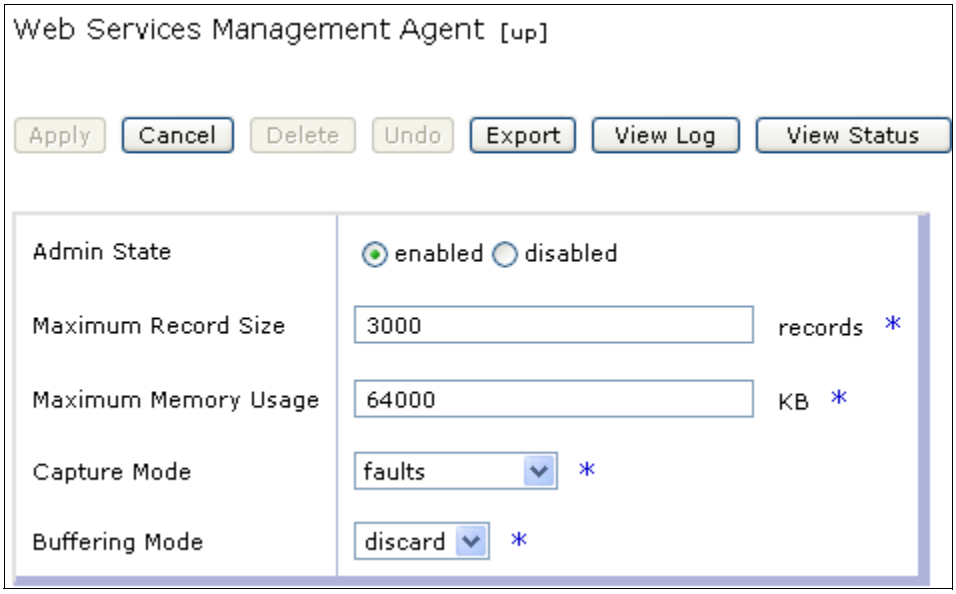


Figure 1-19 Web Services Management Agent

Enabling the DataPower data collector

You configure the DataPower environment for Data collection as explained in the following sections.

DataPower configuration file

For the DataPower data collector, the **`KD4configDC`** command manipulates the contents of a special DataPower configuration file. It adds sections to the file when new DataPower monitoring is enabled and removes sections from the file when monitoring is disabled. Each invocation of the **`KD4configDC`** command is adding, updating, or removing one section of the DataPower configuration file. Each section of the DataPower configuration file might be associated with its own data group, or it might be part of a larger data group to which other sections of the configuration file also belong.

The DataPower data collector uses this configuration file to identify the DataPower SOA appliances that are to be monitored and to specify all of the information that is necessary to communicate with those appliances. Typical information that is stored for each connection includes the host name and port, user ID and password, domains to monitor, and polling interval.

The configuration file is located in the *ITM_DIR*\TMAITM6\KD4\config directory and is called *KD4.dpdcConfig.properties*. This file is maintained separately from the existing KD4.dc.properties configuration file.

Example 1-1 shows a sample DataPower configuration file.

Example 1-1 Sample DataPower configuration file

```
# Sample DataPower data collector configuration file
DataPower.count=2
#
DataPower.host.1=datapower.itso.ral.ibm.com
DataPower.port.1=5550
DataPower.path.1=/
DataPower.poll.1=10
DataPower.user.1=admin
DataPower.encpswd.1=cGFzc3dvcmQ=
DataPower.displaygroup.1=dpCaseStudy
#
DataPower.host.2=datapower2.itso.ral.ibm.com
DataPower.port.2=5550
DataPower.path.2=/
DataPower.poll.2=10
DataPower.user.2=admin
DataPower.encpswd.2=cGFzc3dvcmQ=
```

Example 1-1 has two sections in the configuration file. The properties in each of the two sections provide all of the information that is needed to establish and manage a single connection or session with each DataPower SOA appliance.

Running the KD4configDC command

The syntax for running the **KD4configDC** command for the DataPower environment is similar to the syntax for other supported IBM Tivoli Composite Application Manager for SOA data collector environments. To run the **KD4configDC** command, navigate to the location *ITM_DIR*\TMAITM6\KD4\bin and enter the following command:

```
KD4configDC {-enable | -disable} -env 8 <env specific parameters>
```

The <env specific parameters> defined for the DataPower invocation of the **KD4configDC** command are a series of key and value pairs that define the necessary properties for the affected section of the DataPower configuration file. Table 1-2 shows these DataPower key and value pairs.

Table 1-2 DataPower key and value pairs for the KD4configDC command

Parameter	Optional or required	Default value	Description
-host <hostname or ip-address>	Required		Defines the DataPower SOA appliance host name or IP address. This host name is used to establish a socket connection and is used as part of the Web address that points to the DataPower SOA appliance. It can be any length string, with no blank characters.
-user <user-id>	Required		Defines the DataPower SOA appliance authentication user. This user must be a valid user for the DataPower SOA appliance defined by the -host parameter.
-pswd <password>	Optional	User is prompted if necessary	Defines the DataPower SOA appliance authentication password, entered in clear text (not encoded). This password must be valid for the user defined in the –user parameter, and must be valid for the DataPower SOA appliance defined by the –host parameter. This password is automatically converted to an encoded (masked) form and is stored in the DataPower configuration file.

Parameter	Optional or required	Default value	Description
-port <port number>	Optional	5550	Defines the DataPower SOA appliance port number.
-poll <poll interval>	Optional	10 seconds	Defines the DataPower SOA appliance polling interval (in seconds).
-domainlist	Optional	No domainlist property is generated	Defines the DataPower SOA appliance domain list. This is a comma-separated list of domains to be monitored on the associated DataPower SOA appliance. Any domains in this list that are not authorized to the user defined by the -user parameter are not monitored. Each domain can be any string, with no blank characters. If you specify more than one domain name, separated by commas, the entire domain list must be enclosed in double quotation marks, for example, –domainlist "domain1,domain2,domain3".
-displaygroup <dispaly group>	Optional	No displaygroup property is generated	Defines the DataPower SOA appliance display name. The name can be any string, with no blank characters, up to 16 characters long. See “Creating node names in Tivoli Enterprise Portal” in *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492, regarding possible truncation of this value in the node name.

You can use variations of the parameters specified in the **KD4configDC** command to define properties that configure the monitoring of one or more DataPower SOA appliances. The reason why you want to do this is to separate different data collectors to use more than one set of authentication credentials. For more information, refer to *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492.

Starting the DataPower data collector

To start the DataPower data collector, open a command prompt and run the startDPDC script. Support for running this data collector as a Windows service is available in IBM Tivoli Composite Application Manager v6.1 Service pack 1.

When the data collector is started, it monitors the console for commands that are entered by the user. The only supported commands are **stop**, **quit**, and **exit**, all of which initiate an orderly shutdown of the DataPower data collector. When one of these commands is entered, the data collector waits for all communication sessions to end before the process terminates.

While the data collector is running, you can use the **KD4configDC** command to update the DataPower data collector configuration file and change which DataPower SOA appliances and domains are being monitored. You do not need to stop and restart the data collector to activate these changes. The running data collector detects the changed configuration file within 40 seconds and adjust its monitoring to reflect the updated configuration.

1.3.4 Troubleshooting

In this section, we provide tips for troubleshooting.

Communication failures

In the event of a communications failure, the data collector attempts to initialize itself again and re-establish communication with the target DataPower SOA appliance after the next polling interval. This process is repeated for each polling interval until communication is successfully re-established, or until the data collector is stopped. Setting the operations logging level to *info* gives you the best indication of status of the communications between the data collector and the appliance.

Synchronizing time between computer systems

For data to display properly in the Tivoli Enterprise Portal, the DataPower SOA appliance, the data collector system and the Tivoli Enterprise Monitoring Server system must have their clocks synchronized within 5 minutes of each other, in terms of the Coordinated Universal Time (UTC) that they report.

Password problems

User IDs and passwords for DataPower SOA appliances are created and maintained at the appliance. When you reset this information at the DataPower SOA appliance, use the **`KD4configDC`** command to update the DataPower configuration file with the latest user ID and password values for the appropriate section of the file.

Launching the DataPower Web browser interface

You can select a DataPower SOA appliance that is displayed in a row of the Services Inventory attributes table in the Performance Summary workspace of the Tivoli Enterprise Portal. Then follow the procedure that is described in this section to launch a Web browser session that opens the DataPower WebGUI. You can use this sophisticated interface to configure the DataPower SOA appliance and the policies that the appliance applies to Web services traffic.

To launch the DataPower WebGUI:

1. From the Tivoli Enterprise Portal, navigate to the **Performance Summary** workspace and display the Services Inventory attributes table view.
2. As shown in Figure 1-20, select a row in the table from the DataPower system referenced in the Node Name column, and right-click the row and select **Launch** to open the Create or Edit Launch Definitions window.

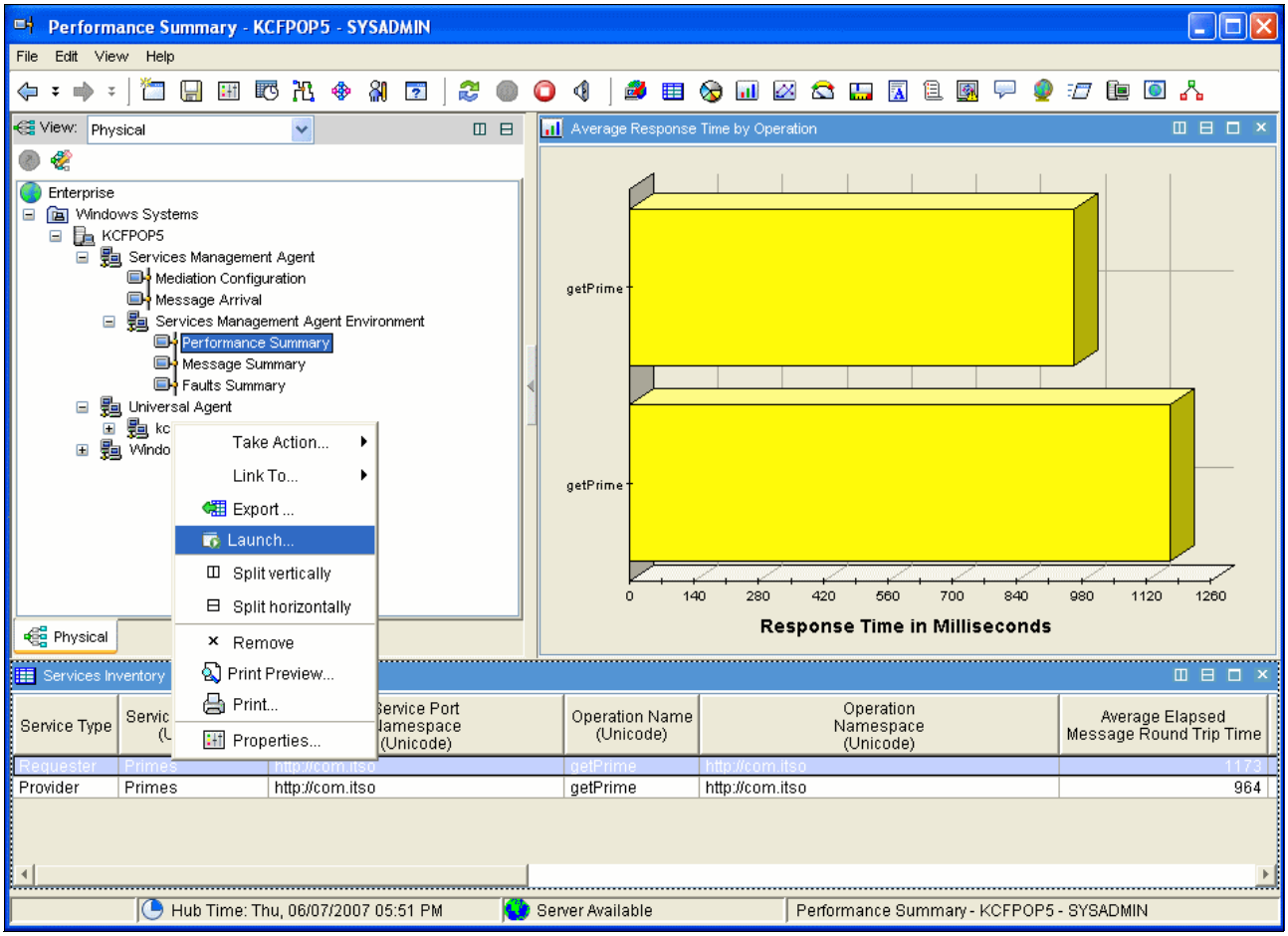


Figure 1-20 Selecting a DataPower row from the Services Inventory Attributes table

The Create or Edit Launch Definitions window opens as shown in Figure 1-21 on page 35. There are certain considerations you need to keep in mind before launching the DataPower GUI from the Tivoli Enterprise Portal. For more information, refer to *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492.

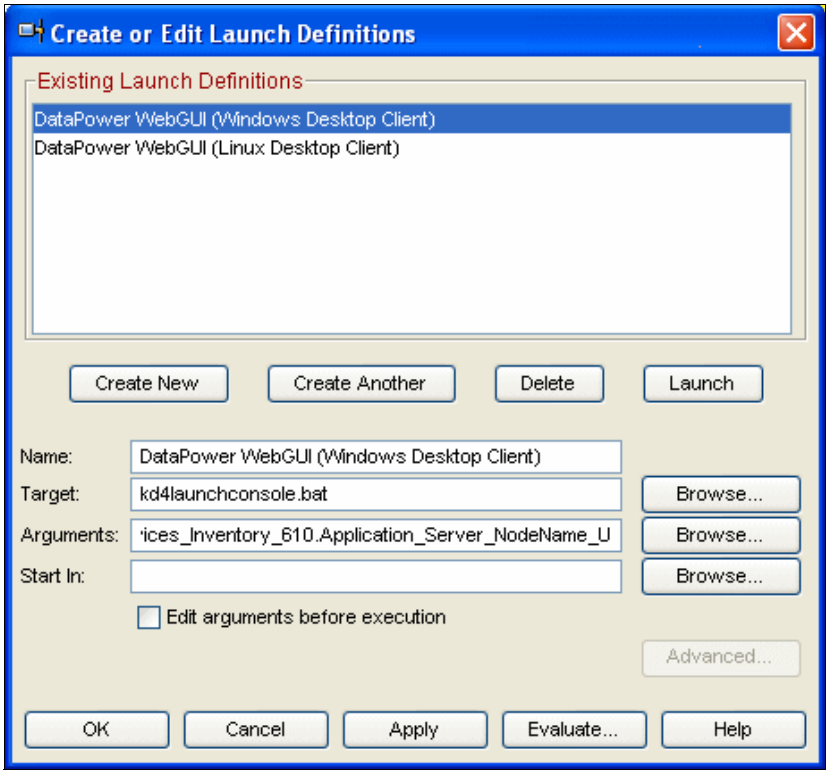


Figure 1-21 Selecting the Windows or Linux desktop client

1.4 ITCAM for SOA usage scenarios

In this section, we gather metrics from the monitored Web services messages. We discuss the use of ITCAM for SOA in the following sections:

- 1.4.1, “Monitoring Web services calls” on page 36
- 1.4.2, “Using historical reporting” on page 39

1.4.1 Monitoring Web services calls

The workspace of ITCAM for SOA (Figure 1-22 shows the default) in the Tivoli Enterprise Portal is arranged to show Web services calls by servers. The Web services calls are typically identified by the following attributes:

- Frequency
- Response time
- Message length

The workspace in Figure 1-22 shows the primary metrics that are collected by ITCAM for SOA. It shows all active Web services calls in the duration. In our Trader application, we have three Web modules, each one accessing DB2, CICS, and IMS. Each Web module serves four Web services calls: getCompanies, getQuote, buy, and sell.

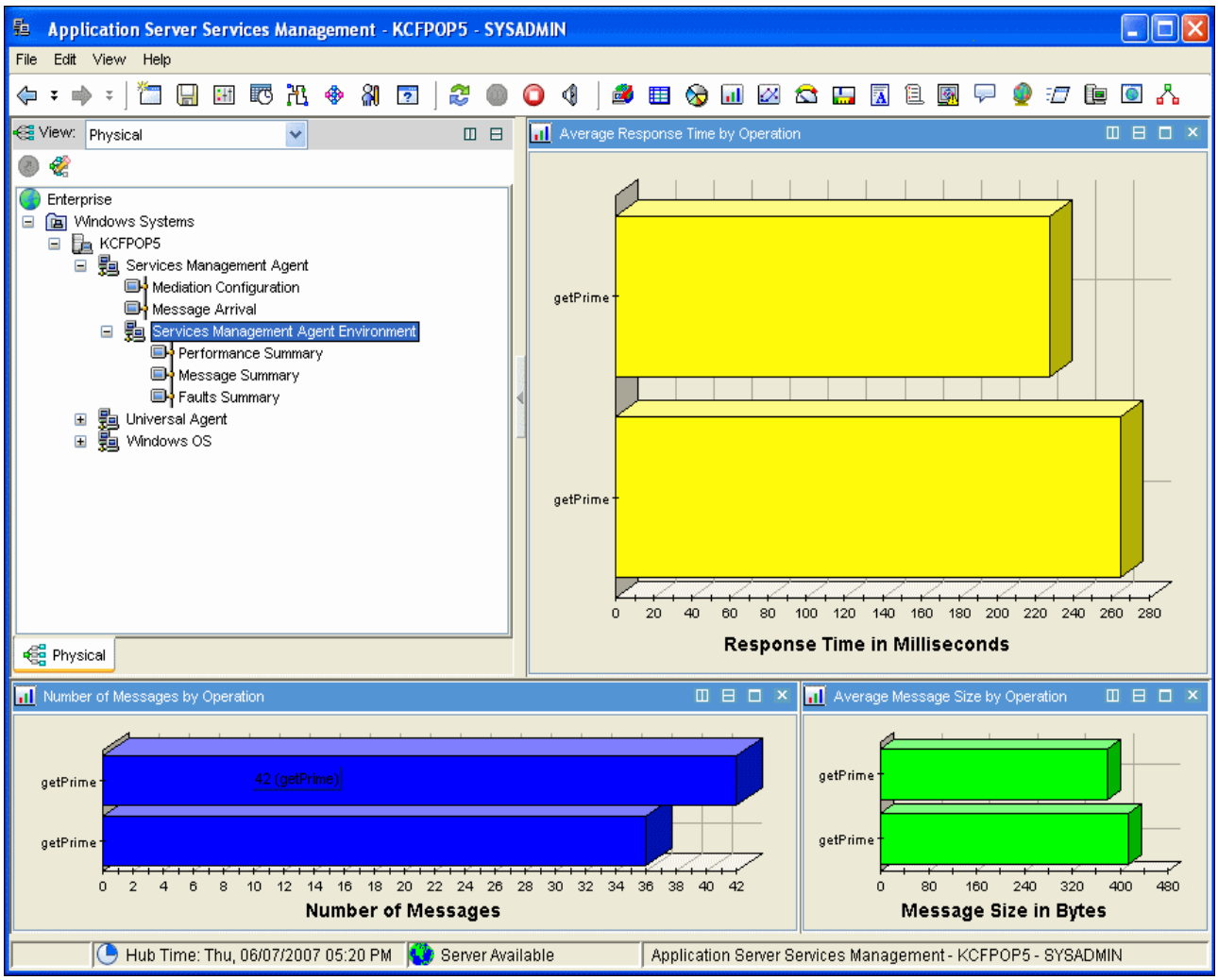


Figure 1-22 Primary workspace for ITCAM for SOA

In the Performance Summary window (Figure 1-23), detailed information about the Web services call performance is shown in a table, along with a response time summary chart.

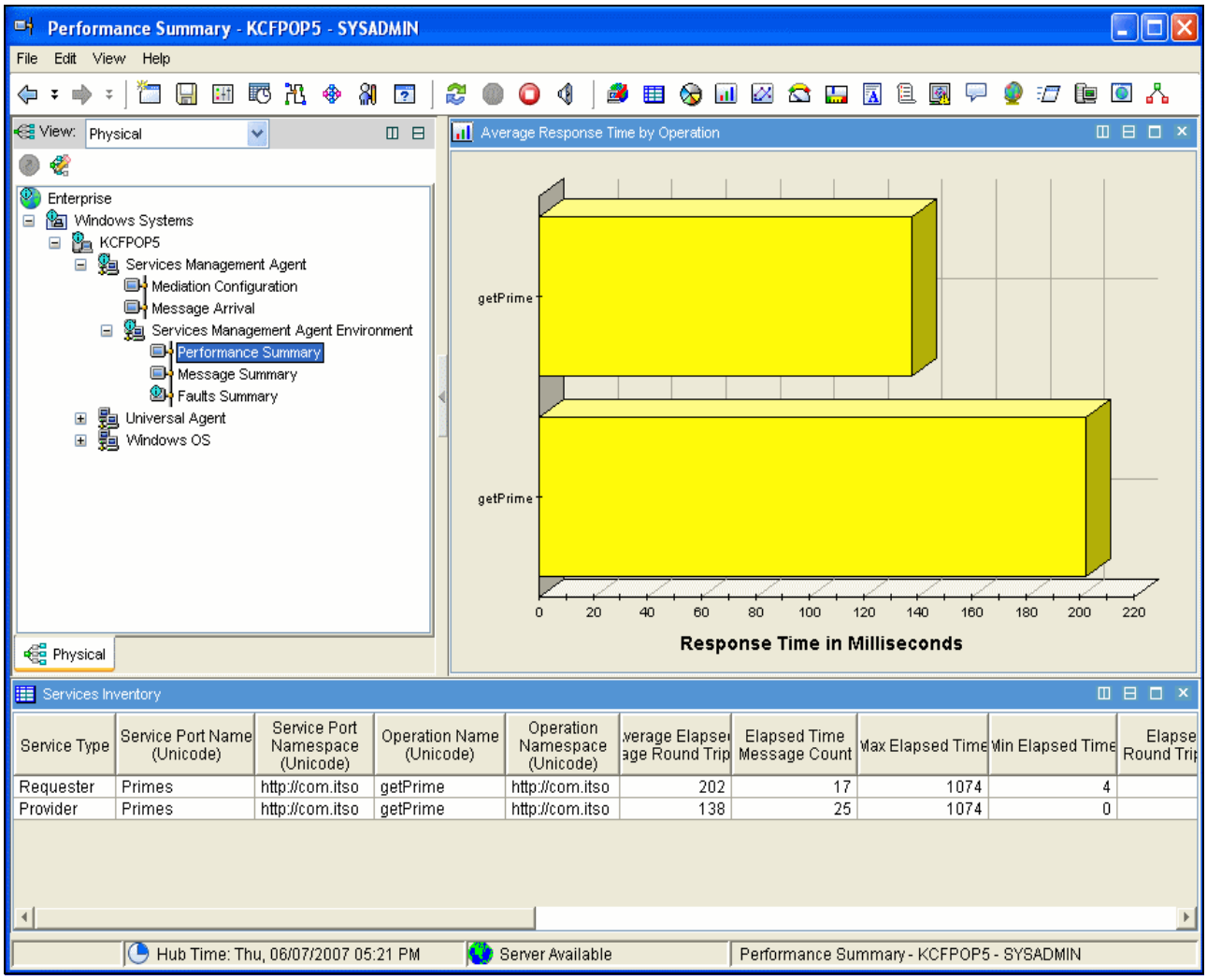


Figure 1-23 Performance Summary window

The Message Summary window (Figure 1-24) shows the message statistics. This page is typically useful for assessing the network capacity requirement for the Web services, because it shows both the length and the number of messages for the server.

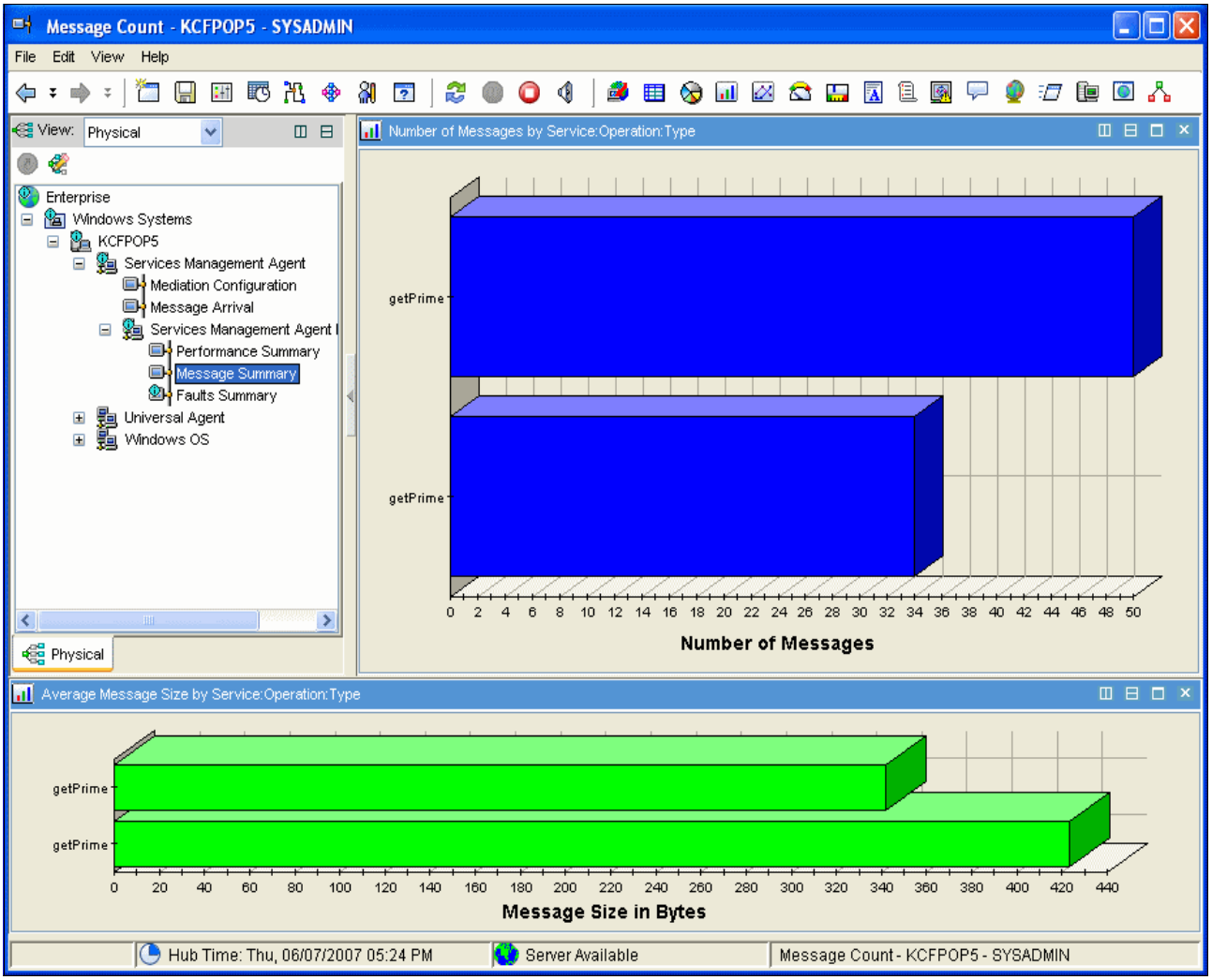


Figure 1-24 Message Summary window

From a different branch, you can see the message arrival rate as shown in Figure 1-25. It shows the activity of the server in general.

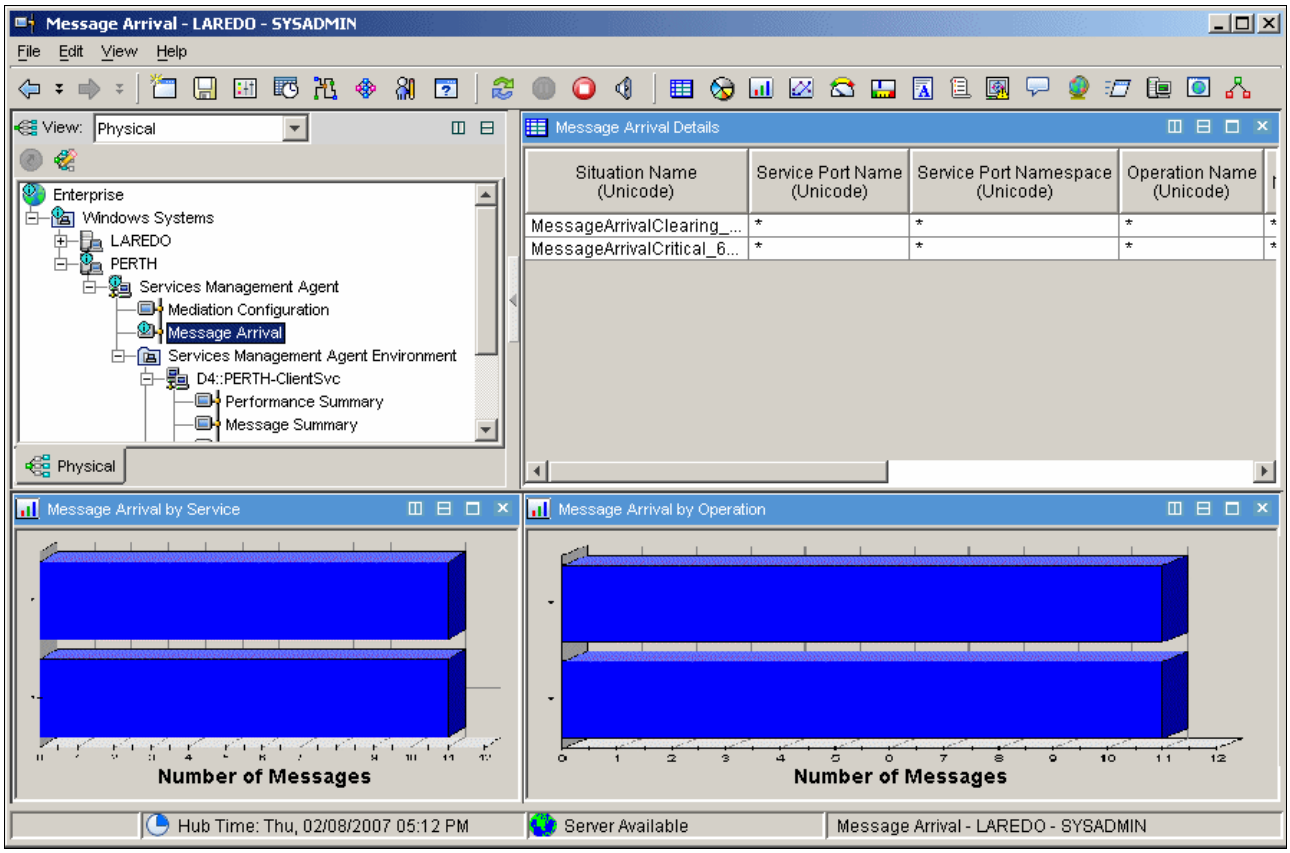


Figure 1-25 Message arrival rate

1.4.2 Using historical reporting

Real-time data is certainly useful, but sometimes we must go back in time to get a report of Web services metrics such as for performance, response time, message size, and the number of faults. In the following sections, we explain how to use historical reporting.

History collection

The historical data is retrieved from binary history files set up through the historical configuration facility on Tivoli Enterprise Portal. If you have enabled the database for the data warehousing facility (see 1.2.5, “Configuring the warehouse proxy” on page 21), you can see historical data for longer periods of time.

For example, you might need to show the number of SOAP-Fault messages that generated over the past week. Tivoli Enterprise Portal extracts the first 24 hours from history binary files that are in the C:\IBM\ITM\TMAITM6\logs directory and the remaining six days from the data warehouse.

After you enable the historical collection, the Time span icon (circled in Figure 1-26) becomes available in each of the workspaces in the navigator view.

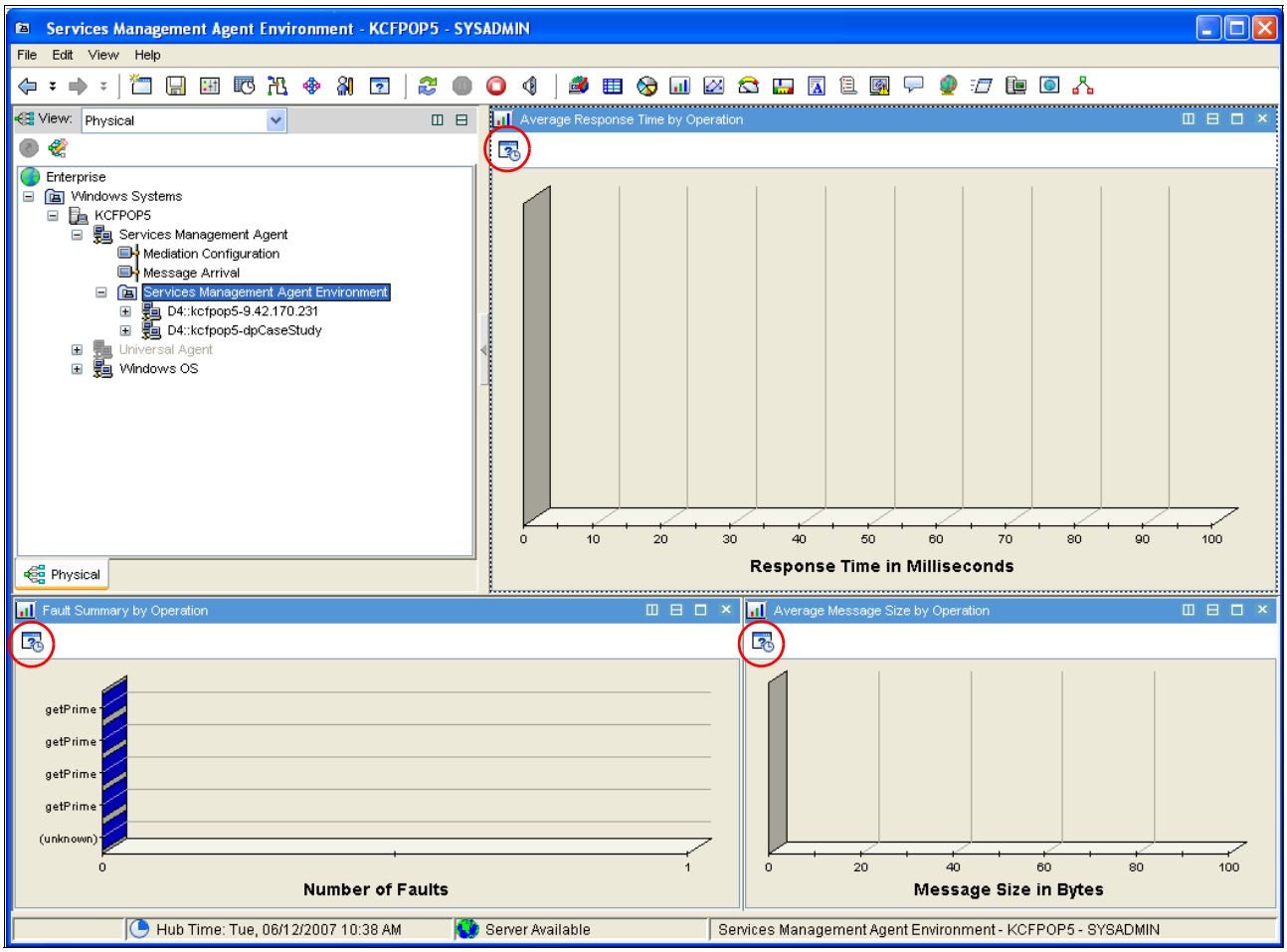


Figure 1-26 Time span icon available after enabling historical collection

Because there is no real-time data flowing, you do not see any graphs displayed. To set the time span:

1. Open the workspace that contains the table or chart where you want to see historical data.
2. Click the **Time span** icon.
3. Select a time frame of **Real time**, **Last**, or **Custom**. If you select Real time, all other options are unavailable as shown in Figure 1-27.

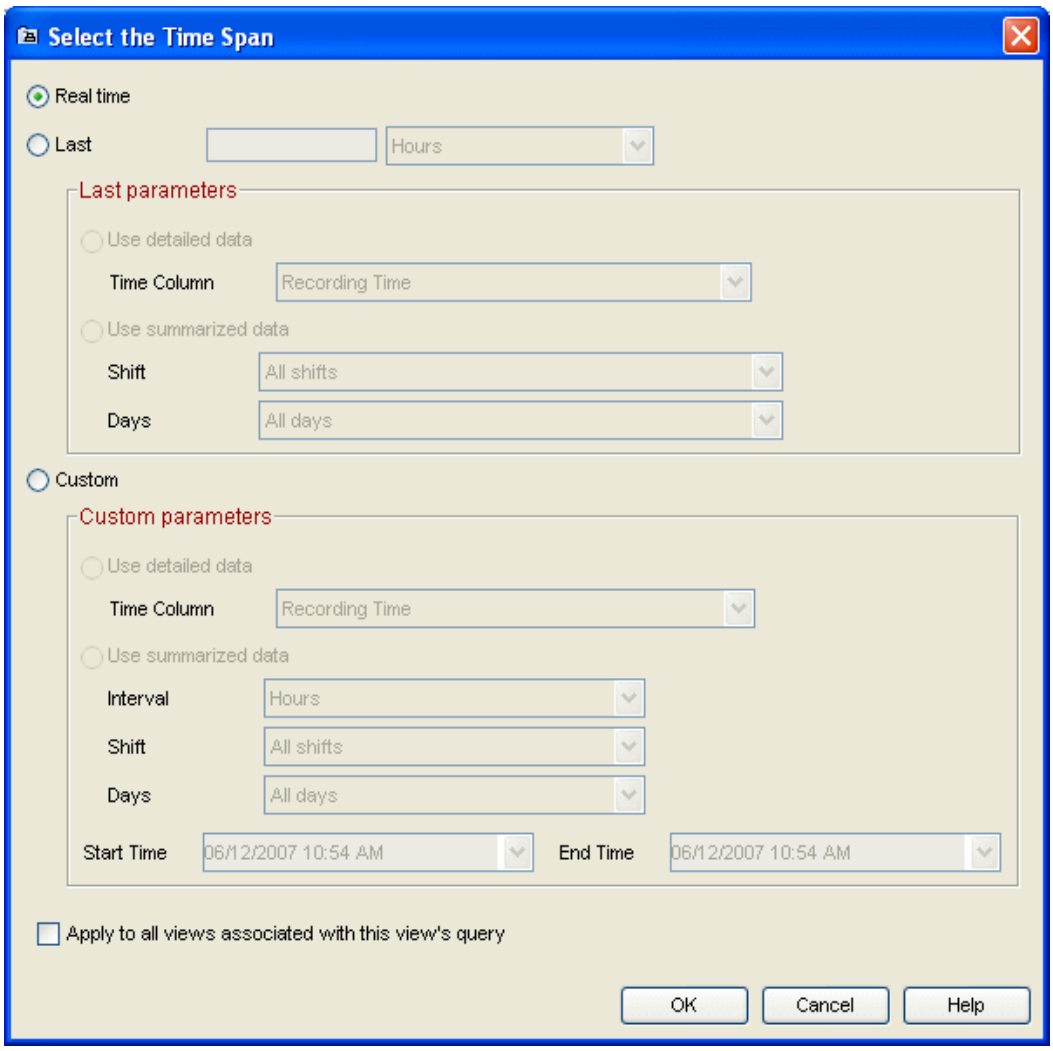


Figure 1-27 Select the Time Span window

Figure 1-28 shows that we selected **Last** and selected **18 Hours** because we want the view of workspaces in the navigator for the last 18 hours. This gives us summarized data across the selected timeframe. Click **OK**.

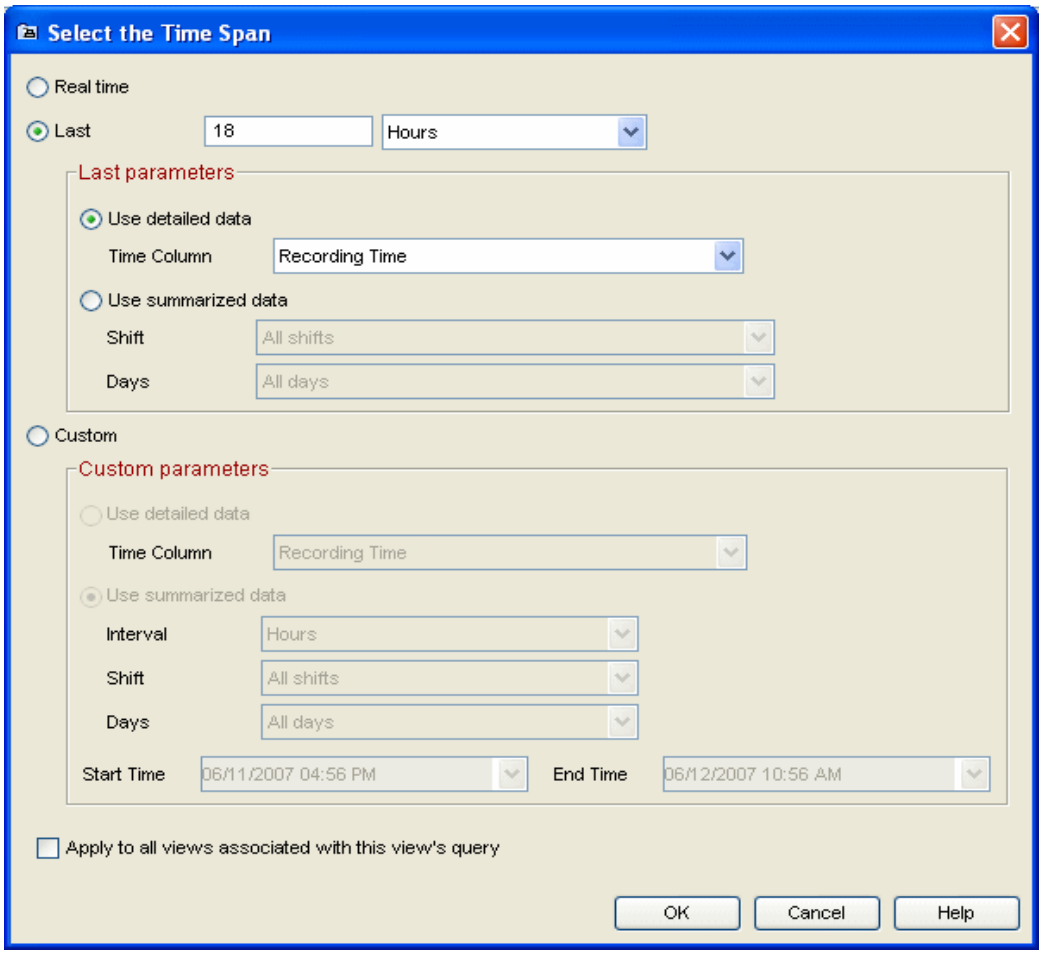


Figure 1-28 Time span for the past 18 hours

The data is now displayed in the navigator window as shown in the Figure 1-29. We can see that there are no fault messages in the past 18 hours.

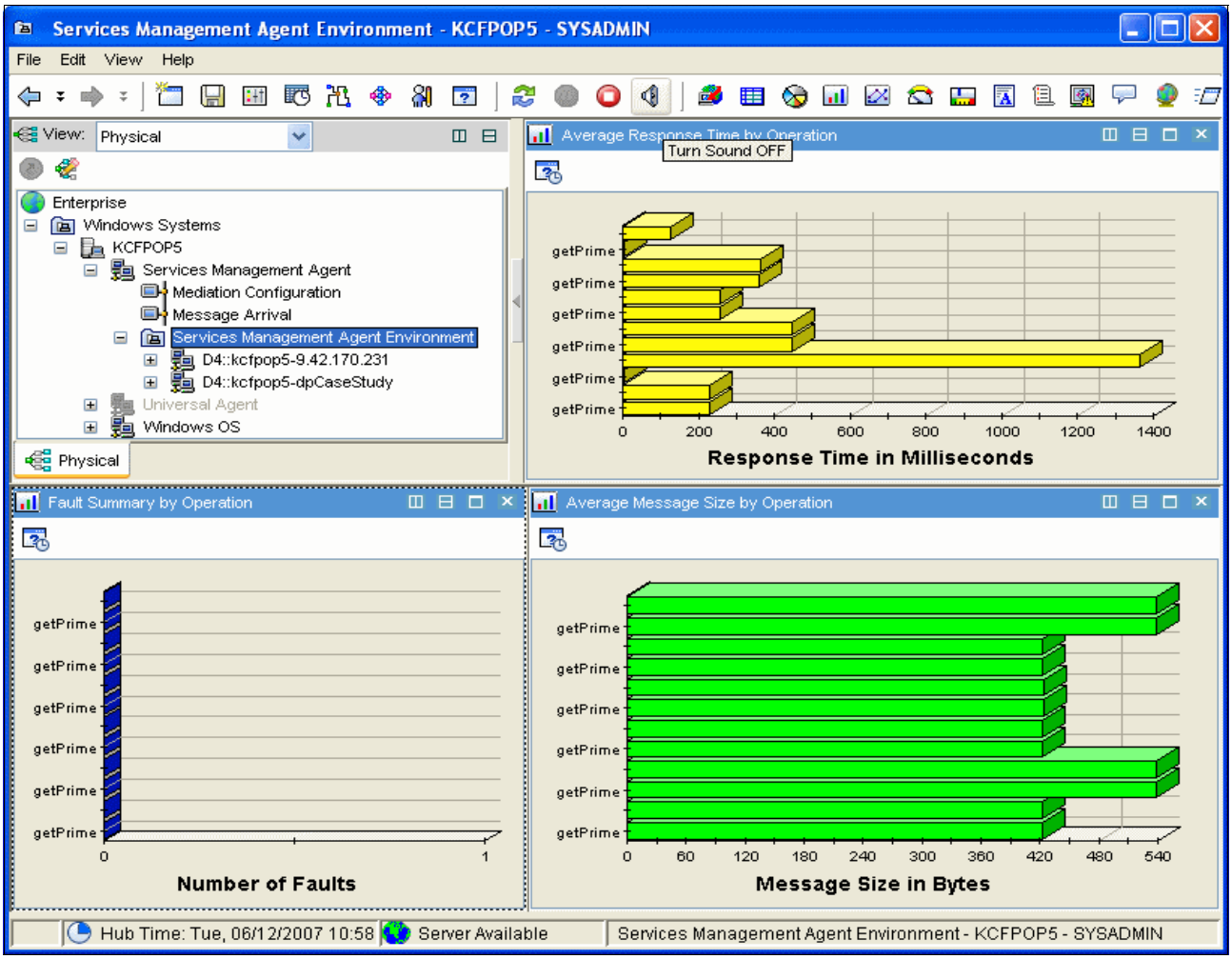


Figure 1-29 Navigator display for the past 18 hours

1.5 Summary

ITCAM for SOA delivers a comprehensive solution for the managing and the deployment of services in an SOA. ITCAM for SOA discovers, monitors, diagnoses, and controls Web services for a supported environment, in our case the DataPower appliance. It meets your daily tactical needs as well as your long-term strategic systems management goals for a wide range of environments from small and medium to very large enterprises.

2

IBM Tivoli Composite Application Manager System Edition for WebSphere DataPower

In this chapter, we explain how to install and configure IBM Tivoli Composite Application Manager System Edition (ITCAM SE) for WebSphere DataPower V6.1.0. This application provides robust multibox management capabilities for DataPower appliances by enabling appliance administrators to efficiently roll out, update, and manage configurations on multiple DataPower appliances.

ITCAM SE for WebSphere DataPower provides a set of capabilities for managing groups of DataPower devices including:

- Centralized backup and restore of DataPower devices and domains to specified versions
- A centralized repository for firmware and the distribution of firmware across multiple devices
- The definition of device clusters that are intended to share similar configuration
- Automatic synchronization of firmware, sharable device settings, and service domain definitions
- The discovery and propagation of changes within a cluster
- Management of version control of firmware, sharable device settings, and service domain definitions with roll back capability
- The tracking of device synchronization and operation state

In this chapter, we discuss the following topics:

- 2.1, “Installation overview” on page 46
- 2.2, “Managing DataPower with ITCAM SE” on page 54

© Copyright IBM Corp. 2008. All rights reserved.

2.1 Installation overview

The installation overview chapter is organized into the following sections:

- Planning for installation
- Supported platforms
- Hardware requirements
- Software requirements
- Required firmware version
- Firewall considerations
- Obtaining the installation images
- Installing ITCAM SE for WebSphere DataPower
- Verifying the installation and starting ITCAM SE
- Enabling the XML Management Interface on the DataPower appliance

2.1.1 Planning for installation

This release of ITCAM SE for WebSphere DataPower is supported on a limited number of operating systems. Before you begin the installation, verify that your system is running on a supported platform and that you meet all hardware and software requirements.

You might also want to review the *Knowledge Collection: Installing ITCAM System Edition for WebSphere DataPower* on the Web at the following address:

http://www.ibm.com/support/docview.wss?rs=2362&uid=swg27011746

2.1.2 Supported platforms

The following operating systems are supported for ITCAM System Edition for WebSphere DataPower:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows Server® 2003 Standard
- Microsoft Windows Server 2003 Enterprise
- Red Hat Enterprise Linux 4.0 for IA32
- SUSE Linux Enterprise Server 9.0 for IA32

Note: This is an inclusive list. For example, ITCAM SE for WebSphere DataPower *is not supported on* and *will not operate on* Microsoft Windows XP.

2.1.3 Hardware requirements

The ITCAM SE for WebSphere DataPower infrastructure components have the following processor, disk, and memory requirements:

- Processor requirements: For best performance, processor speeds should be at least 2 GHz for Intel® architectures.
- Disk requirements: The ITCAM SE for WebSphere DataPower installation process requires at least 1 GB of disk.
- Memory requirements: One GB of RAM is required.

2.1.4 Software requirements

All required software, other than the operating system, is provided on the installation image. The IBM DB2 Universal Database and IBM Tivoli Monitoring software are included on the installation image. You can choose not to install the DB2 and Tivoli Monitoring software from the installation image. If you choose not to install the version of DB2 software that is included on the installation image, you must already have DB2 Version 8.1 fix pack 10, Version 8.2 fix pack 3, or Version 9.1. If you do not to install the version of Tivoli Monitoring included on the installation image, you must already have Tivoli Monitoring, Version 6.1.0 Fix Pack 004.

2.1.5 Required firmware version

The managed IBM WebSphere DataPower devices must have firmware version 3.6.0.4 or later installed.

2.1.6 Firewall considerations

If a firewall exists between the ITCAM SE management stations and the DataPower devices, the Appliance Management Protocol (AMP) event port must be open through the firewall such that the DataPower appliances can communicate with the ITCAM SE management station. The default AMP event port is 5555 over TCP. Similarly, the XML Management Interface port must be open through the firewall, so that the ITCAM SE management station can communicate with the DataPower appliances. The default XML Management Interface port is 5550 over TCP.

2.1.7 Obtaining the installation images

ITCAM SE for WebSphere DataPower installation images are available with the firmware upgrades on the WebSphere DataPower download Web pages. Refer to the Technote *Download wizard to WebSphere DataPower firmware, product documentation, and Release Notes*, which explains how to obtain the files to down load. You can find the Technote on the Web at the following address:

http://www.ibm.com/support/docview.wss?rs=2362&uid=swg21252389

For the installation examples in this book, we use the following download images:

- For a supported Microsoft Window's 2000 and 2003 Server operating systems, download the following files:
  - ITCAM System Edition for DataPower Windows disk 1 (LCD7-1376-01.zip)
  - ITCAM System Edition for DataPower Windows disk 2 (LCD7-1377-02.zip)
  - ITCAM System Edition for WebSphere DataPower Install and Users Guide (ITCAM_Install_UsersGuide.pdf)
- For a supported Linux operating systems, download the following files:
  - ITCAM System Edition for DataPower Linux disk 1 (LCD7-1378-01.tar)
  - ITCAM System Edition for DataPower Linux disk 2 (LCD7-1379-01.tar)
  - TCAM System Edition for WebSphere DataPower Install and Users Guide (ITCAM_Install_UsersGuide.pdf)

Notes:

- The size of the files does not match the size of 500 MB as described on the Web page.
- The file names for the .zip and .tar files may change from those listed at the time of publishing.
- Updates for ITCAM SE for DataPower might also be available on the Web page. For example, ITCAM SE 6.1.0 IF001 for Linux is an update to the Linux installation. Follow the instructions included in the .tar or .zip file to install the update.

2.1.8 Installing ITCAM SE for WebSphere DataPower

There are three parts to the installation process for ITCAM SE for WebSphere DataPower:

- IBM Tivoli Monitoring
- IBM WebSphere DataPower agent for IBM Tivoli Monitoring
- DB2 software

You are prompted through these three parts of the installation process. The installation processes are different for Linux and Windows environments. For the latest installation instructions, consult the Technote *Using the installation images you can download for ITCAM System Edition for WebSphere DataPower* on the Web at the following address:

http://www-1.ibm.com/support/docview.wss?uid=swg21259599

During the installation of the products, you are prompted to define passwords. Refer to the Tivoli OMEGAMON® XE Information Center about passwords at the following Web address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.omegamon_mancon.doc/hlpdg36.htm

In the following instructions, we assume that ITCAM and DB2 are *not* already installed. Additional installation instructions are in the *ITCAM System Edition for WebSphere DataPower Install and Users Guide* (ITCAM_Install_UsersGuide.pdf), which is available with the installation images. Refer to the Technote *Download wizard to WebSphere DataPower firmware, product documentation, and Release Notes*, which describes how to obtain the book to download. You can find the Technote on the Web at the following address:

http://www.ibm.com/support/docview.wss?rs=2362&uid=swg21252389

For the latest information about installing the download images of ITCAM SE for WebSphere DataPower on Linux and Windows operating systems, consult the Technote *Using the installation images you can download for ITCAM System Edition for WebSphere DataPower* at the following Web address:

http://www.ibm.com/support/docview.wss?rs=2362&uid=swg21259599

Installing on Linux operating systems

Your Linux system should have the following packages installed:

- For RedHat:
  - xorg-x11-deprecated-libs
  - xorg-x11-libs
  - freetype

- For SUSE:
  - XFree86-libs
  - Freetype2

Run the installation process as the root user. The root user profile must be sourced. If you use the **su** command to switch to root, use the **su -** command to source the root profile.

To install the ITCAM SE for WebSphere DataPower on the supported Linux operating systems:

1. Confirm that you have downloaded the following files that we are using in our example:
   - ITCAM System Edition for DataPower Linux disk 1 (LCD7-1378-01.tar)
   - ITCAM System Edition for DataPower Linux disk 2 (LCD7-1379-01.tar)
2. Copy the two Linux installation .tar files, LCD7-1378-01.tar and LCD7-1379-01.tar, to a temporary directory, for example to the /tmp directory.
3. Create two installation directories for the tar files, for example:

   ```
   mkdir /tmp/itcamsedp
   mkdir /tmp/itcamsedp/disk1
   mkdir /tmp/itcamsedp/disk2
   ```

   Two directories for tar files: The unpacked tar files must be in two directories as described for the installation to complete successfully.

4. Unpack the tar files to the installation directories, for example:

   ```
   cd /tmp/itcamsedp/disk1
   tar -xvf /tmp/LCD7-1378-01.tar
   cd /tmp/itcamsedp/disk2
   tar -xvf /tmp/LCD7-1379-01.tar
   ```

5. From a command shell, run the following command to install the product. You must be in a graphical console.

   ```
   /tmp/itcamsedp/disk1/setupLinux.bin
   ```

   Text-only Linux console: Running the **setupLinux.bin** command with the `-console` option is not supported. A graphical console is required for both installing and running Tivoli Monitoring.

6. On the Welcome page, click **Next**.
7. On the Software License Agreement page for Tivoli Monitoring and ITCAM System Edition for WebSphere DataPower, read the terms in the license agreement. You must accept the terms of the license agreement to continue the installation. If you agree with the terms, select the **I accept the terms of the license agreement** radio button and click **Next**.
8. On the page that begins the Tivoli Monitoring part of the installation, verify the directory where IBM Tivoli Monitoring will be installed. Click **Next**.
9. On the page that begins the DB2 software part of the installation, a message is displayed that indicates whether the installation process found an installation of the DB2 software. As expected, DB2 is not found in this example, and you see the message "`DB2 Express V8.2 will be installed`." Click **Next**.

10. On the Software License Agreement page that is displayed for the DB2 software, read the terms of the license agreement. You must accept the terms of the license agreement to continue the installation. If you agree with the terms, select the **I accept the terms of the license agreement** radio button and click **Next**.
11. Verify the user name, and then enter and verify the password for DB2 software. You must type the password twice to verify that it is correct. Keep track of this ID and password because you might need them later. Click **Next**.

    The message "`Please wait while installing DB2`" is displayed. This installation step may take approximately five minutes.
12. When the DB2 installation completes, you are prompted for the location of disk 2. Change the directory name from disk1 to disk2 and click **Next**. This installation step may take approximately 10 to 15 minutes.
13. After the installation completes successfully, a page indicating a successful installation is displayed. Click **Finish** to close the installation program.

If the DB2 installation fails, you are directed to a log file that contains information that you can use to troubleshoot the problem. For Linux, look at the /opt/IBM/db2/V8.1/db2_install.log. You cannot change DB2 installation directory on Linux.

After the installation is complete, you must perform a configuration task to ensure that the WebGUI works correctly on Linux operating systems. To perform this configuration task, complete the following steps:

1. Run the following command:

   ```
   ./itmcmd manage
   ```
2. In the Manage Tivoli Enterprise Monitoring Services window, the default location of IBM Tivoli Monitoring is /opt/IBM/ITM/bin/. Click **Action** → **Configure**.
3. In the Enterprise Portal Parameters window, type the path to the browser:

   ```
   /usr/firefox/firefox
   ```
4. Click **Save**.

For more information about installing agents for Tivoli Monitoring, see the following topics in the *IBM Tivoli Monitoring Installation and Setup Guide* on the Tivoli Monitoring Information Center:

- *Installing monitoring agents*

  http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc/itm_install100.htm
- *Installing support for agents on the monitoring server, portal server, and desktop client*

  http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc/itm_install106.htm#agent_support

Installing on Windows operating systems

The installation of ITCAM SE for WebSphere DataPower requires the user to log on to the Windows operating system with full administrator authority. Otherwise, the installation will fail. The installation creates user IDs on the Windows operating system, and therefore, needs to install with full administrator authority.

To install the ITCAM SE for WebSphere DataPower on the supported Microsoft Windows operating systems:

1. Confirm that you have downloaded the two Windows installation compressed files that we are using in our example to a temporary directory, such as C:\temp:
   - LCD7-1376-01.zip
   - LCD7-1377-01.zip
2. Open a command prompt window and create two installation directories for the compressed files, for example:

   ```
   mkdir C:\temp\itcamsedp\disk1
   mkdir C:\temp\itcamsedp\disk2
   ```
3. Extract the compressed files to the separate installation directories, for example:
   - Use an extraction utility to extract the C:\temp\LCD7-1376-01.zip file to C:\temp\itcamsedp\disk1.
   - Use an extraction utility to extract the C:\temp\LCD7-1377-01.zip file to C:\temp\itcamsedp\disk2.

   Note: The installation will not complete as expected if the files are not properly extracted to the directories as described.

4. From a command prompt window, navigate to the directory that contains the installation image for disk 1, for example C:\temp\itcamsedp\disk1 (LCD7-1376-01.zip), and use the **`setupwin32.exe`** command to run the installation process.
5. On the welcome page that opens, click **Next**.
6. On the Software License Agreement page that is displayed for Tivoli Monitoring and ITCAM SE for WebSphere DataPower, read the terms of the license agreement. If you agree with the terms, select the **I accept the terms of the license agreement** radio button and click **Next**. You must accept the terms of the license agreement to continue the installation.
7. On the page that begins the IBM Tivoli Monitoring part of the installation, verify the installation directory location of Tivoli Monitoring and ITCAM SE for WebSphere DataPower. Click **Next**.
8. Type the password for the Tivoli Enterprise Portal Server. Type the password again to verify that it is correct. Keep track of this ID and password because you might need them later. Click **Next**.
9. On the page that begins the DB2 software part of the installation, you see a message that explains whether the installation process found an installation of the DB2 software. Assuming that an installation is not found, click **Next**.
10. On the Software License Agreement page for the DB2 software, read the terms in the license agreement. You must accept the terms of the license agreement to continue the installation. If you agree with the terms, select the **I accept the terms of the license agreement** radio button and click **Next**.
11. On the page that prompts you to specify the target directory where DB2 software is to be installed, accept the default location that is displayed in the Directory Name field, type over it to specify the location, or click **Browse** to navigate to the location. Click **Next**.
12. Verify the user name and type the password for DB2 software. You must type the password twice to verify that is correct. Keep track of this ID and password because you might need them later. Click **Next**.

13. The installation prompts you for the directory of disk 2. Change the directory and click **Next**.
14. If there is a problem during the DB2 installation, the installation program gives you the full path to the DB2 logs. You can also find the logs in *<DB2_Destination>*\db2_install.log, for example c:\Program Files\IBM\SQLLIB\db2_install.log.
15. After the installation completes successfully, a page opens that prompts you to restart the system. Before you start ITCAM SE for WebSphere DataPower, you must restart the system. Choose whether to restart now or later. Click **Finish** to close the installation program.

If the installation fails, you are directed to a log file, such as \IBM\ITM\Install, that contains information that you can use to troubleshoot the problem.

For more information about installing agents for Tivoli Monitoring, see the following topics in the *IBM Tivoli Monitoring Installation and Setup Guide* in the Tivoli Monitoring information center:

- *Installing monitoring agents*

  http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc/itm_install100.htm

- *Installing support for agents on the monitoring server, portal server, and desktop client*

  http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc/itm_install106.htm#agent_support

2.1.9 Verifying the installation and starting ITCAM SE

To verify that the installation is successful, you can start ITCAM SE for WebSphere DataPower and view the Navigation tree in the Tivoli Enterprise Portal.

For Linux

To start ITCAM SE for WebSphere DataPower from a Linux operating system:

1. To start the Tivoli Enterprise Portal desktop client, run the following command from a graphical console:

   ```
   ./itmcmd agent start cj
   ```

   The default location of IBM Tivoli Monitoring is /opt/IBM/ITM/bin/.

2. Type the logon ID and password for Tivoli Enterprise Portal. For the Tivoli Enterprise Portal, the default user name is `sysadmin`. On systems with the Linux operating system, by default the sysadmin ID does not require a password. On systems with the Windows operating system, you specified the password during the installation.

   Click **OK**.

3. Go to the Physical Navigator view (upper left portlet on the user interface). This view shows the hierarchy of your monitored enterprise, from the top level (Enterprise) to individual groups of information collected by ITCAM SE for WebSphere DataPower (or other Tivoli Enterprise Monitoring Agents). When you click an item in the Navigator, its default workspace is displayed in the application window.
4. Expand the tree in the Physical Navigator view until you see DataPower Management Agent. Click the **DataPower Management Agent** entry in the tree.

   In the application window, the DataPower tree lists the devices, managed sets, and firmware. If you see the DataPower tree, you have successfully started ITCAM SE for WebSphere DataPower.

For Windows

To start ITCAM SE for WebSphere DataPower from the Windows Start menu:

1. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Service**.
2. Right-click the **Tivoli Enterprise Portal - Desktop** and then click **Start**.
3. Type the logon ID and password for Tivoli Enterprise Portal and click **OK**.
4. Go to the Physical Navigator view (upper left portlet on the user interface). This view shows the hierarchy of your monitored enterprise, from the top level (Enterprise) to individual groups of information collected by ITCAM SE for WebSphere DataPower (or other Tivoli Enterprise Monitoring Agents).

   When you click an item in the Navigator, its default workspace is displayed in the application window. If you are in browser mode, you can save this URL to the Favorites list of your browser. The links to the other information resources (for example, the Tivoli Enterprise Portal tour) can be helpful if you want more information about Tivoli Monitoring software.
5. Expand the tree in the Physical Navigator view until you see DataPower Management Agent. Click the **DataPower Management Agent** entry in the tree.

   In the application window, the DataPower tree lists the devices, managed sets, and firmware. If you see the DataPower tree, you have successfully started ITCAM SE for WebSphere DataPower.

2.1.10 Enabling the XML Management Interface on the DataPower appliance

To enable ITCAM SE for WebSphere DataPower to manage an appliance, you must enable the AMP setting in the XML interface and the XML interface itself:

1. Log on to the WebGUI of the DataPower appliance.
2. From the left navigation bar, click **Network** → **Management** → **XML Management Interface**.
3. On the XML Management Interface page (Figure 2-1 on page 54), for Admin State, click the **enabled** radio button, select the **AMP EndPoint** box, and click **Apply**.
4. Click the **Save Configuration** button at the top of the page.

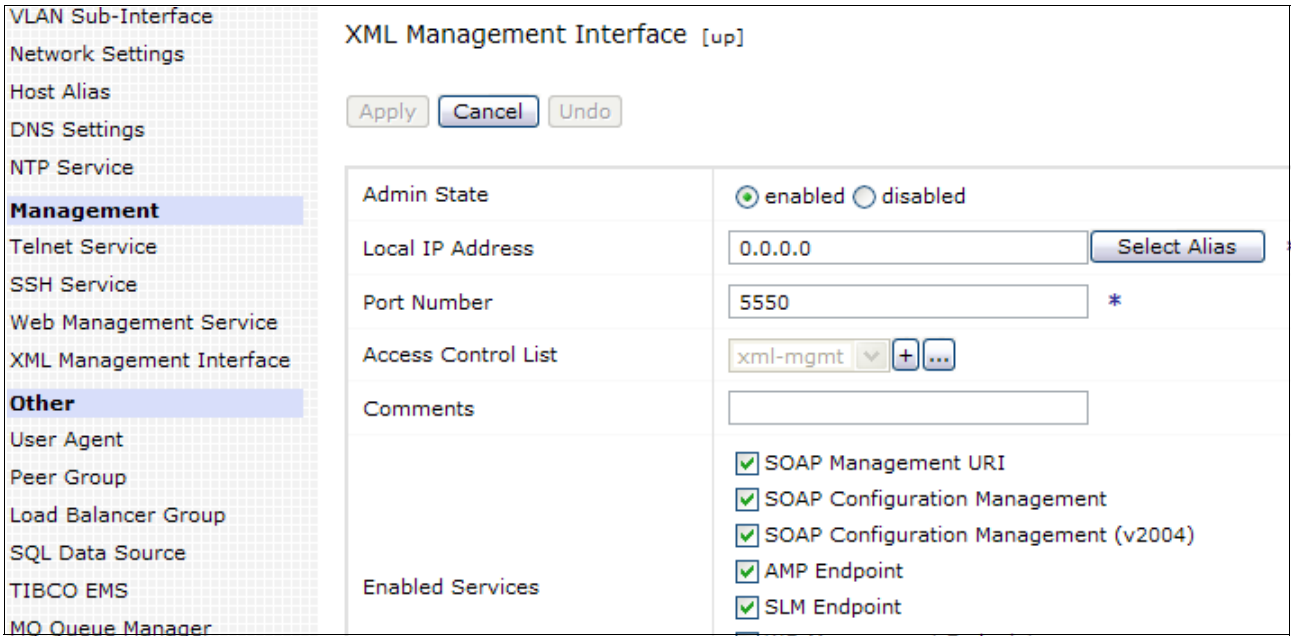


Figure 2-1 Enabling ITCAM SE for WebSphere DataPower to manage an appliance

2.2 Managing DataPower with ITCAM SE

The managing DataPower example with ITCAM SE shown in this section is organized into the following sections:

- Example overview
- Downloading the firmware
- Creating a managed set
- Creating a device
- Adding a master device to a managed set
- Adding domains to a managed set
- Adding a slave device to the managed set (ITSO_managedSet)

2.2.1 Example overview

In this section, we show how you can manage DataPower appliances with ITCAM SE. The example describes the steps to keep the firmware and application domains of two DataPower appliances in synch.

With ITCAM SE, you can define a set of DataPower appliances in a managed set. A *managed set* is a collected group of appliances that keep their firmware and application domains consistent across all the appliances in the managed set. A device cannot belong to more than one managed set.

In this example, we demonstrate how to use ITCAM SE for managing DataPower. We synchronize the firmware and selected application domains across this managed set for two devices (dp1 and dp2).

To duplicate this scenario, you must have two DataPower devices and a user ID that has administrative privileges. You also need to import the configuration file for dp1. This configuration file contains all of the domains that have been used throughout this document.

The entire ITCAM SE configuration is done via the Tivoli Portal Enterprise Client Desktop version. We refer to the DataPower Managed Agent configuration view as the *application window* (Figure 2-2).

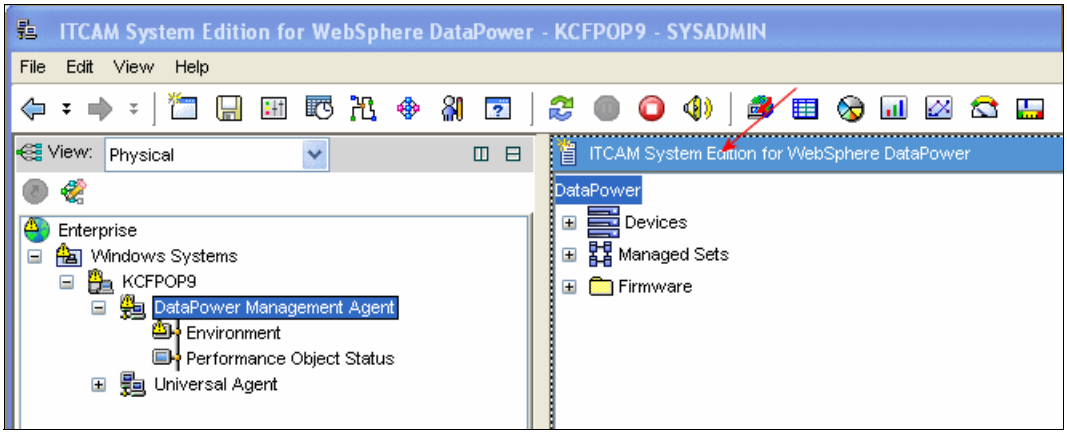


Figure 2-2 DataPower application window

Important note about devices and firmware: Any *devices* that must be in the *same* managed set must also be the same model and hardware type, as well as have the same *licensed features*. If they do not have the same features, they cannot reside on the same managed set.

The *firmware* should also have the same licensed features as the devices in the managed set.

2.2.2 Downloading the firmware

Firmware upgrades for the WebSphere DataPower appliances are available on ibm.com. For information about how to obtain the files and download them, refer to Technote *Download wizard to WebSphere DataPower firmware, product documentation, and Release Notes* on the Web at the following address:

http://www.ibm.com/support/docview.wss?rs=2362&uid=swg21252389

2.2.3 Managing the firmware

One benefit of using ITCAM SE for DataPower is the synchronization of the firmware levels across managed devices. In our example, we want to synchronize dp1 and dp3. Currently they have different firmware levels with the same licensed features.

To synchronize the firmware levels:

1. In the application window (Figure 2-2), Devices, Manage Sets, and Firmware are listed in the tree. In our example, no firmware versions are known to ITCAMSE. Therefore, we must upload the firmware images. To upload new firmware images, right-click **Firmware** and select **Add Firmware Image**.

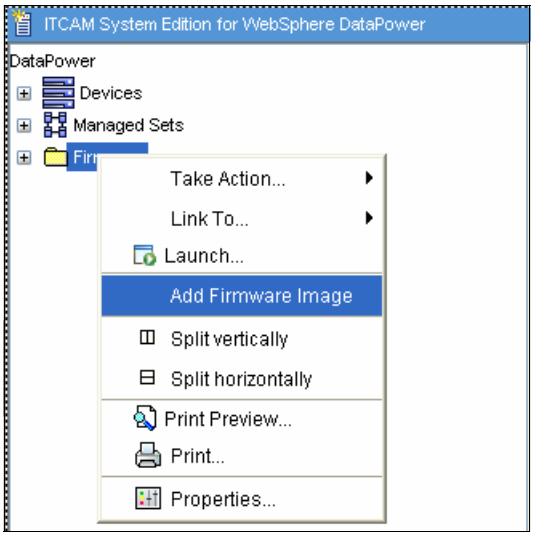


Figure 2-3 Selecting the Add Firmware Image option

2. Browse to the directory where the firmware image has been downloaded (Figure 2-4). In the User comment field, enter a description that explains why you want to deploy this firmware. Click **OK**.

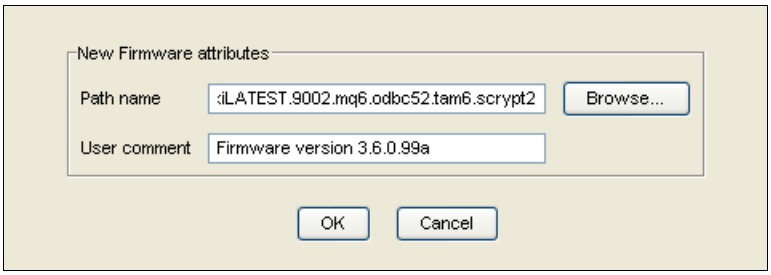


Figure 2-4 Adding the firmware image

3. From the application window, expand **Firmware**. The firmware image is now in the repository as shown in Figure 2-5.

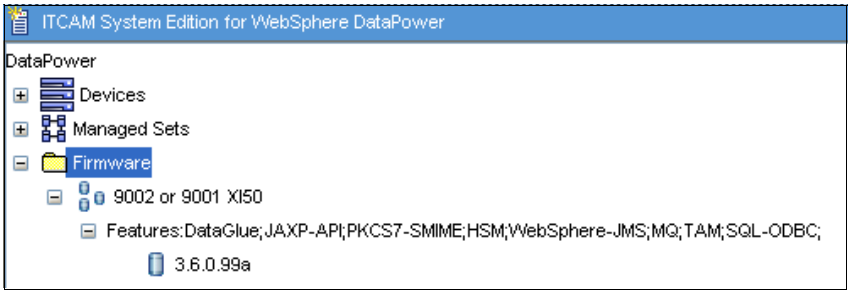


Figure 2-5 Firmware image now in the repository

If any errors occur, refer to the logs in C:*Installdirectory*\ITM\TMAITM6\KBC\logs.

You can also see list of actions in the DataPower Action Status view, as shown in Figure 2-6.

DataPower Action Status

Correlator	Submission Time	Description	Current Message
1181836953469.637	Fri Jun 15 11:46:3...	Create managed set: tests .	KBC9200I The action completed successfully.
1181836953469.640	Fri Jun 15 11:49:3...	Delete managed set: test .	KBC9200I The action completed successfully.
1181836953469.649	Fri Jun 15 12:11:0...	Delete managed set: tests .	KBC9200I The action completed successfully.
1181836953469.659	Fri Jun 15 12:29:2...	Manage domain: AAA in managed set: ITSO_managedSet .	KBC9200I The action completed successfully.
1181836953469.656	Fri Jun 15 12:22:4...	Stop management of domain: AAA in managed set: ITSO_...	KBC9200I The action completed successfully.

Figure 2-6 DataPower Action Status View

You must deploy the firmware image to a managed set in order to synchronize the DataPower devices. We perform this task in 2.2.6, “Adding a master device to a managed set” on page 61, but first we must create the managed set as explained in the following section.

2.2.4 Creating a managed set

To create a managed set:

1. In the application window, right-click **Managed Sets** and select **Create Managed Set** as shown in Figure 2-7.

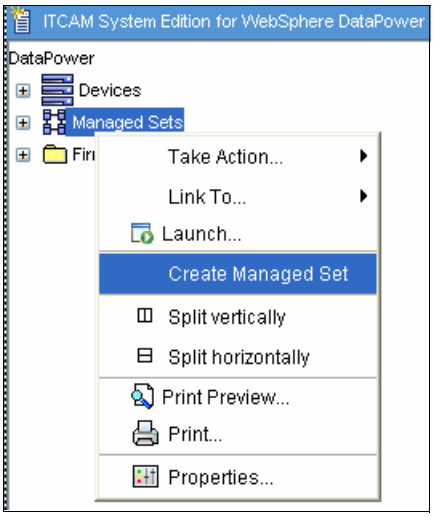


Figure 2-7 Selecting Create Managed Set

2. In the New Managed Set window (Figure 2-8), in the New managed set name field, type a name, for example `ITSO_managedSet`. Click **OK**.

Figure 2-8 Naming the the managed set

3. A message window opens that shows the message "`KBC9200I Action Completed Successfully`." Click **OK**.
4. To display the created managed set, expand **Managed Sets** → **ITSO_managedSet**.

Synchronizing the firmware

To synchronize our firmware across the managed set, deploy the firmware image that we uploaded in the previous section to this managed set:

1. In the application window, expand **Firmware** → **9002 (or 9001) XD** → **3.6.0.99a** → **Features**. Right-click and select **Deploy Image** (Figure 2-9).

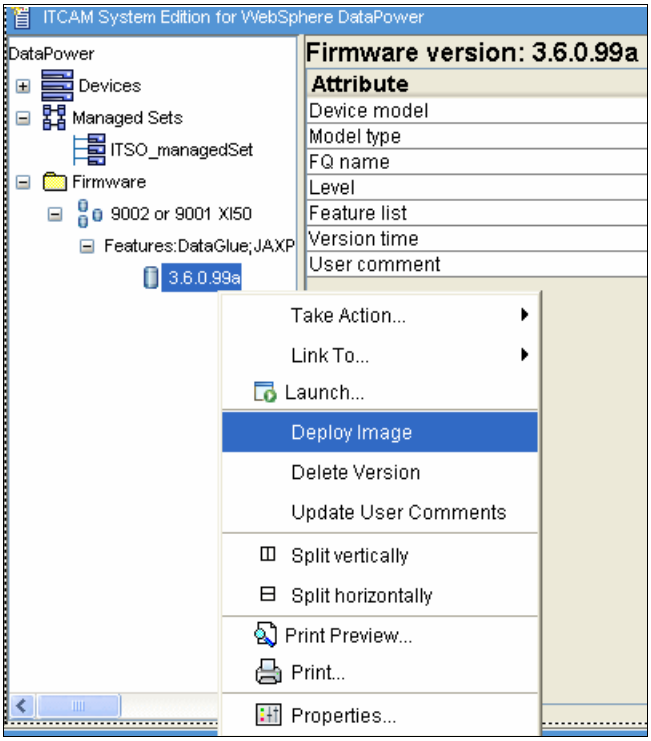


Figure 2-9 Deploy Firmware version to Managed Set

2. In the Deploy 3.6.0.99a to Device window (Figure 2-10), select the managed set that you plan to deploy the image. In this example, there is only one managed set (ITSO_managedSet), and it is selected by default. Click **OK**.

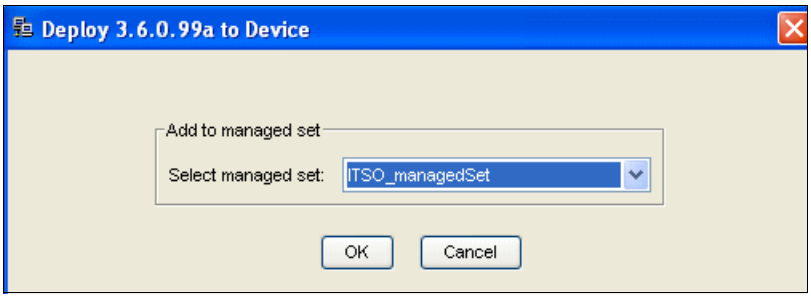


Figure 2-10 Deploy firmware image to managed set

3. In the window that shows the message "`A KBC9200I Action Completed Successfully`," click **OK**.

4. In the application window, select **Managed Sets** → **ITSO_managedSet** and verify that Deployed firmware is set to 3.6.0.9aa as shown in Figure 2-11.

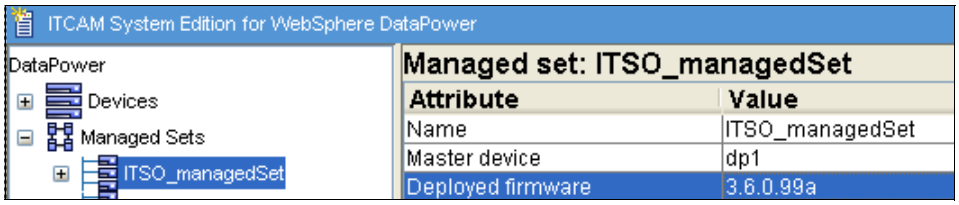


Figure 2-11 Firmware image now deployed to the managed set

2.2.5 Creating a device

A DataPower device must be created in ITCAM SE before any managing can be performed. In this section, we assume that this is the first time that you are using this application. To create the device:

1. In the application window (Figure 2-12), right-click **Device** and select **Create Device**.

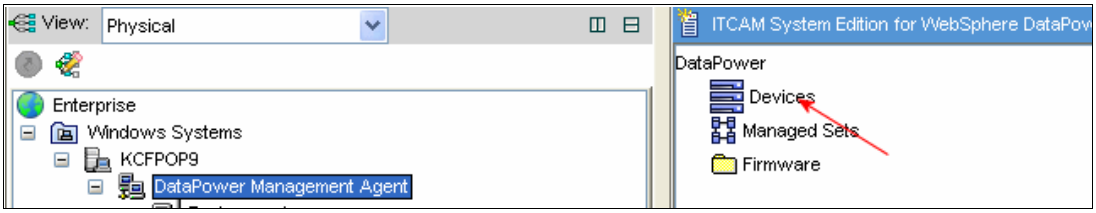


Figure 2-12 Creating a device

2. In the New Device window (Figure 2-13 on page 60), complete the properties for dp1:
   a. For Device name, type `dp1`. The name must be unique. It is only a symbolic name for your purposes.
   b. For Hostname or IP address of the DataPower device, type `itso`.
   c. For User ID, enter a user ID that is associated with this device. The user ID must have administrative privileges for the device. In this example, we use the `admin`.
   d. For Management port, enter the management port for the device. The management port is used by the XML Management Interface. The default port is `5550`. To verify the port:
      i. Log in to the DataPower WebGUI. Open a Web browser and type the address for the DataPower device, for example:

         `https://itso:9090`

         Enter your user ID, password, select the **Default** domain, and click **Logon**.
      ii. On the Control Panel page, from the left navigation bar, expand **NETWORK** and click **XML Management Interface**.
      iii. Verify that the port number is 5550.
   e. Click **OK**.

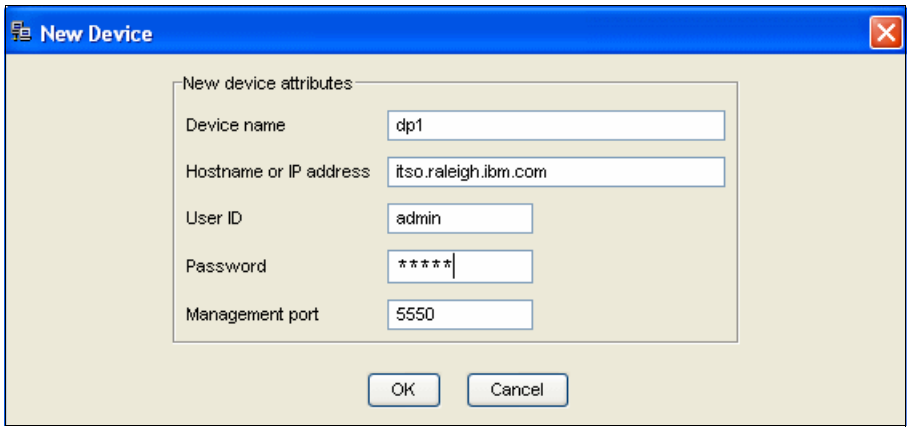


Figure 2-13 New Device window

3. In the window that shows the message "`A KBC9200I Action Completed Successfully`," click **OK**.
4. In the application window (Figure 2-14), expand **Devices**. You see the new dp1 is displayed along with the list of all the domains for this device.

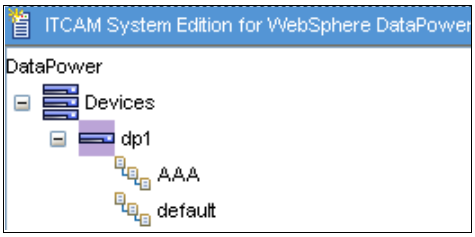


Figure 2-14 Domains for the DataPower device

5. Repeat steps 1 on page 59 through 4 for your second device and call it `dp2`.
6. To see both newly created devices from the application window, expand **Devices** (Figure 2-15).

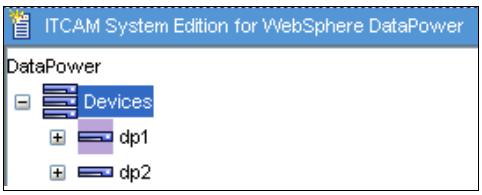


Figure 2-15 DataPower devices

7. As shown in Figure 2-16, expand **dp2** to see that it includes the default domain.

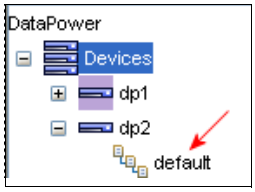


Figure 2-16 dp2 domains

2.2.6 Adding a master device to a managed set

To add the created device (dp1) to the managed set (ITSO_managedSet):

1. In the application window, expand **Devices**. Right-click **dp1** and click **Add to Managed Set** as shown in Figure 2-17.

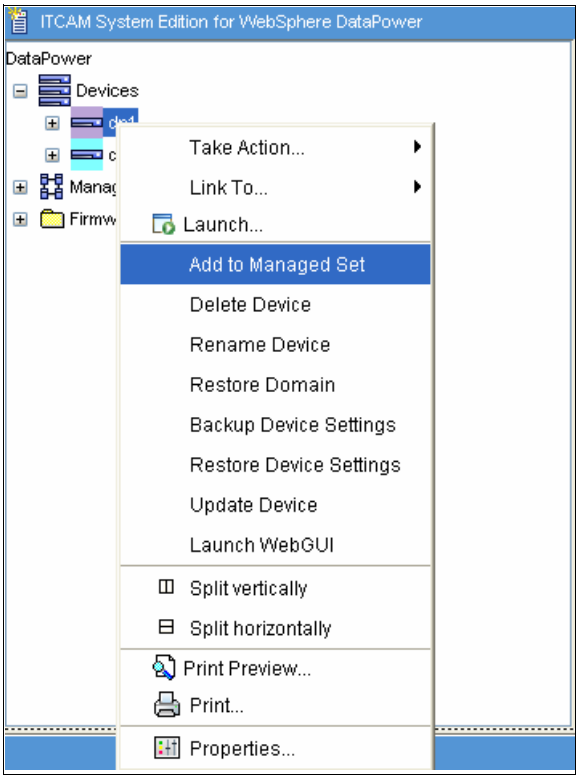


Figure 2-17 Selecting the option Add to Managed Set

2. In the Add dp1 to managed set window (Figure 2-18), we only created one managed set, **ITSO_managedSet**, which should be the only one in the Select managed set drop-down list. We want dp1 to be our primary or our “master” device. Therefore, select the **Add as master** check box. Click **OK**.

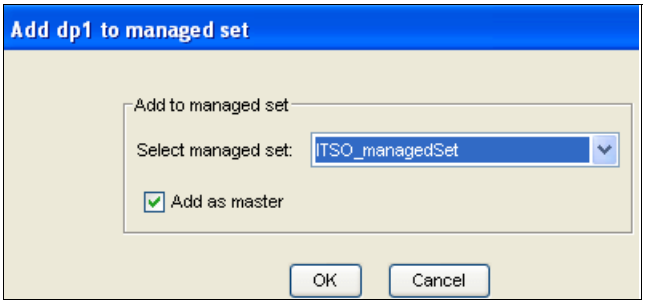


Figure 2-18 Adding dp1 to the managed set as the master device

Notes:

- Device dp1 is the master device that will have its firmware, settings and selected domains copied to the slave device or devices (dp2) in the managed set (ITSO_managedSet). We add the slave device in 2.2.8, “Adding a slave device to the managed set (ITSO_managedSet)” on page 64.
- Because we have already set the firmware for the managed set, when dp1 is added to the managed set, the existing firmware on dp1 is replaced with the managed set firmware that was set previously.

3. In the window that shows the message “`A KBC9200I Action Completed Successfully`,” click **OK**.
4. After the window refreshes, in the application window, expand **Managed Sets** → **ITSO_managedSet** to view the device *dp1* added to the managed set. It takes a few minutes for the firmware upgrade to be performed and the Settings Version to be captured. You can monitor the progress in the DataPower Actions Status view.
5. Each managed set has a master device, which has a purple background, as shown in Figure 2-19. Expand **dp1** to see the other entries in the tree. These entries are the domains that are associated with this master device.

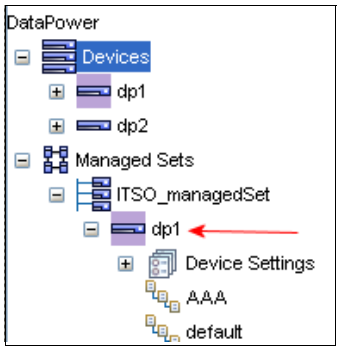


Figure 2-19 Device dp1 has been added to ITSO_managedSet

6. When a device is added to a managed set, its firmware and settings are automatically managed. Expand **ITSO_managedSet** → **dp1** → **Device Settings**.

   As shown in Figure 2-20, you see *ITSO_managedSet, Version1*. This is the first backup copy of the master device’s settings that were made when the master device was added to the managed set. When the master device’s settings change, they are automatically backed up and cloned to the slave devices in the managed set.

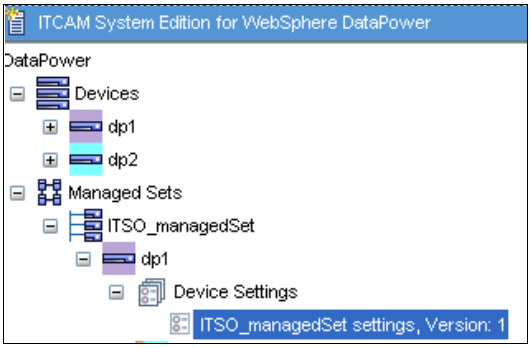


Figure 2-20 Original managed set settings

2.2.7 Adding domains to a managed set

Next, we must select the domain or domains in the master device dp1 that will be managed. Managing a domain replicates it and keeps it in sync across all the devices in the managed set. By default, no domains are managed. You must select the domains to be managed.

Sharable and non-sharable non-service configuration: A *sharable non-service configuration* (that is, the NTP configuration) from the default domain is already synchronized across the managed set, which is known as "Settings." Settings are automatically captured and synchronized when a device is added to a managed set.

A *non-sharable non-service configuration* (that is, the Ethernet Interface IP address) is never synchronized across the managed set. The service configuration (that is, the XML firewall) from the default domain is not synchronized across the managed set unless the default domain is selected to be managed. As a result, the sharable non-service configuration can be synchronized within the managed set without requiring the default domain to be managed.

To add the domain AAA to the ITSO_managedSet:

1. Expand **Managed Sets** → **ITSO_managedSet** → **dp1** if you have not already done so. ITSO_managedSet is the only managed set created in this example. dp1 is the only member of this managed set.

   Right-click **AAA** and select **Manage Domain**. The domain AAA must already exist on the master device (dp1) before you can select it to be managed. See Figure 2-21.

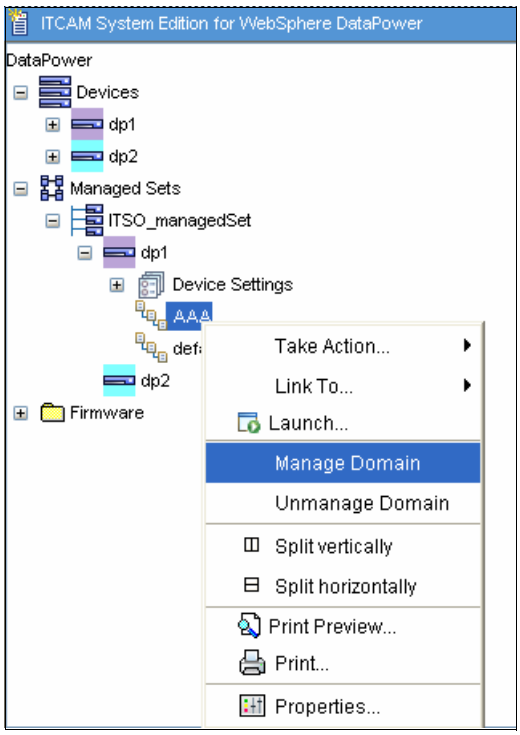


Figure 2-21 Managed domains

2. In the window that opens, a confirmation message is displayed. Click **OK** to confirm the management of the domain.

Any modifications to this domain are propagated from the master to the nonmaster devices in the ITSO_managedSet. As shown in Figure 2-22, the domains that are “managed” have a blue background. AAA, Version1 of this domain is created is created, in order to restore to the original changes.

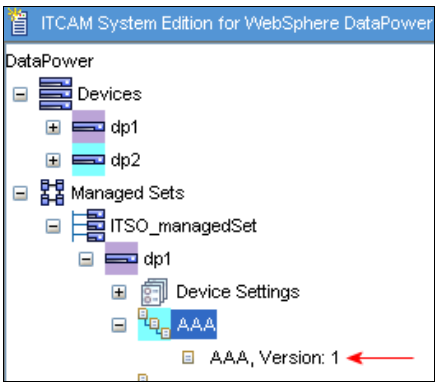


Figure 2-22 AAA, Version 1

Unmanage a domain: To “unmanage” a domain, select the domain and select **Unmanage Domain**.

2.2.8 Adding a slave device to the managed set (ITSO_managedSet)

Finally, we must register our second device dp2 with ITSO_managedSet. The new device is not kept in sync with dp1 until it is added to the managed set.

1. In the application window, expand **Devices**, right-click **dp2** and select **Add to Managed Set**.
2. We have only created one managed set in this demo. Therefore, it should be the only managed set in the list. We have already created dp1 as a master device. Therefore, leave the **Add as master** check box for deselected. Click **OK**.
3. Press F5 to refresh the window and see the new device dp2 as shown in Figure 2-23. It may take a few minutes for the synchronization to complete. You can monitor the progress in the DataPower Action Status view.

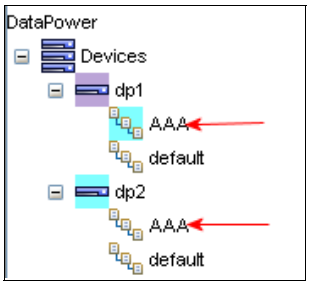


Figure 2-23 dp1 synced with dp2

Now a copy of the AAA domain is propagated to dp2. Any changes that are made to the AAA domain are automatically cloned and distributed throughout the managed set.

Firmware synchronization and domain backup: After dp2 is added to the managed set, it is automatically synchronized with the firmware version that is deployed to the managed set, along with the managed domain. The firmware is the first to be synchronized.

When a managed domain, AAA in our example, is modified on the master device, it is automatically backed up and cloned to the slave devices in the managed set. If the managed domain is modified on a slave device, it is automatically replaced by the current version of the domain taken from the managed set. A user can deploy the backup version to the domain and it will be distributed throughout the managed set. This version can be used for recovery or to restore the configuration of the device that was replaced.

2.3 Summary

In this chapter, we demonstrated how ITCAM SE for Websphere DataPower acts as a manager for one or many for DataPower devices. This functionality makes it easy to perform the following actions:

- Maintain a centralized backup and restore of DataPower device settings and domains.
- Maintain a centralized distribution of firmware to DataPower devices.
- Allow a set of DataPower devices, called a *managed set*, to keep their firmware, device settings, and selected domains in sync, so that they will always be the same across the managed devices.

3

Service level monitoring

IT services often require a certain level of quality in terms of response time, throughput, and availability. The IT infrastructure must provide a means to measure the current status and react appropriately if specified thresholds of indicators are reached, thus ensuring the quality of service expected by the customers. The evolving paradigm of service-oriented architecture (SOA) adds new challenges by its distributed character. Appliances, such as the DataPower appliance, allow for elegant ways of implementing service level monitoring (SLM) as all messages entering and leaving the network may be monitored.

In this chapter, we discuss the SLM abilities of the DataPower appliance. We begin with a general overview of the concepts and then describe the following two implementation examples:

- SLM policy configuration with a multiprotocol gateway
- SLM policy configuration with a Web service proxy

In this chapter, we discuss the following topics:

- “Overview of the SLM concepts in the DataPower device” on page 68
- “Types of monitors in the DataPower device” on page 68
- “SLM policy configuration example in a multiprotocol gateway” on page 72
- “SLM policy configuration example in a Web service proxy” on page 88

© Copyright IBM Corp. 2008. All rights reserved.

3.1 Overview of the SLM concepts in the DataPower device

SLM is used to monitor key indicators that help to identify problems in time and to perform adequate reactions. The goal is that customer expectations on service quality are met. By using the DataPower appliance, you can achieve this with the following steps:

1. Select (filter) the messages that match the defined criteria.
2. Apply a policy to the selected messages that contains a measurement interval, thresholds, and actions to be taken.
3. Execute the specified actions if defined thresholds are reached.

The SLM capabilities in the DataPower appliance offer the following benefits:

- Avoid abuse and overuse of services and secure services from Denial of Service (DoS) attacks.
- Enforce service level agreements (SLAs).
- Differentiate between users with different needs for service quality.
- Define actions to be taken if thresholds for indicators are reached, such as sending notifications if there is a bad response time or too many error messages from the back end.
- Optimize response times and share resources adequate between the parties that access the services.

When deciding on the use of a Web services management and monitoring product, consider IBM Tivoli Composite Application Manger for SOA (ITCAM for SOA), which is described in Chapter 1, “IBM Tivoli Composite Application Manager for SOA in the DataPower environment” on page 1. ITCAM for SOA covers the SLM topics in a broader scope. It takes the whole enterprise IT infrastructure into account. It provides the ability for doing end-to-end operations level monitoring and has a more sophisticated means for consolidating data, creating graphs, generating historical reports, and so on.

3.2 Types of monitors in the DataPower device

The DataPower device has the following types of monitors:

- Message monitors (count monitors, duration monitors)
- Web service monitors
- SLM policy action

The monitoring options differ between the DataPower services as shown in Table 3-1 on page 69. Message monitors and Web service monitors are applied directly to the DataPower service object. When creating DataPower services, message monitors and Web service monitors can be added on the Monitors tab (Figure 3-1 on page 70). SLM policies are configured as an action that is part of a DataPower service’s processing policy.

Note: In the DataPower WebGUI, you can see the full set of options that is available for a DataPower service only when you access the service that is using the objects menu in the left navigation bar of the DataPower interface.

Table 3-1 Monitoring options in the different DataPower services

Service type	Message monitors	Web service monitors	Service level monitors
XSL proxy	Yes	No	No
Web application firewall	Yes	No	No
XML firewall	Yes	Yes	No
Web service proxy	Yes	No	Yes
Multiprotocol gateway	Yes	Yes	Yes

3.2.1 Message monitors

Message monitors are a basic means of monitoring the messages that move through the appliance by defining thresholds and actions. There are two types of message monitors: message count and message duration.

Message count monitors

A message count monitor counts the messages per time interval and performs an action if the allowed number is exceeded, for example:

1. The message count monitor matches an incoming message based on the source IP address, requested URL, HTTP header field values, or HTTP method.
2. The message count monitor can differentiate requests, responses, errors, and allows to use a custom style sheet.
3. The message count monitor increments a counter and compares it to the specified message number allowed per time interval. It is also possible to configure a message burst limit, which is useful if there is a high variance of message rate.
4. The message count monitor performs an action to notify, shape, or reject a message when the specified number of messages in the specified time interval is exceeded. A log at the specified log priority is written.

Message duration monitors

A message duration monitor (Figure 3-1) measures the time that a message needs for processing. It measures the time interval between the receipt of a client's request and the transmission of the response back to the client, including the time needed for processing in back-end systems.

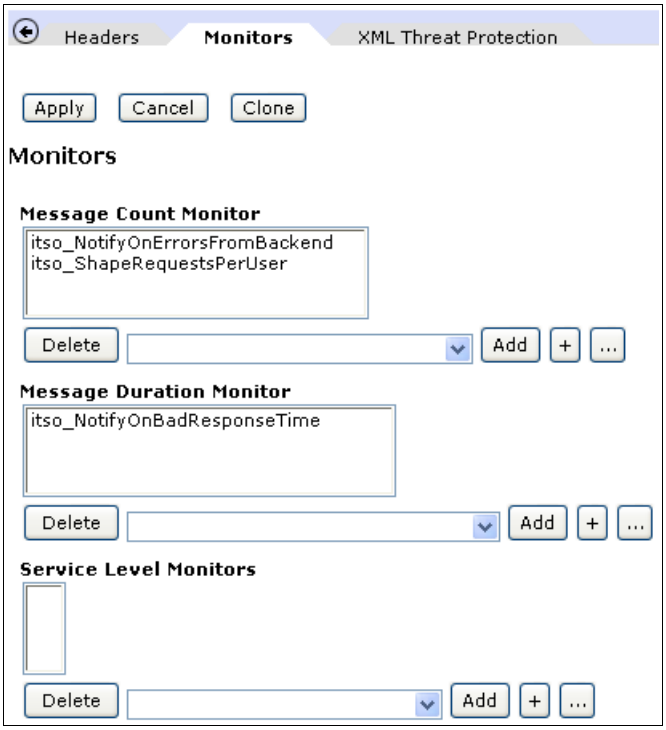


Figure 3-1 Message monitors

DoS threat protection configuration

DataPower services allow for threat protection configurations. If a service, such as XML firewall, is configured via the WebGUI, you can find these configurations on the XML Threat Protection tab. You can also find the Multiple Message XML DoS Protection configuration (Figure 3-2) on this tab.

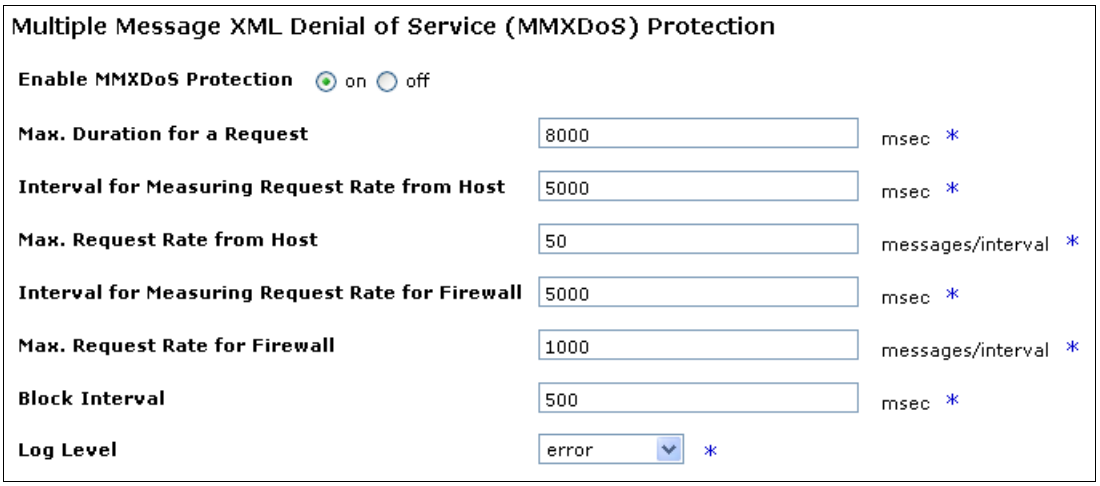


Figure 3-2 XML DOS Protection configuration

This configuration is automatically translated into two additional message monitors, *ServiceName-count-monitor-firewall* and *ServiceName-count-monitor-from-ip*, and one duration monitor, called *ServiceName-duration-monitor*. They are attached to the respective DataPower service as shown in Figure 3-3. To make changes to these three monitors, you must go to the XML Threat Protection tab for the changes to override all changes that are made directly to the monitors.

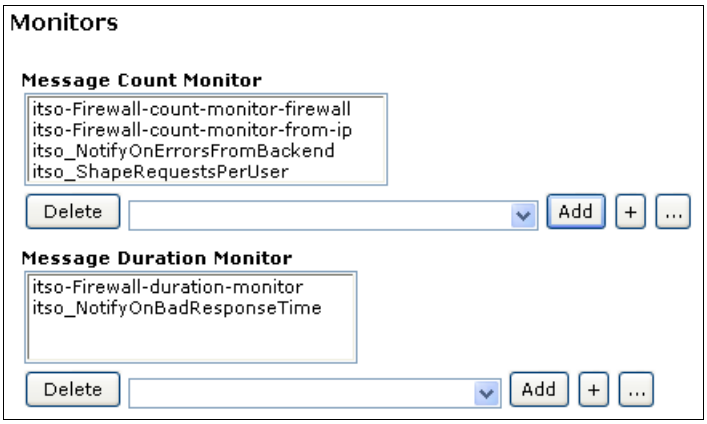


Figure 3-3 Additional message monitors automatically created by XML DOS Protection configuration

3.2.2 Web service monitors

Web service monitors are configured by providing the URL of a Web Services Definition Language (WSDL). The main difference to message monitors is that a Web service endpoint to be monitored can be specified. Web service monitors are also configured on the Monitor tab of the DataPower WebGUI (Figure 3-1 on page 70) with basic and simple configuration options.

Contrary to Web service monitors, SLM policy actions, as described in 3.2.3, “SLM policy actions” on page 71, are a more sophisticated and flexible way of monitoring Web services.

3.2.3 SLM policy actions

SLM policy actions offer the most fine-grained and sophisticated approach for setting up SLM in the DataPower device. Currently these actions can be used in the Web service proxy and the multiprotocol gateway services (Table 3-1 on page 69).

An SLM action consists of one to many policy statements (Figure 3-4). Every statement has a numerical identifier. These identifiers define the order in which the statements are processed.

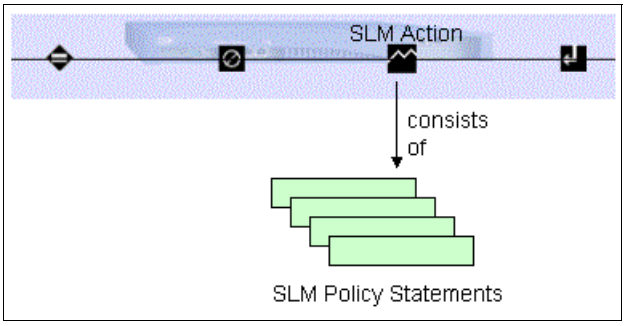


Figure 3-4 An SLM action consisting of policy statements

A basic property of an SLM policy is the mode in which the contained policy statements should be handled. The following modes are available:

- Processing of all statements of a policy
- Processing of statements until the first action (notify, shape, reject) is taken
- Processing of statements until a reject occurs

Synchronization of SLM status among multiple appliances

An SLM policy can specify membership in a *peer group*. Peer groups enable the exchange of SLM data among a group of specified DataPower appliances. This exchange is needed for the enforcement of SLM policies across multiple devices. The SLM configurations must be identical for all involved appliances. SOAP over HTTP is used to exchange the periodic update messages.

SLM policy statement definitions

An SLM policy consists of policy statements. The main configuration of an SLM statement involves the following steps:

1. Each policy statement has a sophisticated means of doing message matching. Message matching is done based on numerous message credentials and resource characteristics, including user credentials, sender IP address, or Web-service operation requested.
2. Specify a schedule when this SLM policy statement should be active, for example between 9:00 a.m. and 5:00 p.m., from Monday to Friday.
3. All messages that pass the matching step are handled by the message counters and latency monitors. If specified thresholds are reached, the configured action is taken. Thresholds to specify are time interval, message count, allowed bursts, and latency.
4. Specify the actions, either reject (throttle), shape (queue) or notify, to be executed for the message if the criteria is met.

Whether policy statement processing is aborted after the first match or reject or if all statements are always processed depends on your policy configuration. See the configuration examples in 3.3, “SLM policy configuration example in a multiprotocol gateway” on page 72, and 3.4, “SLM policy configuration example in a Web service proxy” on page 88.

3.3 SLM policy configuration example in a multiprotocol gateway

In this example, the enterprise ITSOCorp provides a simple Web service to customers. Messages can be sent over HTTP in this example, but it is also possible to configure, for example, the use of MQ or Java Message Service (JMS). A *gold user* should have high privileges and a good service level. *Normal users* should have basic access to the Web service. Refer to Table 3-2 on page 73, which describes the properties.

The messages that are sent to the Web service should include a Web Services Security (WS-Security) header with the user credentials. If this header is not present in the message, then anonymous user credentials are assumed by giving the users normal user access in this example. The Web service itself returns a prime number with the specified number of digits from the request message.

Table 3-2 Service level properties for the users in this example

Priority	Policy
Gold user 1	This is an important customer who is allowed to send 10 requests per minute and bursts of up to 30 requests (30 requests in quick succession). If the user exceeds this limit, messages are shaped (queued). The gold user is identified by user name from WS-Security header authenticated against an Lightweight Directory Access Protocol (LDAP) server. In this example, the gold user is called “Jane Doe.”
Normal users	Everyone else is allowed to send one request per minute. If more requests are sent, then messages are throttled (rejected). Furthermore the total round trip time of the messages sent by normal users is considered. This includes the time for processing in the DataPower device plus the time in the back-end system. If the time is greater than 5 seconds, messages of normal users are throttled to provide a better behavior for the gold user.

Figure 3-5 illustrates the layout of the multiprotocol gateway service configuration.

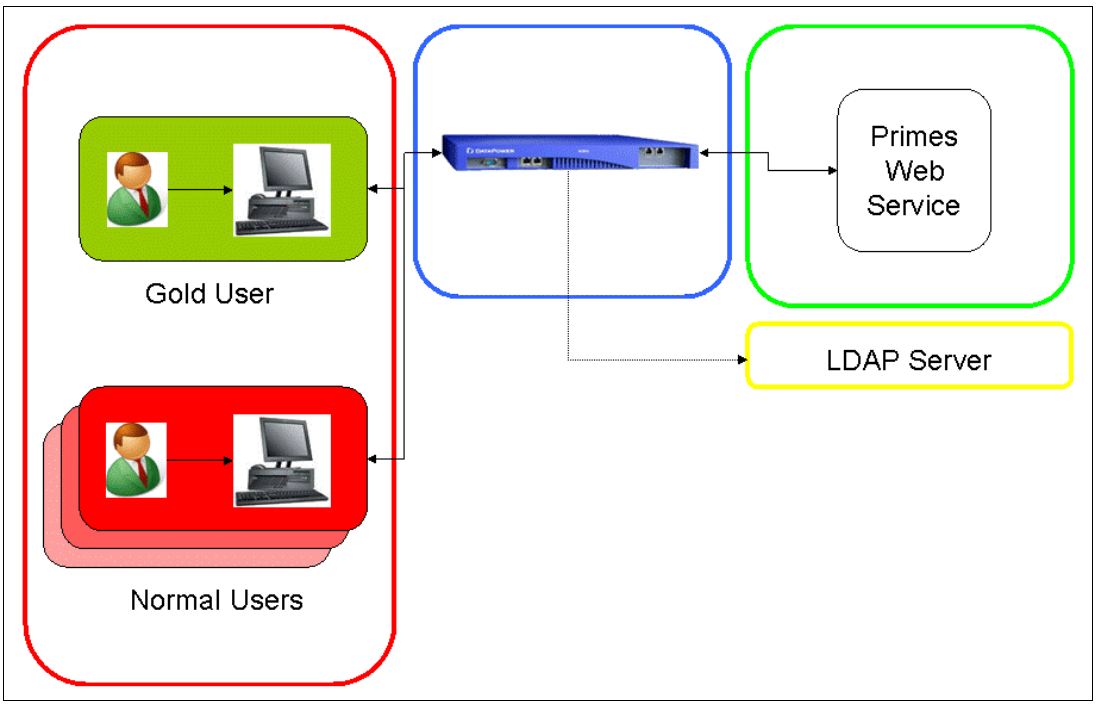


Figure 3-5 Layout of the multiprotocol gateway service configuration

Figure 3-6 illustrates the flow of the request messages through the multiprotocol gateway to the back end (Primes Web service).

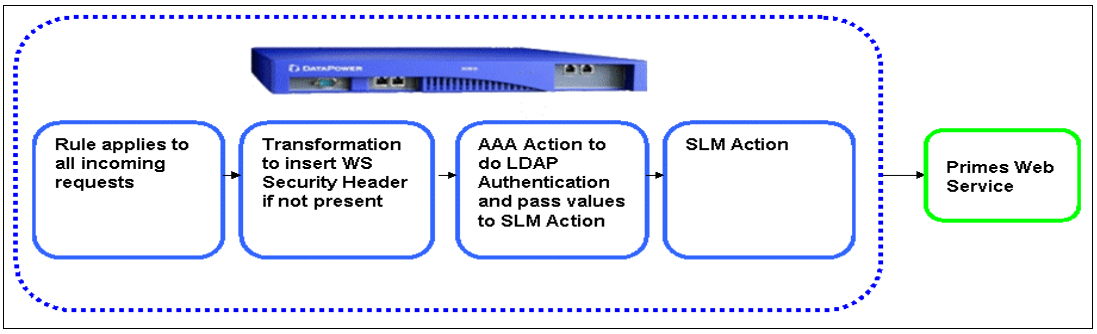


Figure 3-6 Flow of request messages through multiprotocol gateway to the back end

Figure 3-7 shows the LDAP users.

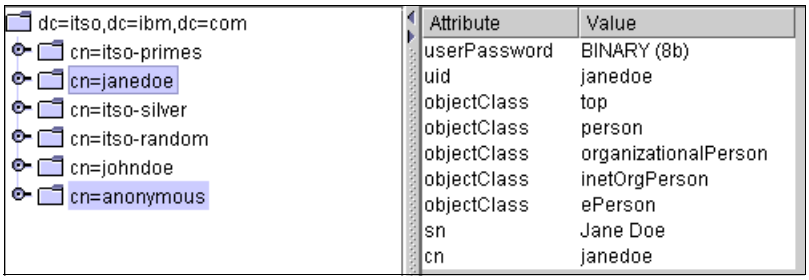


Figure 3-7 LDAP users

Example 3-1 shows the sample message that was sent to the Web service.

Example 3-1 A sample message sent to the Web service

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:q0="http://com.itso"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-sec
ext-1.0.xsd">
  <soapenv:Header>
   <wsse:Security>
    <wsse:UsernameToken>
     <wsse:Username>janedoe</wsse:Username>
     <wsse:Password>passw1rd</wsse:Password>
    </wsse:UsernameToken>
   </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
   <q0:getPrime>
    <numDigits>95</numDigits>
   </q0:getPrime>
  </soapenv:Body>
</soapenv:Envelope>
```

3.3.1 Configuring the multiprotocol gateway service in the DataPower device

To configure the service:

1. From the Control Panel, select **Multi-Protocol Gateway**.

> **Note:** We use a multiprotocol gateway in this example to demonstrate SLM and do not use the multiprotocol gateway capabilities that are available.

2. Configure the gateway as shown in Figure 3-8. On the General tab is a list of the back-side and front-side handlers (see Figure 3-10 on page 76). Click **Create new** to build a new front-side protocol handler.

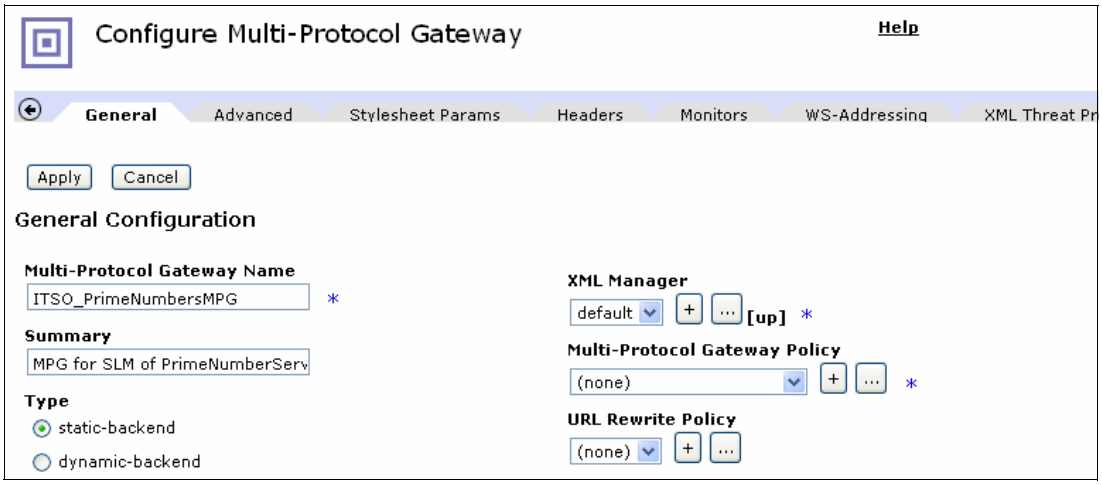


Figure 3-8 Configure Multi-Protocol Gateway page (partial)

3. Build a front-side protocol handler to listen for incoming messages. As shown in Figure 3-9, configure a plain HTTP handler that listens on all interfaces of this device (`0.0.0.0`) and on TCP port `8052`. Click **Apply** and close this window.

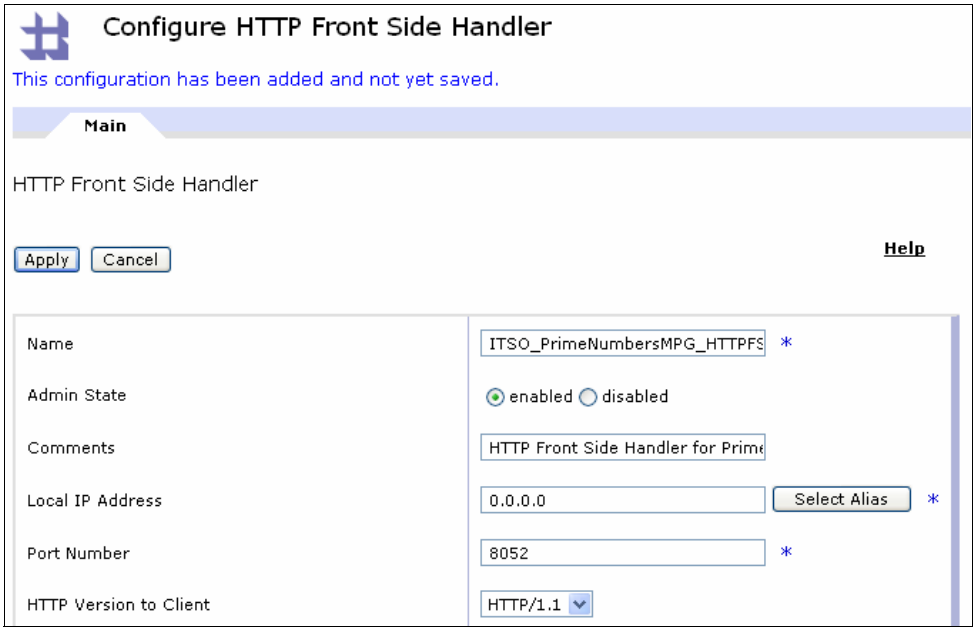


Figure 3-9 Configure HTTP Front Side Handler

4. Add the new front-side handler to the gateway. In the Front side settings section (Figure 3-10), select the new front side handler from the drop-down list and click **Add to gateway**. For Backend URL, type the following URL:

   `http://itsolab1:9080/PrimesWebService/services/Primes`

   This is the URL of the Web service that is running on a WebSphere Application Server.

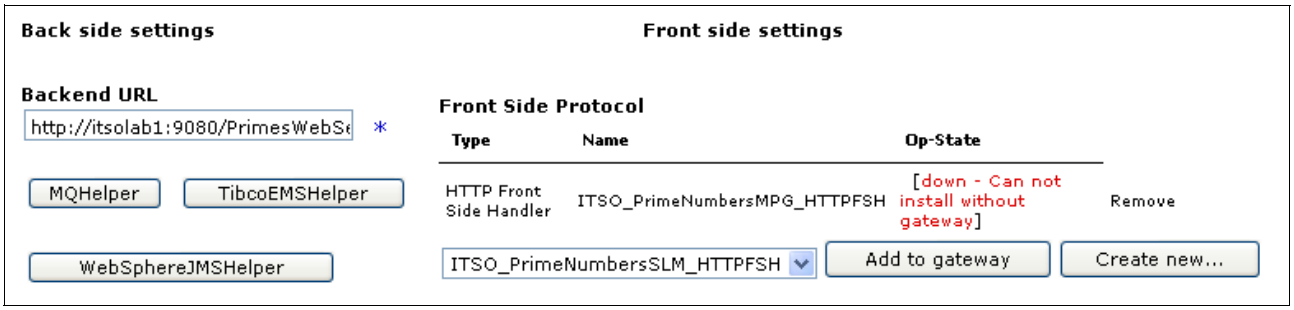


Figure 3-10 Front and back side handler (continuation of the Configure Multi-Protocol Gateway page)

5. Back on the Configure Multi-Protocol Gateway page (Figure 3-8 on page 75), in the Multi-Protocol Gateway Policy field, click the plus sign (**+**) button to create a new policy. Enter a name for the policy and click **OK**.
6. In the configuration page for the policy, change the rule name to a more meaningful name. Change the direction by selecting the **Client to Server** radio button. Then double-click the **=** (match action symbol).
7. Configure a matching rule that matches all URLs as shown in Figure 3-11. For Matching Type, select **url** and for the URL Match field, type an asterisk (*).

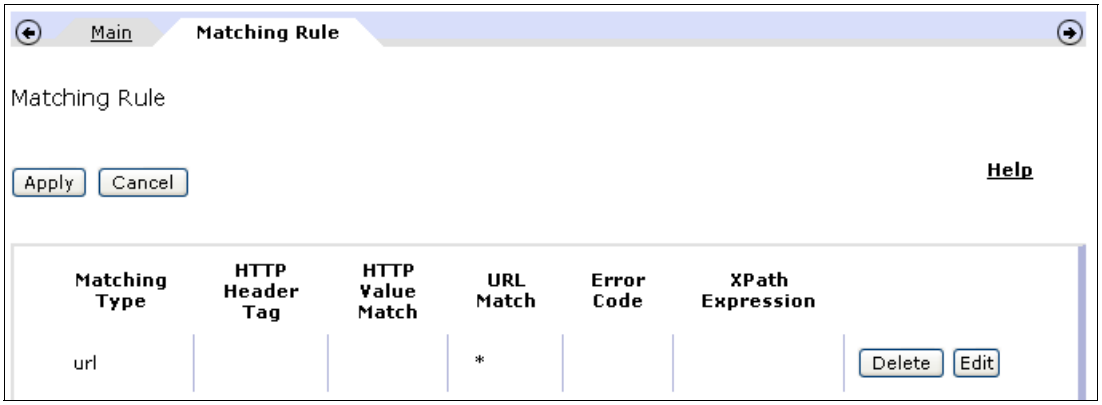


Figure 3-11 Configuring a matching rule

8. Make changes to messages that do not include the WS-Security information that we need in the following steps. Add a WS-Security header to messages that come without this header and give it the credentials of user “anonymous.”

a. Drag a **Transform** action to the policy rule and double-click it to configure this action (Figure 3-12).

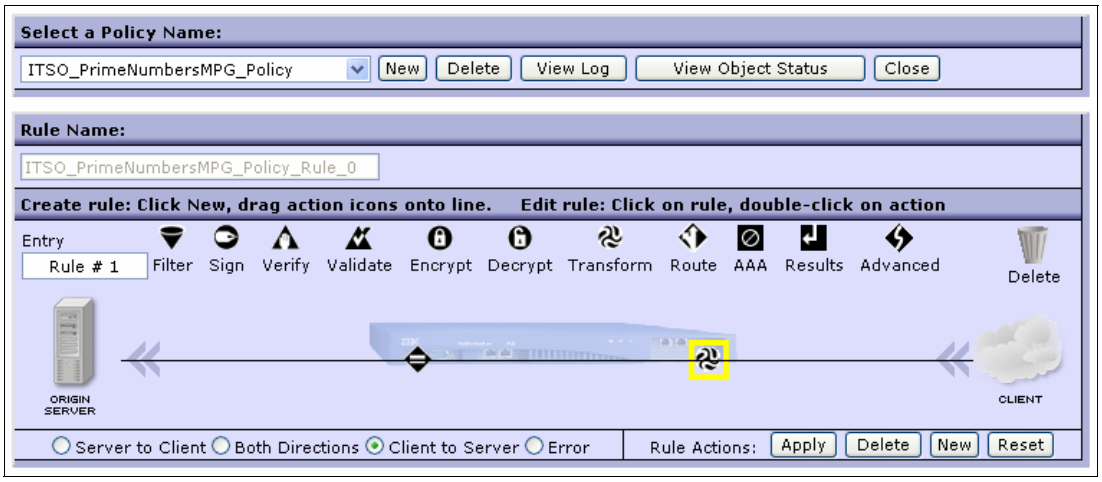


Figure 3-12 Adding a Transform action

b. On the Configure Transform Action page (Figure 3-13 on page 78), specify the XSLT file to be used. Example 3-2 shows the file that does the transformations that we need.

Example 3-2 The XSLT file 'rewriteforanonymous.xsl' used in the Transform Action

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:dp="http://www.datapower.com/extensions"
xmlns:dpconfig="http://www.datapower.com/param/config"
extension-element-prefixes="dp" exclude-result-prefixes="dp dpconfig">
<xsl:template match="/">
   <xsl:choose>
      <!--Make a copy of the whole request message if the header with user
      credentials is present in the request message.-->
      <xsl:when test="/*[namespace-uri()='http://schemas.xmlsoap.org/soap/envelop
      e/'and local-name()='Envelope']/*[namespace-uri()='http://schemas.xmlsoap.o
      rg/soap/envelope/' and local-name()='Header']">
         <xsl:copy-of select="."></xsl:copy-of>
      </xsl:when>
      <!--If no WSS header with the user credentials is present in the request
      just put the credentials 'anonymous' in and create a new message that
      includes values for the prime numbers web service from original request.-->
      <xsl:otherwise>
         <soapenv:Envelope xmlns:q0="http://com.itso"
         xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssec
         urity-secext-1.0.xsd">
            <soapenv:Header>
               <wsse:Security>
                  <wsse:UsernameToken>
                     <wsse:Username>anonymous</wsse:Username>
                     <wsse:Password>anonymous</wsse:Password>
                  </wsse:UsernameToken>
               </wsse:Security>
```

```
            </soapenv:Header>
            <xsl:if test="/*[namespace-uri()='http://schemas.xmlsoap.org/soap/enve
            lope/' and local-name()='Envelope']/*[namespace-uri()='http://schemas.
            xmlsoap.org/soap/envelope/' and local-name()='Body']/*[namespace-uri()
            ='http://com.itso' and local-name()='getPrime']/numDigits">
               <soapenv:Body>
                  <q0:getPrime>
                     <numDigits>
                     <xsl:value-of select="/*[namespace-uri()='http://schemas.xmls
                     oap.org/soap/envelope/' and local-name()='Envelope']/*[namesp
                     ace-uri()='http://schemas.xmlsoap.org/soap/envelope/'and loca
                     l-name()='Body']/*[namespace-uri()='http://com.itso' and loca
                     l-name()='getPrime']/numDigits"></xsl:value-of>
                     </numDigits>
                  </q0:getPrime>
               </soapenv:Body>
            </xsl:if>
         </soapenv:Envelope>
      </xsl:otherwise>
   </xsl:choose>
</xsl:template>
</xsl:stylesheet>
```

For Processing Control File, click the **Upload** button and select the XSLT file to upload to the local:// folder of the DataPower device. Verify that the correct files are used, apply the changes, and close the window.

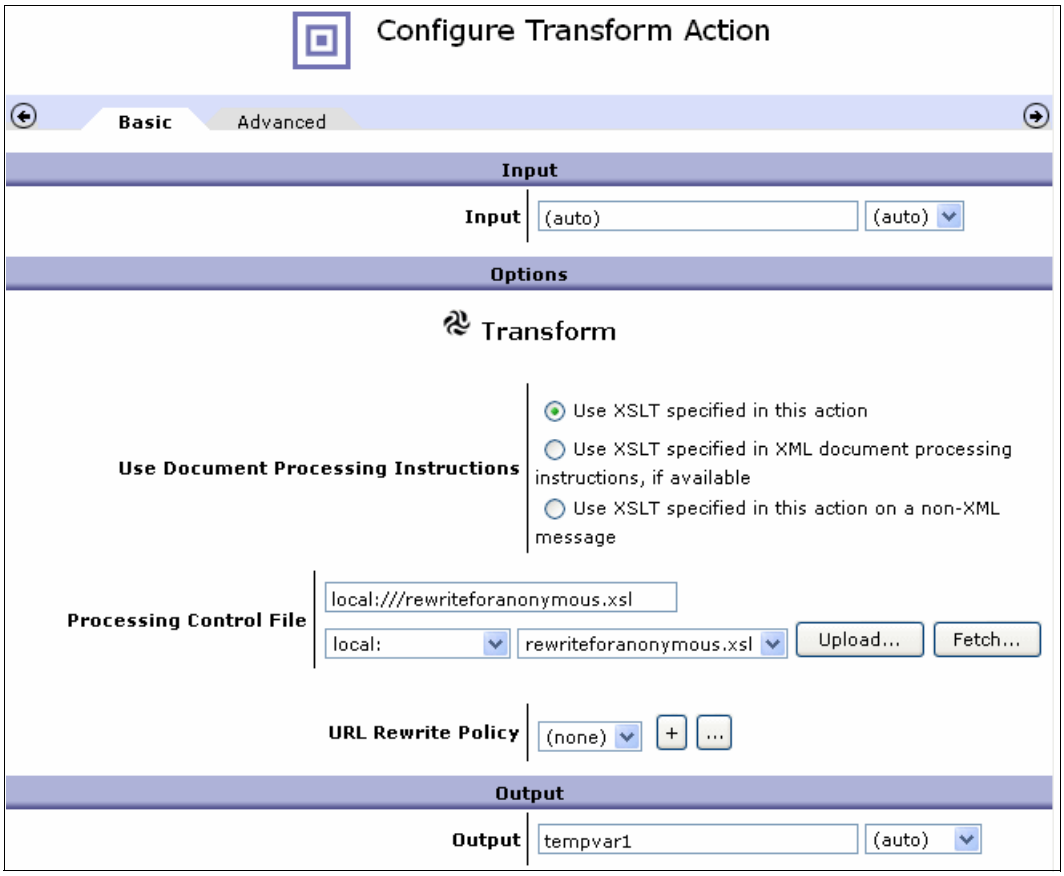


Figure 3-13 Configuring the Transform action to use the specified XSL file

9. Insert an authentication authorization, and auditing (AAA) action. We need this action to extract the user credential information to the SLM action for identifying the gold users. We want to use this action to authenticate users against an LDAP server. Drag the **AAA** icon to the policy diagram and double-click it to configure the action.
10. On the Basic page (Figure 3-14), click the **+** button next to AAA Policy to create a new policy. The wizard guides you through the AAA configuration steps. Set a name of choice.

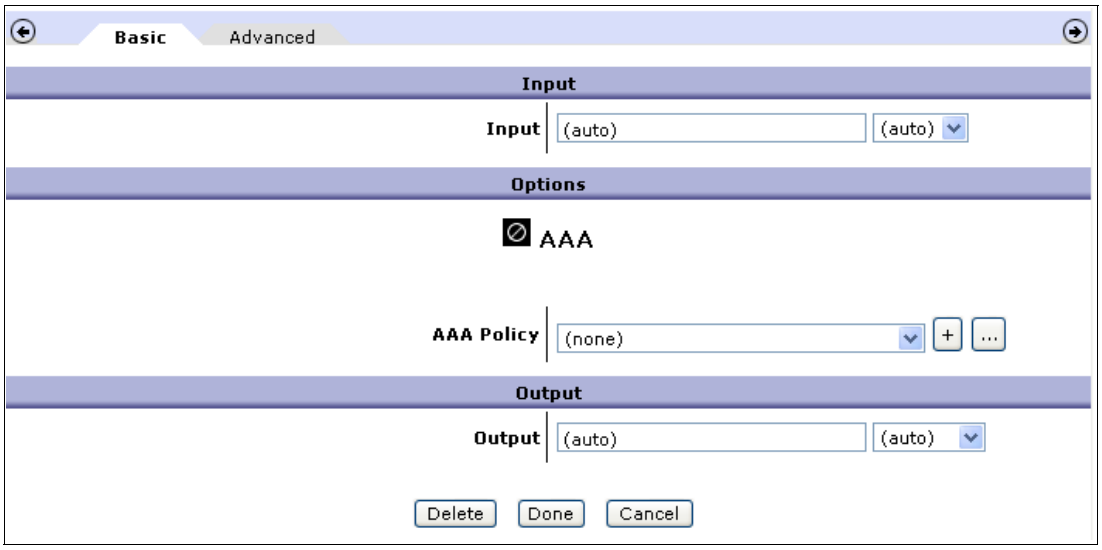


Figure 3-14 Configuring the AAA action

11. On the Configure an Access Control Policy page (Figure 3-15), select **Password-carrying UsernameToken Element from WS-Security Header** for the method to extract a user's identity.

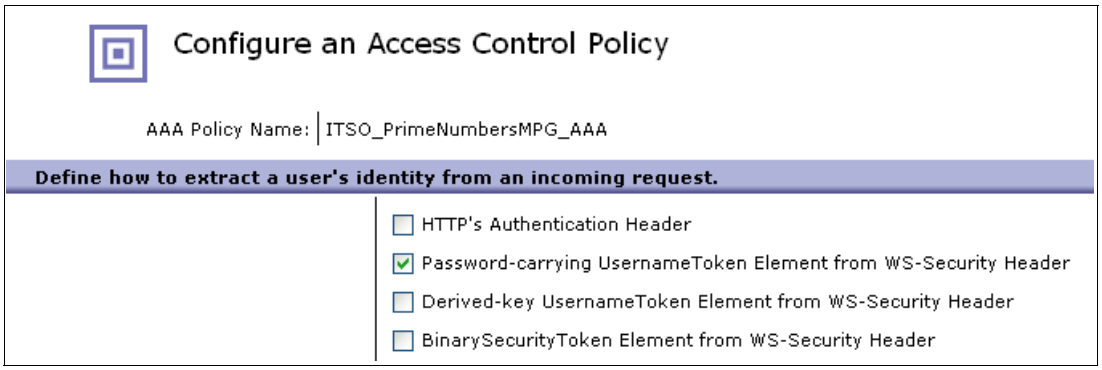


Figure 3-15 Extracting a user's identity from an incoming request for the AAA action

12. On the next page, use “bind to specific LDAP server” for authentication. Configure the connection to use the LDAP server. See also the LDAP users shown in Figure 3-7 on page 74. Figure 3-16 shows the values that are used in our example.

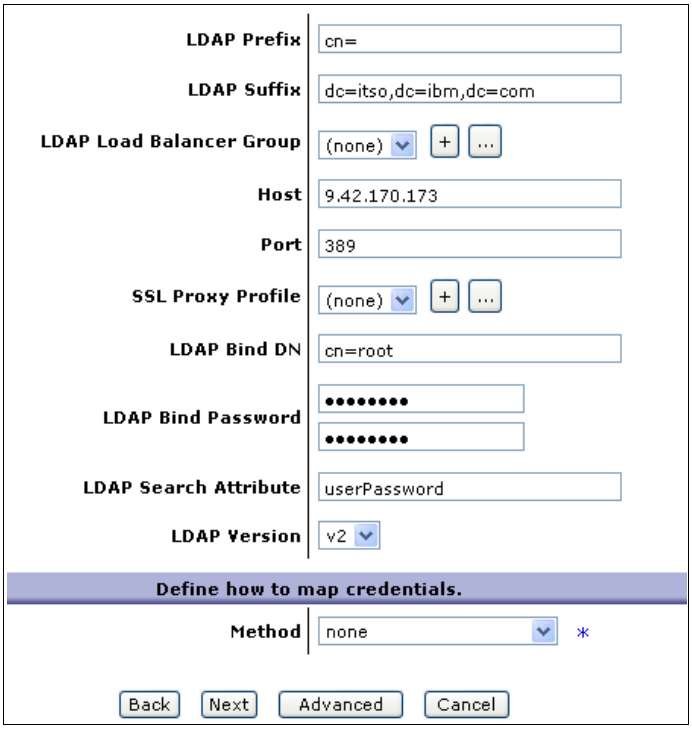


Figure 3-16 LDAP server binding configuration for the AAA action

13. On the following page, define the way to extract the resources. Select **URL sent to Back End**.
14. In the Define how to authorize a request page, choose **Allow Any Authenticated Client**. By selecting this option, messages of every client that has succeeded to do an authentication against the LDAP server are allowed.
15. On the next page, accept the default values as they are and click **Commit**.
16. Confirm the other windows, so that you return to the Configure Multi-Protocol Gateway page.

> **Cache lifetime:** You can set the cache lifetime for LDAP authentication results. The default value is 3 seconds. You can change it to a higher value by navigating to **Objects** → **XML Processing** → **AAA Policy**.

17. Add the SLM action to the policy under the **Advanced** tab. Select **SLM** as the action type as shown in Figure 3-17.

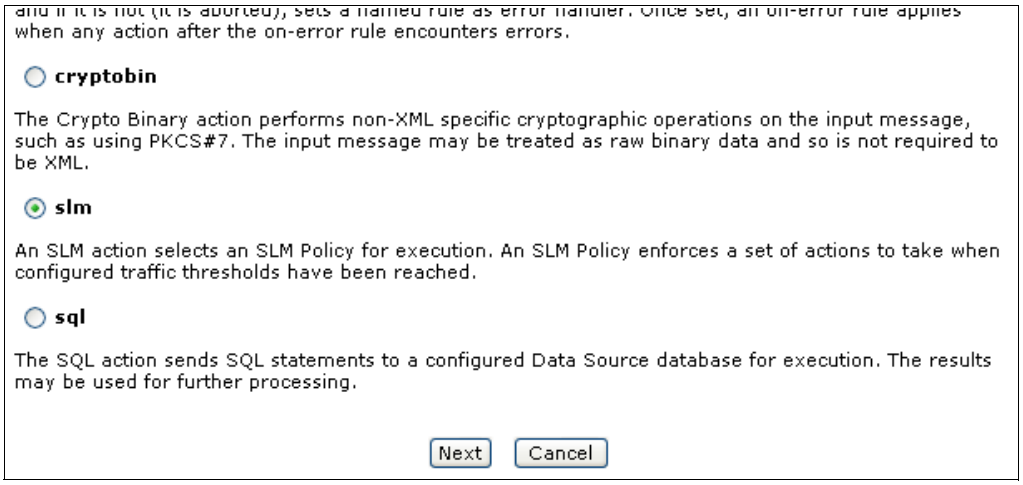


Figure 3-17 Setting the Advanced action to slm

18. On the Configure SLM Rule Action page (Figure 3-18), for SLM Policy, click the **+** button to create a new SLM policy.

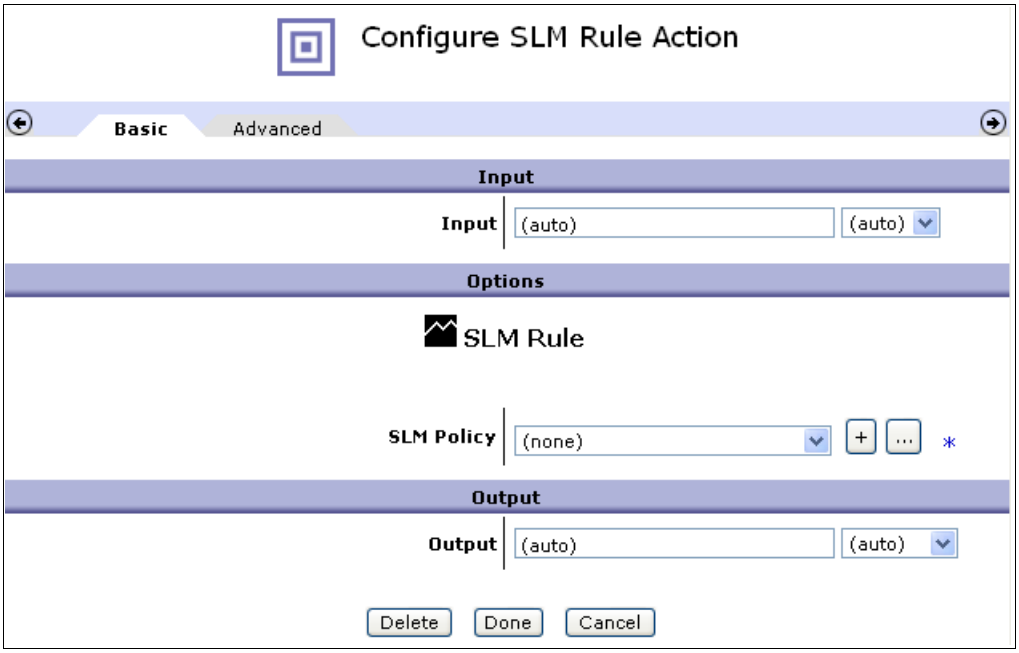


Figure 3-18 Configuring the SLM action

19. On the Main tab of the Configure SLM Policy page (Figure 3-19), for Evaluation Method, choose **terminate-at-first-action**. We select this method because we use it to stop the processing for gold users.

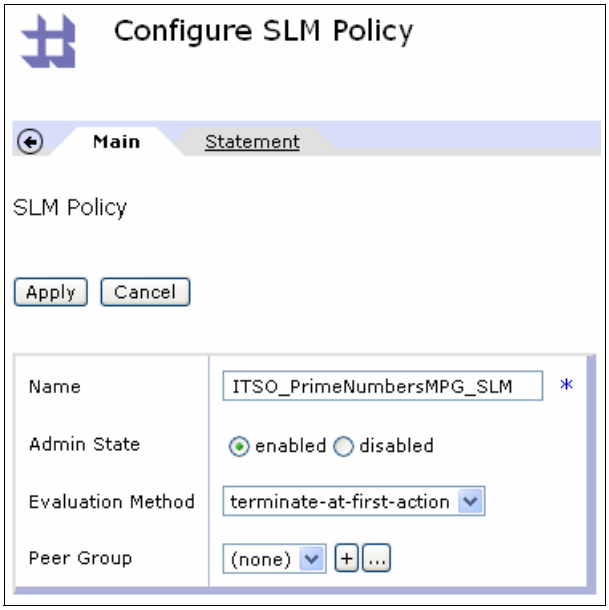


Figure 3-19 Configuring the SLM policy basics for the SLM action

20. Click the **Statement** tab and add a new statement for the gold user. The identifier of the statement is an integer number and specifies the processing sequence of the statements. To process this statement first, set the identifier to `1`.

21. Create a new credential class because, in this example, we are matching the messages by defining a user name that has been extracted by the AAA action before. Because this should be the policy statement for the gold user, for Credential Value, add `janedoe` (Figure 3-20).

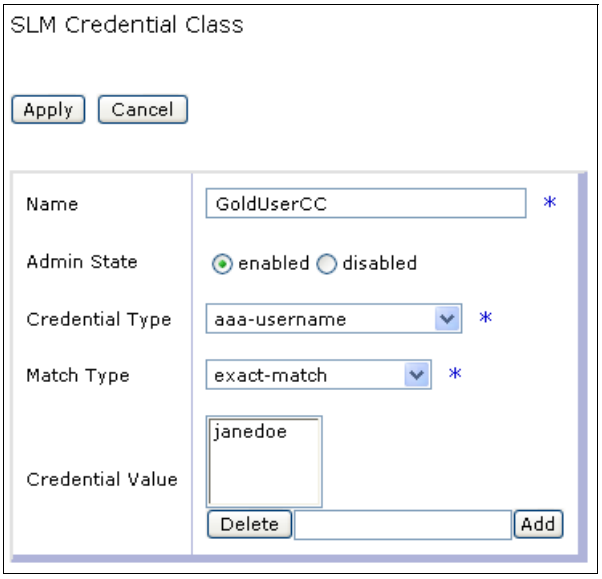


Figure 3-20 Configuring the SLM credential class of the SLM statement for the SLM action

22. We do not define a schedule so that this statement is always active. Define threshold values according to your desired behavior for the gold user (Figure 3-21). In this example, the user is allowed to send 10 requests per minute and bursts of up to 30 requests (30 requests in quick succession). If the gold user exceeds this limit, messages are shaped (queued).

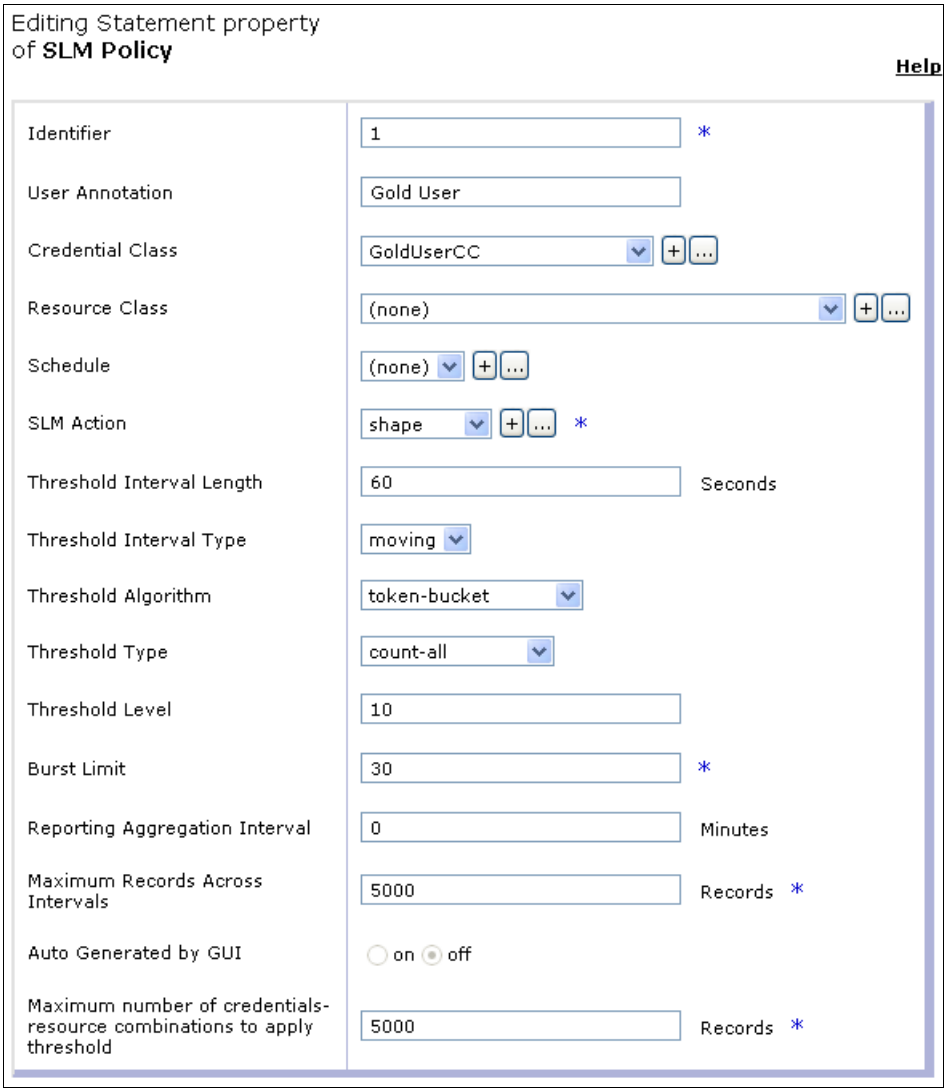


Figure 3-21 SLM Policy

23. Create a second statement that ends processing of further statements in the policy for the gold user. If you do not add a statement here, a message might be accepted because it is from a gold user. The message might then be processed by the next statement in the sequence, which is a normal user statement in our case. Then this message might be rejected by one of the user statements.

Remember that we set the evaluation method of our policy to terminate-at-first-action. Therefore, create a statement that sends a notification of debug priority as shown in Figure 3-22.

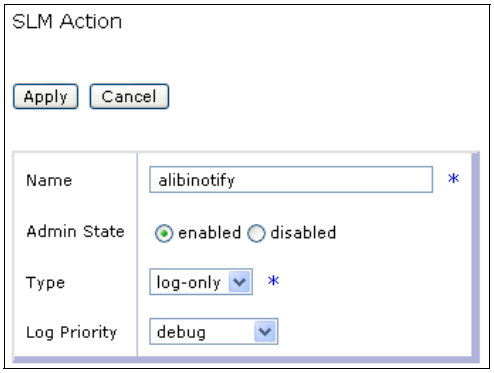


Figure 3-22 Creating a custom SLM action

Create a new SLM action by clicking the **+** button next to SLM Action field. Figure 3-23 shows the SLM statement, in the User Annotation field, to send debug messages in the gold user context.

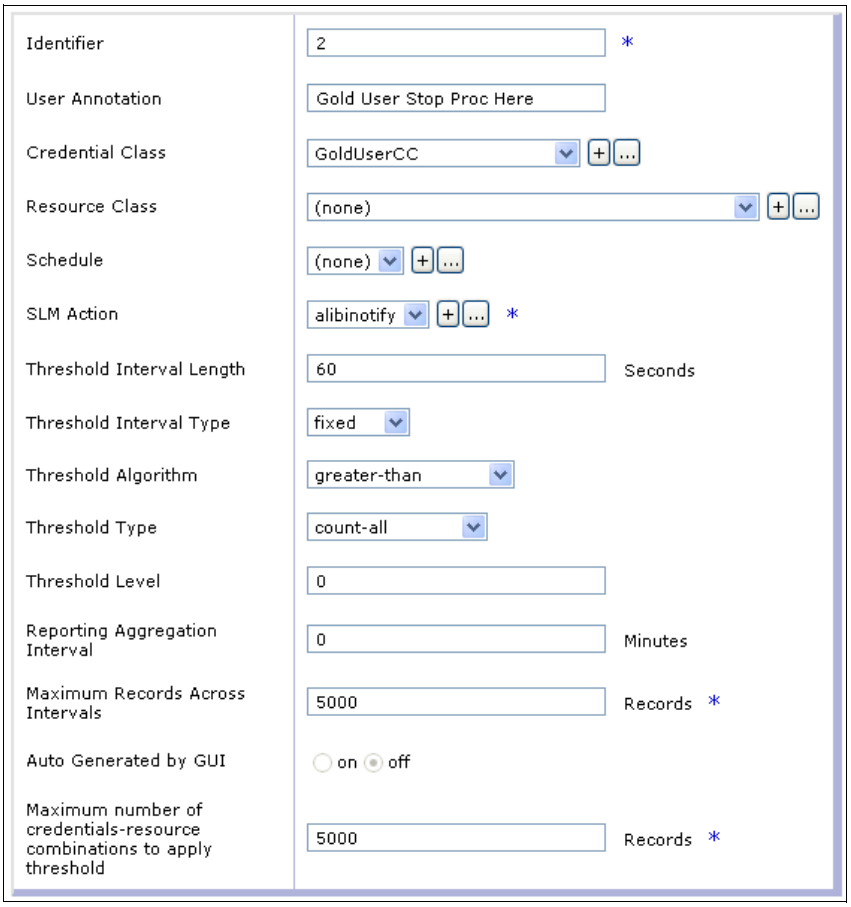


Figure 3-23 SLM statement for sending debug messages in the gold user context

24. Create two statements for the default behavior for all other users without special privileges, who are considered normal users. The first statement enforces that only one message per minute is sent as defined in Figure 3-24.

Identifier	99 *
User Annotation	Normal Users
Credential Class	NormalUsersCC + ...
Resource Class	(none) + ...
Schedule	(none) + ...
SLM Action	throttle + ... *
Threshold Interval Length	60 Seconds
Threshold Interval Type	fixed
Threshold Algorithm	greater-than
Threshold Type	count-all
Threshold Level	1
Reporting Aggregation Interval	0 Minutes
Maximum Records Across Intervals	5000 Records *
Auto Generated by GUI	on off
Maximum number of credentials-resource combinations to apply threshold	5000 Records *

Figure 3-24 SLM statement for normal users allowing only one message sent per minute per user

As shown in Figure 3-25, create a credential class called `NormalUsersCC`. We differentiate users by their IP address. With the match type of per-extracted-value, the definitions of counters and thresholds in the SLM statement are separately used for each client IP address. Every client IP address has its own message counters.

SLM Credential Class

Apply Cancel

Name	NormalUsersCC *
Admin State	enabled disabled
Credential Type	client-ip *
Match Type	per-extracted-value *

Figure 3-25 SLM Credential Class

The second statement, as defined in Figure 3-26, allows the sending of requests only if the latency for message processing is less than 5 seconds.

Threshold Type latency: The Threshold Type measures the total processing time (a value of *latency-total* in our example) when one message is sent by a normal user. If that value exceeds the threshold level that is set (5000 milliseconds in our example), then for a Threshold Interval Length of 60 seconds in our example, the specified action is applied to the messages.

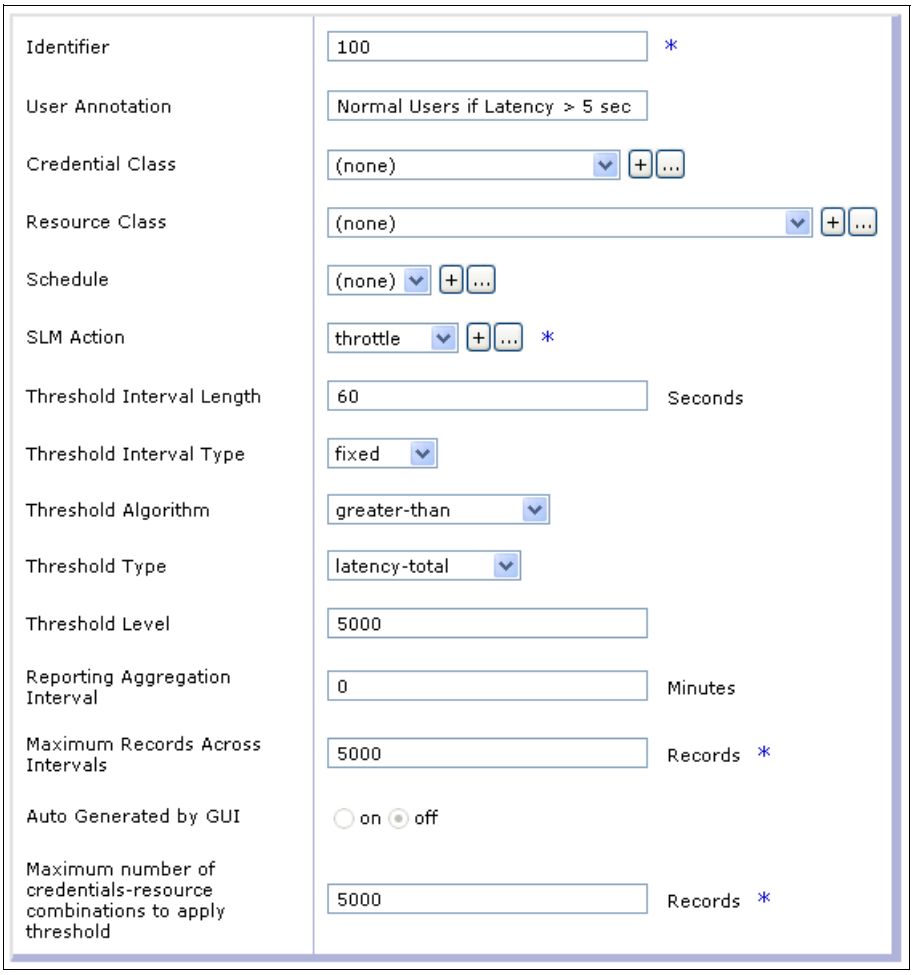
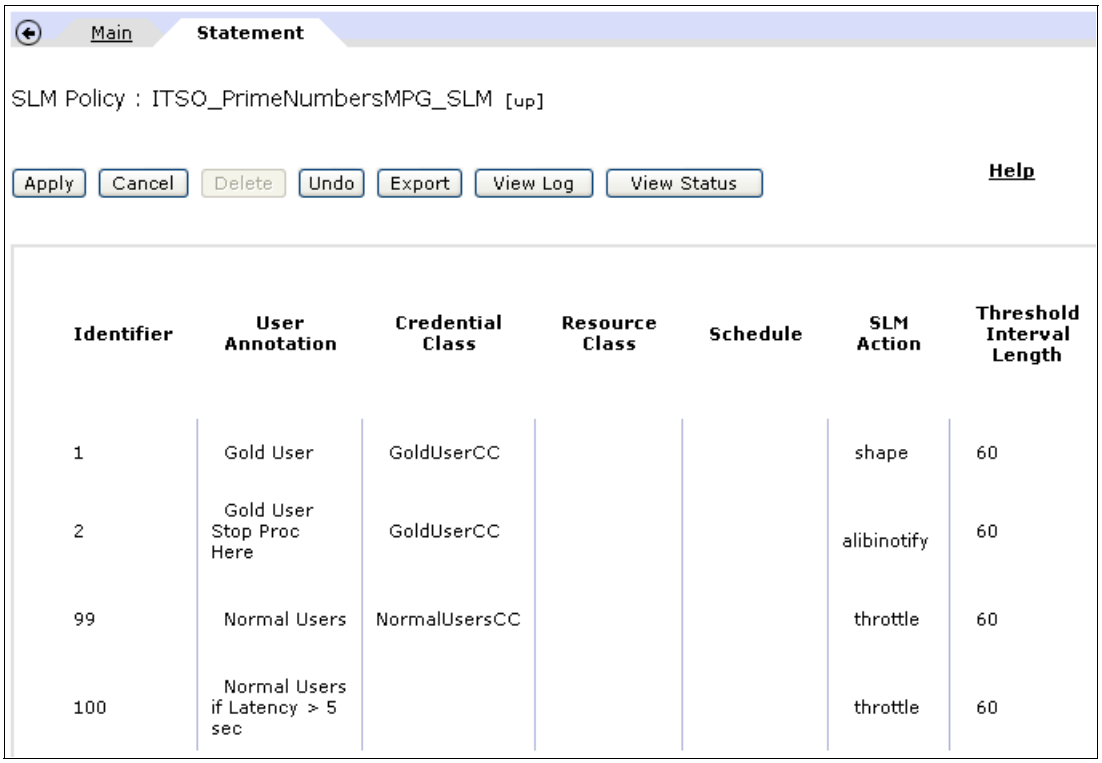


Figure 3-26 SLM statement for normal users that rejects (throttles) messages if latency is too high

25. Apply the changes. You now have four SLM statements as shown in Figure 3-27.



Identifier	User Annotation	Credential Class	Resource Class	Schedule	SLM Action	Threshold Interval Length
1	Gold User	GoldUserCC			shape	60
2	Gold User Stop Proc Here	GoldUserCC			alibinotify	60
99	Normal Users	NormalUsersCC			throttle	60
100	Normal Users if Latency > 5 sec				throttle	60

Figure 3-27 Overview of the configured SLM statements

26. Apply the changes and close the SLM configuration windows. See Figure 3-28.

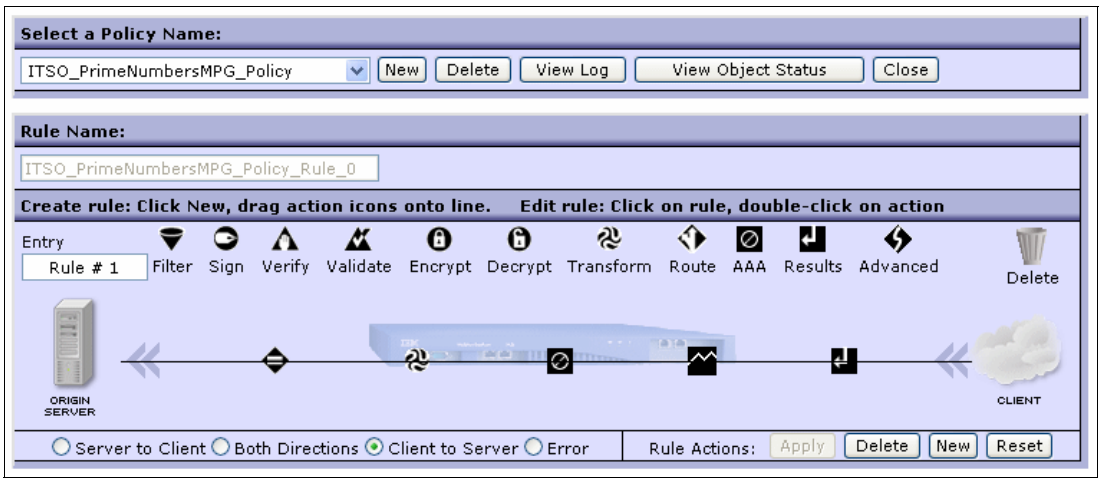


Figure 3-28 The Client to Server message processing rule

The Client to Server processing rule is now finished, but we still need a rule for the replies from the server:

1. Click the **New** button next to Rule Actions.
2. Change the direction from Both Directions to **Server to Client**.
3. Double-click the automatically created **=** (match) icon.
4. Specify that all messages should be matched. We use the match all URLs definition that we use in our other rule. See Figure 3-29.

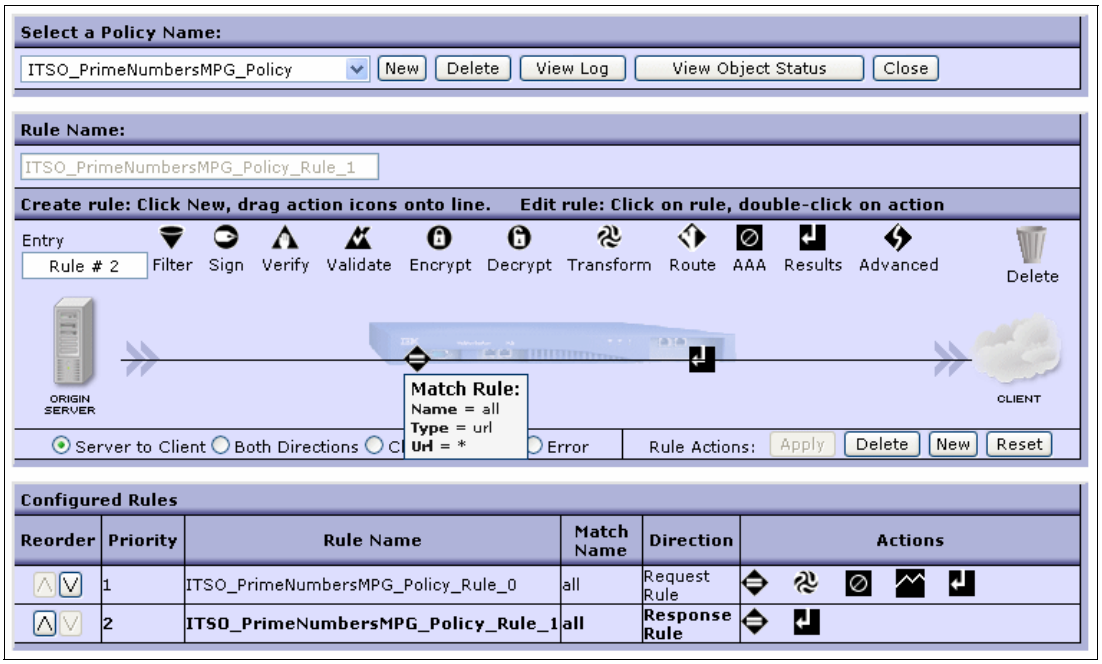


Figure 3-29 The Server to Client message processing rule

This multiprotocol gateway is now enabled to do SLM.

> **Tip:** If the behavior of the policy is not as expected, the Input and Output context of the policy actions might not be set correctly, which is a common error. To check this, move the mouse over the **Action** icon on the processing rule. The Input of one action should be set to the appropriate Output of another previous action. If in doubt or when configuring a plain policy rule, change the values to *auto*, so that the Output of the previous action is always taken as Input for the following action.

3.4 SLM policy configuration example in a Web service proxy

In this example, we demonstrate the SLM capabilities in a DataPower Web service proxy. This is a Web service proxy for a Prime Numbers Web service that has a couple of operations. We want to protect our back end from abuse or overuse, but we do not want single users to consume all of the capacity of the service.

Therefore, the configuration involves one operation of the Web service, called getPrime, that should be generally allowed to send 150 requests per minute to this operation. The other three operations should only receive 40 requests per minute or less. All together, at a maximum of 220 requests per minute, they should be sent to the back end. If these numbers are exceeded, requests should be queued. If a single user sends more than 50 requests per

minute to this Web service, messages are rejected (throttled), but it should be possible to send bursts of 100 messages.

The WebGUI configuration of the Web service proxy service offers a convenient way to configure SLM. A separate tab is dedicated to the SLM configuration.

1. Create a new Web service proxy. From the Control Panel, click **Web Service Proxy**.
2. On the WSDLs page (Figure 3-30 on page 90), define the Web service proxy as shown:
   a. Select **Add WSDL**.
   b. Specify a WSDL URL.
   c. Upload the WSDL file, which is shown in Example 3-3.
   d. The remote endpoints are configured automatically as defined in the WSDL file. Therefore, you only have to create the front side handler, which is a simple HTTP handler that listens on port 8053 in this case.

      See 3.3, “SLM policy configuration example in a multiprotocol gateway” on page 72, for details about how to create an endpoint handler.
   e. Accept all other default values as they are.
   f. Click **Apply**.

Example 3-3 The (shortened) primes.wsdl used in this example

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://com.itso"
xmlns:impl="http://com.itso"
...
<wsdl:types>
<element name="getPrime">
   <complexType>
      <sequence>
         <element name="numDigits" type="xsd:int"/>
      </sequence>
   </complexType>
</element>
...
</wsdl:types>

<wsdl:message name="mainResponse">
   <wsdl:part element="intf:mainResponse" name="parameters"/>
</wsdl:message>
...
<wsdl:portType name="Primes">
   <wsdl:operation name="getPrime">
      <wsdl:input message="intf:getPrimeRequest" name="getPrimeRequest"/>
      <wsdl:output message="intf:getPrimeResponse" name="getPrimeResponse"/>
   </wsdl:operation>
...
</wsdl:portType>
<wsdl:binding name="PrimesSoapBinding" type="intf:Primes">
...
</wsdl:binding>
<wsdl:service name="PrimesService">
   <wsdl:port binding="intf:PrimesSoapBinding" name="Primes">
      <wsdlsoap:address
```

```
      location="http://itsolab1:9080/PrimesWebService/services/Primes"/>
   </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

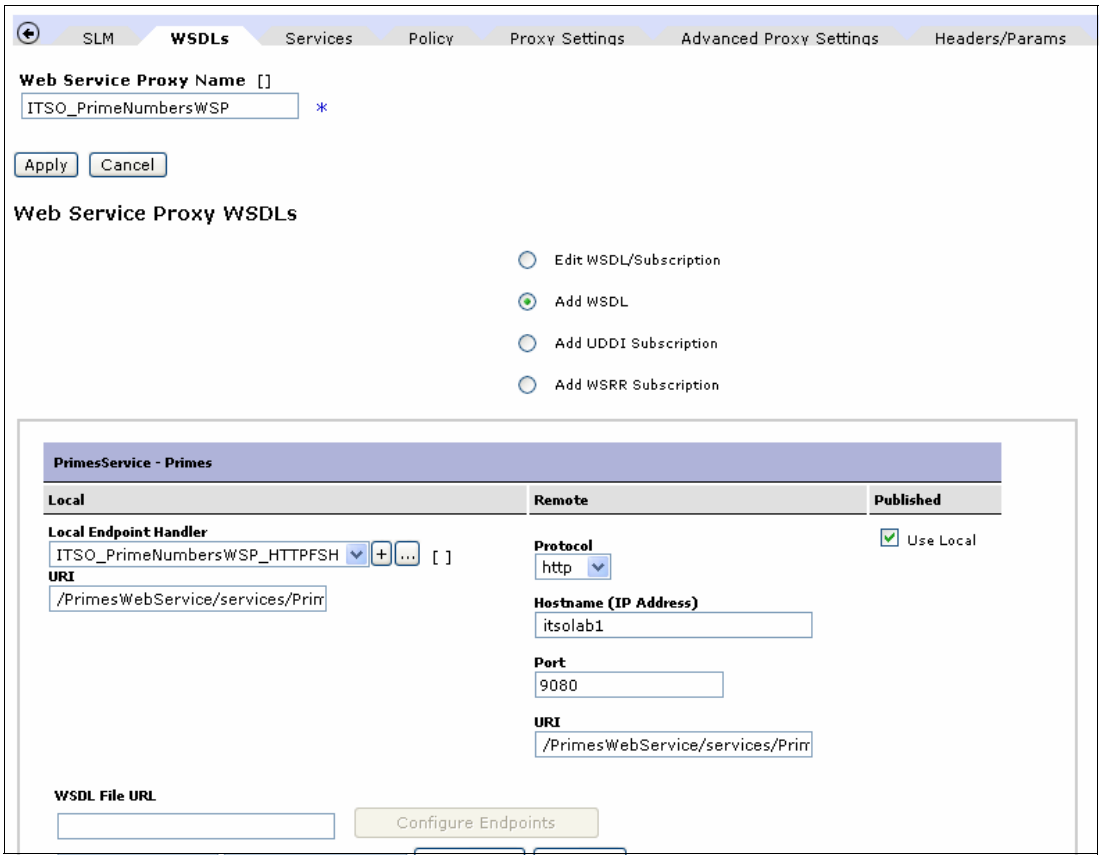


Figure 3-30 Basic Configuration of the Web service proxy

3. The basic policies for this WSDL are configured automatically. The Policy tab (Figure 3-31) shows the policies, which can now be modified. An SLM Policy Action is automatically inserted into the request rule. It is not possible to change the SLM policy here.

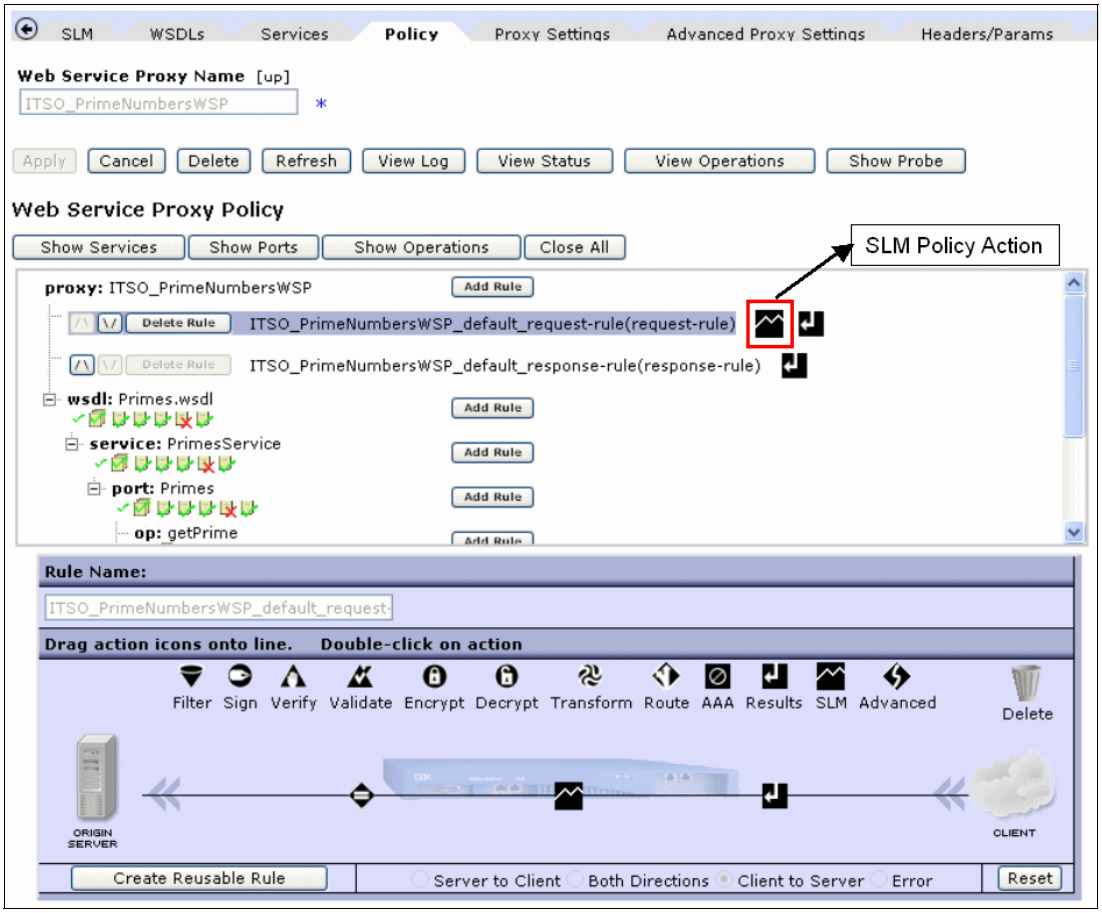


Figure 3-31 Default Policies that are automatically created

4. On the SLM tab (Figure 3-32), you can configure the SLM Policy Action. In the top area of the page, values for the messages per time interval and the corresponding action are configured for every level of the Web service proxy.

   Under Peers, you can enter the URLs of participating DataPower devices in an SLM peer group to enforce SLM policies if more than one DataPower device is used. In the bottom area, you can create custom SLM statements.

   Insert the values for the desired behavior as shown in the example and apply the changes.

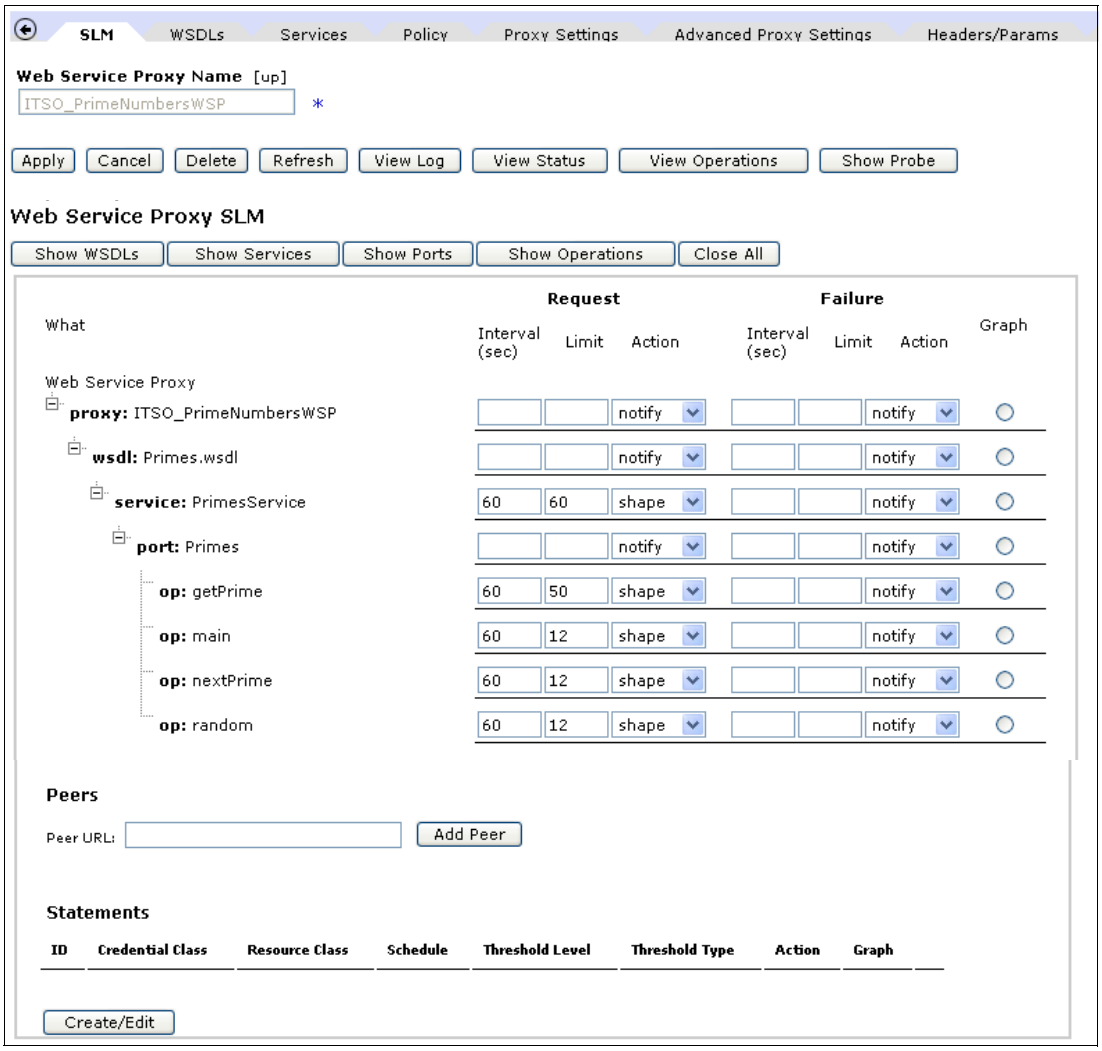


Figure 3-32 SLM configuration with a Web service proxy

DataPower internally produces SLM statements. To see what was configured, navigate to **Objects** → **Monitoring** → **SLM Policy**. The SLM Policy that is automatically created has the same name as the Web service proxy. In our case, we create an SLM policy with five statements. Figure 3-32 shows, as an example, the generated statement for the getPrime operation. You can change the values here, which would change this basic statement to an advanced custom statement.

Figure 3-33 illustrates an example of an automatically configured SLM statement.

Editing Statement property
of **SLM Policy**

Help

Identifier	94 *
User Annotation	Auto Generated
Credential Class	(none)
Resource Class	rsrc-ITSO_PrimeNumbersWSP-wsdl-operation8
Schedule	(none)
SLM Action	shape *
Threshold Interval Length	60 Seconds
Threshold Interval Type	fixed
Threshold Algorithm	greater-than
Threshold Type	count-all
Threshold Level	50
Reporting Aggregation Interval	0 Minutes
Maximum Records Across Intervals	5000 Records *
Auto Generated by GUI	on off
Maximum number of credentials-resource combinations to apply threshold	5000 Records *

Figure 3-33 Example of an automatically configured SLM statement

5. Create a rule that allows a single user to send only one request per minute. Use a custom statement to configure this rule. On the Web Service Proxy SLM tab (Figure 3-34), click the **Create/Edit** button in the Statement section at the bottom of the page.

Statements

ID	Credential Class	Resource Class	Schedule	Threshold Level	Threshold Type	Action	Graph

Create/Edit

Figure 3-34 Create custom statements here

6. On the Configure SLM Credential Class page (Figure 3-35), create a new credential class that will be used to apply the rule on every client distinguished by their client IP address.

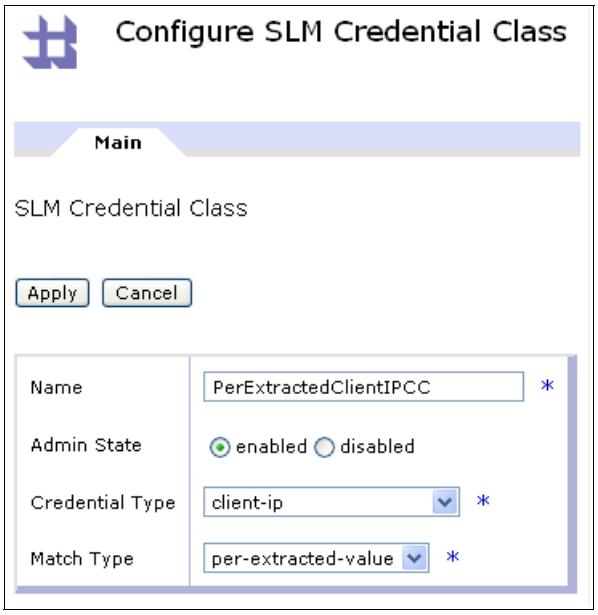


Figure 3-35 Configure SLM Credential Class

7. As shown in Figure 3-36, set the necessary values to achieve the desired outcome of one message allowed per 60 seconds and bursts of up to five messages. For bursts to work, choose **token-bucket** for Threshold Algorithm.

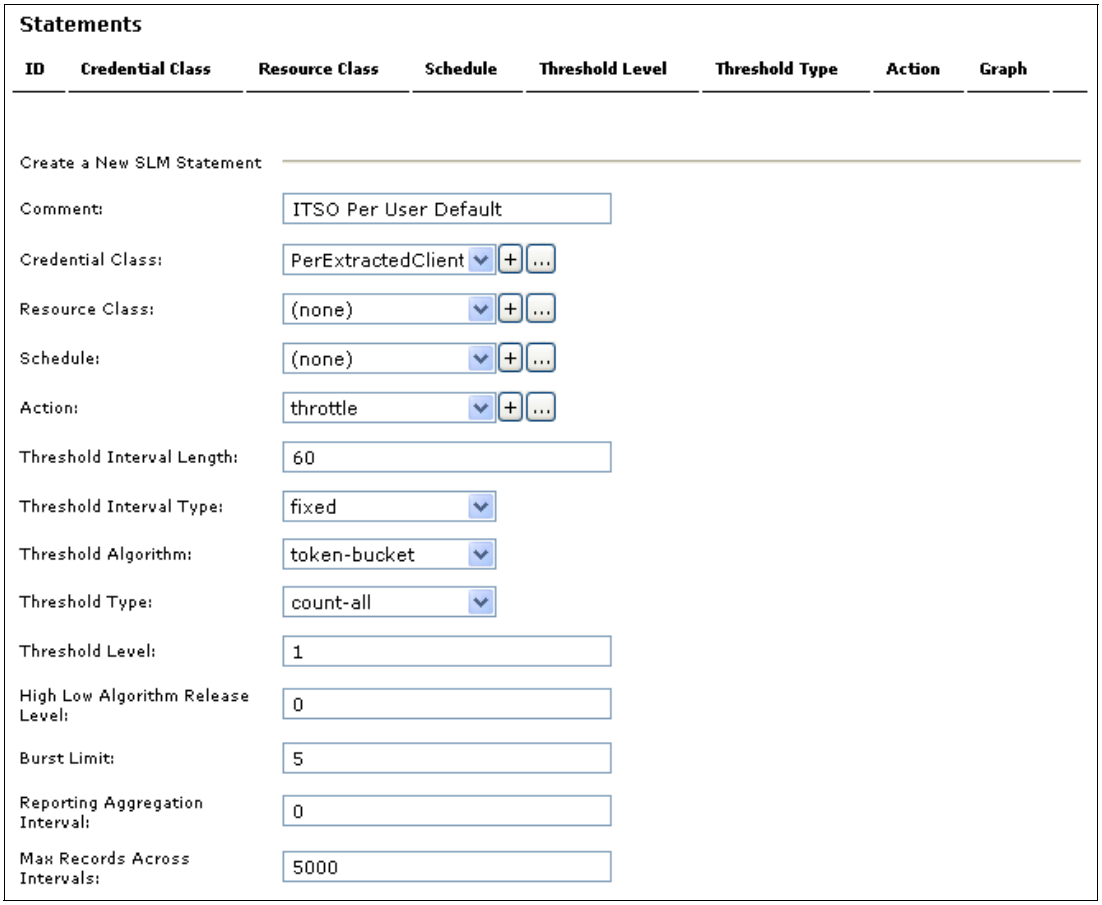


Figure 3-36 Configuration of the custom statement

The configuration of the service level monitor of our Web service proxy is now finished. You can apply the changes and start testing its behavior. In our example, we use the simple command line tool cURL to send simple SOAP messages such as the one shown in Example 3-4 to the DataPower appliance named *dp01*. We have configured our service level monitor to allow users to send five messages at a maximum in a burst. If more messages are sent, they will be rejected.

Example 3-4 The SOAP request message getPrime_REQ.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:q0="http://com.itso"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <soapenv:Body>
   <q0:getPrime>
    <numDigits>12</numDigits>
   </q0:getPrime>
  </soapenv:Body>
</soapenv:Envelope>
```

You see in Example 3-5 the testing of the Web service and that the service level monitor worked as expected.

Example 3-5 Testing the Web service

```
// the 5th message within some seconds from one client to the getPrime operation -
// everything works fine, as the client is using his burst entitlement
C:\Curl>curl --data-binary @getPrime_REQ.xml -i http://dp01:8053/PrimesWebServic
e/services/Primes
HTTP/1.1 200 OK
X-Backside-Transport: OK OK
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/xml; charset=utf-8
Content-Language: en-US
Date: Tue, 02 Oct 2007 14:00:51 GMT
Server: WebSphere Application Server/6.1
X-Client-IP: 9.42.171.105

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmln
s:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsd="http://www.w3.o
rg/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><soapen
v:Header/><soapenv:Body><p234:getPrimeResponse xmlns:p234="http://com.itso"><get
PrimeReturn>650410822843</getPrimeReturn></p234:getPrimeResponse></soapenv:Body>
</soapenv:Envelope>

// the 6th message from the same client is rejected and an error message is sent.
C:\Curl>curl --data-binary @getPrime_REQ.xml -i http://9.42.170.230:8053/PrimesW
ebService/services/Primes
HTTP/1.0 500 Error
X-Backside-Transport: FAIL FAIL
Content-Type: text/xml
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"><env:Body><e
nv:Fault><faultcode>env:Client</faultcode><faultstring>Rejected by SLM Monitor (
from client)</faultstring></env:Fault></env:Body></env:Envelope>
```

By clicking the Graphs button on the right side, you can see a diagram of message rate, latency, and count over time. Rate and count are shown for transactions, errors, and throttled messages (see Figure 3-37 on page 97 and Figure 3-39 on page 98). The latency is shown as internal and back-end latency (see Figure 3-38 on page 97).

In this scenario, we use the tool Apache JMeter, which generates and sends messages for us and can be conveniently configured to display sophisticated behavior.

Figure 3-37 shows the SLM Message Rate graph.

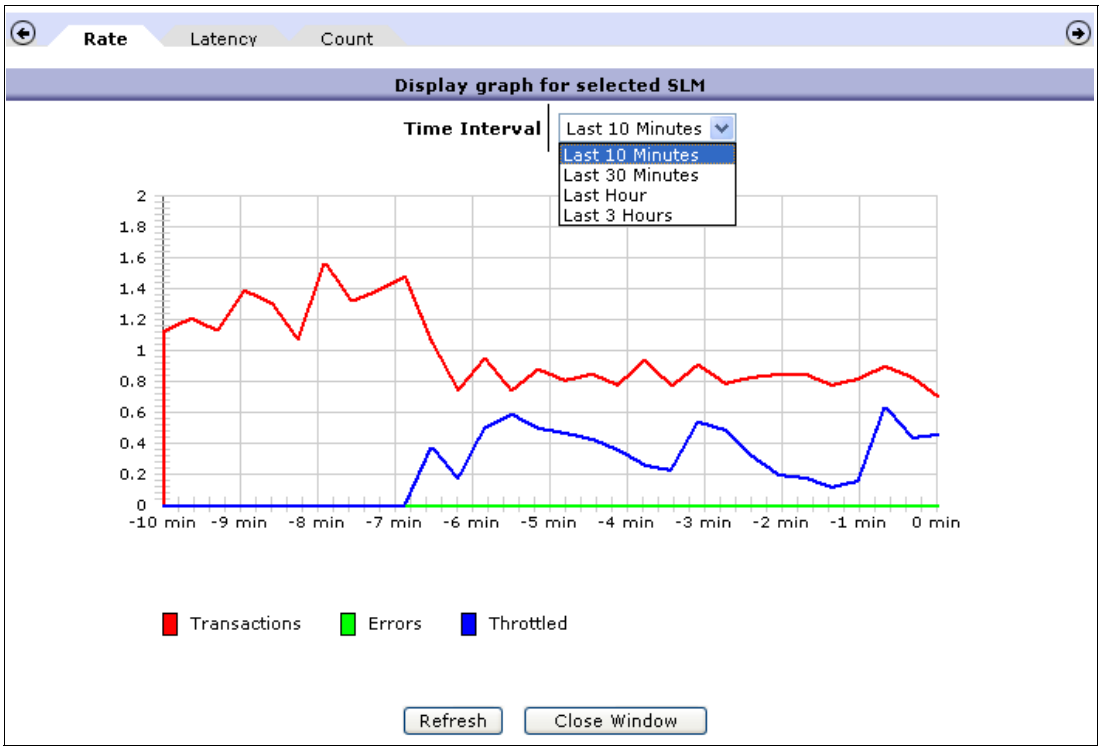


Figure 3-37 SLM Message Rate graph

Figure 3-38 shows the SLM Message Latency graph.

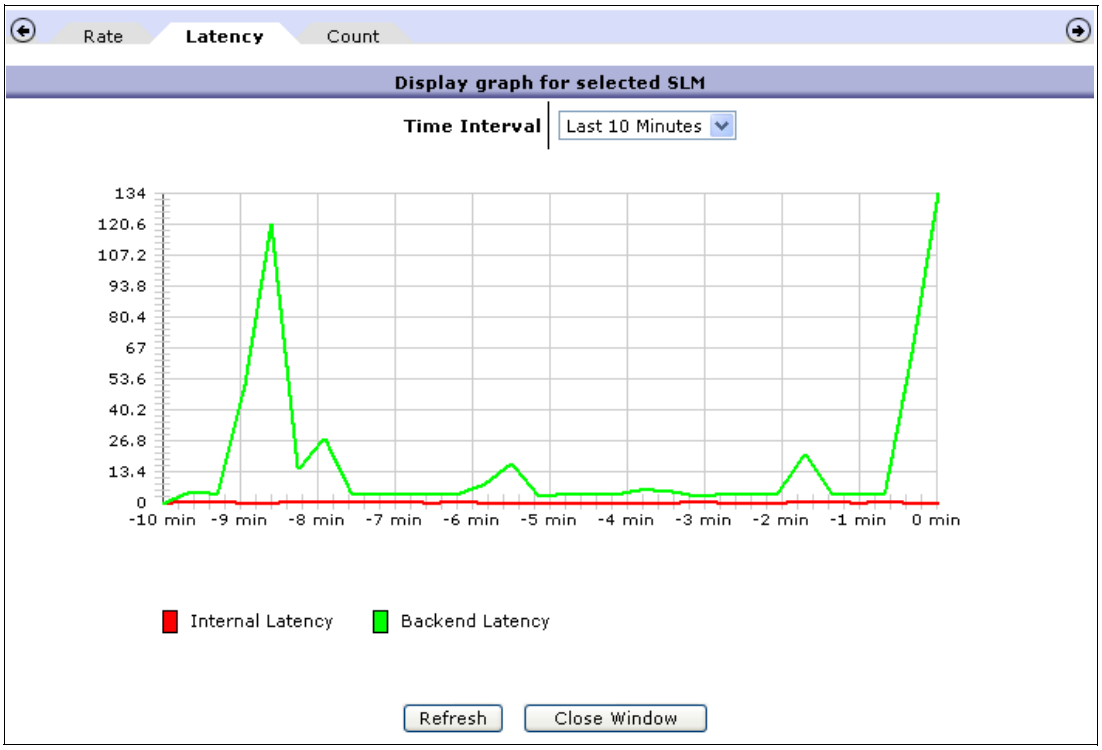


Figure 3-38 SLM Message Latency graph

Figure 3-39 shows the SLM Message Count graph.

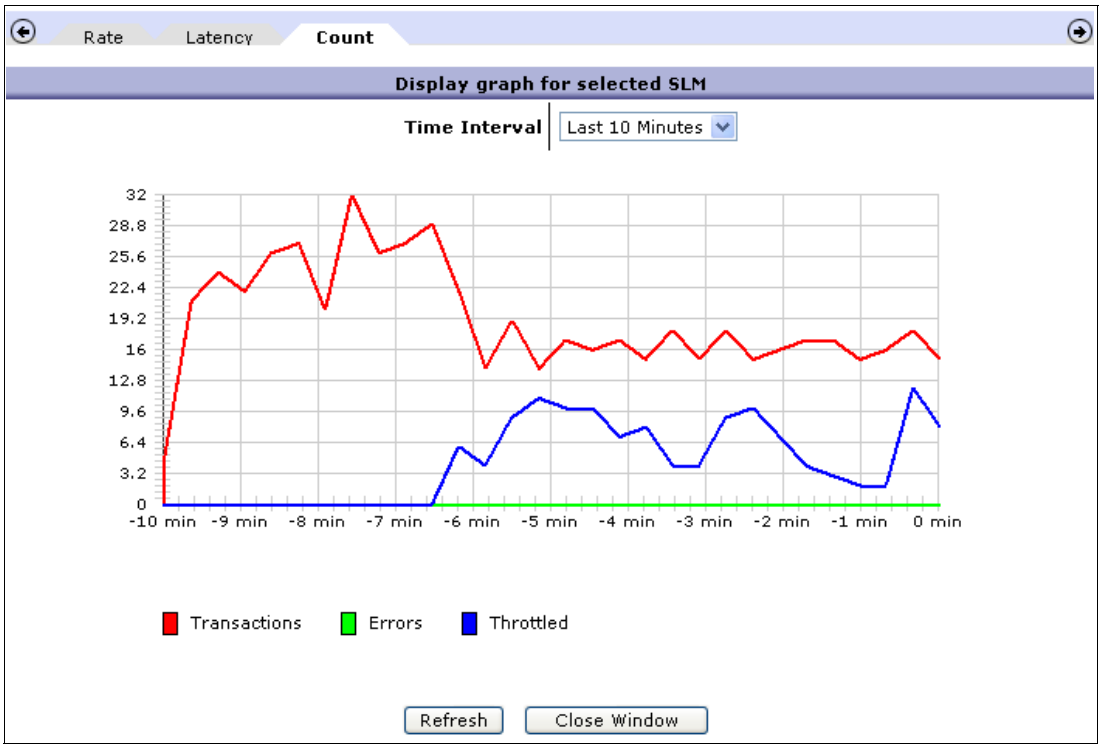


Figure 3-39 SLM Message Count graph

3.5 Summary

SLM in the DataPower appliance can be configured in different ways and with more or less fine-grained options to customize the behavior. We suggest that you decide how fine-grained and sophisticated you want to make the customization of the monitoring.

Use message count monitors and message duration monitors that are available with all main DataPower services for the basic approach. Also, use the SLM policies that are available with Web service proxy and multiprotocol gateway if you need a higher grade of customization abilities.

4

Web service proxy with WebSphere Registry and Repository

WebSphere Registry and Repository offers the following functionality:

- Provides clear visibility into service associations and relationships
- Encourages reuse of services
- Provides support for dynamic service selection and binding at run time
- Ensures service interoperability and leverages existing investments with support for open standards such as Web Services Description Language (WSDL), XML, and Universal Description Discovery and Integration (UDDI)
- Helps institute best practices and enforce policies in your service-oriented architecture (SOA) deployments
- Enables governance of the entire services life cycle

In this chapter, we explain the interaction of the DataPower device with the WebSphere Registry and Repository server to automate service maintenance. This interaction includes the following components:

- DataPower, Firmware 3.6.0.17 or later
- WebSphere Registry and Repository v6.0.0.1
- Rational Application Developer v7

Specifically in this chapter, we discuss the following topics:

- 4.1, “SOA governance” on page 100
- 4.2, “WebSphere Service Registry and Repository” on page 101
- 4.3, “A sample scenario” on page 102
- 4.4, “Summary” on page 129

© Copyright IBM Corp. 2008. All rights reserved.

4.1 SOA governance

SOA increases the level of cooperation and coordination that is required between business and information technology (IT), as well as among IT departments and teams. This cooperation and coordination is provided by SOA governance, which covers the tasks and processes for specifying and managing how services and SOA applications are supported.

In general, *governance* means establishing and enforcing how a group agrees to work together. Specifically, there are two aspects to governance:

- Establishing chains of responsibility, authority, and communication to empower people, determining who has the rights to make what decisions
- Establishing measurement, policy, and control mechanisms to enable people to carry out their roles and responsibilities

Governance is distinct from management in the following ways:

- Governance determines who has the authority and responsibility for making the decisions.
- Management is the process of making and implementing the decisions.

Governance defines what should be done, while management ensures that it gets done.

A more specific form of governance is *IT governance*, which entails the following actions:

- Establishes decision-making rights associated with IT
- Establishes mechanisms and policies that are used to measure and control the way IT decisions are made and carried out

IT governance is about who is responsible for what in an IT department and how the department knows those responsibilities are being performed.

SOA adds the following unique aspects to governance:

- Acts as an extension of IT governance that focuses on the life cycle of services to ensure the business value of SOA
- Determines who should monitor, define, and authorize changes to existing services within an enterprise

Governance becomes more important in SOA than IT in general. In SOA, service consumers and service providers run in different processes. They are developed and managed by different departments and require a lot of coordination to work together successfully. For SOA to succeed, multiple applications must share common services, which means they need to coordinate on how to make those services common and reusable. These are governance issues, and they are much more complex than in the days of monolithic applications or even reusable code and components.

As companies use SOA to better align IT with the business, they can ideally use SOA governance to improve overall IT governance. Employing SOA governance is key if companies are to realize the benefits of SOA. For SOA to be successful, SOA business and technical governance is not optional. It is required.

4.2 WebSphere Service Registry and Repository

IBM WebSphere Service Registry and Repository is a tool that enables better management and governance of your services. It does this through its registry and repository capabilities and its integration with the IBM SOA Foundation.

WebSphere Registry and Repository enables you to store, access, and manage information about services and service interaction endpoint descriptions (referred to as service *metadata*) in an SOA. This information is used to select, invoke, govern, and reuse services as part of a successful SOA.

This service information includes traditional Web services that implement WSDL interfaces with SOAP/HTTP bindings. It also includes a broad range of SOA services that can be described by using WSDL, XML Schema Definition (XSD), and policy decorations, but might use a range of protocols and be implemented according to a variety of programming models.

More information: For more information about the IBM SOA programming model and how it relates to the notion of service, see *SOA programming model for implementing Web services, Part 1: Introduction to the IBM SOA programming model* on the Web at the following address:

`http://www.ibm.com/developerworks/webservices/library/ws-soa-progmodel/`

You can use WebSphere Service Registry and Repository to store information about services in your systems or in other organizations' systems that you already use, plan to use, or want to be aware of. For example, an application can check with WebSphere Registry and Repository just before it invokes a service to locate the most appropriate service that satisfies its functional and performance needs. This capability helps make an SOA deployment more dynamic and more adaptable to changing business conditions.

WebSphere Service Registry and Repository includes the following components:

- A *service registry* that contains information about services, such as the service interfaces, its operations, and parameters
- A *metadata repository* that has the robust framework and extensibility to suit the diverse nature of service usage

As the integration point for service metadata, WebSphere Service Registry and Repository establishes a central point for finding and managing service metadata acquired from a number of sources. Such sources include service application deployments and other service metadata and endpoint registries and repositories, such as UDDI. It is where service metadata that is scattered across an enterprise is brought together to provide a single, comprehensive description of a service. When this happens, visibility is controlled, versions are managed, proposed changes are analyzed and communicated, and usage is monitored. In addition, other parts of the SOA foundation can access service metadata with the confidence that they have found the copy of record.

WebSphere Service Registry and Repository does not manage all service metadata, and it does not manage service metadata across the whole SOA life cycle. It focuses on a minimalist set of metadata that describes capabilities, requirements, and the semantics of deployed service endpoints. It interacts and federates with other metadata stores that play a role in managing the overall life cycle of a service.

In summary, WebSphere Service Registry and Repository offers the following benefits:

- Provides awareness of service associations and relationships while encouraging reuse of services to avoid duplication and reduce costs
- Enhances connectivity with dynamic service selection and binding at run time
- Enables governance of services throughout the service life cycle
- Ensures interoperability of services with a registry and repository built on open standards

  You can use other standard registries and repositories to ensure a unified view across a variety of service information sources.
- Helps institute best practices and enforce policies in SOA deployments

More information: For more information about WebSphere Service Registry and Repository, see *WebSphere Service Registry and Repository Handbook*, SG24-7386.

4.3 A sample scenario

Interaction with WebSphere Registry and Repository must be done from a Web service proxy in a DataPower device. We have already developed the core scenario in the previous chapters by using a multiprotocol gateway. In this section, we use a new back-end application that is running in WebSphere Application Server for the sake of simplicity, rather than convert the core scenario to a Web service proxy. This new sample service is called *GetPrimes*.

GetPrimes: GetPrimes is a simple Web service that generates prime numbers.

Figure 4-1 on page 103 illustrates the sample scenario and describes two separate interactions:

- The request/response dataflow, numbered 1 to 4
- The asynchronous interaction with WebSphere Registry and Repository, shown as A and B

  This interaction takes place automatically at a preset interval of time.

As shown the Figure 4-1, the scenario includes five components:

- Web services client
- DataPower device
- WebSphere Registry and Repository server
- Web services server
- WebSphere Request and Response messages

The request/response flow is executed as follows:

1. The Web services client sends a request message to the DataPower device.
2. Based on information from the registry, the DataPower device sends a request to the Web services server.
3. The Web services server sends the response to the DataPower device.
4. The DataPower device sends the response to the Web services client.

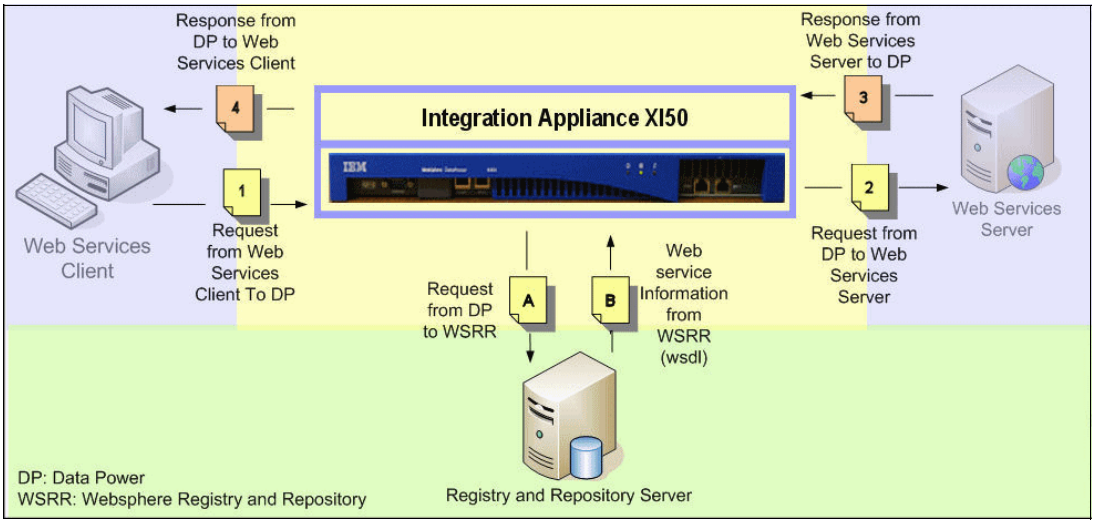


Figure 4-1 Scenario of using a Web service proxy with WebSphere Registry and Repository

The asynchronous interactions A and B occur independently of the request or response interaction as follows:

1. DataPower uses *concept information* to invoke the WebSphere Registry and Repository to obtain the parameters about the Web service server, including the location.
2. Based on the concept parameter, WebSphere Registry and Repository looks for a WSDL file and other details of the Web service and sends the information to the DataPower device.

4.3.1 Registering the WSDL file

In this section, we register the WSDL file in the WebSphere Registry and Repository. Example 4-1 shows the WSDL that is used in this sample scenario. This WSDL file is packaged in the additional materials, which you can download as explained in Appendix A, “Additional material” on page 131.

Example 4-1 WSDL file

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://com.itso" xmlns:impl="http://com.itso"
xmlns:intf="http://com.itso" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:wsi="http://ws-i.org/profiles/basic/1.1/xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <wsdl:types>
  <schema targetNamespace="http://com.itso"
xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <element name="getPrimeResponse">
    <complexType>
     <sequence>
      <element name="getPrimeReturn" nillable="true" type="xsd:string"/>
     </sequence>
    </complexType>
   </element>
```

```
    <element name="getPrime">
     <complexType>
      <sequence>
       <element name="numDigits" type="xsd:int"/>
      </sequence>
     </complexType>
    </element>
   </schema>
  </wsdl:types>

    <wsdl:message name="getPrimeResponse">
      <wsdl:part element="intf:getPrimeResponse" name="parameters"/>

   </wsdl:message>

    <wsdl:message name="getPrimeRequest">
      <wsdl:part element="intf:getPrime" name="parameters"/>

   </wsdl:message>

    <wsdl:portType name="Primes">
      <wsdl:operation name="getPrime">
        <wsdl:input message="intf:getPrimeRequest" name="getPrimeRequest"/>

        <wsdl:output message="intf:getPrimeResponse" name="getPrimeResponse"/>

     </wsdl:operation>

   </wsdl:portType>

    <wsdl:binding name="PrimesSoapBinding" type="intf:Primes">
  <wsaw:UsingAddressing wsdl:required="false"
 xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"/>

      <wsdlsoap:binding style="document"
 transport="http://schemas.xmlsoap.org/soap/http"/>

      <wsdl:operation name="getPrime">
        <wsdlsoap:operation soapAction="getPrime"/>

        <wsdl:input name="getPrimeRequest">
          <wsdlsoap:body use="literal"/>

       </wsdl:input>

        <wsdl:output name="getPrimeResponse">
          <wsdlsoap:body use="literal"/>

       </wsdl:output>

     </wsdl:operation>

   </wsdl:binding>

    <wsdl:service name="PrimesService">
```

```
    <wsdl:port binding="intf:PrimesSoapBinding" name="Primes">
      <wsdlsoap:address
location="http://itsolab1:9080/PrimesWebService/services/Primes"/>

    </wsdl:port>

  </wsdl:service>

</wsdl:definitions>
```

In the following steps, we assume that WebSphere Registry and Repository has been already installed. For more information about the installation steps, see *WebSphere Service Registry and Repository Handbook*, SG24-7386.

1. Verify that the WebSphere Application Server is running:
   - Open the WebSphere Registry and Repository administration console (Figure 4-2):

     `http://system-host-name:9080/ServiceRegistry`
   - If you activated WebSphere security, enter the following URL:

     `https://system-host-name:9443/ServiceRegistry`

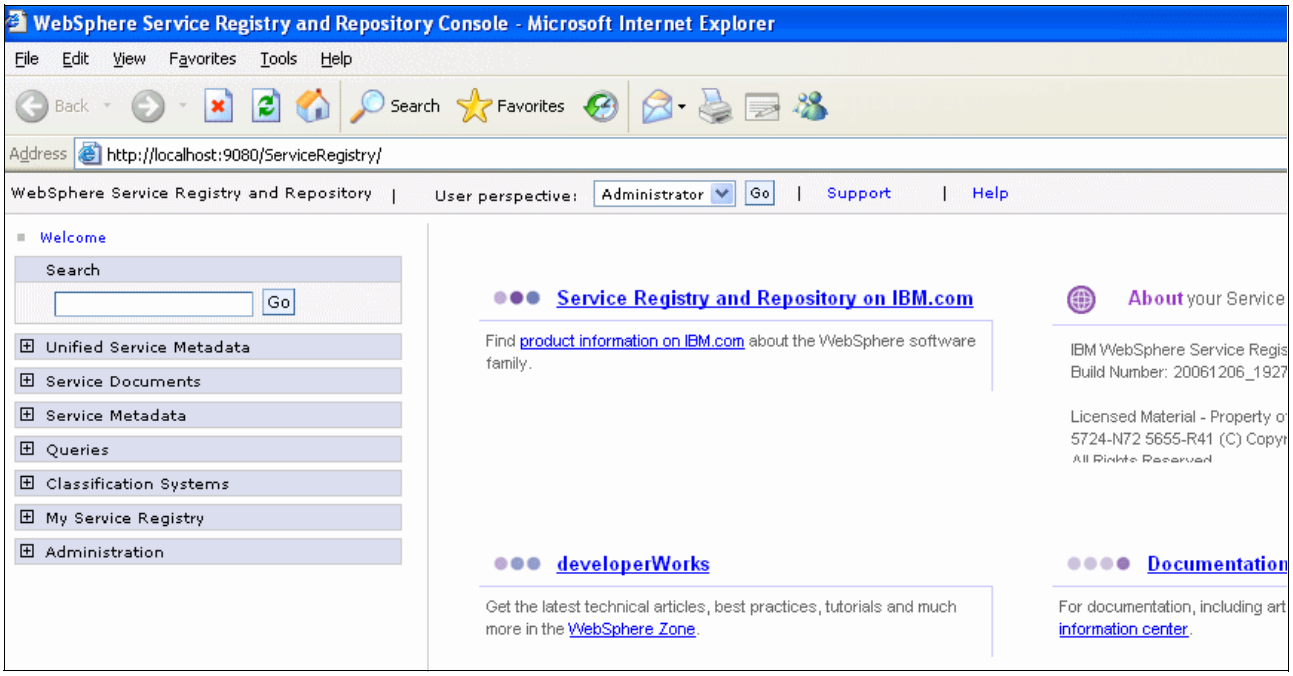


Figure 4-2 WebSphere Registry and Repository administration console

2. Load the WSDL file. From the left navigation pane, select **Services Documents** → **Load Document** (Figure 4-3).

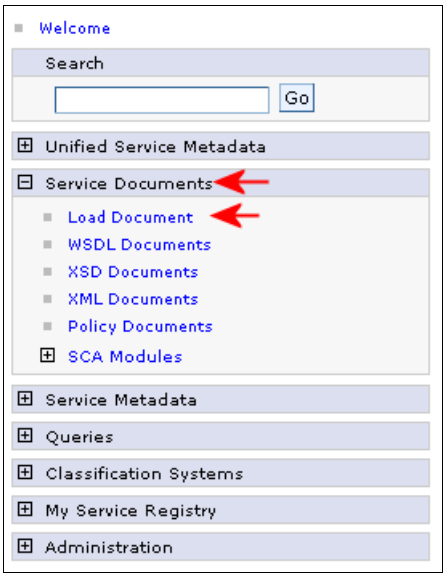


Figure 4-3 Selecting the option to load the WSDL file

3. On the Load document page (Figure 4-4), for Path to the service document, either type the path of your WSDL file or click **Browse** to find it. Then enter the values shown in Table 4-1 and click **OK**.

Table 4-1 WSDL field values

Field	Value
Document Type	WSDL
Description	*PrimeServices*
Version	1.0

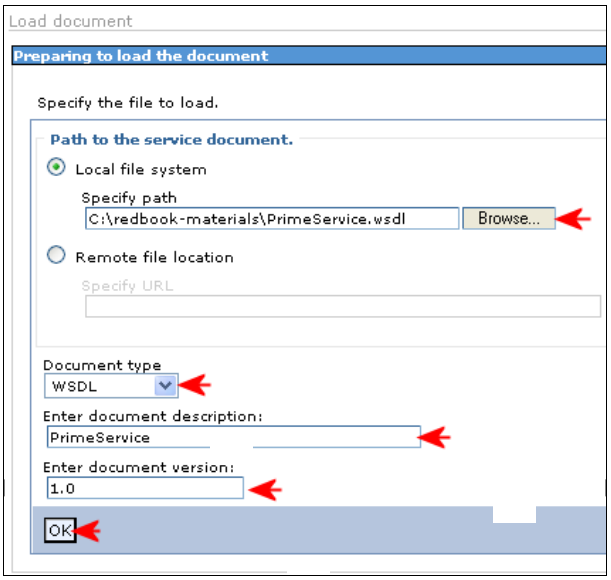


Figure 4-4 Loading the WSDL file

4. Verify that the file was loaded successfully. As shown in Figure 4-5, click **Apply** and then click **OK**.

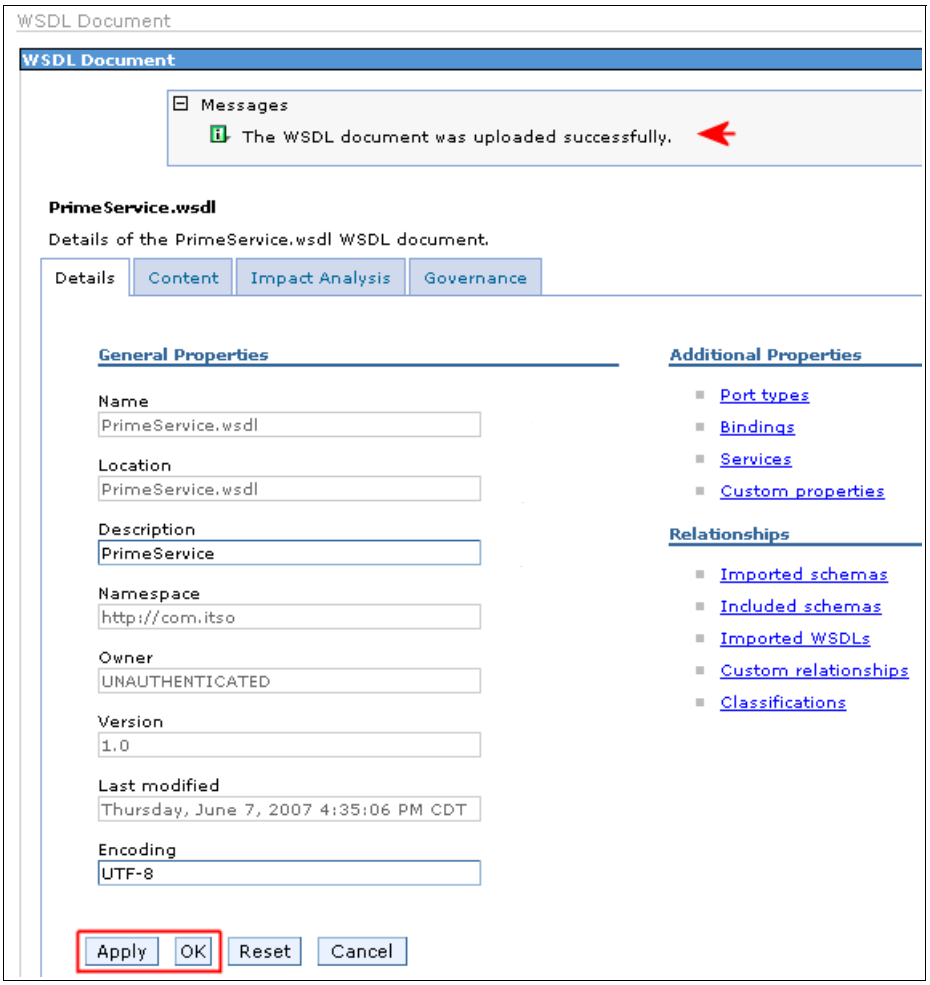


Figure 4-5 WSDL file loaded

5. From the navigation pane, select **Unified Service Metadata** → **Concepts** as shown in Figure 4-6.

> **More information:** For information about concepts, see *WebSphere Service Registry and Repository Handbook*, SG24-7386.

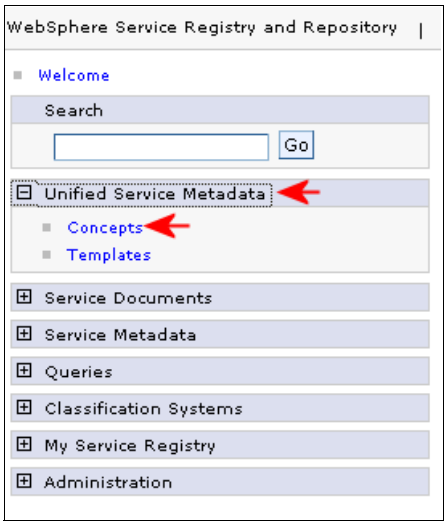


Figure 4-6 Concept navigation pane

6. On the Concepts page (Figure 4-7), click **New**.

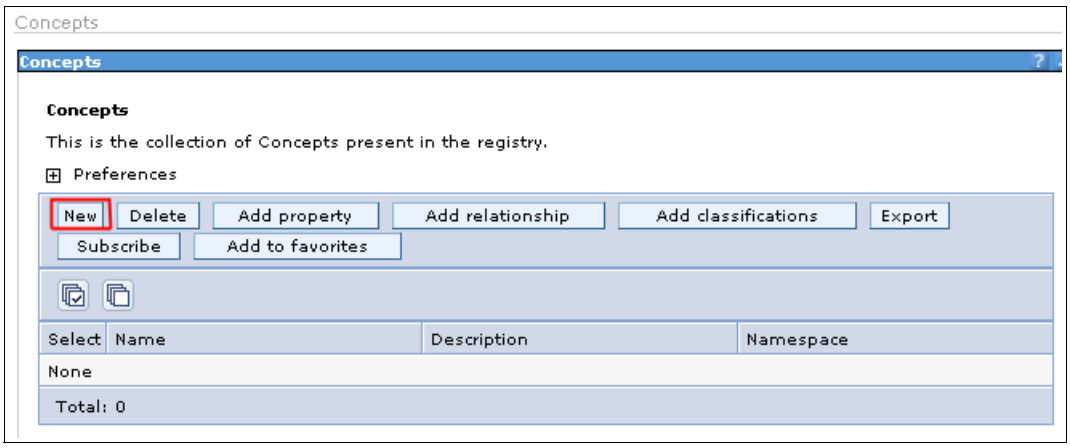


Figure 4-7 New concept

7. On the Concept page (Figure 4-8), enter the values listed in Table 4-2. Click **Apply** and then click **OK**.

Table 4-2 New concepts parameters

Field	Value
Name	PrimeService
Description	PrimeServiceConcept
NameSpace	www.ibm.com/datapower/
Version	1.0

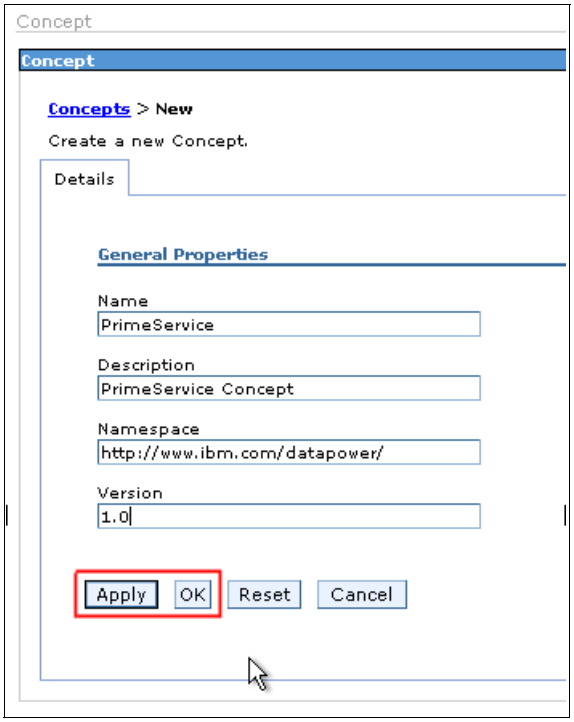


Figure 4-8 New concepts values

8. Back on the Concepts page (Figure 4-9), select the new concept. Click **PrimeService**.

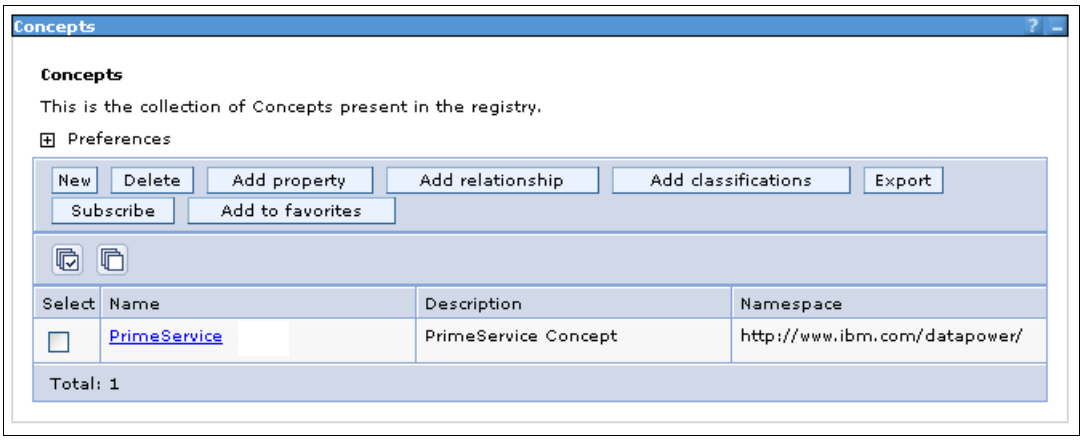


Figure 4-9 PrimeService concept

9. On the Details tab of the next page, click the **Custom relationships** link on the right under Relationships.

> **More information:** For information about Custom Relationships, see *WebSphere Service Registry and Repository Handbook*, SG24-7386.

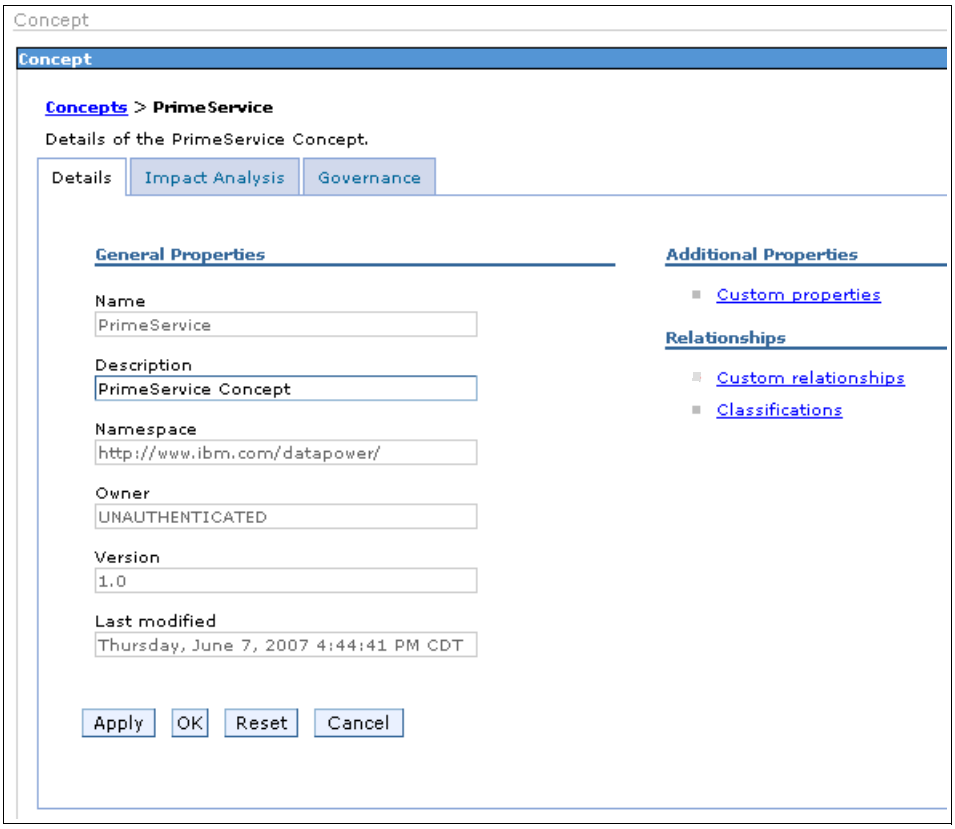


Figure 4-10 Custom relationships link

10. On the Custom Relationships page (Figure 4-11), click **New**.

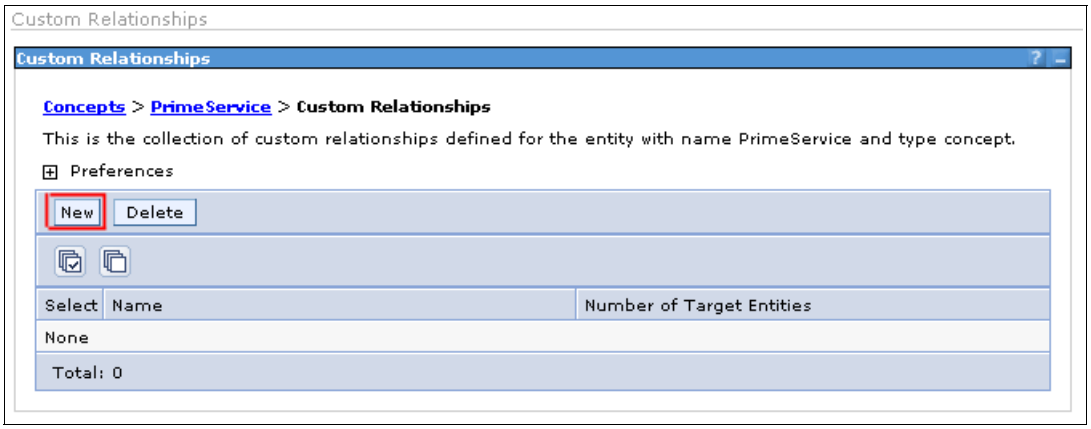


Figure 4-11 New custom relationships

11. On the Create relationship page (Figure 4-12), in the relationship name field, enter `PrimeService`. Click **Next**.

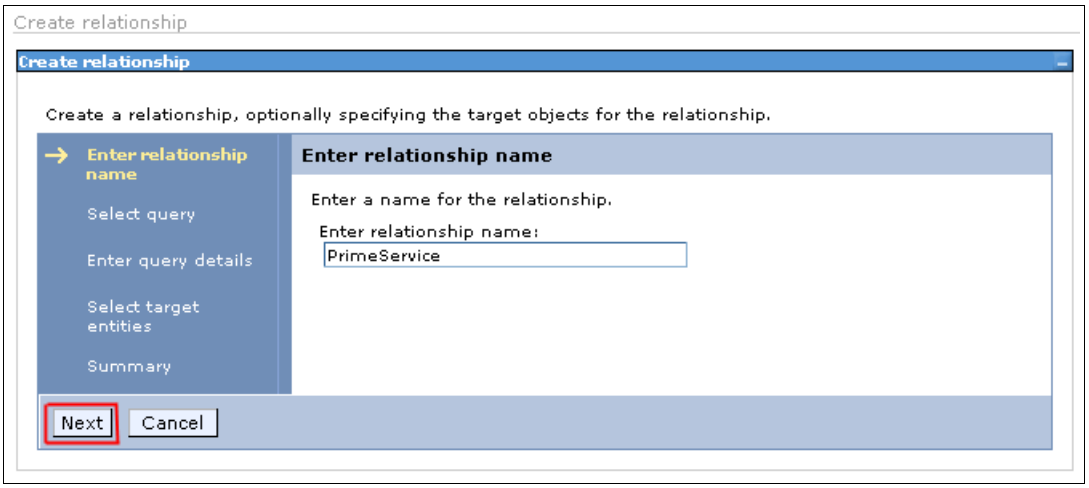


Figure 4-12 Relationship name

12. On the next page (Figure 4-13), in the query field, select **WSDL Documents**. Click **Next**.

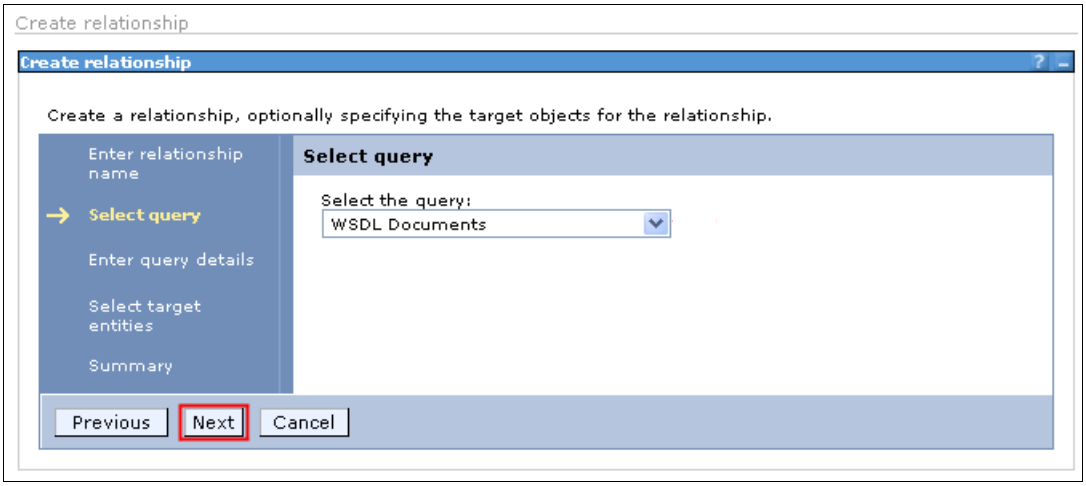


Figure 4-13 Create relationship page - Select query section

13. On the next page (Figure 4-14) under Enter query details, for Query: WSDL Documents, select **Use any of the following (OR)**. For Name, type `PrimeService.wsdl`. Click **Next**.

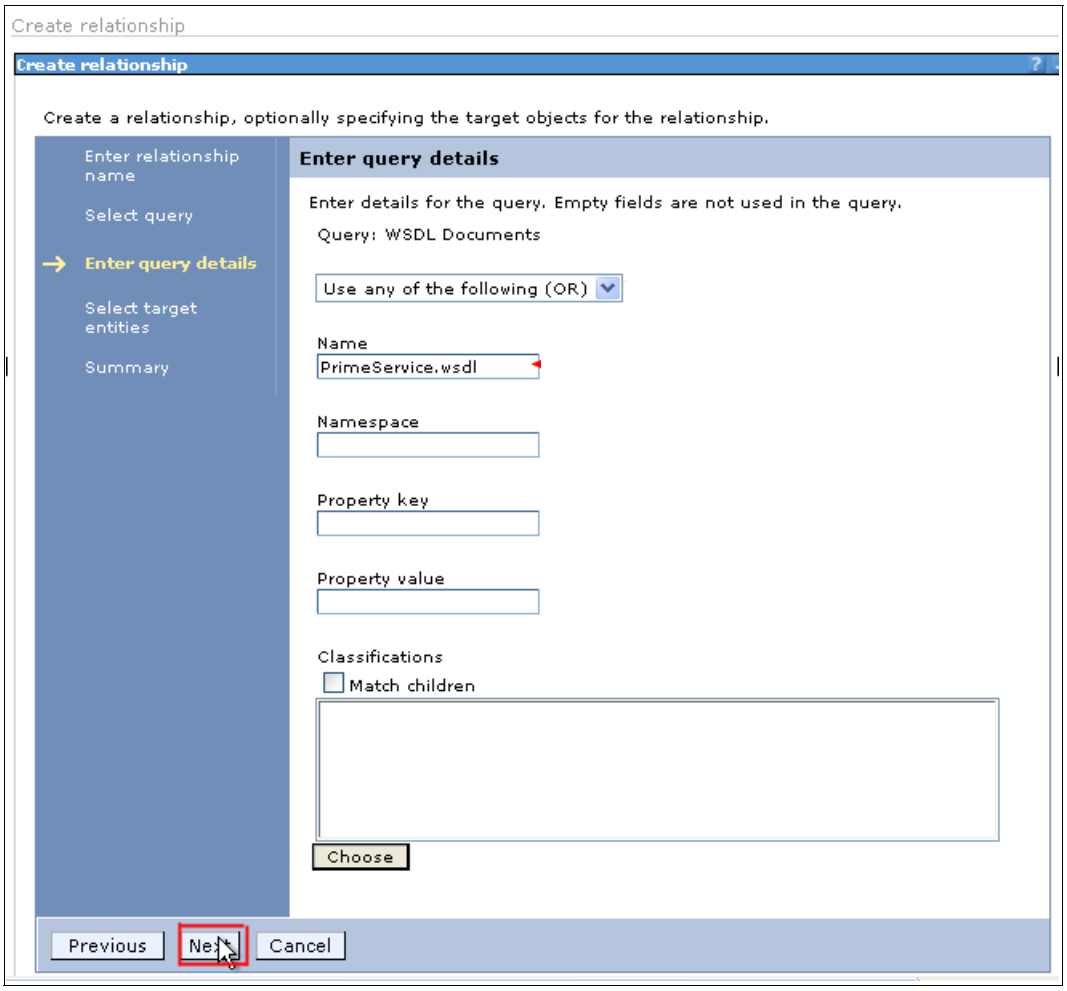


Figure 4-14 Create relationship page - Enter query details section

14. The query returns the WSDL file as shown in Figure 4-15. Select the file and click **Next**.

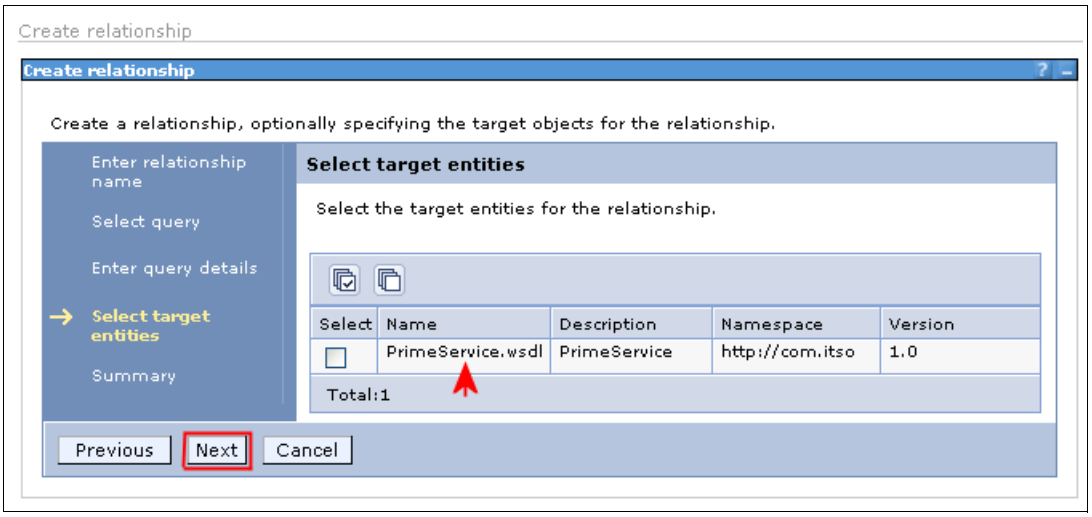


Figure 4-15 Create relationship page - Select target entities section

15. The WebSphere Registry and Repository displays a relationship summary between the concept and the WSDL file as shown in Figure 4-16. Click **Finish**.

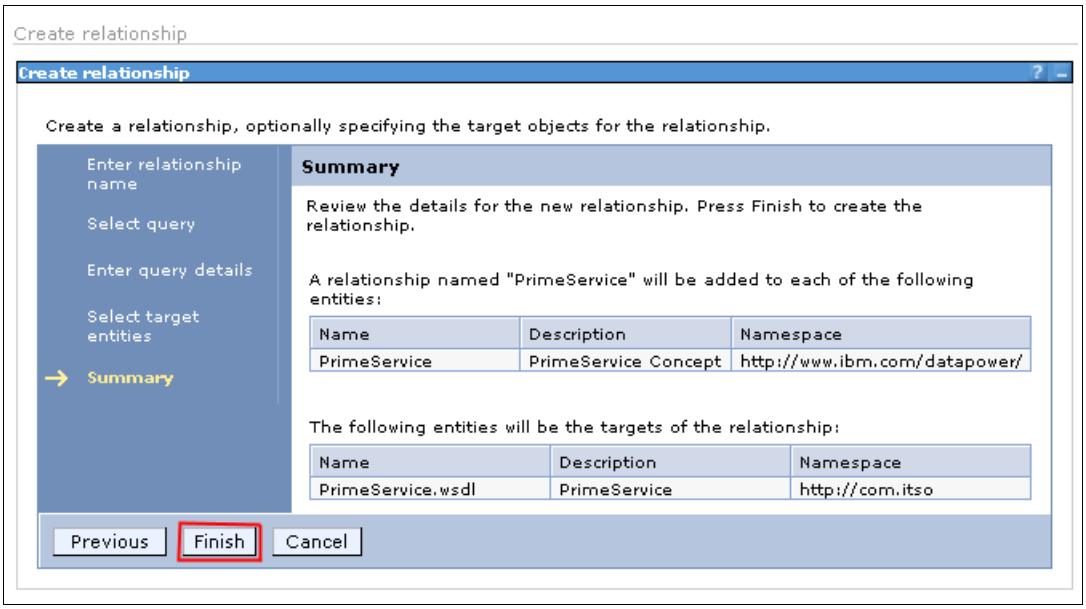


Figure 4-16 Relationship summary

16. Close the WebSphere Registry and Repository console administration.

4.3.2 Configuring a Web service proxy

In this section, we explain how to create a Web Services Proxy (WS-Proxy) in the DataPower device. By using the WSDL file or files that describe the proxy service, a Web service proxy offers near automatic configuration. In addition to all the standard support of a DataPower firewall, WS-Proxy helps to simplify the implementation of service level monitoring (SLM) capabilities at different levels of the Web service such as operation and port.

Configure the DataPower device to work with WebSphere Registry and Repository:

1. Start the DataPower console administration.
2. From the DataPower device console, select **Control Panel**. In the Services section, click **Web Service Proxy** as shown in Figure 4-17.

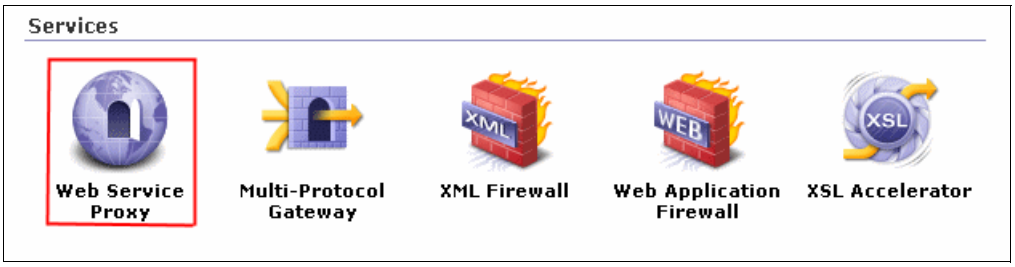


Figure 4-17 Web Services Proxy

3. On the Configure Web Service Proxy page (Figure 4-18), click the **Add** button to add a new Web service proxy.

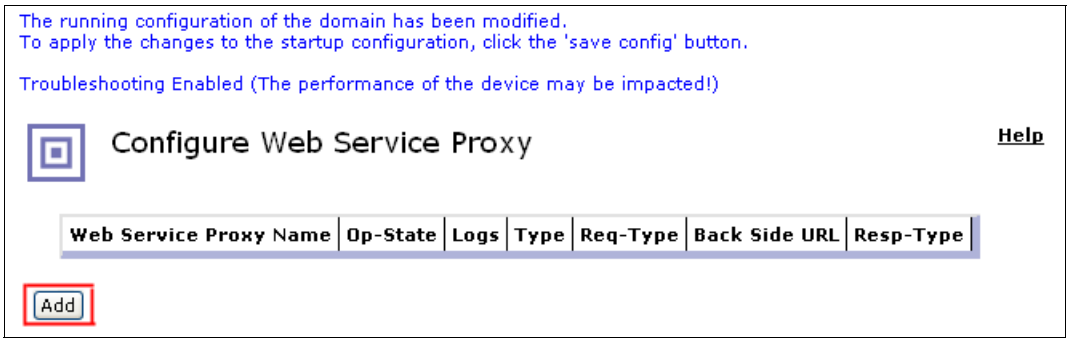


Figure 4-18 Adding a Web service proxy

4. Click the **WSDLs** tab (Figure 4-19). In the Web Service Proxy Name field, enter a name, for example `PrimeServiceProxy`. Then select **Add WSRR Subscription**.

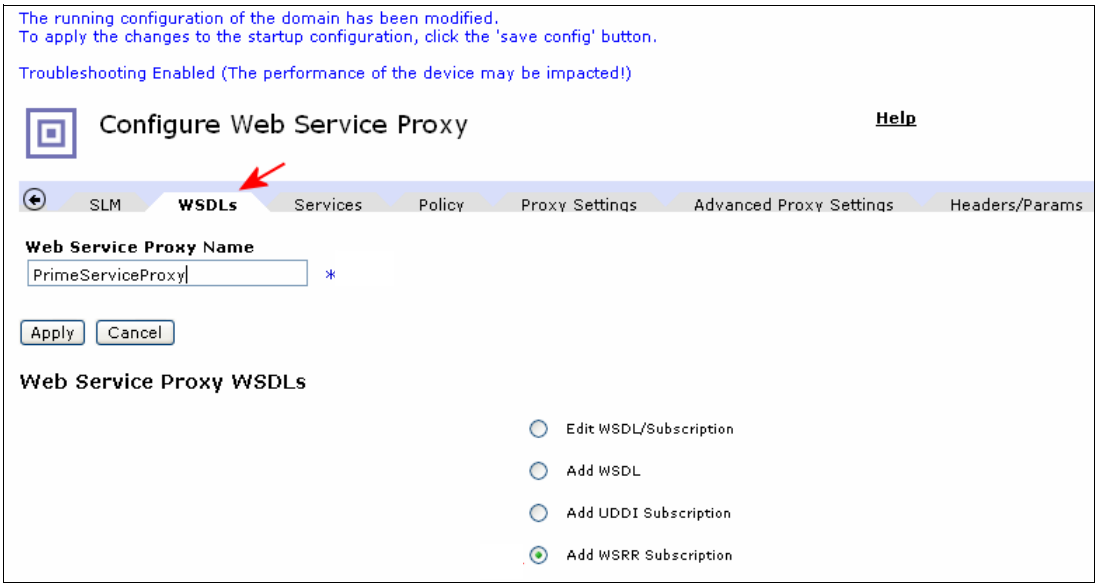


Figure 4-19 WSDLs page

5. In the WSRR Subscription Parameters section (Figure 4-20 on page 115), enter the parameter values as listed in Table 4-3.

Table 4-3 WSRR Subscription Parameters

Field	Values
WSRR Subscription Name	*PrimeServiceSubscription*
Subscription Object	*Concept*
Object Name	*PrimeService*
Namespace	http://www.ibm.com/datapower/
Refresh Interval	60

Then under WSRR Server, click the plus sign (**+**) button to create a new WSRR server.

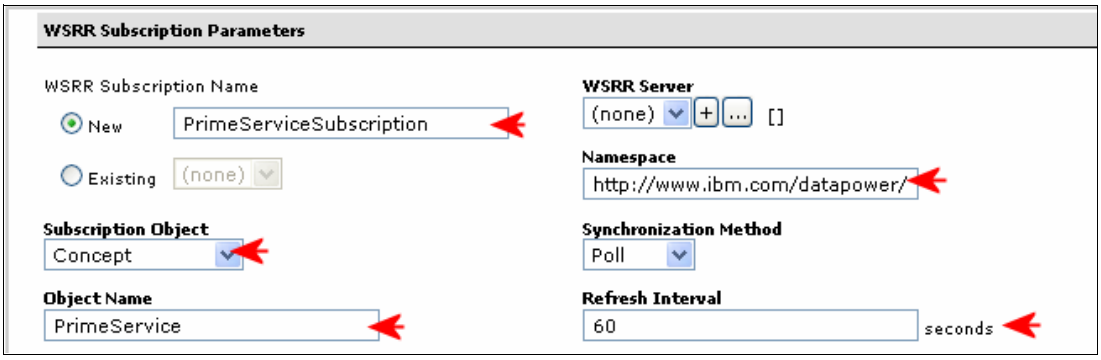


Figure 4-20 WSRR Subscription Parameters

6. On the Main page (Figure 4-21), in the Name field, enter a name, for example `myWSRR`. In the SOAP URL field, enter the following URL:

   `http://dp_wsrr:9080/WSRRCoreSDO/services/WSRRCoreSDOPort`

   Click **Apply**.

   Note: Select the proper port number, IP address, and host name in your environment.

Figure 4-21 WSRR server parameters

7. Under Local (Figure 4-22), create a new local endpoint. For Local Endpoint Handler, click the **+** button and select **HTTP Front Side Handler**.

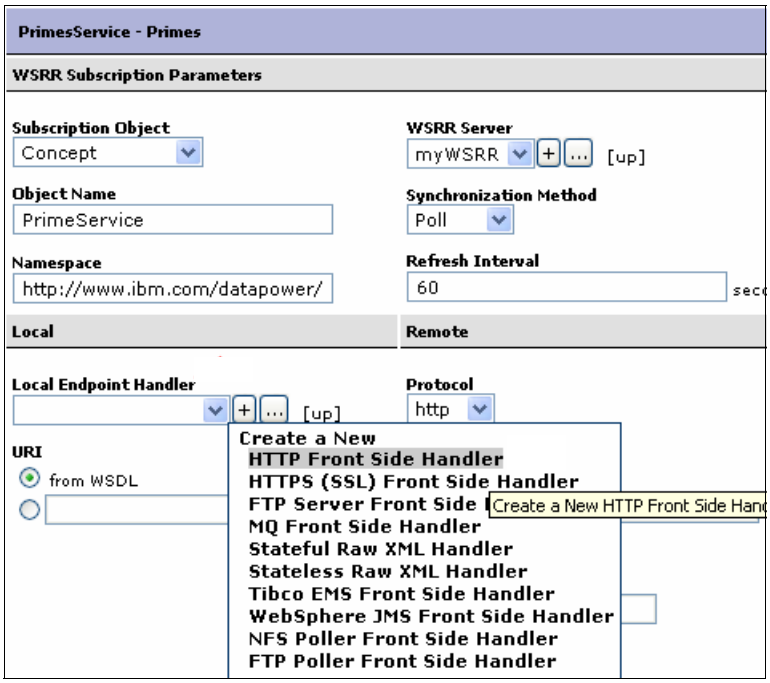


Figure 4-22 New Local Endpoint Handler

8. On the HTTP Front Side Handler page (Figure 4-23), enter the values for the new front side handler. In the Name field, enter a name, for example `PrimeServiceProxyFSH`. Change the port number to `7070`. Click **Apply**.

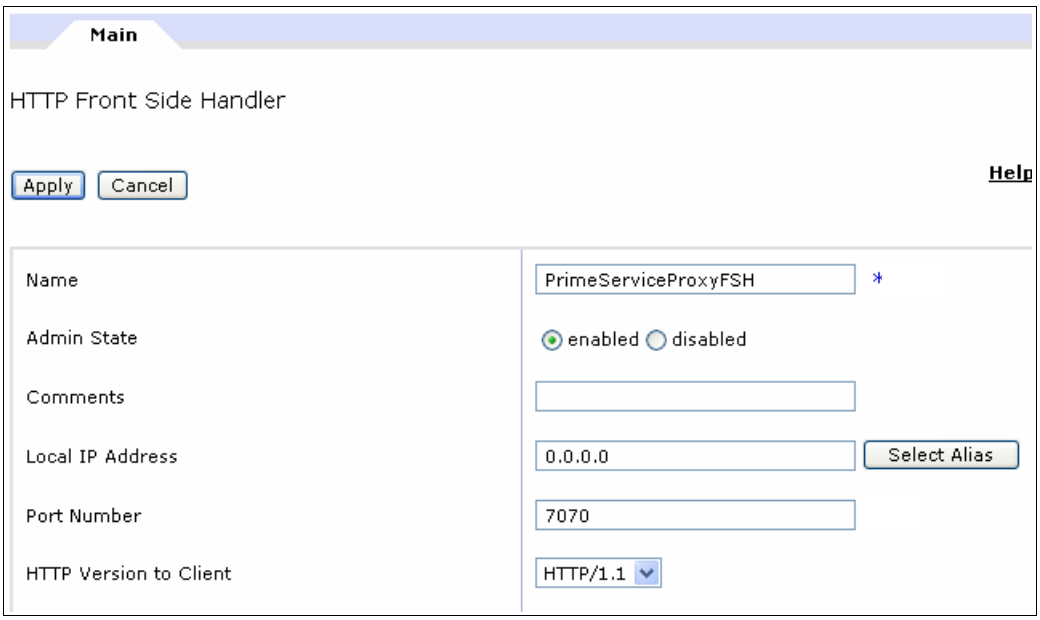


Figure 4-23 HTTP Front Side Handler parameters

9. In the Remote section (Figure 4-24), all parameters remain as default values for this scenario. Click **Apply**.

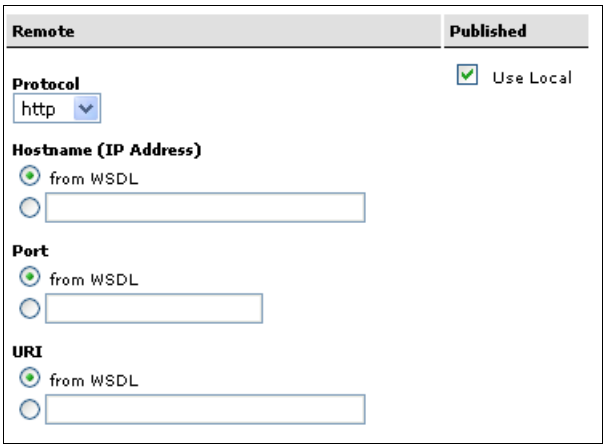


Figure 4-24 Remote section parameters

10. When the configuration process finishes, verify that the Web service proxy status is *Okay* as shown in Figure 4-25.

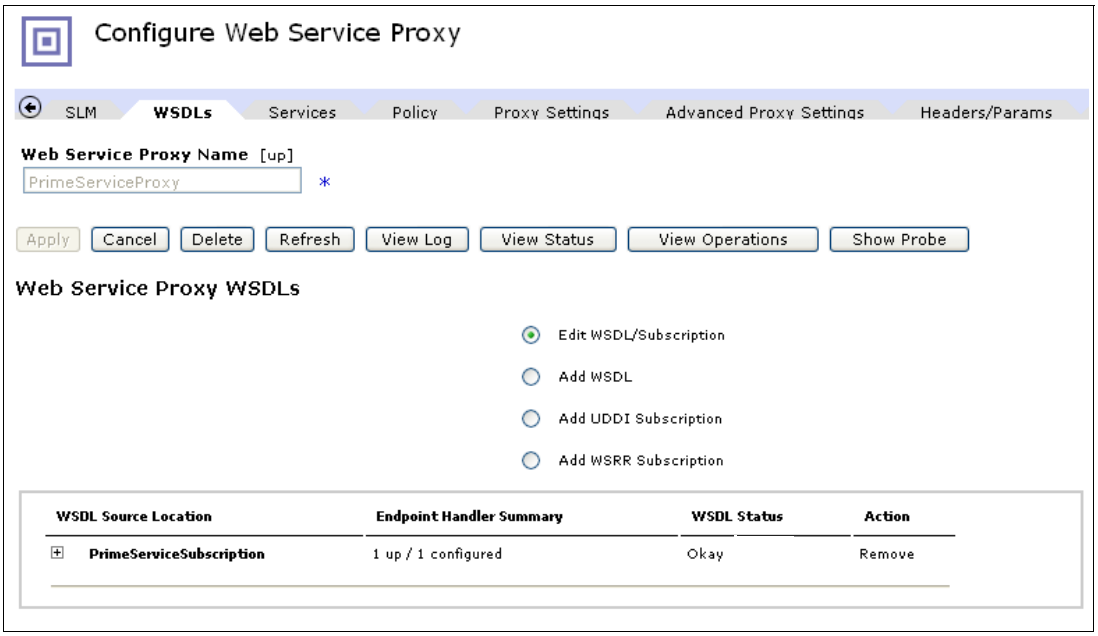


Figure 4-25 Configuring the Web service proxy status

11. Add an SLM rule. Click the **SLM** tab. You can define the following types of service level monitors and assign a service level monitor to the current Web service proxy from the Configure Web Service Proxy page (WSDLs):
    - A global SLM that monitors all Web service proxy transactions
    - A WSDL-specific SLM that monitors all services described in a specific WSDL file
    - A service-specific SLM that monitors a single Web service
    - A port-specific SLM that monitors a single Web service port
    - An operation-specific SLM that monitors a single Web service operation
    - A custom SLM that provides more precise control of monitored transactions

a. Expand **PrimeServiceProxy** as shown in Figure 4-26.

b. For PrimeServiceSubscription, add an SLM rule. Enter the following values for this scenario:

   i. In the Action field, select **throttle**.
   ii. In the Interval field, enter 10.
   iii. In the Limit field, type 1.
   iv. Click **Apply** and then click **Save Config**.

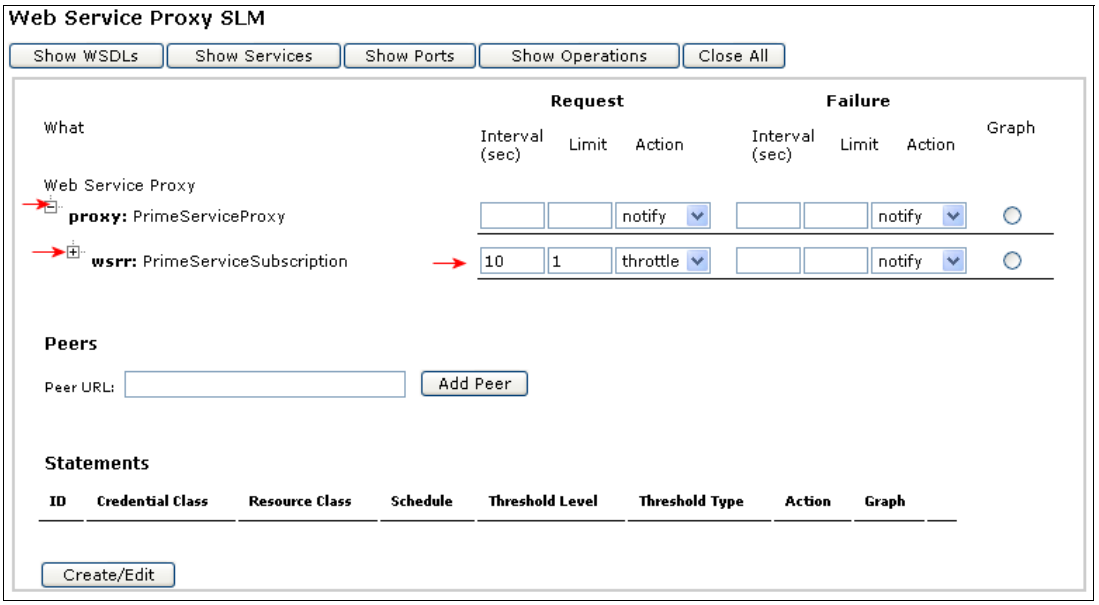


Figure 4-26 SLM rule parameters

With this SLM setup, the WS-Proxy allows up to one request every 10 seconds.

4.3.3 Creating a host alias

Using a host alias for your WebSphere Registry and Repository server is optional. If you want to use names instead of an IP address, you can create host aliases in the default domain as explained in the following steps:

1. Log in to the DataPower console as shown in Figure 4-27.

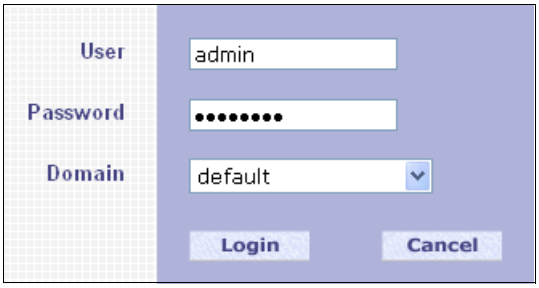


Figure 4-27 Signing in to the DataPower device

2. In the navigation pane, select **Network** → **Host Alias** as shown in Figure 4-28.

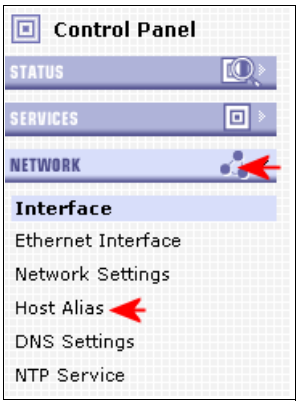


Figure 4-28 Selecting the Host Alias option

3. On the Main tab in the Host Alias section (Figure 4-29), click **Add**. Enter the required field values. You must enter the proper IP address of your WebSphere Registry and Repository server. Click **Apply**.

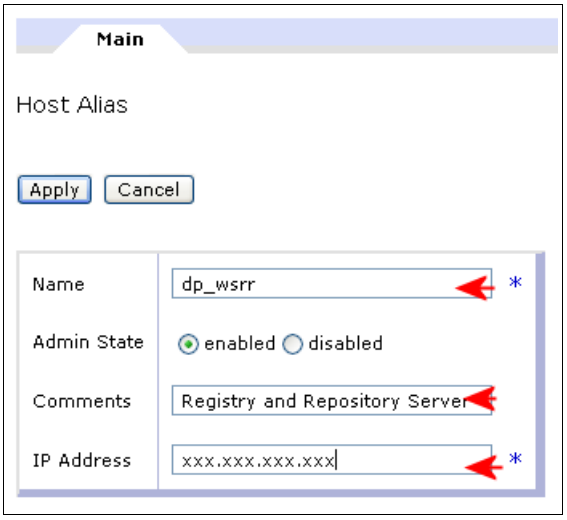


Figure 4-29 Host Alias values

4.3.4 Verifying the connectivity

As an option, you can also verify the connectivity as explained in the following steps:

1. In the DataPower console, click **Control Panel**. In the Monitoring and Troubleshooting section, click **Troubleshooting** as shown in Figure 4-30.

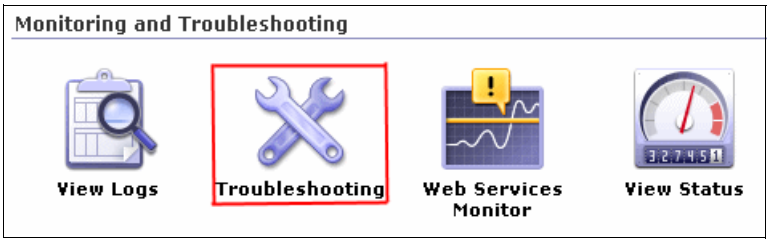


Figure 4-30 Selecting the Troubleshooting icon

2. On the Troubleshooting Panel page, click the **Main** tab (Figure 4-31). Under the Networking section, in the Remote Host field, enter `dp_wsrr`. Click **Ping Remote**.

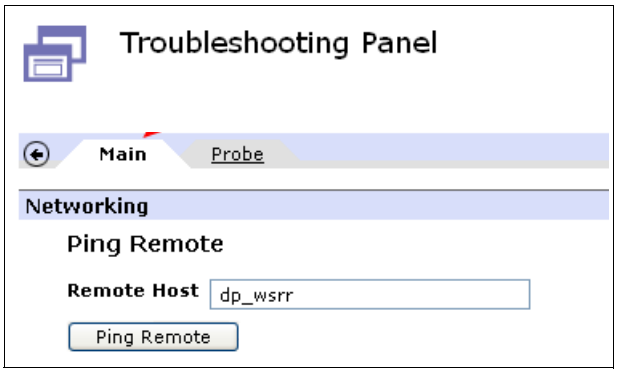


Figure 4-31 Troubleshooting panel

3. Confirm the task and check the ping results as shown in Figure 4-32.

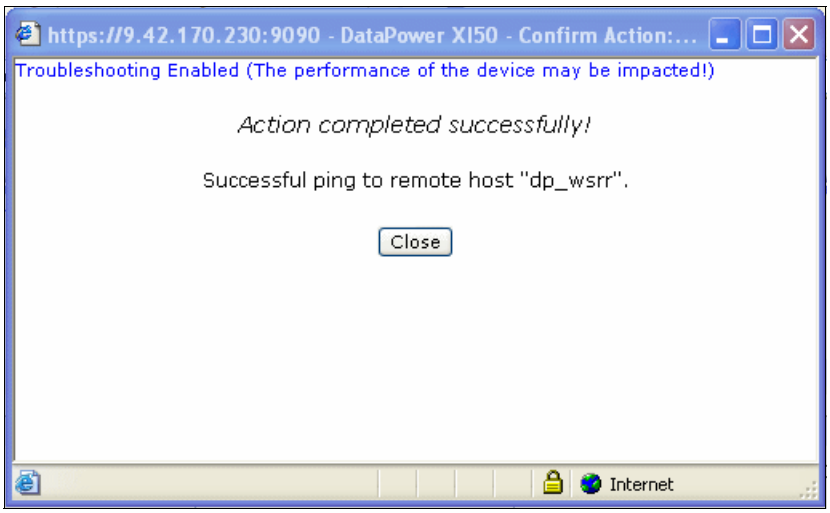


Figure 4-32 Ping results

4.3.5 Verifying a transaction result by using the Probe section

As an option, you can use the probe to verify a transaction result when a transaction is executed in the DataPower device. This allows you to follow the transaction process step by step:

1. In the Troubleshooting panel (Figure 4-31), click the **Probe** tab.
2. Under the Web Service Proxy section (Figure 4-33), select the Web service proxy, which in this scenario is **PrimeServiceProxy**. Click **Add Probe**.

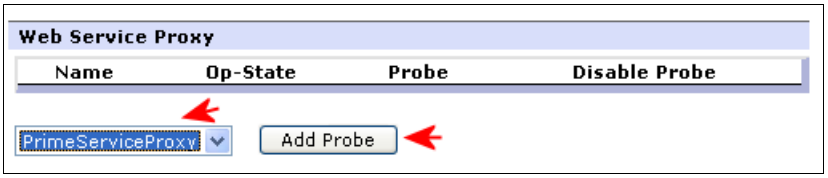


Figure 4-33 Probe - Adding a probe

3. In the confirmation window that opens, click **Close**.
4. As shown in Figure 4-34, the Web Service Probe indicates an operational status of *up*. To see the results, click the **magnifying glass** icon.

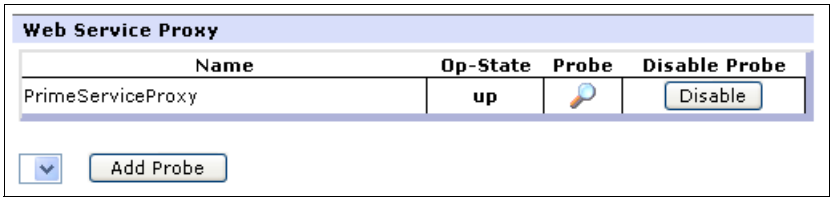


Figure 4-34 Web Service Proxy Probe status

4.3.6 Executing the scenario

You must configure the Web services client. In this scenario, Rational Application Developer is used as a Web services client. You begin by adding a new binding to invoke the service through the DataPower device:

1. In Web Services Explorer (Figure 4-35), select **PrimesSoapBinding** and click **Add**.

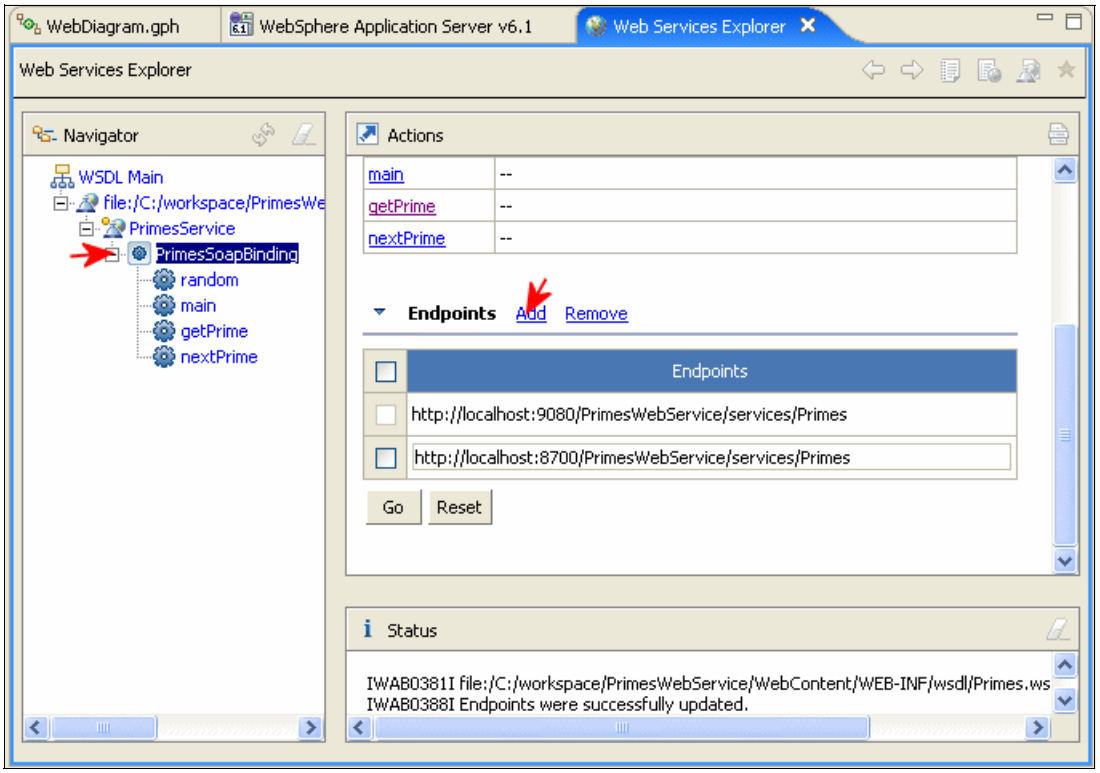


Figure 4-35 Adding a binding

2. Modify the new binding address. Use the DataPower IP address or edit the host file and use a name for the device. This scenario has the following binding address:

   `http://dp_box:7070/PrimesWebService/services/Primes`

3. Select the binding and click **Go** as shown in Figure 4-36.

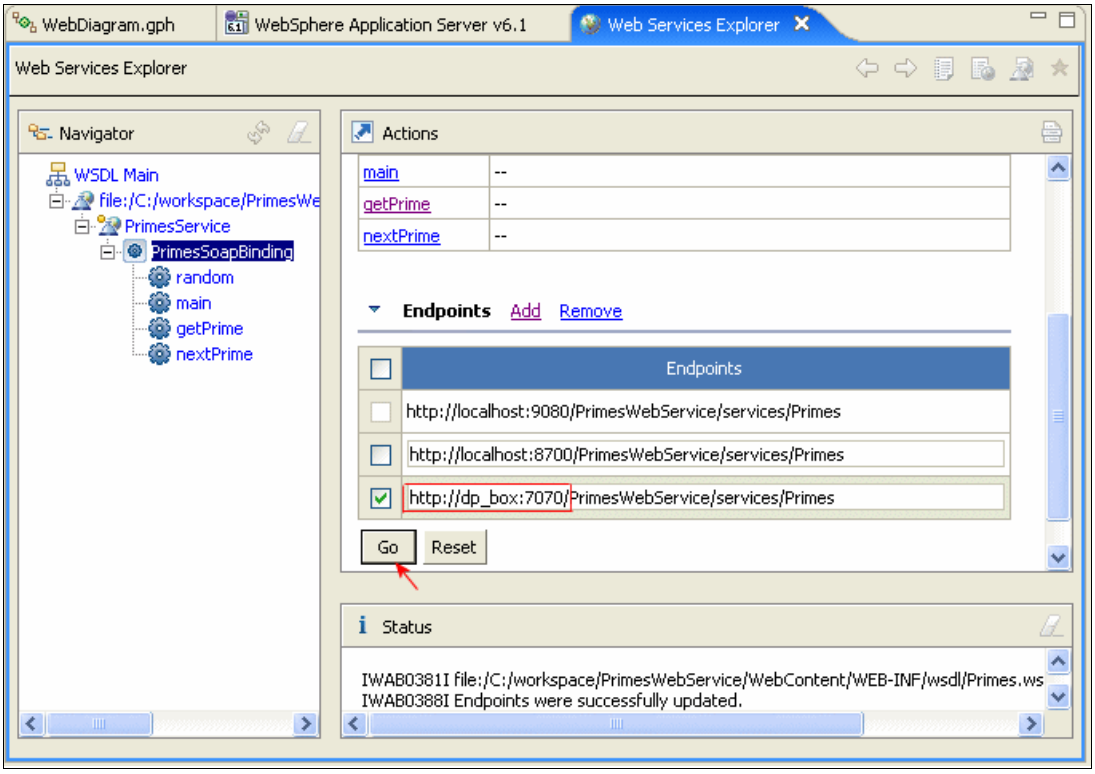


Figure 4-36 New binding address

4. Select the new binding to execute the Web service as shown in Figure 4-37.

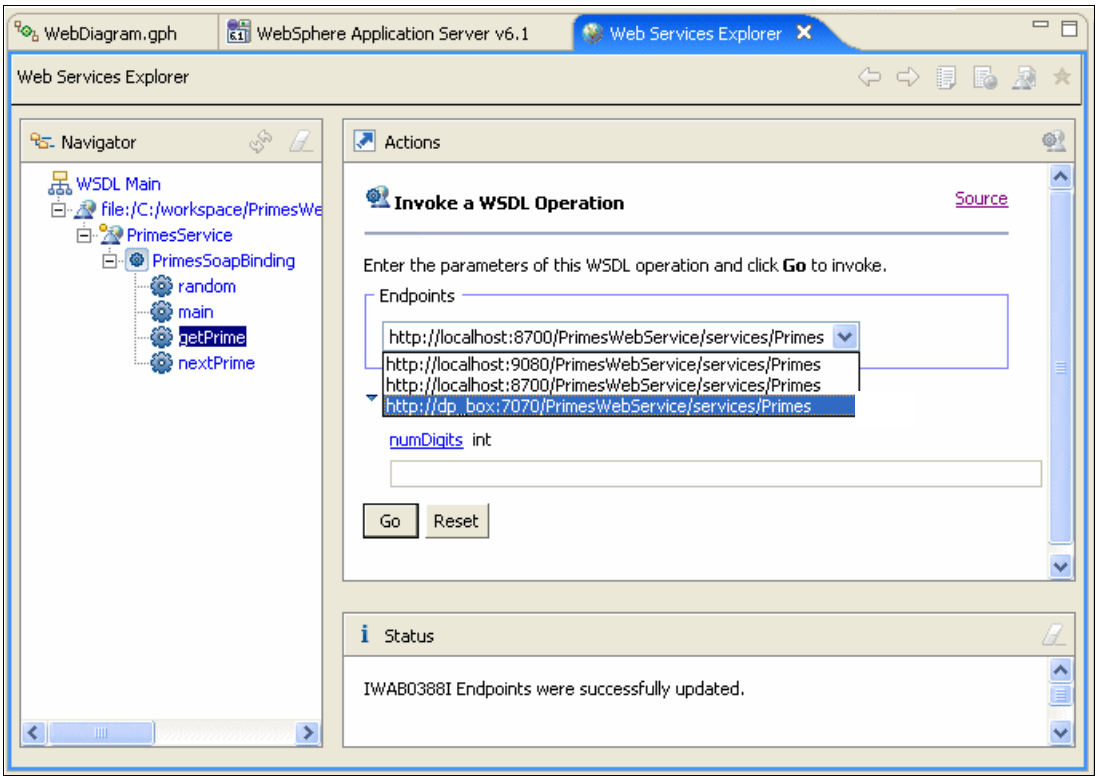


Figure 4-37 New binding selection

5. Enter a number required by the Web service application and click **Go** as shown in Figure 4-38.

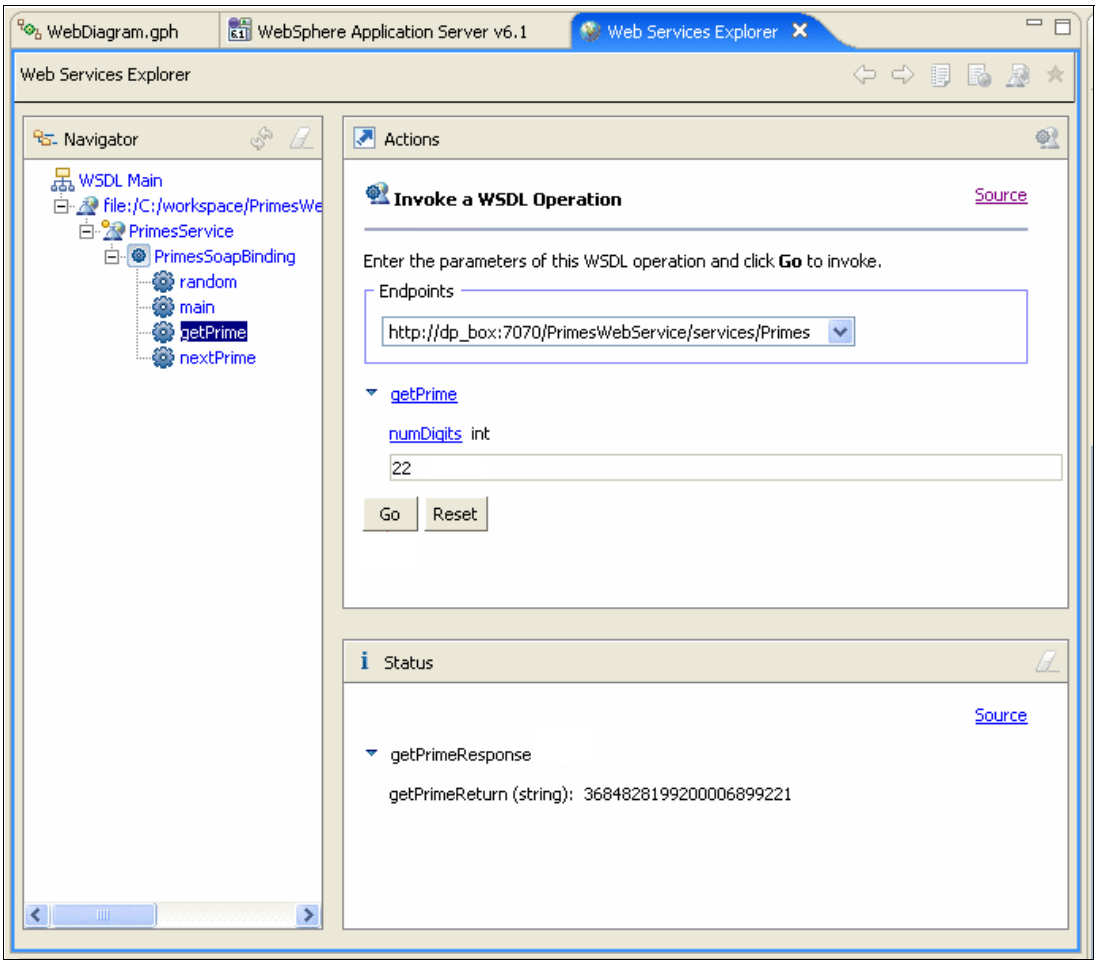


Figure 4-38 Web service execution

6. To trace the flow of the request or response, go to Web Service Proxy Probe Tool on the Troubleshooting page. Click the **magnifying glass** icon and verify the results.

   The probe displays the request and response messages as shown in Figure 4-39.

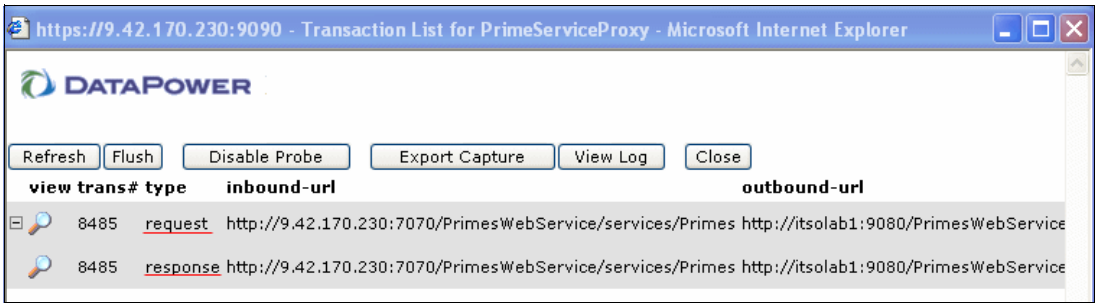


Figure 4-39 Probe results

7. Click the **magnifying glass** icon for the request message and review the content and header information as shown in Figure 4-40.

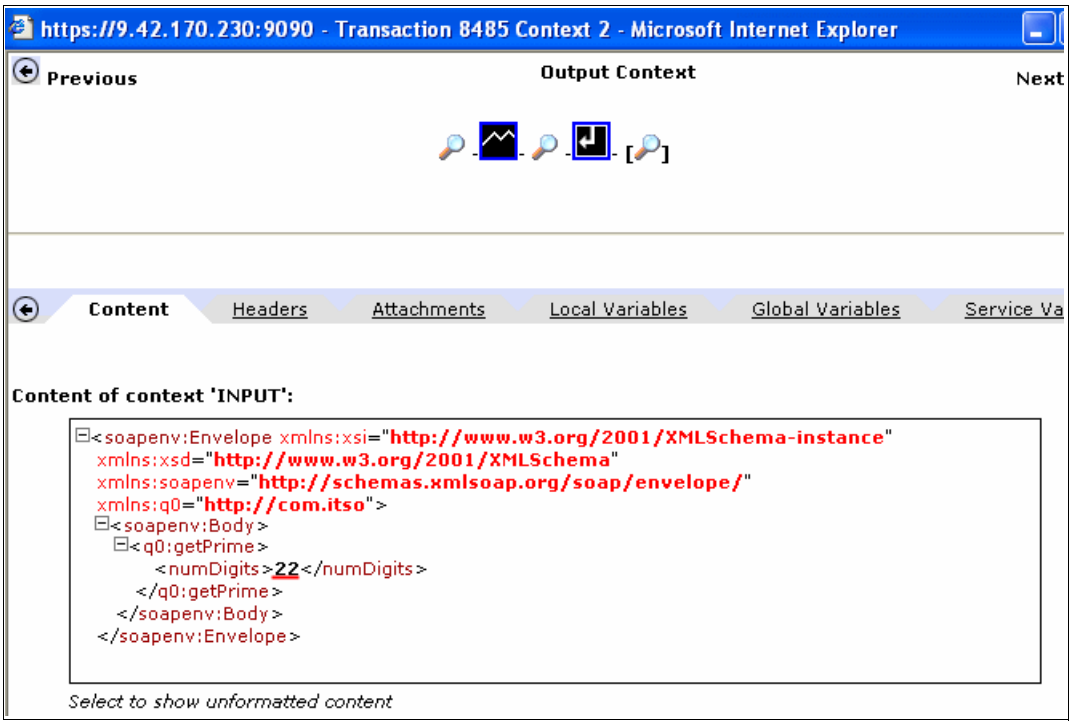


Figure 4-40 Request message details

Figure 4-41 shows the request header details.

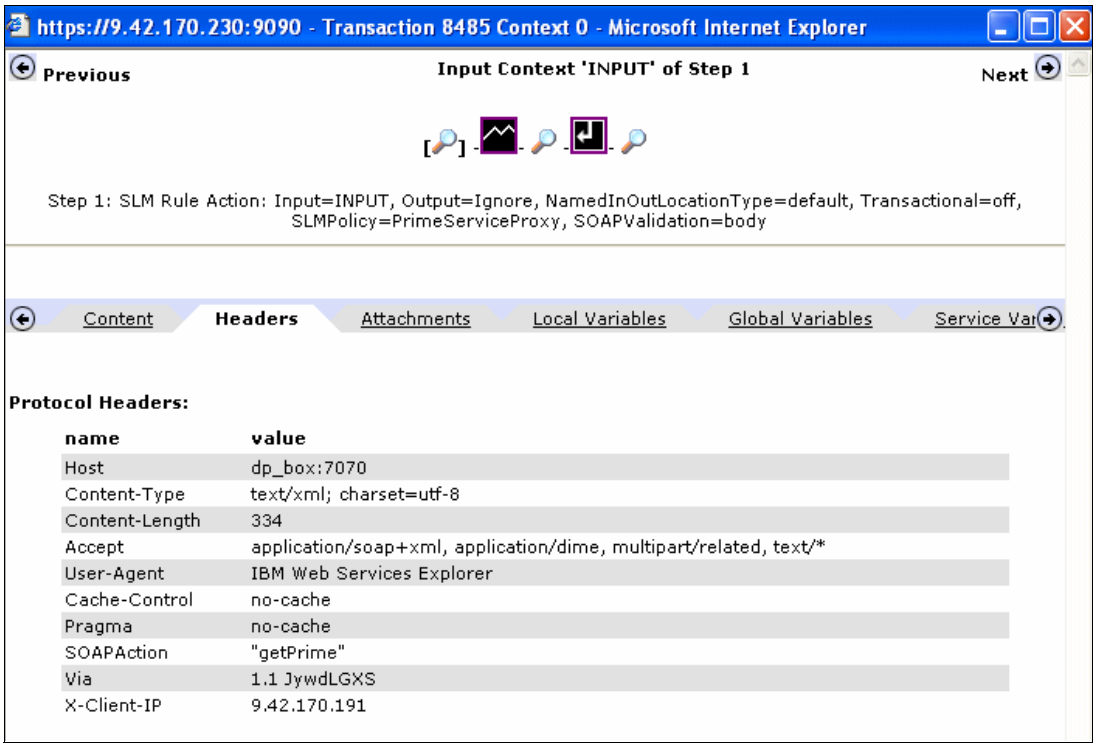


Figure 4-41 Request header details

8. Click the **magnifying glass** icon for the response message, and review the content and header information as shown in Figure 4-42.

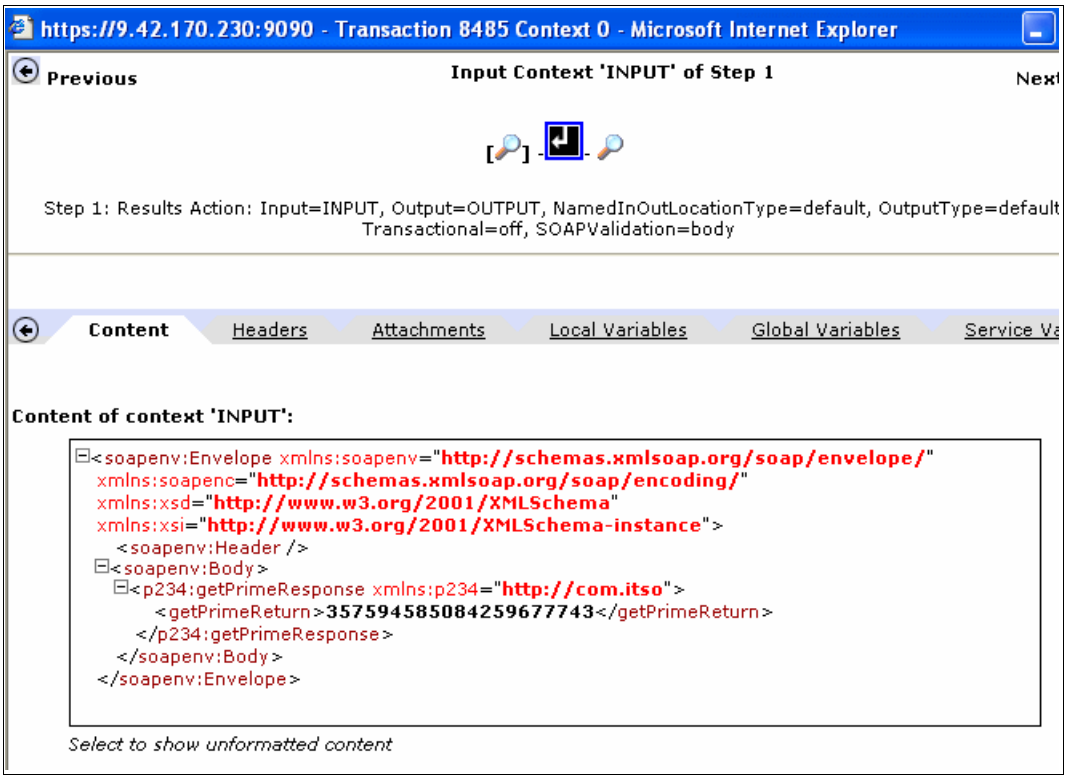


Figure 4-42 Response message details

Figure 4-43 shows the response header details.

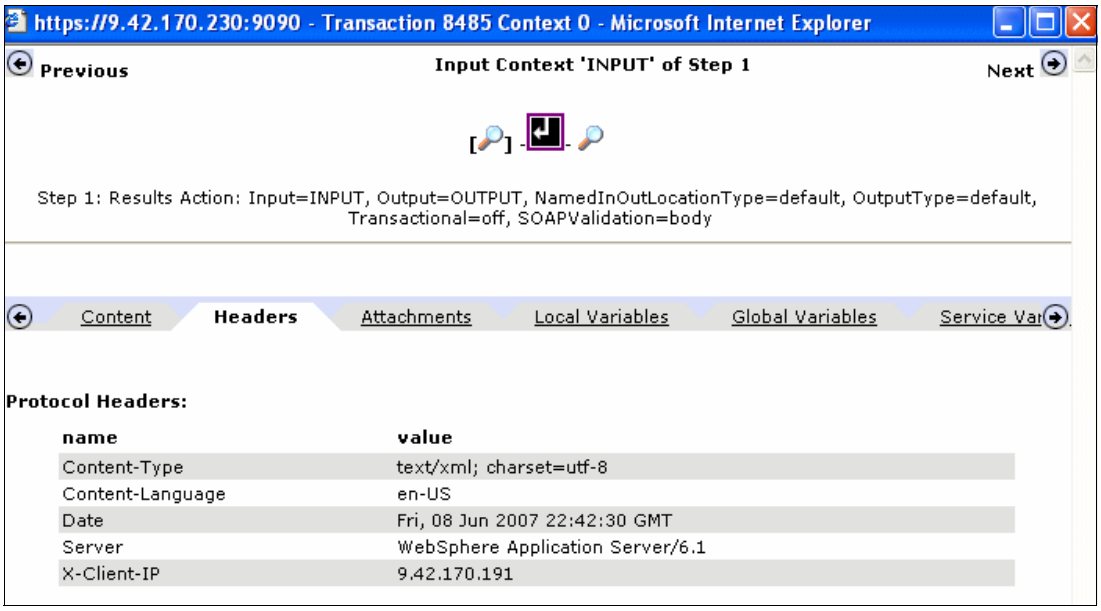


Figure 4-43 Response header details

9. To verify the SLM rule (up to one request allowed every 10 seconds), execute the test many times within the 10 second window.

10. Based on the SLM rule, the Web services client displays a message such as the example shown in Figure 4-44. Click the **Source** link.

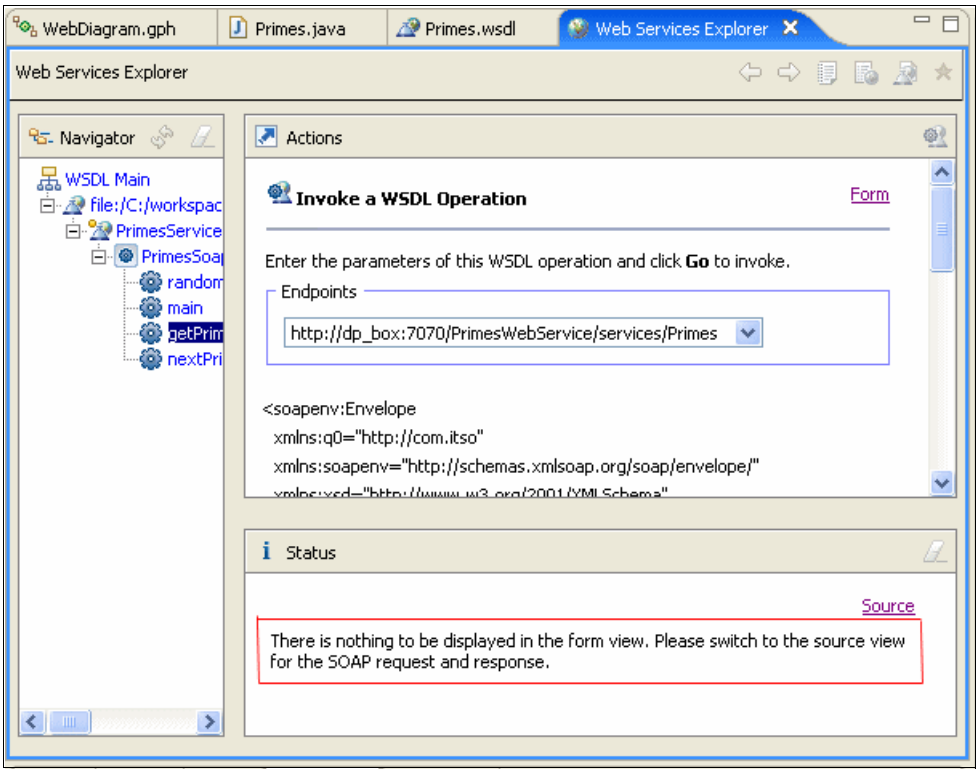


Figure 4-44 SLM Rule status message

Figure 4-45 shows the internal message that is displayed.

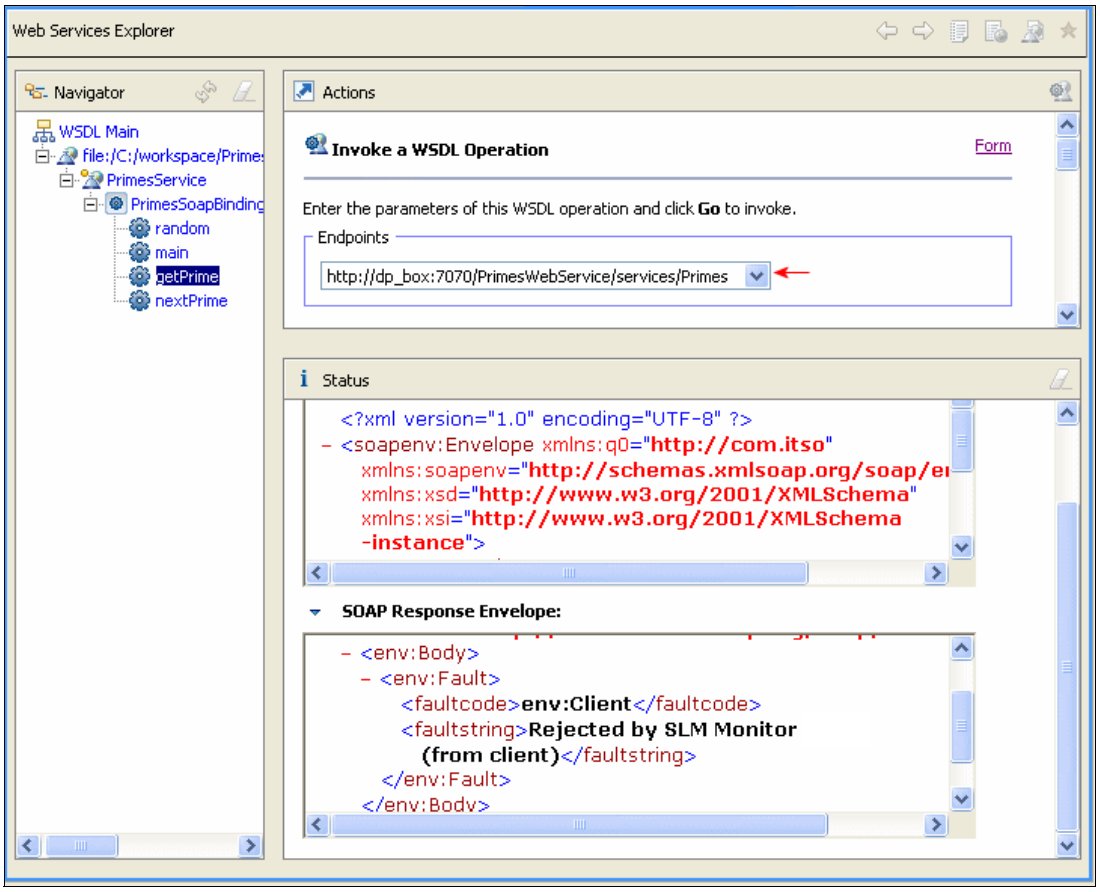


Figure 4-45 SLM message

11. Go to the Probe section, and review the messages shown in Figure 4-46.

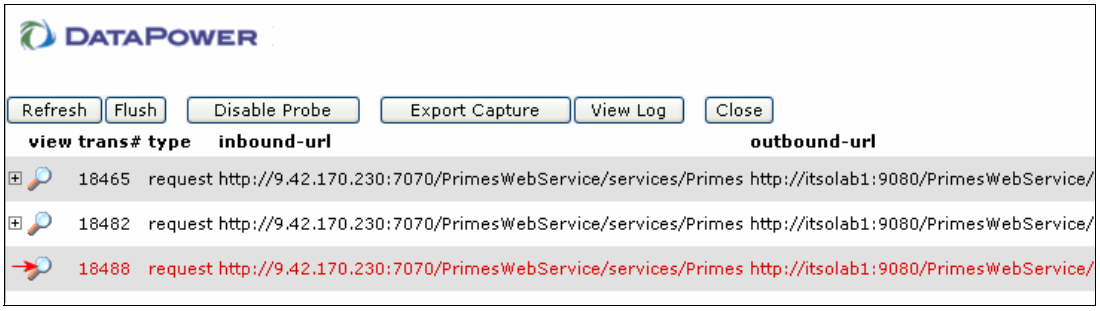


Figure 4-46 Probe messages

12. Click the **magnifying glass** icon and follow the message step-by-step as shown in Figure 4-47.

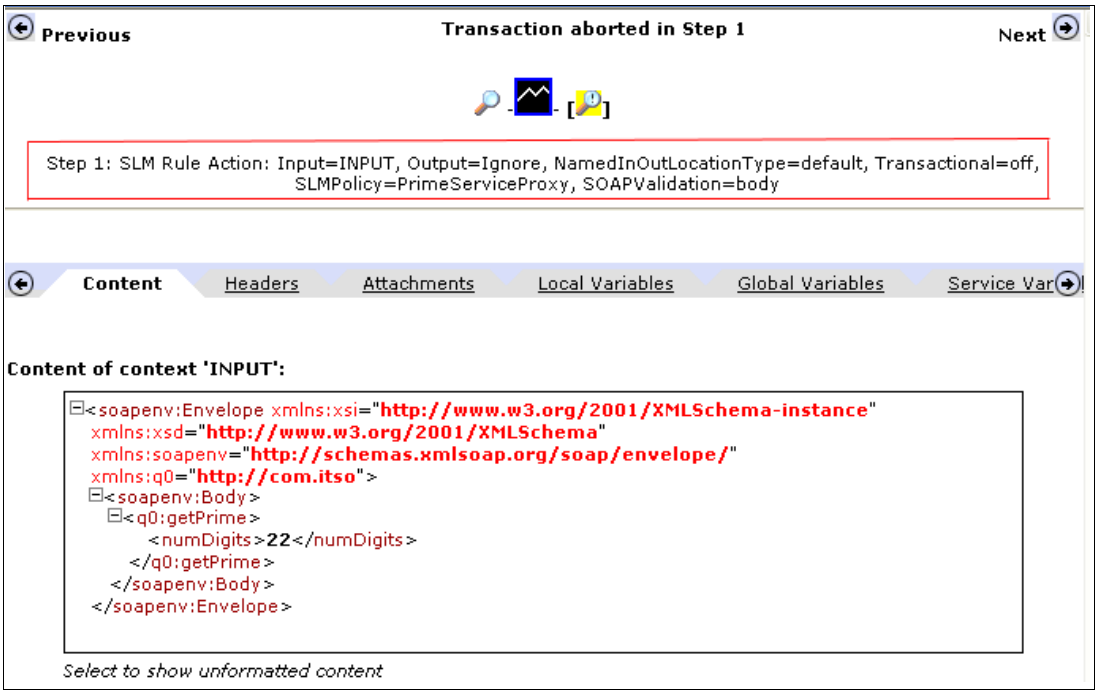


Figure 4-47 SLM rule details

4.4 Summary

In this chapter, we illustrated the main steps to integrate WebSphere Registry and Repository with DataPower, so that Web services can be managed from a central repository. In WebSphere Registry and Repository, the most important tasks are to create the concept and register the WSDL file. The rest of the configuration is performed in the DataPower appliance. For example, you can create a Web service proxy and execute the steps to configure the Web service proxy.

A

Additional material

This paper refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material associated with this paper is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser at:

ftp://www.redbooks.ibm.com/redbooks/REDP4366

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select the **Additional materials** and open the directory that corresponds with the IBM Redpaper form number, REDP4366.

Using the Web material

The additional Web material that accompanies this paper includes the following files:

File name	*Description*
redp4366.zip	Compressed code samples

System requirements for downloading the Web material

The following system configuration is recommended:

Hard disk space: 4 MB minimum
Operating System: Windows
Processor: 1.5 GHz or higher
Memory: 2 GB or higher

© Copyright IBM Corp. 2008. All rights reserved.

How to use the Web material

Create a subdirectory (folder) on your workstation, and extract the contents of the Web material compressed file into this folder.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

For information about ordering these publications, see “How to get Redbooks” on page 134. Note that some of the documents referenced here may be available in softcopy only.

- *Enabling SOA Using WebSphere Messaging*, SG24-7163
- *Getting Started with IBM Tivoli Monitoring 6.1 on Distributed Environments*, SG24-7143
- *IBM WebSphere DataPower SOA Appliances Part I: Overview and Getting Started*, REDP-4327
- *IBM WebSphere DataPower SOA Appliances Part II: Authentication and Authorization*, REDP-4364
- *IBM WebSphere DataPower SOA Appliances Part III: XML Security Guide*, REDP-4365
- *Patterns: SOA Design Using WebSphere Message Broker and WebSphere ESB*, SG24-7369
- *WebSphere Message Broker Basics*, SG24-7137
- *WebSphere Service Registry and Repository Handbook*, SG24-7386

Other publications

The following publications are also relevant as further information sources. Some are either available as part of the product or orderable for a fee. The common documentation is available on the Web at the following address:

http://www-1.ibm.com/support/docview.wss?rs=2362&uid=swg24014405

- *Configuring IBM Tivoli Composite Application Manager for SOA z/OS*, SN32-9493
- *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492
- *IBM Tivoli Composite Application Manager for SOA Release Notes*, GI11-4096
- *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407
- *IBM WebSphere DataPower Example Configurations Guide*
- *IBM WebSphere DataPower Common Installation Guide*
- *IBM WebSphere DataPower Integration Appliance XI50 Reference Kit*, part number 42C4212
- *IBM WebSphere DataPower WebGUI User's Guide*

© Copyright IBM Corp. 2008. All rights reserved.

- *IBM WebSphere DataPower XML Accelerator XA35 Reference Kit*, part number 42C4210
- *IBM WebSphere DataPower XML Integration Appliance XI50 CLI Reference Guide Release 3.6.0*
- *IBM WebSphere DataPower XML Security Gateway XS40 Reference Kit*, part number 42C4211

Online resources

These Web sites are also relevant as further information sources:

- Integrating WebSphere DataPower SOA Appliances with WebSphere MQ

  http://www.ibm.com/developerworks/websphere/library/techarticles/0703_crocker/0703_crocker.html
- Integrating WebSphere DataPower XML Security Gateway XS40 with WebSphere Message Broker

  http://www.ibm.com/developerworks/websphere/library/techarticles/0710_crocker/0710_crocker.html
- Integrating DataPower with WebSphere Message Broker using the Broker Explorer

  http://www.ibm.com/developerworks/websphere/library/techarticles/0707_storey/0707_storey.html

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

IBM WebSphere DataPower SOA Appliances

Part IV: Management and Governance

Monitor DataPower with IBM Tivoli Composite Application Manager for SOA

Integrate WebSphere Registry and Repository with DataPower

Manage configurations on multiple DataPower devices

IBM WebSphere DataPower SOA Appliances represent an important element in the holistic approach of IBM to service-oriented architecture (SOA). IBM SOA appliances are purpose-built, easy-to-deploy network devices that simplify, secure, and accelerate XML and Web services deployments while extending the SOA infrastructure. These appliances offer an innovative, pragmatic approach to harness the power of SOA. By using them, you can simultaneously use the value of existing application, security, and networking infrastructure investments.

This series of IBM Redpaper publications is written for architects and administrators who need to understand the implemented architecture in WebSphere DataPower appliances to successfully deploy it as a secure and efficient enterprise service bus (ESB) product. These papers give a broad understanding of the new architecture and traditional deployment scenarios. They cover details about the implementation to help identify the circumstances under which to deploy DataPower appliances. They include a sample implementation and architectural best practices for an SOA message-oriented architecture in an existing production ESB environment.

This part provides ways to integrate the DataPower appliance with other products such as WebSphere Registry and Repository, IBM Tivoli Composite Application Manager for SOA, and Tivoli Composite Application Manager System Edition. The entire series includes the following papers:

- *IBM WebSphere DataPower SOA Appliances Part I: Overview and Getting Started*, REDP-4327
- *IBM WebSphere DataPower SOA Appliances Part II: Authentication and Authorization*, REDP-4364
- *IBM WebSphere DataPower SOA Appliances Part III: XML Security Guide*, REDP-4365
- *IBM WebSphere DataPower SOA Appliances Part IV: Management and Governance*, REDP-4366

REDP-4366-00

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks