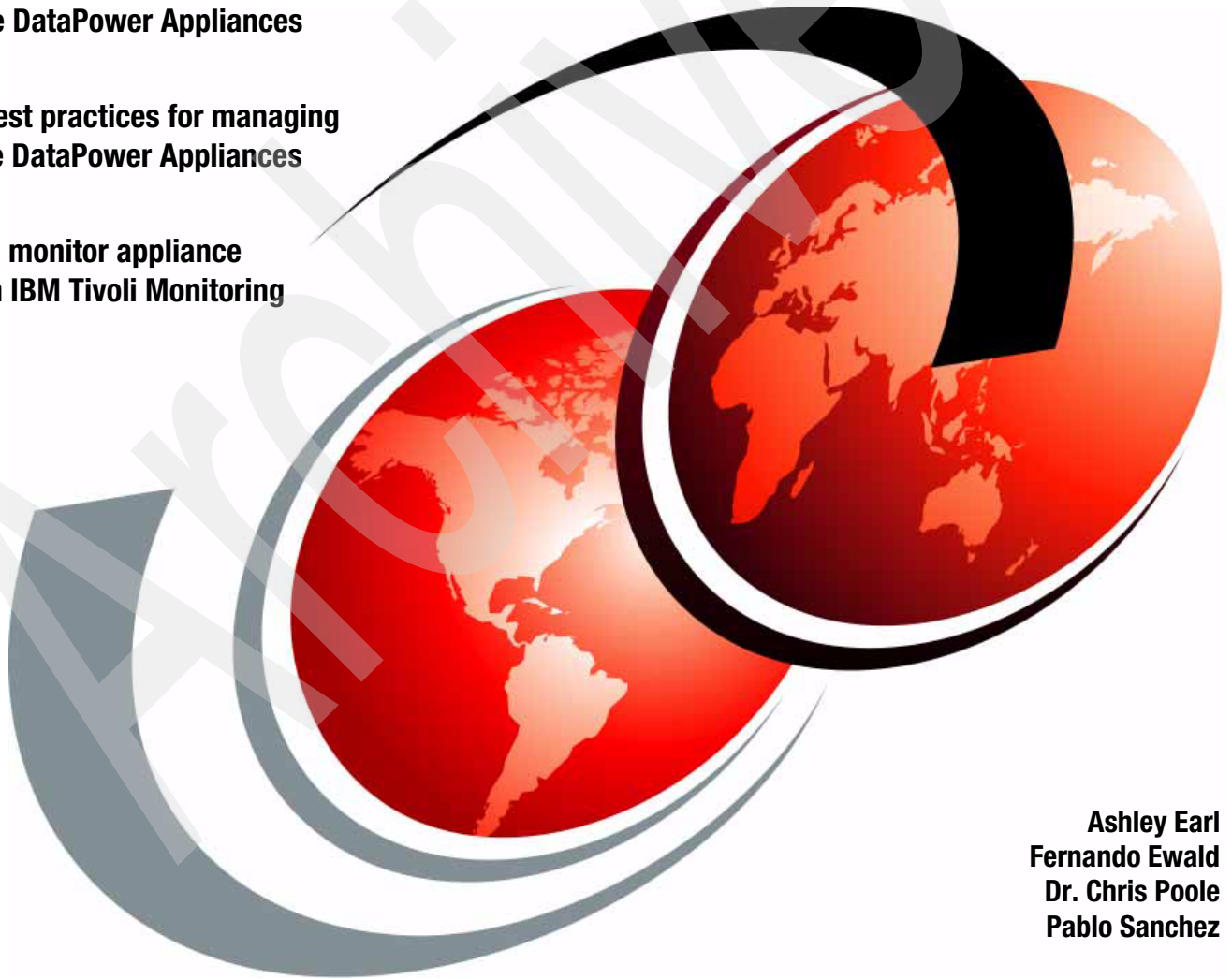


IBM WebSphere Appliance Management Center for WebSphere Appliances

Learn about centralized administration of IBM
WebSphere DataPower Appliances

Discover best practices for managing
WebSphere DataPower Appliances

See how to monitor appliance
status with IBM Tivoli Monitoring



Ashley Earl
Fernando Ewald
Dr. Chris Poole
Pablo Sanchez



International Technical Support Organization

**IBM WebSphere Appliance Management Center for
WebSphere Appliances**

April 2013

Archived

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

Archived

First Edition (April 2013)

This edition applies to the September 2012 release of IBM WebSphere Appliance Management Center for WebSphere Appliances.

© Copyright International Business Machines Corporation 2013. 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	vii
Trademarks	viii
Preface	ix
The team who wrote this book	ix
Now you can become a published author, too!	x
Comments welcome	xi
Stay connected to IBM Redbooks	xi
Chapter 1. Introduction to WebSphere Appliance Management Center	1
1.1 Overview of WebSphere Appliance Management Center	2
1.1.1 Management component	3
1.1.2 Monitoring component	3
1.2 Business value	4
1.3 Solution architecture	4
1.4 Supported operating environments	6
1.4.1 Supported operating systems and platforms	6
1.4.2 Hardware requirements	7
1.4.3 Supported web browsers	8
1.5 Supported WebSphere DataPower Appliances	8
1.6 A usage scenario	8
1.7 Ordering information	16
Chapter 2. Administration fundamentals	17
2.1 Installing the management component	18
2.1.1 Installing the management component by using the GUI	18
2.1.2 Installing the management component by using the unattended mode	27
2.2 Starting and stopping WebSphere Appliance Management Center	29
2.2.1 Starting the WebSphere Appliance Management Center server	30
2.2.2 Stopping the WebSphere Appliance Management Center server	30
2.3 Default ports	31
2.4 Managing users and roles	32
2.4.1 Managing users by using the local repository	33
2.4.2 Managing users by using LDAP	39
2.5 Adding and removing WebSphere DataPower Appliances	42
2.5.1 Adding a WebSphere DataPower Appliance	43
2.5.2 Removing a WebSphere DataPower Appliance	45
2.5.3 Grouping WebSphere DataPower Appliances	47
Chapter 3. Disaster recovery	51
3.1 Introduction to disaster recovery of WebSphere DataPower Appliances	52
3.1.1 Disaster recovery mode	52
3.1.2 WebSphere DataPower cryptographic objects	53
3.2 Secure backup	53
3.2.1 Secure backup basics	53
3.2.2 Encryption and security	54
3.2.3 Considerations for secure backup	54
3.3 Backing up WebSphere DataPower Appliances	55
3.3.1 Before you begin	55

3.3.2 Performing a secure backup	56
3.4 Secure restore	59
3.4.1 Secure restore basics	59
3.4.2 Considerations for the secure restore process	59
3.5 Restoring a WebSphere DataPower Appliance	60
3.5.1 Before you begin	60
3.5.2 Performing a secure restore	61
3.5.3 What to do next	63
Chapter 4. Firmware management	67
4.1 Managing the firmware repository	68
4.1.1 Introducing WebSphere DataPower Appliance firmware	68
4.1.2 Identifying and downloading firmware images	68
4.1.3 Managing firmware images	68
4.2 Hints and tips before you upgrade the firmware	71
4.2.1 Confirming a working WebSphere DataPower administrator user ID	71
4.2.2 Configuration backups	72
4.2.3 Cleaning the file system space	72
4.2.4 Avoiding live traffic and impact	73
4.3 Defining a firmware upgrade policy	74
4.3.1 Deciding when to upgrade	74
4.3.2 Firmware support lifecycle for WebSphere DataPower Appliance	74
4.3.3 Upgrading non-critical WebSphere DataPower Appliances first	75
4.3.4 Running service conformity tests after you upgrade the firmware	76
4.3.5 Avoiding impact to the production environment	76
4.4 Deploying the firmware	77
4.4.1 Single WebSphere DataPower Appliance upgrade	78
4.4.2 Multiple WebSphere DataPower Appliance upgrade	81
4.4.3 Verifying the firmware upgrade	83
4.4.4 Rolling back the firmware	84
Chapter 5. Managing domains and services	85
5.1 Managing application domains	86
5.1.1 Application domains	86
5.1.2 Application domain configuration	86
5.1.3 Creating domain configuration files	87
5.1.4 Creating domains	90
5.1.5 Updating domains	93
5.1.6 Quiescing and unquiescing domains	96
5.1.7 Deleting domains	98
5.1.8 Managing groups of domains	99
5.2 Managing services	102
5.2.1 Exporting service configuration	102
5.2.2 Creating services	104
5.2.3 Updating services	107
5.2.4 Updating services by using IBM WebSphere Registry and Repository	110
5.2.5 Quiescing and unquiescing services	111
5.2.6 Deleting services	112
5.3 Deployment policies	113
5.3.1 Understanding deployment policies	113
5.3.2 Creating deployment policies	115
5.3.3 Using deployment policies	121
5.4 Automatic synchronization of a configuration	125

5.4.1 Understanding the behavior of automatic synchronization	126
5.4.2 Considering the impact of automatic synchronization.	127
5.4.3 Toggling automatic synchronization for existing domains.	128
Chapter 6. Managing the software development lifecycle.	131
6.1 The software development lifecycle	132
6.2 A lifecycle scenario	132
6.3 The development environment	133
6.3.1 Single WebSphere DataPower Appliance.	133
6.3.2 Multiple WebSphere DataPower Appliances	134
6.4 Deployment models	134
6.4.1 Defining the scope of exported configuration	135
6.4.2 Selecting a deployment process	136
6.4.3 Updating existing configuration.	139
6.4.4 Evaluating the approaches	140
6.5 Promoting configuration	142
6.5.1 Promoting configuration through a single WebSphere DataPower Appliance	142
6.5.2 Promoting configuration through multiple WebSphere DataPower Appliances	145
Chapter 7. Effective monitoring of WebSphere DataPower Appliances	147
7.1 Monitoring architecture	148
7.2 Installing the monitoring component	148
7.2.1 Installing IBM Tivoli Monitoring	149
7.2.2 Installing ITCAM Agent for a WebSphere DataPower Appliance	157
7.3 Adding WebSphere DataPower Appliances to ITCAM Agents	168
7.3.1 Editing the configuration settings of an ITCAM Agent instance	173
7.4 Monitoring WebSphere DataPower Appliances	174
Chapter 8. Troubleshooting	187
8.1 Issues with the installer	188
8.1.1 Problems running the installer.	188
8.1.2 Installer log files	188
8.1.3 Problems running the uninstaller.	189
8.2 Issues with the graphical user interface	189
8.2.1 Verifying the server address that is used	189
8.2.2 Checking the state of the server	190
8.2.3 Web browser problems	192
8.2.4 Checking the login credentials	192
8.3 Issues with WebSphere DataPower Appliances	194
8.3.1 Checking the WebSphere DataPower Appliance and firmware support.	194
8.3.2 Checking the connection to the WebSphere DataPower Appliance	194
8.3.3 Checking the configuration of the XML management interface	195
8.3.4 Checking the login credentials	197
8.3.5 Setting up firewalls	197
8.4 Issues with firmware	197
8.4.1 Problems adding firmware to the repository	198
8.4.2 Problems matching firmware to a WebSphere DataPower Appliance	199
8.4.3 Problems deploying firmware	200
8.4.4 Unable to connect to web GUI or SSH after upgrading firmware	201
8.4.5 Management Information Base changes in firmware	202
8.5 Logging and trace	203
8.5.1 Logging in WebSphere Appliance Management Center.	203
8.5.2 Trace in WebSphere Appliance Management Center.	204
8.5.3 The WebSphere DataPower Appliance system log	205

8.6 Technotes	206
8.7 Other hints and tips	206
Related publications	207
IBM Redbooks	207
Online resources	207
Help from IBM	208

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 grant 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

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

AIX®
DataPower®
DataStage®
DB2®

Domino®
IBM®
Redbooks®
Redbooks (logo) ®

System z®
Tivoli®
WebSphere®
zEnterprise®

The following terms are trademarks of other companies:

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 and other countries.

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

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

Preface

IBM® WebSphere® Appliance Management Center for WebSphere Appliances simplifies the management and monitoring of environments that consist of multiple IBM WebSphere DataPower® Appliances. This web-based application provides centralized multi-appliance administration to support daily WebSphere DataPower Appliance operation. WebSphere Appliance Management Center for WebSphere Appliances provides the following key services:

- ▶ Centralized firmware management
- ▶ Disaster recovery
- ▶ Domain and service configuration
- ▶ Configuration life cycle deployment
- ▶ Monitoring multiple appliances, collecting key metrics, and presenting them in a central location

This IBM Redbooks® publication helps administrators of WebSphere DataPower Appliances to perform daily administration tasks by using WebSphere Appliance Management Center. The topics in this book include health monitoring of an environment, disaster recovery (secure backup and restore), firmware management, and environment promotion. This book also includes best practices, tips and techniques, and general recommendations for administrators of WebSphere DataPower Appliance deployments.

The team who wrote this book

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



Ashley Earl is a Test Specialist working on WebSphere Appliance Management Center for WebSphere Appliances in the IBM Hursley laboratory in the UK. He has been with the team for just over a year since development of the product was relocated to the Hursley lab. Prior to this he worked for the IBM Java Technology Center in a System Verification Test role. Ashley has a particular interest in software testing with a strong focus on test automation and the tooling that supports automated testing. Before joining IBM, Ashley gained a BSc in Computer Science and German at the University of Sheffield.



Fernando Ewald is Level 2 IT Specialist Certified in Divinopolis - MG, Brazil, and has 12 years experience in IT solutions. He joined IBM in 2009 as an IT Specialist for IGA Canada - CDT, supporting internal IBM accounts as a member of the Innovation and Technical Leadership team. His specializes in middleware and server support, including WebSphere DataPower Appliances, IBM Information Server DataStage®, and reverse proxy. Previous work experience includes creating high availability solutions. He also taught computer science and system information undergraduate courses and computer network specialization courses for Universidade de Franca - Brazil.



Dr. Chris Poole is a member of the WebSphere Appliance Management Center development team in Winchester, UK. Additionally, he has worked on a small team to develop a solution to bring role-based access control to IBM Hursley laboratories. His areas of expertise include Java, UNIX shell programming, web development, and Python. Before joining IBM, Chris earned a doctorate degree (PhD) in Theoretical Physics from Lancaster University.



Pablo Sanchez is an Application Integration and Middleware Support Specialist for IBM Brazil in Cordeirópolis, Brazil. He has been working with WebSphere DataPower since 2007. In September 2012, he became the Global Product Leader for IBM WebSphere DataPower for WME at IBM GTS. Pablo specializes in middleware and SOA-related technologies, such as WebSphere DataPower, WebSphere MQ, WebSphere Application Server, and WebSphere Message Broker. He is IBM Certified for SOA, IBM Certified Solution Implementer for WebSphere DataPower, and MQ V7.0 System Administrator. Pablo has co-authored other Redbooks publications.

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

David Currie, WebSphere Appliance Management Center Development Team Lead
IBM United Kingdom

Debbie Landon, Project Leader
ITSO, Raleigh Center

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

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 books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

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

ibm.com/redbooks

- ▶ Send your comments in an email 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

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:

<http://www.facebook.com/IBMRedbooks>

- ▶ Follow us on Twitter:

<http://twitter.com/ibmredbooks>

- ▶ Look for us on LinkedIn:

<http://www.linkedin.com/groups?home=&gid=2130806>

- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>

- ▶ Stay current on recent Redbooks publications with RSS Feeds:

<http://www.redbooks.ibm.com/rss.html>

Archived

Introduction to WebSphere Appliance Management Center

This chapter introduces IBM WebSphere Appliance Management Center for WebSphere Appliances. It includes the following sections:

- ▶ Overview of WebSphere Appliance Management Center
- ▶ Business value
- ▶ Solution architecture
- ▶ Supported operating environments
- ▶ Supported WebSphere DataPower Appliances
- ▶ A usage scenario
- ▶ Ordering information

For more information and additional resources about WebSphere Appliance Management Center, see “Related publications” on page 207.

WebSphere DataPower Appliances used: The WebSphere DataPower Appliances that were used in the creation of this IBM Redbooks publication were the IBM WebSphere DataPower Integration XI52 Appliance and IBM WebSphere DataPower XC10 Appliance.

1.1 Overview of WebSphere Appliance Management Center

WebSphere Appliance Management Center for WebSphere Appliances is a no-charge downloadable offering that simplifies the management and monitoring of environments that consist of multiple WebSphere DataPower Appliances. The management component of WebSphere Appliance Management Center is a web application that provides multibox operational management for WebSphere DataPower SOA Appliances. By using the management component, system administrators can easily and quickly carry out WebSphere DataPower Appliance administration tasks:

- ▶ Managing firmware across multiple WebSphere DataPower Appliances
- ▶ Performing backup and restore operations
- ▶ Managing domain and service configuration

For more information about the management component, see 1.1.1, “Management component” on page 3. Figure 1-1 shows the WebSphere Appliance Management Center graphical user interface (GUI).

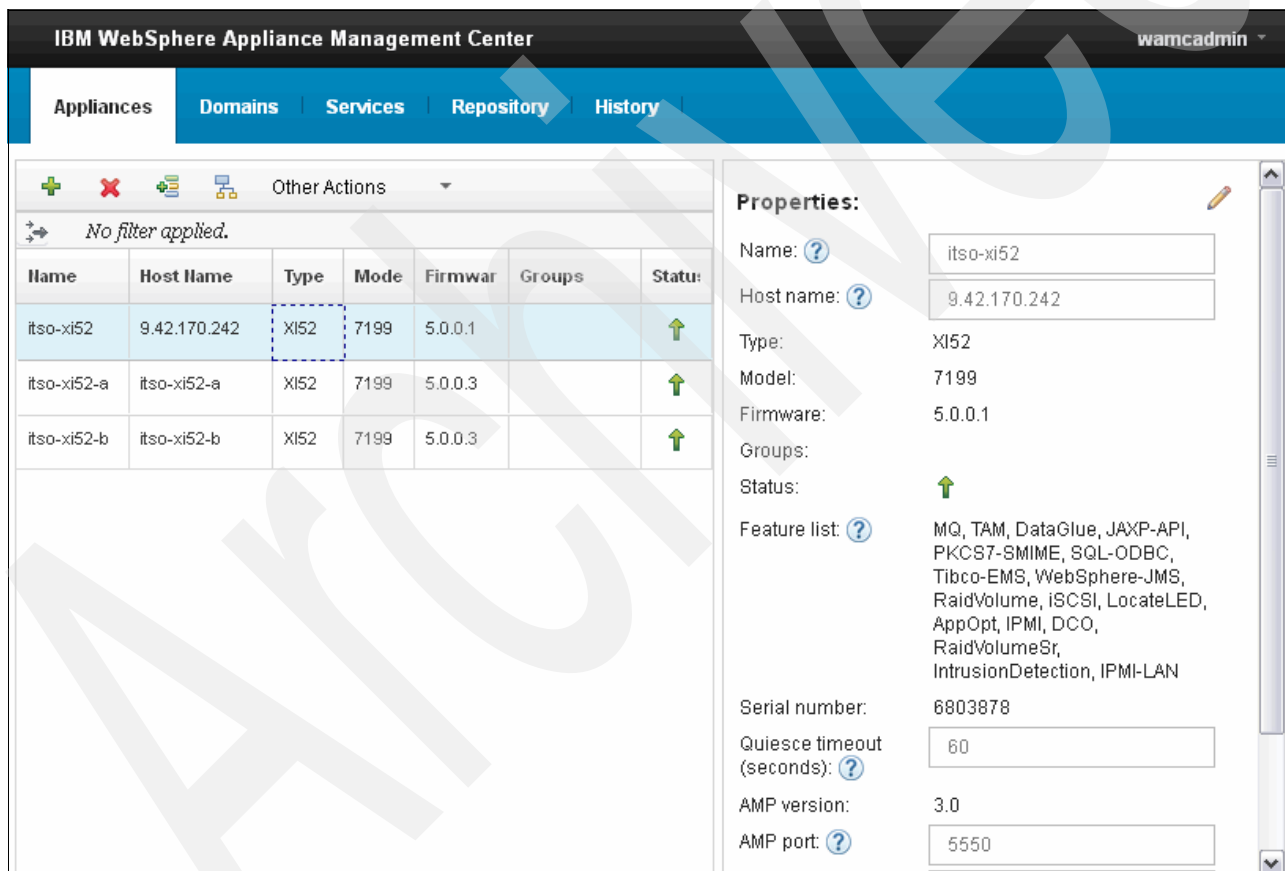


Figure 1-1 WebSphere Appliance Management Center graphical user interface

WebSphere Appliance Management Center also includes IBM Tivoli® Composite Application Manager (ITCAM) Agent for WebSphere DataPower Appliances. You can use this feature to monitor multiple WebSphere DataPower Appliances, collect key metrics, and present them in a central location. For more information about the monitoring component, see 1.1.2, “Monitoring component” on page 3.

WebSphere Appliance Management Center supports the management and monitoring of a various WebSphere DataPower Appliance types and models. For a list of WebSphere

DataPower Appliances that are supported by WebSphere Appliance Management Center, see 1.5, “Supported WebSphere DataPower Appliances” on page 8.

1.1.1 Management component

The management component of WebSphere Appliance Management Center for WebSphere Appliances is a web-based graphical interface. WebSphere DataPower administrators use this component to manage their WebSphere DataPower Appliances from a single, central location.

WebSphere Appliance Management Center provides the following functions:

- ▶ Quick status overview at the appliance, application domain, and service levels
- ▶ Disaster recovery by using secure backup and restore
- ▶ Firmware management that allows for firmware operations on multiple WebSphere DataPower Appliances in a single action
- ▶ Traffic processing management with quiesce and unquiesce operations at the appliance, application domain, and service levels
- ▶ The ability to create, update, and delete application domains across multiple appliances
- ▶ The ability to create, update, and delete services on application domains
- ▶ The ability to upload a file to a domain
- ▶ The ability to restart appliances and restart application domains

Important: The functions that are presented in this section are applicable to WebSphere Appliance Management Center for WebSphere Appliances Release 2012-09-25. Earlier releases might not support all of the features that are described, and later releases might introduce changes to the features described. Also, actions at the service level require WebSphere DataPower Appliances to be running at firmware version 5.0.0.0 or later.

1.1.2 Monitoring component

The monitoring component of WebSphere Appliance Management Center includes the IBM Tivoli Monitoring and IBM Tivoli Composite Application Manager (ITCAM) Agent for WebSphere DataPower Appliances. IBM Tivoli Monitoring consists of a Tivoli Enterprise Monitoring Server and a Tivoli Enterprise Portal Server. The monitoring component can be used to monitor multiple WebSphere DataPower Appliances, collect key metrics, and present these metrics in a central location.

ITCAM monitors the following metrics at the WebSphere DataPower Appliance level:

- ▶ Resource utilization
- ▶ Object status
- ▶ System log
- ▶ Event notifications
- ▶ Transaction latency
- ▶ Network and connection statistics

ITCAM also supports subnodes to make it easy to monitor multiple WebSphere DataPower Appliances with one agent. ITCAM monitors remotely through SOAP Configuration Management (SOMA) requests for WebSphere DataPower Appliances or Simple Network Management Protocol (SNMP) for WebSphere DataPower XC10 Appliances. ITCAM can also monitor the system logs of a WebSphere DataPower Appliance.

For more information about ITCAM, see Chapter 7, “Effective monitoring of WebSphere DataPower Appliances” on page 147.

1.2 Business value

WebSphere Appliance Management Center helps to simplify the management of a WebSphere DataPower Appliance infrastructure by introducing a centralized point of administration. This way, system administrators can handle most common administrative tasks, including the following tasks:

- ▶ Firmware deployment
- ▶ Domain and service deployment
- ▶ Appliance, domain, and service-level quiescing and unquiescing
- ▶ Secure backup and restore of WebSphere DataPower Appliances

WebSphere Appliance Management Center also provides real-time monitoring of the health and usage of WebSphere DataPower Appliances. This way, system administrators can target their activities and proactively make changes to their environment in response to usage patterns. The reports and charts that are presented by WebSphere Appliance Management Center can help your company to better target spending on new hardware based on these usage patterns.

WebSphere Appliance Management Center is a multiplatform, easy-to-deploy solution that saves time for system administrators by streamlining often repeated tasks. This way, system administrators can focus on developing the environment instead of simply maintaining it.

1.3 Solution architecture

As explained in 1.1, “Overview of WebSphere Appliance Management Center” on page 2, WebSphere Appliance Management Center is made up of two components:

- ▶ Management component

Often referred to as *WebSphere Appliance Management Center*, the management component allows for WebSphere DataPower Appliances to be administered from a single, web browser-based GUI.

- ▶ Monitoring component

Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the ITCAM Agent for WebSphere DataPower Appliances make up the monitoring component of WebSphere Appliance Management Center.

The management component is installed on a server machine that becomes the host for a web application. Users of WebSphere Appliance Management Center connect to the web application by using one of the supported web browsers from their client machine.

The server communicates directly with multiple WebSphere DataPower Appliances by using the XML management interface of the appliances. WebSphere DataPower XC10 Appliances are managed through their management console by using a Secure Shell (SSH) connection.

The management component allows for multiple WebSphere DataPower Appliances to be managed. WebSphere DataPower Appliances are added to WebSphere Appliance Management Center so that the user can see the properties and status for each appliance.

An administrator can drill down into a WebSphere DataPower Appliance and see a view of all of the application domains on that appliance. For WebSphere DataPower Appliances that run with firmware versions of 5.0.0.0 or later, you can drill down further and see the services that are part of an application domain. Figure 1-2 shows an overview of this concept.

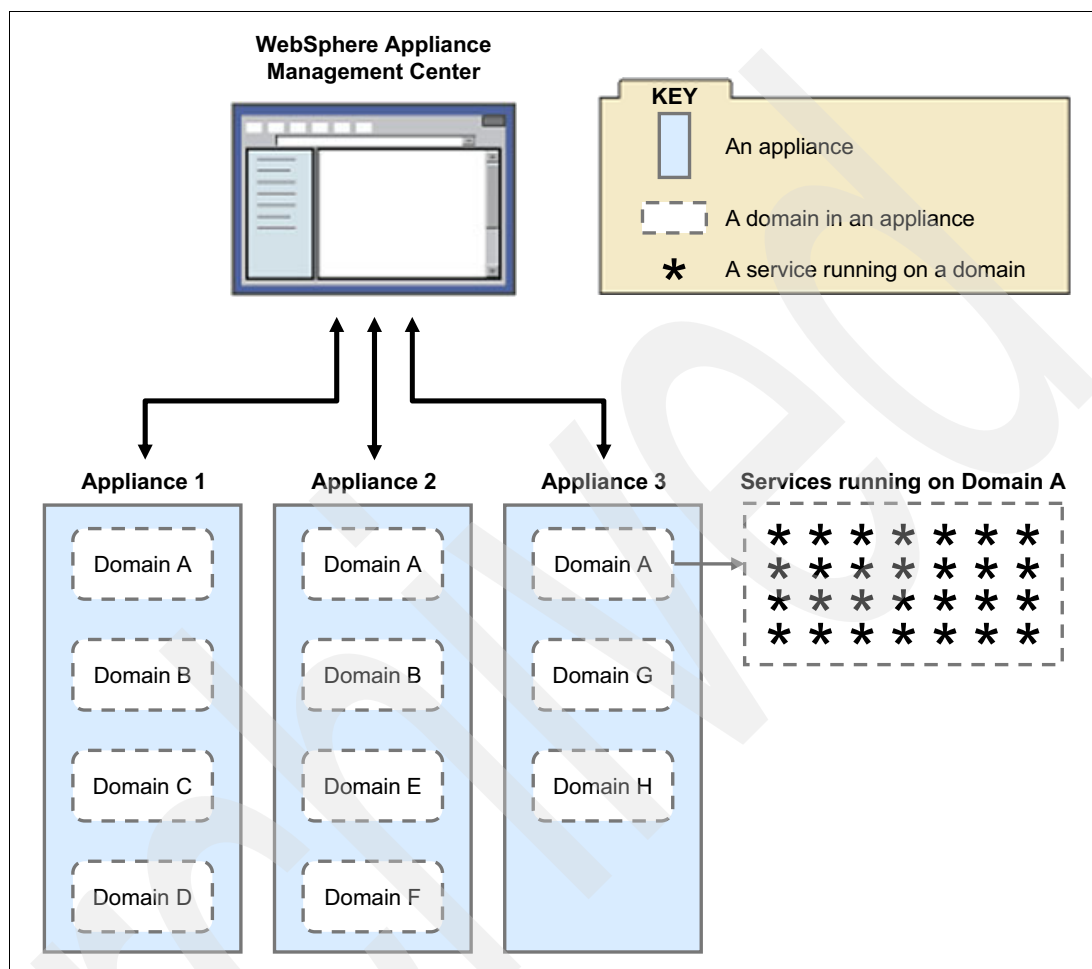


Figure 1-2 Management component with WebSphere DataPower Appliances, domains, and services

The monitoring component of WebSphere Appliance Management Center monitors the behavior and status of WebSphere DataPower Appliances. It provides useful performance metrics and can be helpful when diagnosing a problem. It can display such information as HTTP transaction rate, processor usage, and system load.

Included in the monitoring component is ITCAM Agent for WebSphere DataPower Appliances. IBM Tivoli Monitoring consists of Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server.

One or more WebSphere DataPower Appliances can be monitored by an instance of the ITCAM Agent, which polls the WebSphere DataPower Appliance and forwards the data to a Tivoli Enterprise Monitoring Server host. The Tivoli Enterprise Portal Server then pulls data from Tivoli Enterprise Monitoring Server.

The ITCAM Agent uses SOMA or syslog to monitor most WebSphere DataPower Appliances. The exception is the WebSphere DataPower XC10 Appliance, for which it uses SNMP.

Figure 1-3 shows the complete architecture of a WebSphere Appliance Management Center deployment.

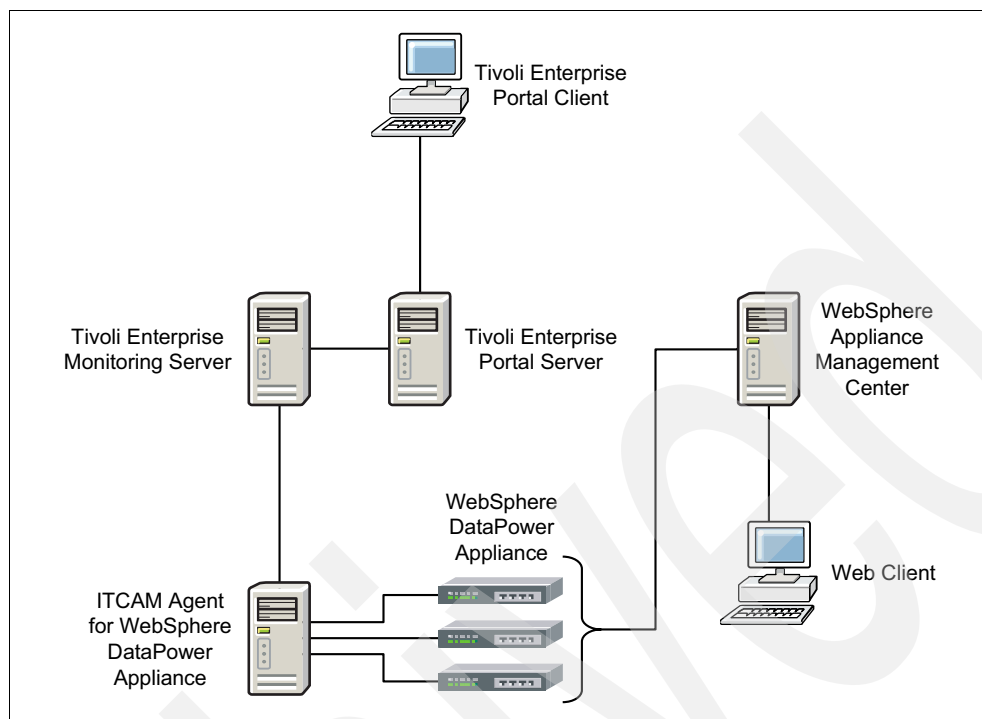


Figure 1-3 WebSphere Appliance Management Center system architecture

1.4 Supported operating environments

WebSphere Appliance Management Center is supported on many operating systems and server platforms. It has basic hardware requirements and supported web browser versions.

1.4.1 Supported operating systems and platforms

The following operating systems and platforms are supported by WebSphere Appliance Management Center:

- ▶ IBM AIX®
 - AIX 6.1 (64-bit)
 - AIX 7.1 (64-bit)
- ▶ Microsoft Windows
 - Windows Server 2008 Standard Edition (64-bit)
 - Windows Server 2008 Enterprise Edition (64-bit)
 - Windows Server 2008 DataCenter Edition (64-bit)
 - Windows Server 2008 Standard Edition - R2 (64-bit)
 - Windows Server 2008 Enterprise Edition - R2 (64-bit)
 - Windows Server 2008 DataCenter Edition - R2 (64-bit)

Exception: Installation of IBM Tivoli Monitoring is not supported on Microsoft Windows Server 2008 DataCenter Edition and Microsoft Windows Server 2008 DataCenter Edition - R2.

- ▶ SUSE Linux Enterprise Server (SLES)
 - SLES 10.0 for IBM System z® 64-bit
 - SLES 10.0 for Intel
 - SLES 11.0 for System z 64-bit
 - SLES 11.0 for Intel
- ▶ Red Hat Enterprise Linux (RHEL)
 - RHEL Advanced Platform 5.0 for System z 64-bit
 - RHEL Advanced Platform 5.0 for Intel
 - RHEL Advanced Platform 6.0 for z/Series 64-bit
 - RHEL Advanced Platform 6.0 for Intel

1.4.2 Hardware requirements

To use WebSphere Appliance Management Center, your environment must meet the following hardware requirements:

- ▶ Memory requirements:
 - Management component:
 - 2 GB minimum
 - 4 GB recommended
 - Monitoring component:
 - 2 GB minimum
 - 3 GB recommended
- ▶ Disk space requirements:
 - Management component:
 - 1 GB of temporary disk space during the installation
 - 2 GB of disk space in the installation target location
 - Sufficient disk space for the storage of the repository and log files

Consider the number of firmware images that you intend to store in WebSphere Appliance Management Center. Also consider the typical sizes of the firmware images, and allow sufficient room for future growth.
 - For the Tivoli Enterprise Monitoring Server:
 - On Windows: 1.1 GB of disk space
 - On Linux and AIX: 1.3 GB on the installation folder and an extra 300 MB in the temporary directory
 - For the Tivoli Enterprise Portal Server:
 - 1.4 GB of disk space in the installation target location
 - 1.2 GB of extra disk space in the temporary directory to allow for the installation of the embedded WebSphere Application Server and the Eclipse Help Server

- For the ITCAM Agent for WebSphere DataPower Appliance:
 - 500 MB of disk space for the first agent
 - 50 MB of disk space for each additional agent

1.4.3 Supported web browsers

The following web browsers are supported for use with WebSphere Appliance Management Center:

- ▶ Mozilla Firefox 3.6
- ▶ Mozilla Firefox 10 ESR
- ▶ Internet Explorer 8
- ▶ Internet Explorer 9

Tip: Most modern web browsers also work with WebSphere Appliance Management Center, but only the web browsers that are listed here are officially supported.

1.5 Supported WebSphere DataPower Appliances

WebSphere Appliance Management Center supports management of the following WebSphere DataPower Appliances:

- ▶ WebSphere DataPower Appliances at firmware version 3.8.0 or later:
 - IBM WebSphere DataPower XML Accelerator XA35 (9235 model only)
 - IBM WebSphere DataPower XML Security Gateway XS40 (9235 model only)
 - IBM WebSphere DataPower Integration Appliance XI50 (9235 model only)
 - IBM WebSphere DataPower Integration Blade XI50B
 - IBM WebSphere DataPower Integration Appliance XI50 for IBM zEnterprise®
 - IBM WebSphere DataPower B2B Appliance XB60
 - IBM WebSphere DataPower Low Latency Appliance XM70
 - IBM WebSphere DataPower Service Gateway XG45
 - IBM WebSphere DataPower Integration Appliance XI52
 - IBM WebSphere DataPower B2B Appliance XB62
- ▶ WebSphere DataPower Appliances at firmware version 1.0 or later:
 - IBM WebSphere DataPower Edge Appliance XE82
- ▶ WebSphere DataPower Appliances at firmware version 2.0.0.1 or later:
 - IBM WebSphere DataPower XC10 Appliance

1.6 A usage scenario

To demonstrate the features and benefits of WebSphere Appliance Management Center, follow this scenario about a fictional telecommunications company, called *Redbooks Telecoms*. Redbooks Telecoms recently purchased more WebSphere DataPower Appliances. The company wants to streamline the management of these WebSphere DataPower Appliances by reducing the amount of time that is spent on administrative tasks.

Redbooks Telecoms owns the following WebSphere DataPower Appliances:

- ▶ itso-xi52: WebSphere DataPower XI52 Appliance that operates as the production server for a web service proxy and an XML firewall service.
- ▶ itso-xi52-a: WebSphere DataPower XI52 Appliance that operates as the development server for the development team. This WebSphere DataPower Appliance is used to create services as new applications are developed.
- ▶ itso-xi52-b: WebSphere DataPower XI52 Appliance that operates as the test server for the quality assurance and test teams. This WebSphere DataPower Appliance is used to test the new services so that they can be confirmed as working correctly before they are moved into the production environment.

The system administrator begins by installing WebSphere Appliance Management Center, including the management and monitoring components. Then, the system administrator adds the three WebSphere DataPower Appliances to the management component of WebSphere Appliance Management Center.

The system administrator starts a web browser and enters the web address of the WebSphere Appliance Management Center server. After logging in, the system administrator sees the **Appliances** tab and, as shown in Figure 1-4, the Appliances grid is initially empty.

Name	Host Name	Type	Mod	Firm	Groups	Status
No items to display						

Properties:
Name:
Host name:
Type:
Model:
Firmware:
Groups:
Status:
Feature list:
Serial number:
Quiesce timeout (seconds):
AMP version:
AMP port:
Appliance administrator ID:
Appliance administrator password:

Figure 1-4 Logging in to WebSphere Appliance Management Center for the first time

To add WebSphere DataPower Appliances to WebSphere Appliance Management Center, you use the *add appliance function*. In this scenario, the system administrator can quickly add the three WebSphere DataPower XI52 Appliances to WebSphere Appliance Management Center. Figure 1-5 shows the three WebSphere DataPower Appliances in the Appliances grid. When the system administrator selects the itso-xi52 WebSphere DataPower Appliance, the Properties area on the right side of the window shows the properties of this appliance.

The screenshot displays the IBM WebSphere Appliance Management Center interface. The top navigation bar includes 'Appliances', 'Domains', 'Services', 'Repository', and 'History'. The 'Appliances' tab is active, showing a table of appliances. The table has columns: Name, Host Name, Type, Mode, Firmware, Groups, and Status. Three appliances are listed: 'itso-xi52', 'itso-xi52-a', and 'itso-xi52-b'. The 'itso-xi52' appliance is selected, and its properties are displayed on the right side of the window. The properties include Name, Host name, Type, Model, Firmware, Groups, Status, Feature list, Serial number, Quiesce timeout (seconds), AMP version, and AMP port.

Name	Host Name	Type	Mode	Firmware	Groups	Status
itso-xi52	9.42.170.242	XI52	7199	5.0.0.1		↑
itso-xi52-a	itso-xi52-a	XI52	7199	5.0.0.3		↑
itso-xi52-b	itso-xi52-b	XI52	7199	5.0.0.3		↑

Properties:

- Name: itso-xi52
- Host name: 9.42.170.242
- Type: XI52
- Model: 7199
- Firmware: 5.0.0.1
- Groups:
- Status: ↑
- Feature list: MQ, TAM, DataGlue, JAXP-API, PKCS7-SMIME, SQL-ODBC, Tibco-EMS, WebSphere-JMS, RaidVolume, iSCSI, LocateLED, AppOpt, IPMI, DCO, RaidVolumeSr, IntrusionDetection, IPMI-LAN
- Serial number: 6803878
- Quiesce timeout (seconds): 60
- AMP version: 3.0
- AMP port: 5550

Figure 1-5 Adding appliances to WebSphere Appliance Management Center

The system administrator then decides to ensure that the current configuration of the three WebSphere DataPower Appliances can be restored, which is a best practice before modifying the configuration of an appliance. By using WebSphere Appliance Management Center, the system administrator takes a secure backup of each WebSphere DataPower Appliance. These backups are stored in a central, secure, regularly backed up location as defined by Redbooks Telecoms standard operating procedures. The backup destination can also be set as an FTP server if backups are to be stored remotely.

Figure 1-6 shows the Backup Appliance window on which the system administrator defines where to save the backup.

Backup Appliance

Specify where to save the backup:

☒ File for download ?

☐ Appliance local file directory:

☐ Appliance temporary file directory:

☐ Remote FTP location:

local://

temporary://

Host name: ?

Port:

Filepath:

FTP user ID:

FTP user password:

Figure 1-6 Selecting the destination location for a backup

If problems occur that lead to a situation where the WebSphere DataPower Appliance configuration needs to be restored, the system administrator can use the secure restore function that is provided.

The Redbooks Telecoms development team is starting development of a new web application. The team intends to use the WebSphere DataPower XI52 Appliance to host an XML firewall service. Before the team starts developing, it ensures that the WebSphere DataPower Appliance that it develops on is running the latest available firmware version. The system administrator downloads the latest WebSphere DataPower XI52 Appliance firmware from the IBM Support Fix Central site and saves the firmware image to a local file system. The firmware image is added to WebSphere Appliance Management Center by using the **Repository** tab.

Figure 1-7 shows the **Repository** tab and the firmware image that the system administrator added to the repository.

The screenshot shows the IBM WebSphere Appliance Management Center interface. The top navigation bar includes 'Appliances', 'Domains', 'Services', 'Repository' (selected), and 'History'. The 'Repository' tab displays a table of firmware images. The table has columns for 'Appliance Type', 'Model', 'Firmware Version', and 'User Comment'. A single row is visible for 'XI52' appliances, model '9005', with firmware version '5.0.0.3' and user comment 'Firmware v5.0.0.3'. The 'Firmware Version' cell is highlighted with a dashed blue border. To the right of the table, the 'Properties' section for the selected firmware image is shown, including fields for 'Appliance type', 'Model', 'Firmware version', 'User comment', 'Firmware features', 'Manufacture date', and 'Upload date'.

Appliance Type	Model	Firmware Version	User Comment
XI52	9005	5.0.0.3	Firmware v5.0.0.3

Properties:

- Appliance type: XI52
- Model: 9005
- Firmware version: 5.0.0.3
- User comment: Firmware v5.0.0.3
- Firmware features: DataGlue, JAXP-API, PKCS7-SMIME, HSM, XG4, CompactFlash, iSCSI, RaidVolume, LocateLED, IPMI, AppOpt, MQ_7.0.1.1, TAM_6.0, SQL-ODBC_6.1, WebSphere-JMS_1.2.3, DCO_4.20, RaidVolumeMpt, RaidVolumeSr, IntrusionDetection, IPMI-LAN, zBX, IPMI-SEL, IPv6
- Manufacture date: 2012 10 4 22:09:44
- Upload date: 2012 11 1 00:56:17

Figure 1-7 Repository grid showing a firmware image for a WebSphere DataPower XI52 Appliance

The system administrator can now use the uploaded firmware image to upgrade the WebSphere DataPower XI52 Appliances. From the **Appliance** tab, the system administrator selects the WebSphere DataPower Appliances to be upgraded. The system administrator can select and then upgrade multiple WebSphere DataPower Appliances at the same time.

For this scenario, only the development WebSphere DataPower Appliance is upgraded. The test and production WebSphere DataPower Appliances need to be scheduled for upgrading later. The system administrator selects the development appliance, itso-xi52-a, and chooses to deploy firmware to the appliance.

Figure 1-8 shows the Deploy Firmware window.

Deploy Firmware

Set the target firmware:

☒ List upgrades only
☐ List all compatible firmware versions

Specify the firmware version: [?](#)

Summary:

Appliance Name	Appliance Type	Appliance Mode	Current Firmware	Target Firmware
itso-xi52-a	XI52	7199	4.0.2.0	5.0.0.3 details

☒ I accept the terms in the license agreements.

Note: After you click **Deploy**, you cannot stop this operation.

Figure 1-8 Deploying a firmware upgrade to a WebSphere DataPower XI52 Appliance

With the development WebSphere DataPower Appliance now at the correct firmware version, the developers begin writing their web application. They create an application domain on the itso-xi52-a appliance and create an XML firewall service within this domain by using the WebSphere DataPower Appliance GUI.

After the development activities are complete, the developers create an export of their domain configuration and send the export archive file to the test team. The test team requires the domain configuration to be deployed to an application domain on the WebSphere DataPower Appliance, itso-xi52-b. A user with the solution deployer role in WebSphere Appliance Management Center takes the domain configuration export and uses the Create Domain or Update Domain function to import the configuration into the test environment.

Figure 1-9 shows the Create Domain process where the domain configuration export is selected.

Create Domain

Specify the configuration source for this domain:

The configuration source can be:

- A backup that contains a domain of the same name, or a configuration export that contains objects to include in this domain, loaded from one of the following locations:
 - A local file
 - A remote location accessed through HTTP or HTTPS
- An existing domain of the same name on another appliance

☒ Local file

Select File:

☐ Remote location (URL)

Specify URL: ?

☐ An existing domain of the same name

Select domain:

Figure 1-9 Creating a domain from a domain configuration export that is stored locally

After the domain is created, the solution deployer can drill down from the WebSphere DataPower Appliance to see a list of domains on the appliance. The solution deployer can then stop and start traffic that is flowing through the domain by using the quiesce and unquiesce functions. In addition, the solution deployer can restart the domain, update the configuration with new configuration from another export, and upload files to the domain.

It is possible to drill down further from the domain to see a view of the services that are deployed in the domain. The solution deployer can also manage these services and update their configuration. Service-level management allows the Redbooks Telecoms team to choose to handle configuration deployment at a more refined level than the domain level and to limit the impact to production services of configuration updates.

Figure 1-10 shows the view of services on a WebSphere DataPower Appliance in WebSphere Appliance Management Center.

The screenshot displays the IBM WebSphere Appliance Management Center interface. The top navigation bar includes tabs for Appliances, Domains, Services, Repository, and History. The 'Services' tab is active. Below the navigation bar, there is a table listing various services. The table has columns for Name, Type, Domain, Appliance, and Status. The service 'wsproxy-ser...' is highlighted, and its properties are shown on the right side of the interface.

Name	Type	Domain	Appliance	Status
wsproxy-ser...	Web Service ...	development	itso-xi52	↓
http-service	HTTP Service	dfgdfg	itso-xi52	↓
wsproxy-ser...	Web Service ...	production	itso-xi52	↑
ITSORedbook...	Web Service ...	production-s...	itso-xi52	↑
AddressSear...	Web Service ...	Proxyland	itso-xi52	↓
AddressSearch	Web Service ...	Proxyland	itso-xi52	↑
envo	Multi-Protoc...	Proxyland	itso-xi52	↑
wsp_ITSORe...	Web Service ...	staging-saw...	itso-xi52	↑
wsp_Testitca...	Web Service ...	test	itso-xi52	↑
xml_ITCAM4S...	XML Firewall ...	test	itso-xi52	↑
XMLFirewall_...	XML Firewall ...	testOnly4SO...	itso-xi52	↑
wsp_Testitca...	Web Service ...	testOnly4SO...	itso-xi52	↑
xml_ITCAM4S...	XML Firewall ...	testOnly4SO...	itso-xi52	↑

Properties:

Name: wsproxy-service
Type: Web Service Proxy
Domain: production
Appliance: itso-xi52
Status: ↑

Figure 1-10 Viewing services on a WebSphere DataPower Appliance

After a period of testing, the web application and the XML firewall service are promoted to the production environment and enter general use. To effectively monitor the flow of traffic through the production WebSphere DataPower Appliance, the domains on the appliance, and down to the service level, Redbooks Telecoms uses the monitoring component of WebSphere Appliance Management Center.

By using IBM Tivoli Monitoring, the system administrators can view usage statistics and system load information for their WebSphere DataPower Appliances and services.

Figure 1-11 shows a workspace in the Tivoli Enterprise Portal Server web browser client.

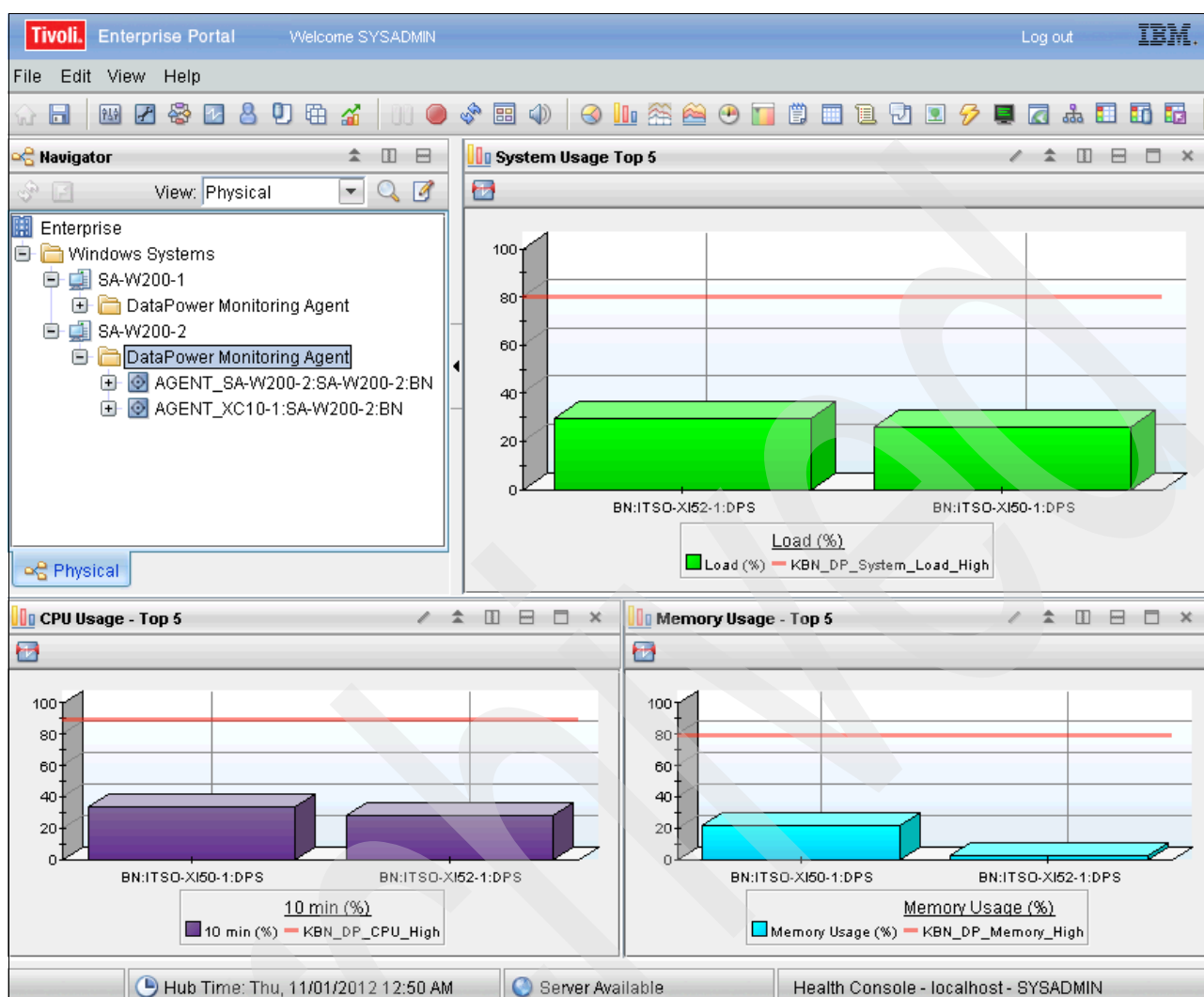


Figure 1-11 Monitoring WebSphere DataPower Appliances with WebSphere Appliance Management Center

1.7 Ordering information

You can download the latest version of WebSphere Appliance Management Center for WebSphere Appliances free of charge from the following website:

<http://www.ibm.com/support/docview.wss?uid=swg24032265>

WebSphere Appliance Management Center for WebSphere Appliances is a supported offering and carries program defect service. For information about conditions of support, including how to request support, see the download site.

Administration fundamentals

IBM WebSphere DataPower administrators can perform basic administration tasks to manage their WebSphere DataPower Appliances by using IBM WebSphere Appliance Management Center for WebSphere Appliances. This chapter explains how to install WebSphere Appliance Management Center and includes information about default configuration options. This chapter also explains how to manage users and assign roles to them and how to configure a Lightweight Directory Access Protocol (LDAP) server as the user registry. In addition, this chapter describes how to start managing WebSphere DataPower Appliances by adding them to and removing them from WebSphere Appliance Management Center.

This chapter includes the following sections:

- ▶ Installing the management component
- ▶ Starting and stopping WebSphere Appliance Management Center
- ▶ Default ports
- ▶ Managing users and roles
- ▶ Adding and removing WebSphere DataPower Appliances

2.1 Installing the management component

You can install and configure the management component of WebSphere Appliance Management Center by using either of the following methods:

- ▶ A graphical user interface (GUI) as explained in 2.1.1, “Installing the management component by using the GUI” on page 18
- ▶ An unattended installation as explained in 2.1.2, “Installing the management component by using the unattended mode” on page 27

The unattended installation mode is useful when you are required to install multiple WebSphere Appliance Management Center servers on different machines that use the same configuration.

For information about installing the monitoring component of WebSphere Appliance Management Center, see 7.2, “Installing the monitoring component” on page 148.

In the examples in this section, the installation is done by using Microsoft Windows Server 2008. For specific information about how to install the WebSphere Appliance Management Center server on AIX and Linux, see the *Installing WebSphere Appliance Management Center* topic of the WebSphere Appliance Management Center Information Center at:

<http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/install.html>

For a list of supported servers, see 1.4, “Supported operating environments” on page 6.

2.1.1 Installing the management component by using the GUI

To install WebSphere Appliance Management Center by using the GUI:

1. Download the WebSphere Appliance Management Center installation compressed file from the WebSphere Appliance Management Center for WebSphere Appliances website at:
<http://www.ibm.com/support/docview.wss?rs=171&uid=swg24032265>
2. Extract the image to a temporary folder.
3. Go to the temporary folder and run **install.exe**.

Linux and AIX systems: For Linux and AIX machines, run the **install.sh** script.

4. In the WebSphere Appliance Management Center Introduction window (Figure 2-1), click **Next**.

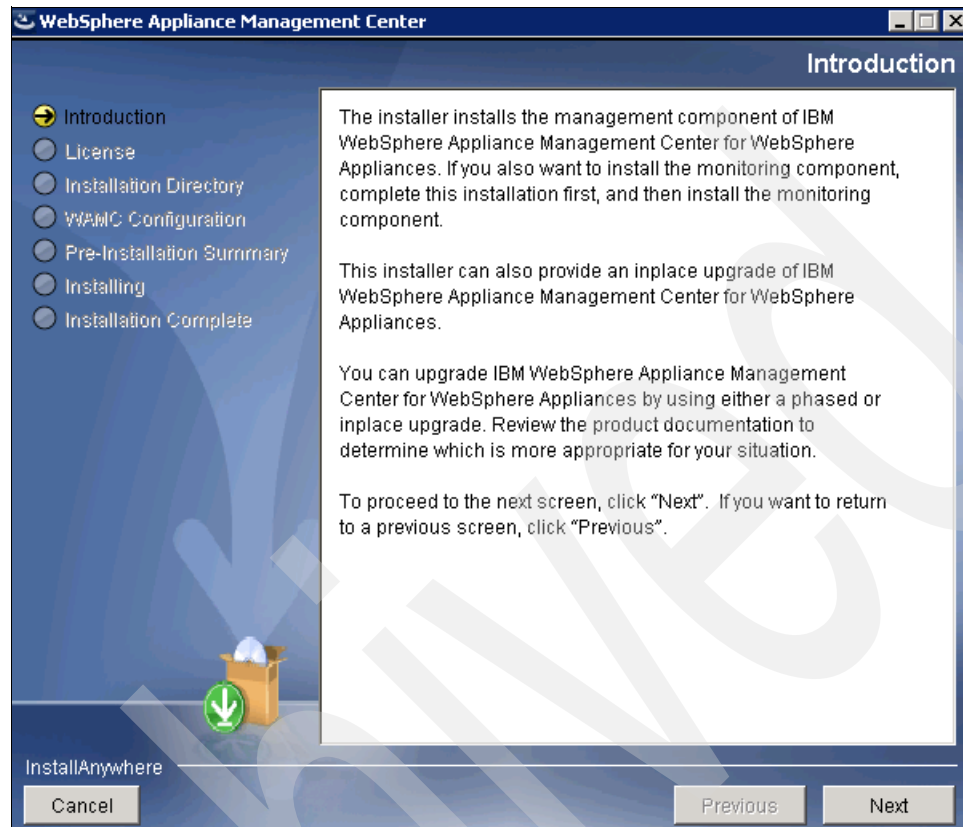


Figure 2-1 Introduction to WebSphere Appliance Management Center installation

5. In the Software License Agreement window (Figure 2-2), read the terms and conditions. If you agree, click **I accept the terms in the license agreement**. Click **Next**.

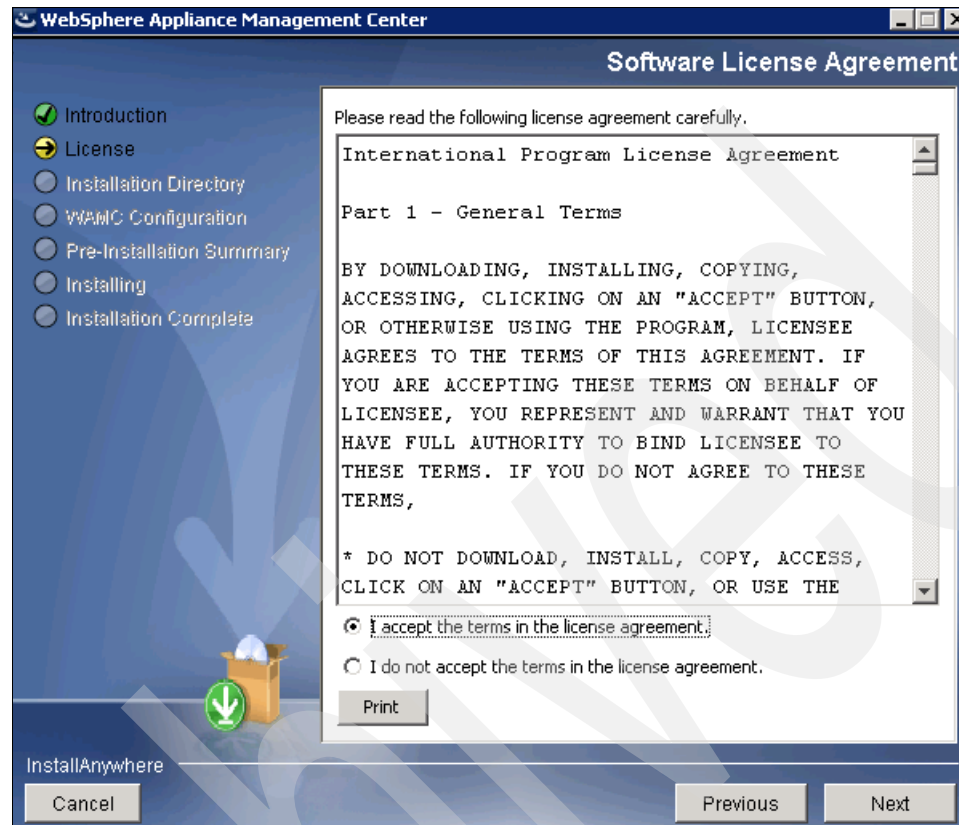


Figure 2-2 Software license agreement

6. In the Choose the Installation Directory window (Figure 2-3), select the location to install WebSphere Appliance Management Center and click **Next**.

Write access: The user who installs the WebSphere Appliance Management Center server must have *write* access to the installation directory.

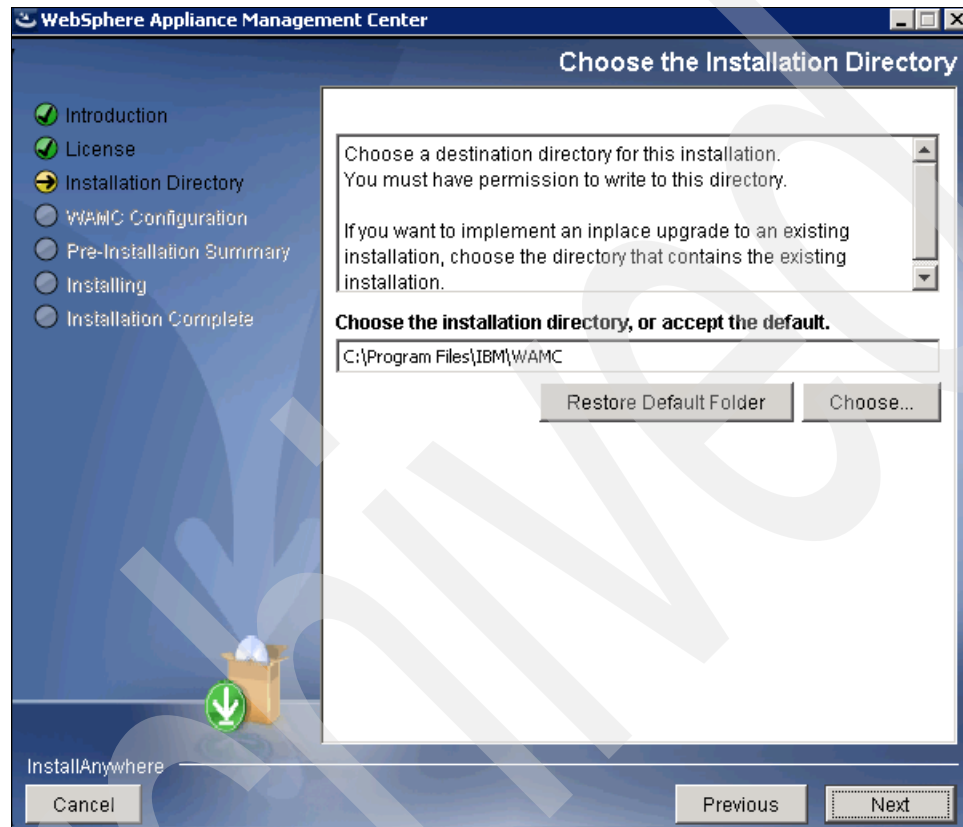


Figure 2-3 Selecting the installation location

7. In the Assign the Port Numbers window (Figure 2-4), specify the ports that WebSphere Appliance Management Center will run, and then click **Next**.

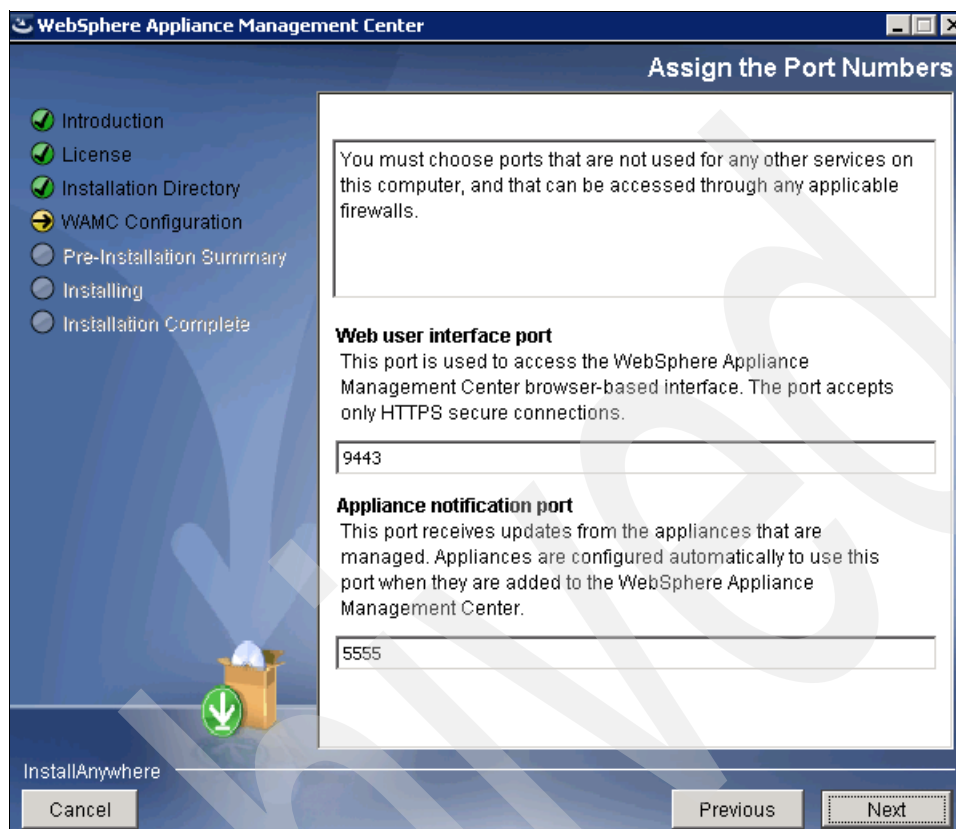


Figure 2-4 Assigning the port numbers

Firewalls: If a firewall is between the WebSphere Appliance Management Center server and the administration workstation, make sure that the firewall port is opened. Otherwise, access to the WebSphere Appliance Management Center server does not work. For information about configuring firewalls to allow WebSphere Appliance Management Center to work correctly, see 8.3.5, “Setting up firewalls” on page 197.

8. In the Configure the Repository Location window (Figure 2-5), select the location of WebSphere Appliance Management Center repository.

The repository location stores information about the WebSphere DataPower Appliances and firmware. The space of this location should be large enough to save all firmware images that will be available. In addition, the person who is installing must have access to this location.

Then, click **Next**.

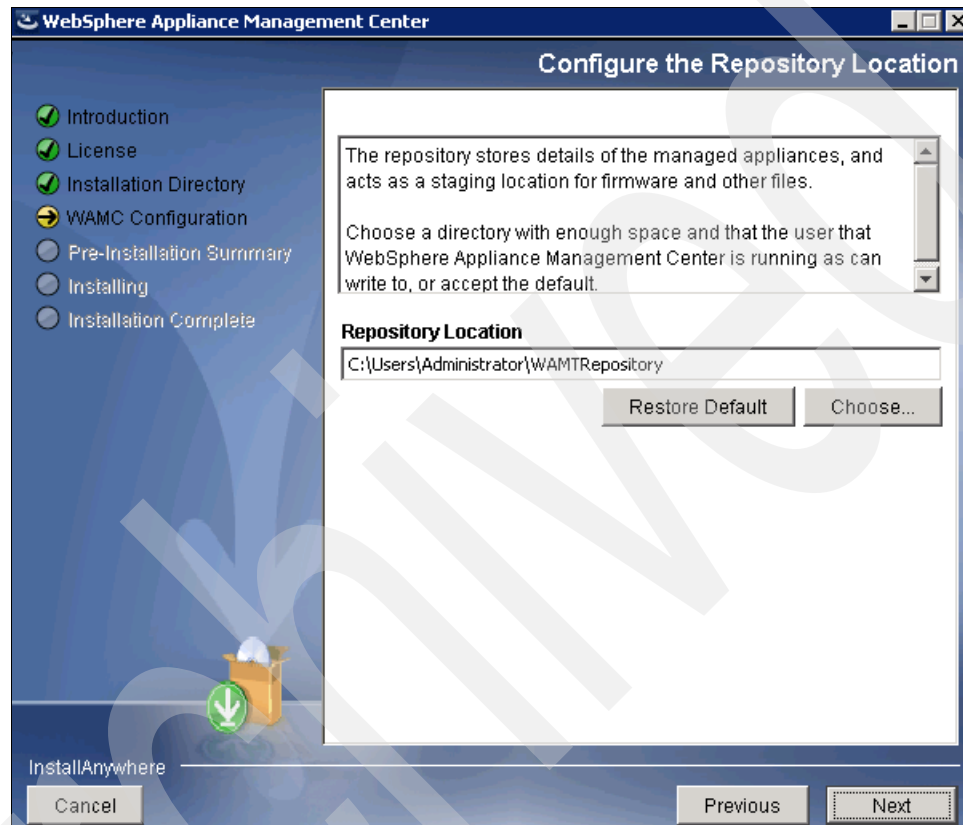


Figure 2-5 Configuring the location of the WebSphere Appliance Management Center repository

9. In the Create the Initial User window (Figure 2-6), specify the credentials for the administrator. During the installation, this user is created locally. However, WebSphere Appliance Management Center also supports LDAP authentication. For more information, see 2.4.2, “Managing users by using LDAP” on page 39.

The password for this user is encoded and can be changed later. To change the password for this user after the installation, see “Changing a user password” on page 37.

Then, click **Next**.

WebSphere Appliance Management Center

Create the Initial User

Introduction
License
Installation Directory
WAMC Configuration
Pre-Installation Summary
Installing
Installation Complete

Create a user for logging on to WebSphere Appliance Management Center. This user is stored in WebSphere Appliance Management Center, not your operating system.

You can create additional users or connect to an external directory server after the installation is complete.

User name
wamcadmin

Password

Retype password

Cancel Previous Next

Figure 2-6 Administrator credentials configuration

10. In the Pre-Installation Summary window (Figure 2-7), verify that all the information listed is correct, and then click **Install** to start the installation procedure.

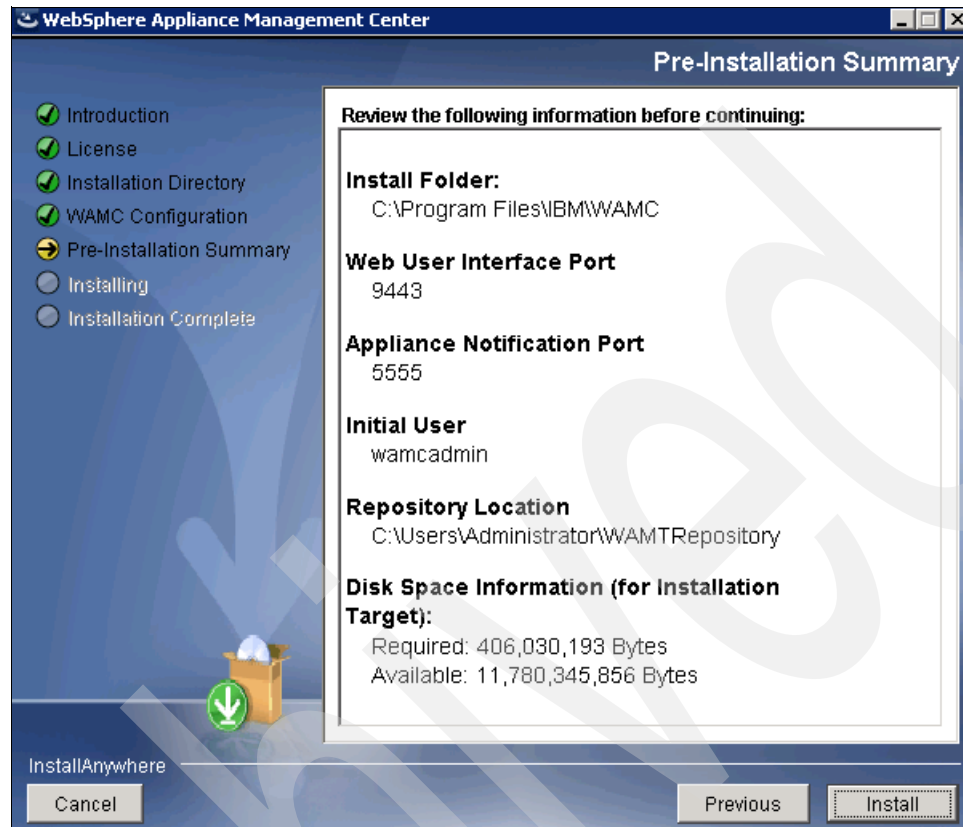


Figure 2-7 Pre-installation summary

During the installation procedure, you see the Installing WebSphere Appliance Management Center window (Figure 2-8). This window shows the tasks that are being run by the installer and the status bar.



Figure 2-8 Installation progress

11. When the installation is complete, in the Install Complete window (Figure 2-9), review the installation summary. The summary shows a message that indicates the location where the WebSphere Appliance Management Center server was installed and how to start the server. For information about starting the WebSphere Appliance Management Center server, see 2.2.1, “Starting the WebSphere Appliance Management Center server” on page 30.

Then, click **Done**.

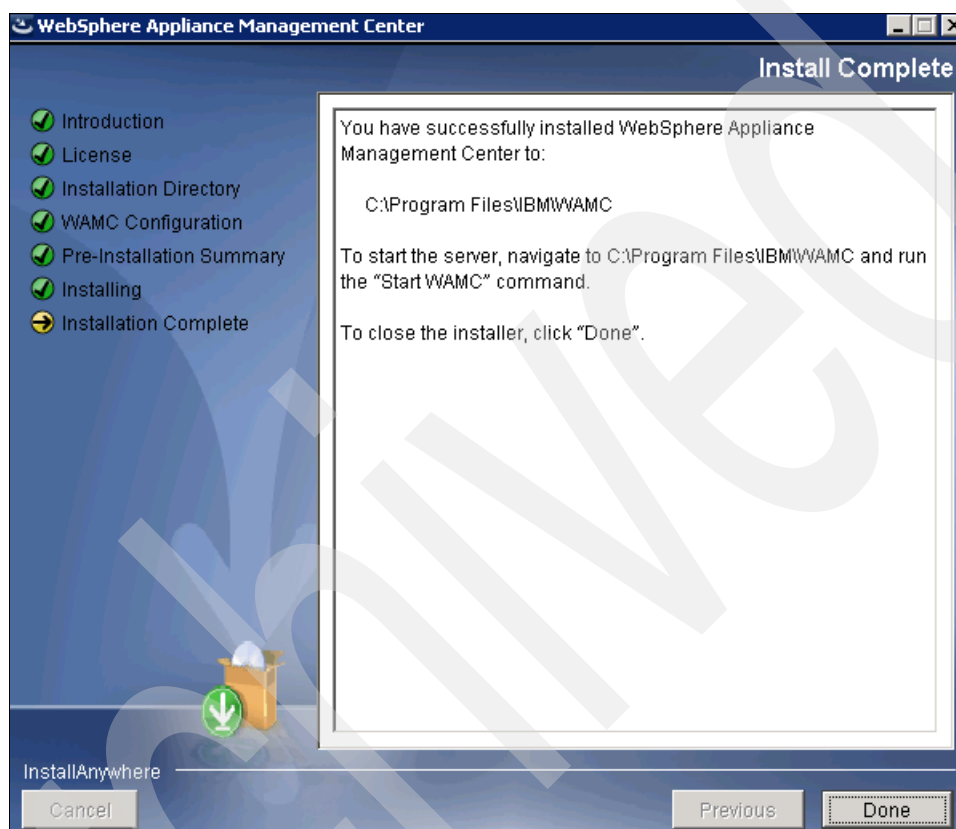


Figure 2-9 Post installation summary

2.1.2 Installing the management component by using the unattended mode

The other option to install the management component of the WebSphere Appliance Management Center is to do an unattended installation. By using this approach, you can run WebSphere Appliance Management Center on a server, such as on an AIX server, without the graphical mode enabled. The unattended installation mode is useful when you are required to install multiple WebSphere Appliance Management Center servers on different machines that use the same configuration.

To do an unattended installation:

1. Download the WebSphere Appliance Management Center installation compressed file from the WebSphere Appliance Management Center for WebSphere Appliances website at:
<http://www.ibm.com/support/docview.wss?rs=171&uid=swg24032265>
2. Extract the image to a temporary folder.

3. Go to the temporary folder, and edit the `sample-response.txt` file. This file contains all of the options that are requested during a GUI installation. You must update this file with your installation requirements.

- a. Update the following statement in the `sample-response.txt` file to accept the software license agreement:

```
LICENSE_ACCEPTED=TRUE
```

- b. If you need to change the installation directory location, uncomment the `USER_INSTALL_DIR=` line in the `sample-response.txt` file. Then, enter the directory information. The default installation directory path location for Windows is `C:\Program Files\IBM\WAMC`. For Linux and AIX, the default location is `/opt/ibm/wamc`. The installation directory path has a maximum of 90 characters.

If you are using the default location, make sure that the user who is running the installation has sufficient access privileges to write to this location.

For example, to change the default location:

- On a Windows server, enter:

```
USER_INSTALL_DIR=C:\\IBM\\WAMC
```

Directory path for a Windows server: Notice the two back slashes (\\) between each folder in the Windows response file. One backslash is the escape character, and the other backslash is for the folder location.

- On a Linux or AIX server, enter:

```
USER_INSTALL_DIR=/usr/IBM/WAMC
```

- c. If required, change the WebSphere Appliance Management Center ports. WebSphere Appliance Management Center uses the following ports by default:

- 443 for the web GUI access (`WEB_UI_PORT`)
- 5555 to receive updates from the WebSphere DataPower Appliances that this server is managing (`APPLIANCE_NOTIFICATION_PORT`)

These ports are defined in the configuration file as shown in the following example:

```
WEB_UI_PORT=9443
APPLIANCE_NOTIFICATION_PORT=5555
```

If you have a firewall, verify that it allows for communication between the WebSphere Appliance Management Center server and the WebSphere DataPower Appliances. For information about how to configure firewalls to allow WebSphere Appliance Management Center to function correctly, see 8.3.5, “Setting up firewalls” on page 197.

For a list of ports that are used by WebSphere Appliance Management Center, see 2.3, “Default ports” on page 31.

- d. Define the administrator and password to access the WebSphere Appliance Management Center. They are defined by the following lines in the `sample-response.txt` file:

```
WAMC_USER=wamcadmin
WAMC_PASSWORD=change_me
```

You can change this password after the installation. For more information, see “Changing a user password” on page 37.

- e. If necessary, change the WebSphere Appliance Management Center server configuration repository. By default, it is in the home folder of the user who is installing the management component. To change this folder, locate the `WAMT_REPOSITORY=` line in

the sample-response.txt file. Uncomment this line and enter in the new location as shown in the following example:

```
WAMT_REPOSITORY=C:\\IBM\\WAMC\\Configuration
```

Directory path for a Windows server: Notice the two back slashes (\\) between each folder in the Windows response file. One backslash is the escape character, and the other backslash is for the folder location.

4. After you update the sample-response.txt file, save it as a response.txt file.
5. Open a command line, and go to the directory that contains the response.txt file. Depending on your server environment, type the following command to start the installation:
 - On a Windows server:

```
start /wait install.exe -f <path_to_response_file>\\response.txt
```
 - On a Linux or AIX server:

```
install.sh -f <path_to_response_file>/response.txt
```

Figure 2-10 shows the installation running on a Windows server.

```
C:\temp\WAMC>start /wait install.exe -f C:\temp\WAMC\\response.txt
C:\temp\WAMC>
```

Figure 2-10 Installation command on a Windows server

6. After the installation completes, check the installation log file to see whether the installation was successful. The installation log file is in the <WAMC_install_dir>\Installer\Logs directory.

For more information about the installation log files, see 8.1.2, “Installer log files” on page 188.

You can now start the WebSphere Appliance Management Center server. For more information, see 2.2.1, “Starting the WebSphere Appliance Management Center server” on page 30.

WebSphere DataPower XC10 Appliances: If you are a WebSphere DataPower XC10 Appliance user, consider modifying the com.ibm.amc.wamHttpPower line in the wamc.properties file. For more information, see the *WebSphere Appliance Management Center properties* topic in the IBM WebSphere Appliance Management Center for WebSphere Appliances Information Center:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/wamc_properties.html

2.2 Starting and stopping WebSphere Appliance Management Center

This section shows you how to start and stop WebSphere Appliance Management Center. WebSphere Appliance Management Center it is not automatically started after installation or after a server restart.

2.2.1 Starting the WebSphere Appliance Management Center server

To start the WebSphere Appliance Management Center server, go to WebSphere Appliance Management Center installation directory and enter the following command:

- ▶ On a Windows server, run the **start wamc.lnk** command.
- ▶ On a Linux or AIX server, run **start-wamc** command.

Figure 2-11 shows the resulting panel, which indicates that the WebSphere Appliance Management Center server is started.

```
C:\Program Files\IBM\WAMC>start wamc.lnk
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
IBM*
Licensed Materials - Property of IBM
KC01

(C) Copyright IBM Corporation 2012 All Rights Reserved.
* Trademark of International Business Machines
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
Starting server...
Server runtime started.
```

Figure 2-11 Starting the WebSphere Appliance Management Center server on Windows

The WebSphere Appliance Management Center is now ready for use. During the installation, if the server ports were not changed, you can access the WebSphere Appliance Management Center server from a web browser with the following address:

`https://<serverName>:9443/wamc`

Unable to access the server: You might receive a message that indicates the server was started, but then get an error when you try to access the server. If this situation happens, wait a minute and try to access the server again because the WebSphere Appliance Management Center server might still be starting.

If a firewall is between the administrator workstation and the WebSphere Appliance Management Center server, make sure the WebSphere Appliance Management Center port is open. For information about the ports that are used by WebSphere Appliance Management Center, see 2.3, “Default ports” on page 31.

2.2.2 Stopping the WebSphere Appliance Management Center server

To stop the WebSphere Appliance Management Center server, go to WebSphere Appliance Management Center installation directory. Depending on your environment, enter one of the following commands:

- ▶ On a Windows server, run the **stop wamc.lnk** command.
- ▶ On a Linux or AIX server, run **stop-wamc** command.

This command stops the WebSphere Appliance Management Center server (Figure 2-12).

```
C:\Program Files\IBM\WAMC>stop wamc.lnk
Server runtime stopped.

C:\Program Files\IBM\WAMC>
```

Figure 2-12 Stopping WebSphere Appliance Management Center server on Windows

2.3 Default ports

The WebSphere Appliance Management Center server uses default ports to the administrator workstation and to the WebSphere DataPower Appliances. The WebSphere Appliance Management Center server uses the ports as described on Table 2-1.

Table 2-1 Default WebSphere Appliance Management Center communication ports

From	To	Port	Type
Administrator machine	WebSphere Appliance Management Center server	9443	HTTPS
WebSphere Appliance Management Center server	WebSphere DataPower Appliances (except XC10)	5550	SOAP over HTTPS
WebSphere Appliance Management Center server	WebSphere DataPower XC10 Appliance	22	SSH
WebSphere DataPower Appliances (except XC10)	WebSphere Appliance Management Center server	5555	XML over HTTPS
WebSphere DataPower XC10 Appliance	WebSphere Appliance Management Center server	5556	HTTP

Figure 2-13 illustrates the communication flow of the communication ports.

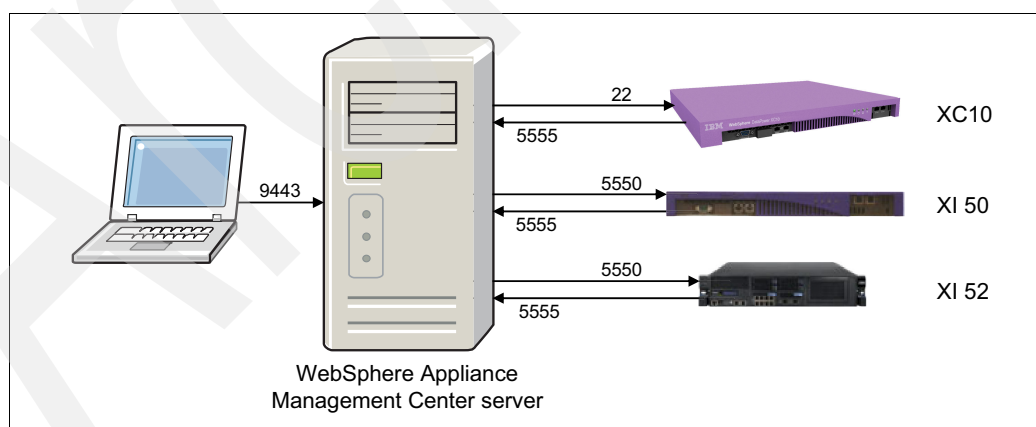


Figure 2-13 Communication flow

Firewalls: If a firewall is between the administrator workstation and the WebSphere Appliance Management Center server or between the WebSphere Appliance Management Center server and the WebSphere DataPower Appliances, open the appropriate ports on the firewall to allow communication.

2.4 Managing users and roles

User management on WebSphere Appliance Management Center can be done by using the local registry or by using an LDAP server. To use the local directory of WebSphere Appliance Management Center, see 2.4.1, “Managing users by using the local repository” on page 33. To use an LDAP server, see 2.4.2, “Managing users by using LDAP” on page 39.

Three groups are defined in WebSphere Appliance Management Center:

- ▶ SolutionDeployers group, which maps to the solution deployer role
- ▶ SystemAdministrators group, which maps to the system administrator role
- ▶ SystemOperators group, which maps to the system operator roles

Permissions are associated with these roles and not with the groups. Table 2-2 lists the permissions for each role. You cannot customize the roles in WebSphere Appliance Management Center.

Table 2-2 Permissions for each role in WebSphere Appliance Management Center

Task	System administrator	Solution deployer	System operator
Adding a firmware image to the repository	✓		
Adding appliances	✓		
Adding or editing information about firmware in the repository	✓		
Backing up appliances	✓		
Creating domains		✓	
Creating services		✓	
Deleting domains		✓	
Deleting services		✓	
Deploying firmware to appliances	✓		
Filtering appliances by group	✓	✓	✓
Filtering domains by group	✓	✓	✓
Grouping appliances	✓		
Grouping domains		✓	
Modifying appliance management properties	✓		
Modifying domain properties		✓	
Quiescing appliances	✓		
Quiescing domains		✓	
Quiescing services		✓	
Rebooting appliances	✓		
Removing appliances	✓		
Removing firmware from the repository	✓		

Task	System administrator	Solution deployer	System operator
Restarting domains		✓	
Restoring an appliance	✓		
Unquiescing appliances	✓		
Unquiescing domains		✓	
Unquiescing services		✓	
Updating an existing domain		✓	
Updating an existing service		✓	
Uploading a file to a domain		✓	
Viewing domains	✓	✓	✓
Viewing information about appliances	✓	✓	✓
Viewing information about firmware	✓	✓	✓
Viewing services	✓	✓	✓
Viewing the domain on which a service is running	✓	✓	✓
Viewing the domains of appliances	✓	✓	✓
Viewing the services on a domain	✓	✓	✓

Tip: A role applies to all WebSphere DataPower Appliances added to a WebSphere Appliance Management Center instance. If you require different permissions for different environments, consider having multiple WebSphere Appliance Management Center instances running.

2.4.1 Managing users by using the local repository

Local user management of WebSphere Appliance Management Center is file-based and is stored in the installation folder. This kind of user administration requires individual password management. The `userRegistry.xml` file is in the `<WAMC_install_dir>/config/` folder.

The Windows default installation folder is `C:\Program Files\IBM\WAMC` and the Linux and AIX default installation folder is `/opt/ibm/wamc`.

When you use the local user authentication of WebSphere Appliance Management Center, the user name must be unique and cannot have a space.

The user management tasks in the following sections are done by using the local user repository:

- ▶ Adding a user
- ▶ Testing user access
- ▶ Changing the groups that a user belongs to
- ▶ Removing a user

Adding a user

To add a user to WebSphere Appliance Management Center:

1. If you plan to encode the user password, complete the following steps. If you do not plan to encode the password, go to step 2.

Password encoding: The user password is *encoded* and *not encrypted*. The intention is to prevent accidental disclosure of the password rather than to provide security.

- a. Go to the <WAMC_install_dir>/bin folder.
- b. Run the following command:

```
password-tool <password>
```

The output is the encoded password as shown on Figure 2-14. Do not close this window. The encoded password is required in step 3 on page 34.

```
C:\Program Files\IBM\WAMC\bin>password-tool.bat testpass
{xor}KzosKy8+LCw=
C:\Program Files\IBM\WAMC\bin>_
```

Figure 2-14 Running the password encoding tool

2. Go to the installation folder, and edit the <WAMC_install_dir>/config/userRegistry.xml user repository file. Example 2-1 shows the WebSphere Appliance Management Center userRegistry.xml user repository file.

Example 2-1 Default userRegistry.xml file

```
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
  </basicRegistry>
</server>
```

3. Add new users after the group creation in the file. For each new user, add the following line to identify the user:

```
<user name="user" password="userPass"/>
```

Adding a user: The user name must be unique. The user password can be text or the encoded password that was created in step 1 on page 34.

Example 2-2 shows how to add two users, `testuser` and `testencodeduser`, to the `userRegistry.xml` user repository file. Notice that the user `testuser` has a password that is entered as text and that `testencodeduser` has a password that is encoded.

Example 2-2 Adding users to the userRegistry.xml user repository file

```
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testuser" password="testuser"/>
    <user name="testencodeduser" password="{xor}KzosKy8+LCw="/>
  </basicRegistry>
</server>
```

4. After you added the users, add them into a group to grant them appropriate access. For the permissions granted to each group, see Table 2-2 on page 32. To add users to a group, add the following line in the `userRegistry.xml` file:

```
<member name="user"/>
```

Groups: A user must be a member of one or more groups, and the permissions are the union of those groups that the user was added to. A user who is not a member of any group is unable to log in to WebSphere Appliance Management Center.

Example 2-3 shows the `userRegistry.xml` file after adding the users to the groups.

Example 2-3 Adding users to groups in the userRegistry.xml user repository file

```
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
      <member name="testuser"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
      <member name="testuser"/>
      <member name="testencodeduser"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testuser" password="testuser"/>
    <user name="testencodeduser" password="{xor}KzosKy8+LCw="/>
  </basicRegistry>
</server>
```

5. Save and close the userRegistry.xml file.

Tip: You do not need to restart the WebSphere Appliance Management Center server after you update the userRegistry.xml user repository file.

Testing user access

To test user access to WebSphere Appliance Management Center:

1. Start a web browser and enter the following address, where 9443 is the default port:
https://<wamc_server:9443/wamc
2. Enter the user ID and password and click **Log in**.

After you log in, WebSphere Appliance Management Center is displayed (Figure 2-15).

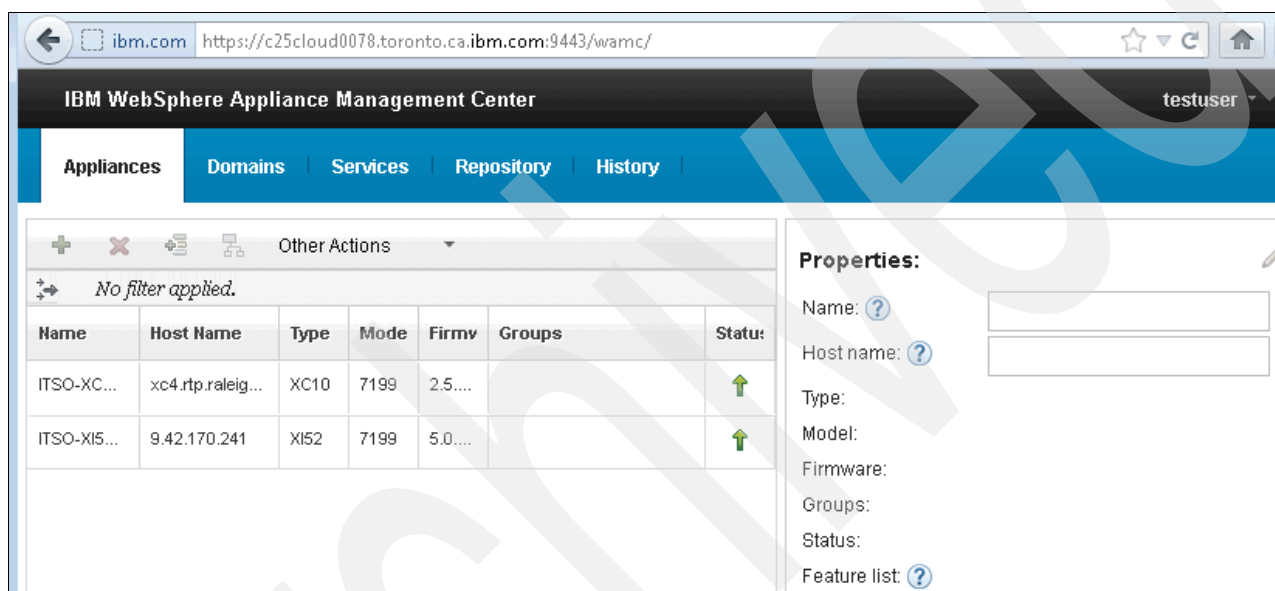


Figure 2-15 WebSphere Appliance Management Center Appliances tab

Changing the groups that a user belongs to

To change the groups that a user belongs to:

1. Go to the installation folder and edit the <WAMC_install_dir>/config/userRegistry.xml user repository file.
2. To remove a user from a group, delete the line <member name="user"/> for that user in the corresponding group from which to remove the user.
3. To add a user to a group, add the line <member name="user"/> for that user in the corresponding group to which to add the user.
4. Save and close the userRegistry.xml file.

Tip: You do not need to restart the WebSphere Appliance Management Center server after you update the userRegistry.xml user repository file.

5. Test the user access by using the steps that are described in “Testing user access” on page 36.

Changing a user password

In WebSphere Appliance Management Center, no option is available on the web interface to change the password of a user. If a user needs to change their password, the user must change it locally in the `userRegistry.xml` file:

1. If you plan to encode the user password, complete the following steps. If you do not plan to encode the user password, go to step 2.

Password encoding: The user password is *encoded* and *not encrypted*. The intention is to prevent accidental disclosure of the password rather than to provide security.

- a. Go to `<WAMC_install_dir>/bin` directory and run the following command:

```
password-tool <password>
```

The output is the encoded password as shown on Figure 2-16. Do not close this window. The encoded password is required in step 3 on page 38.

```
C:\Program Files\IBM\WAMC\bin>password-tool.bat newencodpass
{xor}MT0oOjE8MDsuPius
C:\Program Files\IBM\WAMC\bin>_
```

Figure 2-16 Running the password encoding tool for a new password

2. Go to the installation folder, and edit the user repository file:

```
<WAMC_install_dir>/config/userRegistry.xml
```

Example 2-4 shows the WebSphere Appliance Management Center `userRegistry.xml` user repository file.

Example 2-4 The `userRegistry.xml` uUser repository file

```
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
      <member name="testuser"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
      <member name="testuser"/>
      <member name="testencoduser"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testuser" password="testuser"/>
    <user name="testencodeduser" password="{xor}KzosKy8+LCw="/>
  </basicRegistry>
</server>
```

3. Change the password for the user on the `<user name="user" password="userPass"/>` line for the corresponding user name. If the password to be used is encoded, use the password that was generated in step 1 on page 37. Example 2-5 shows the changed password of `testencodeduser`.

Example 2-5 The userRegistry.xml file with testencodeduser password changed

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
      <member name="testuser"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
      <member name="testuser"/>
      <member name="testencodeduser"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testuser" password="testuser"/>
    <user name="testencodeduser" password="{xor}MToo0jE8MDsvPiws"/>
  </basicRegistry>
</server>
```

4. Save and close the `userRegistry.xml` file.

Tip: You do not need to restart the WebSphere Appliance Management Center server after you update the `userRegistry.xml` user repository file.

5. Test the user access by following the steps in “Testing user access” on page 36.

Removing a user

In WebSphere Appliance Management Center, no option is available to remove a user from the web interface. If you must remove a user, you do this task locally in the `userRegistry.xml` user repository file:

1. Go to the installation folder, and edit the `<WAMC_install_dir>/config/userRegistry.xml` user repository file
2. Delete the lines in the `userRegistry.xml` user repository file where the user name is displayed. For example, if you remove the user `testuser`, remove it from the System Operator and Solution Developers groups and delete the user name line for that user as shown in Example 2-6.

Tip: To find all the places in the `userRegistry.xml` user repository file where the user is listed, use the search tool in your editor.

Example 2-6 Removing user testuser from the userRegistry.xml file

```
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
```

```

        <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
        <member name="wamcadmin"/>
        <member name="testuser"/>
    </group>
    <group name="SolutionDeployers">
        <member name="wamcadmin"/>
        <member name="testuser"/>
        <member name="testencoduser"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testuser" password="testuser"/>
    <user name="testencoduser" password="{xor}MTooOjE8MDsvPiws"/>
</basicRegistry>
</server>

```

After you remove the user testuser, Example 2-7 shows how the userRegistry.xml file looks.

Example 2-7 The userRegistry.xml file after removing the user testuser

```

<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
      <member name="testencoduser"/>
    </group>
    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testencoduser" password="{xor}MTooOjE8MDsvPiws"/>
  </basicRegistry>
</server>

```

3. Save and close the userRegistry.xml file.

Tip: You do not need to restart the WebSphere Appliance Management Center server after you update the userRegistry.xml user repository file.

2.4.2 Managing users by using LDAP

WebSphere Appliance Management Center supports user authentication based on LDAP. By using this feature, you can use an external user repository to allow user management on a centralized box.

WebSphere Appliance Management Center supports many of the different LDAP servers that are available such as IBM Directory Server, IBM Secureway Directory, IBM Domino® Directory Server, Microsoft Active Directory, and Novell eDirectory.

The <WAMC_install_dir>\server\templates\config\ldapRegistry.xml template file in the WebSphere Appliance Management Center installation directory lists all the standards for the supported LDAP servers. For the example used in this section, we used the Microsoft Active Directory.

Configuring the userRegistry.xml file for LDAP

To configure LDAP with WebSphere Appliance Management Center:

1. Stop the WebSphere Appliance Management Center server if it is running. For more information, see 2.2.2, “Stopping the WebSphere Appliance Management Center server” on page 30.
2. Check with the LDAP administrator for the type of LDAP server that will be used.
3. Access the ldapRegistry.xml LDAP template file in the <WAMC_install_dir>\server\templates\config directory in WebSphere Appliance Management Center. Then, copy the LDAP part that corresponds to the type of LDAP server that will be used.

Example 2-8 shows the LDAP template section for Microsoft Active Directory.

Example 2-8 LDAP template section for Microsoft Active Directory

```
<ldapRegistry id="ActiveDirectoryLDAP" realm="SampleLdapADRealm"
  host="host.domain.com" port="389" ignoreCase="true"
  baseDN="cn=users,dc=domain,dc=com"
  bindDN="cn=myuser,cn=users,dc=domain,dc=com"
  bindPassword="mypassword"
  ldapType="Microsoft Active Directory"
  activeFilters="myactivefilters"/>

<activeLdapFilterProperties id="myactivefilters"
  userFilter="(& (sAMAccountName=%v) (objectcategory=user))"
  groupFilter="(& (cn=%v) (objectcategory=group))"
  userIdMap="user:sAMAccountName"
  groupIdMap="*:cn"
  groupMemberIdMap="memberof:member" />
```

4. Go to <WAMC_install_dir>\config directory, and make a backup of the userRegistry.xml file.
5. Edit the userRegistry.xml file. Comment out (or delete) the part about local authentication as shown in Example 2-9.

Example 2-9 Commenting out the local authentication part in the userRegistry.xml file

```
<!-- <server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
      <member name="testuser"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
      <member name="testuser"/>
      <member name="testencoduser"/>
    </group>
```

```

    <user name="wamcadmin" password="{xor}KD4yPC8+LCw="/>
    <user name="testuser" password="testuser"/>
    <user name="testencoduser" password="{xor}KzosKzoxPDA7Lz4sLA=="/>
  </basicRegistry>
</server> -->

```

6. Paste the part that was copied from the `ldapRegistry.xml` file in step 3 on page 40 and complete the information about the LDAP server that will be used as shown in Example 2-10. The LDAP server administrator can tell you the LDAP information for the corresponding fields in the `ldapRegistry.xml` file.

Example 2-10 Configuring the userRegistry.xml file for Microsoft Active Directory

```

<server>
  <ldapRegistry id="ActiveDirectoryLDAP" realm="SampleLdapADRealm"
    host="cdtcore1.rsmcore.mkm.can.ibm.com" port="389" ignoreCase="true"
    bindDN="CN=svc_c25c1078,CN=Users,DC=RSMCORE,DC=mkm,DC=can,DC=ibm,DC=com"
    baseDN="CN=Users,DC=RSMCORE,DC=mkm,DC=can,DC=ibm,DC=com"
    bindPassword="P@ssw0rD"
    ldapType="Microsoft Active Directory"
    activatedFilters="myactivatedfilters"/>
  <activatedLdapFilterProperties id="myactivatedfilters"
    userFilter="(& (sAMAccountName=%v) (objectcategory=user))"
    groupFilter="(& (cn=%v) (objectcategory=group))"
    userIdMap="user:sAMAccountName"
    groupIdMap="*:cn"
    groupMemberIdMap="memberof:member" />
</server>

```

Secure LDAP server: If the LDAP server used is a secure LDAP server, you must insert the following SSL information at the beginning of the `userRegistry.xml` file after the `<server>` line:

```

<featureManager>
  <feature>ssl-1.0</feature>
</featureManager>

```

7. Save and close the `userRegistry.xml` file.

Although the LDAP configuration is ready to be used, you must first change the roles of the users and groups to grant access based on an LDAP user ID or group as explained in the following section.

Granting access to LDAP users

When the WebSphere Appliance Management Center is configured for LDAP authentication, you must grant access for each LDAP user ID or group that needs access to WebSphere Appliance Management Center. The benefit of using an LDAP group is that it is easier for an administrator to grant and remove access for users.

Table 2-2 on page 32 shows the permissions that are granted to each role in WebSphere Appliance Management Center.

To grant access to LDAP users and groups for WebSphere Appliance Management Center:

1. Go to the <WAMC_install_dir>\config directory and make a backup of the roleMapping.xml file.
2. Edit the roleMapping.xml file to insert the LDAP user ID or group:
 - LDAP groups: <group name="WAMC" />
Where WAMC is the LDAP group name.
 - LDAP user IDs: <user name="c25c1078" />
Where c25c1078 is the LDAP user ID.

Example 2-11 shows the roleMapping.xml file with the changes.

Example 2-11 The roleMapping.xml file

```
<server>
  <application id="wamc" location="wamc.war">
    <application-bnd>
      <security-role name="SolutionDeployer">
        <user name="c25c1078" />
      </security-role>
      <security-role name="SystemAdministrator">
        <group name="WAMC" />
        <user name="c25c1078" />
      </security-role>
      <security-role name="SystemOperator">
        <group name="WAMC" />
        <user name="c25c1078" />
      </security-role>
    </application-bnd>
  </application>
</server>
```

3. After you add all the required LDAP user IDs and groups, save and close the roleMapping.xml file.
4. Start the WebSphere Appliance Management Center server. For more information, see 2.2.1, “Starting the WebSphere Appliance Management Center server” on page 30.

2.5 Adding and removing WebSphere DataPower Appliances

WebSphere Appliance Management Center allows for centralized management and configuration of multiple WebSphere DataPower Appliances. Adding and removing WebSphere DataPower Appliances from WebSphere Appliance Management Center does not cause the WebSphere DataPower Appliance configuration to be changed. However, a configuration object in the form of a *logging target* is added to the WebSphere DataPower Appliance configuration when you add an appliance to WebSphere Appliance Management Center. The object is removed when you remove an appliance from WebSphere Appliance Management Center.

You can use WebSphere Appliance Management Center to make configuration changes as described in the following chapters:

- ▶ Chapter 3, “Disaster recovery” on page 51
- ▶ Chapter 4, “Firmware management” on page 67
- ▶ Chapter 5, “Managing domains and services” on page 85

WebSphere Appliance Management Center reads and shows information from the WebSphere DataPower Appliance. The administrator can then send commands to the WebSphere DataPower Appliance, which receives the commands and processes them.

The following ports are used to communicate between WebSphere Appliance Management Center and the WebSphere DataPower Appliance:

- ▶ The XML Management Interface port on WebSphere DataPower SOA Appliances
- ▶ The SSH port on the WebSphere DataPower XC10 Appliance

The port is normally port 5550 for WebSphere DataPower SOA Appliances and port 22 for the WebSphere DataPower XC10 Appliance. Test the communication between the WebSphere Appliance Management Center server and the WebSphere DataPower Appliance. If required, open the firewall port. For more information, see 2.3, “Default ports” on page 31.

Important: WebSphere Appliance Management Center does not have a **Save** button. All changes that are performed are saved automatically.

2.5.1 Adding a WebSphere DataPower Appliance

To add a WebSphere DataPower Appliance to WebSphere Appliance Management Center:

1. From your web browser, go to the following address:
`https://<WAMC_server>:9443/wamc`
2. Log on to WebSphere Appliance Management Center.
3. To add a WebSphere DataPower Appliance, on the **Appliances** tab (Figure 2-17), click the plus symbol (+) button.

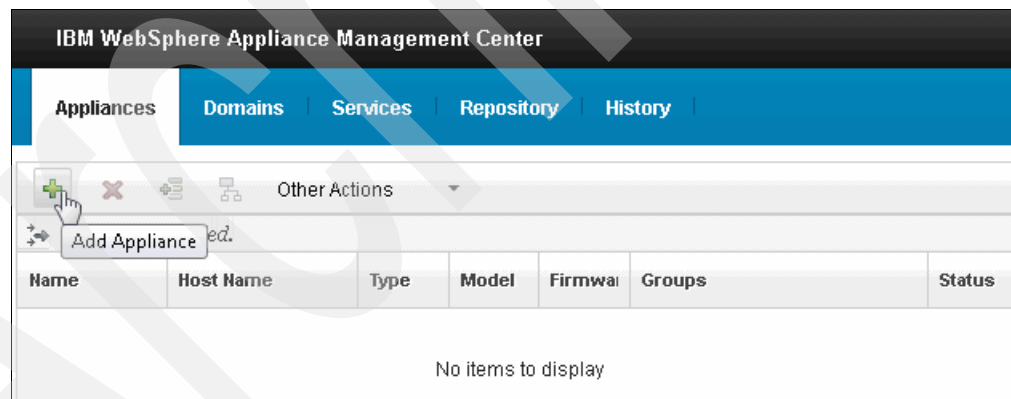


Figure 2-17 Appliances tab on the WebSphere Appliance Management Center

4. In the Add Appliance dialog box (Figure 2-18):
 - a. For Name, enter the WebSphere DataPower Appliance name. This name is the logical name by which the appliance will be known to WebSphere Appliance Management Center and not a pre-existing name.
 - b. For Host name, enter the WebSphere DataPower Appliance host name or IP address.
 - c. For AMP port, enter the port number of the WebSphere DataPower Appliance on which the XML management interface is running with the Appliance Management Protocol (AMP) enabled. By default, this port is port 5550. For WebSphere DataPower XC10 Appliances, the default port is port 22.
 - d. For Appliance administrator ID, enter the user ID of the WebSphere Appliance Management Center administrator.
 - e. For Appliance administrator password, enter the password of the WebSphere Appliance Management Center administrator.
 - f. Click the **Add** button.

Supported WebSphere DataPower Appliances: For a list of WebSphere DataPower Appliances that are supported by WebSphere Appliance Management Center, see 1.5, “Supported WebSphere DataPower Appliances” on page 8.

Add Appliance

* Name: ? ITS0-XI50-TOR-1

* Host name: ? 9.23.237.54

* AMP port: ? 5550

* Appliance administrator ID: Admin1

* Appliance administrator password:

Add **Cancel**

Figure 2-18 Adding a WebSphere DataPower Appliance

The WebSphere DataPower Appliance is then shown in WebSphere Appliance Management Center. As shown in Figure 2-19, when a WebSphere DataPower Appliance is selected, the properties of that appliance are displayed on the right side of the page.

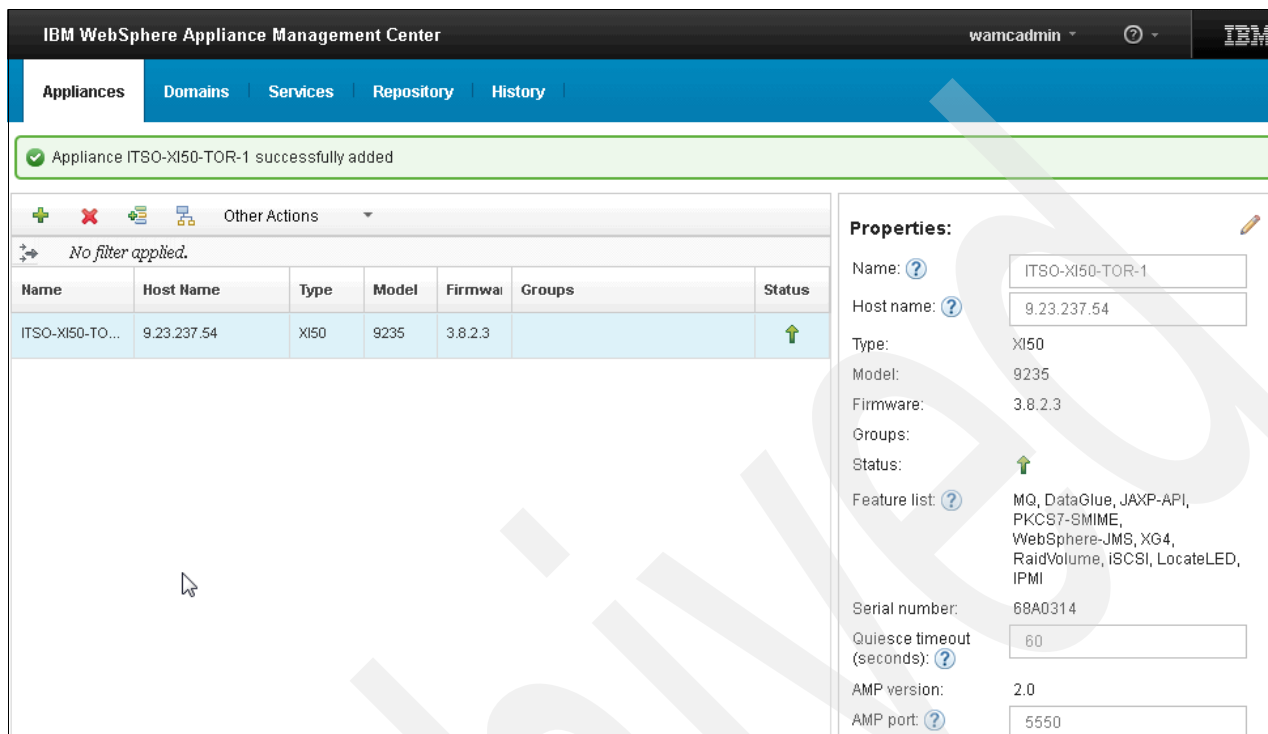


Figure 2-19 Displaying information about a specific WebSphere DataPower Appliance

For more information about the WebSphere DataPower Appliance properties that are displayed, see the *Managing appliances* topic in the WebSphere Appliance Management Center Information Center:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/manage_appliances.html

2.5.2 Removing a WebSphere DataPower Appliance

To remove a WebSphere DataPower Appliance from WebSphere Appliance Management Center:

Attention: Removing the WebSphere DataPower Appliance from WebSphere Appliance Management Center does not erase or delete any data or configuration on the WebSphere DataPower Appliance.

1. From a web browser, go to the following address:
`https://<WAMC_server>:9443/wamc`
2. Log on to WebSphere Appliance Management Center.

- On the **Appliances** tab (Figure 2-20), select the WebSphere DataPower Appliance that will be removed from WebSphere Appliance Management Center. Then, click the **Remove Appliance** (✖) icon.

Tip: After you select the WebSphere DataPower Appliance to remove from WebSphere Appliance Management Center, verify that it is the correct appliance to be removed. To verify whether it is the correct appliance, check the serial number and host name of the appliance that is displayed in the Properties box on the right side of the window. This way, you can avoid removing the wrong WebSphere DataPower Appliance.

IBM WebSphere Appliance Management Center

Appliances Domains Services Repository History

Remove Appliance

Name	Host Name	Type	Model	Firmware	Groups	Status
ITSO-XC10-1	xc4.rtp.raleigh.ibm....	XC10	7199	2.5.0....		↑
ITSO-XI50-TOR-1	9.23.237.54	XI50	9235	3.8.2.3		↑
ITSO-XI52-1	9.42.170.241	XI52	7199	5.0.0.0		↑

Properties:

Name: ITSO-XI50-TOR-1

Host name: 9.23.237.54

Type: XI50

Model: 9235

Firmware: 3.8.2.3

Groups:

Status: ↑

Feature list: MQ, DataGlue, JAXP-API, PKCS7-SMIME, WebSphere-JMS, XG4, RaidVolume, iSCSI, LocateLED, IPMI

Serial number: 68A0314

Quiesce timeout (seconds): 60

AMP version: 2.0

AMP port: 5550

Appliance administrator ID: Admin1

Figure 2-20 Removing a WebSphere DataPower Appliance from WebSphere Appliance Management Center

- In the confirmation dialog box, click **Remove**.

After the WebSphere DataPower Appliance is removed from WebSphere Appliance Management Center, a confirmation message is displayed at the top of the window (Figure 2-21).

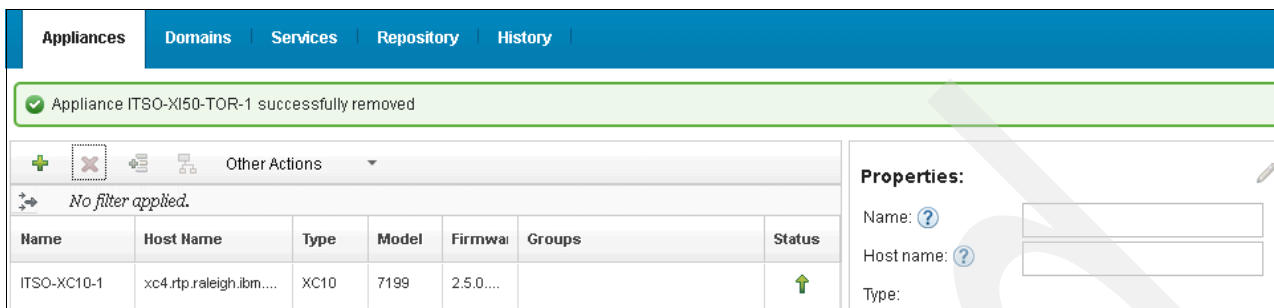


Figure 2-21 WebSphere DataPower Appliance successfully removed confirmation message

2.5.3 Grouping WebSphere DataPower Appliances

WebSphere Appliance Management Center manages multiple WebSphere DataPower Appliances. As more appliances are added to WebSphere Appliance Management Center, it can become difficult to keep track of which appliances belong to which departments or stages of the software development lifecycle (for example, development, test, and production).

To help with the management of large numbers of WebSphere DataPower Appliances, WebSphere Appliance Management Center allows for grouping WebSphere DataPower Appliances together by using user-defined group names. The list of displayed appliances can then be filtered by using the group name so that actions on multiple WebSphere DataPower Appliances can be targeted easily at any specific group.

You can add a WebSphere DataPower Appliance to a group, remove an appliance from a group, and filter a group.

Adding WebSphere DataPower Appliances to a group

To add a WebSphere DataPower Appliance to a group:

1. Log on to WebSphere Appliance Management Center as a user with the system administrator role.
2. On the **Appliances** tab, select the WebSphere DataPower Appliance or Appliances to add to a group. Then, click the **Assign groups** icon (Figure 2-22).

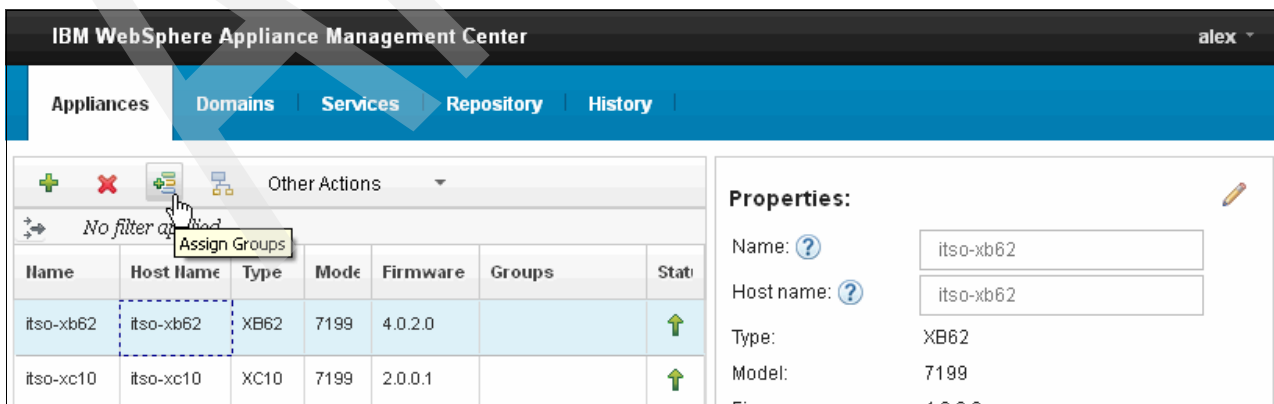
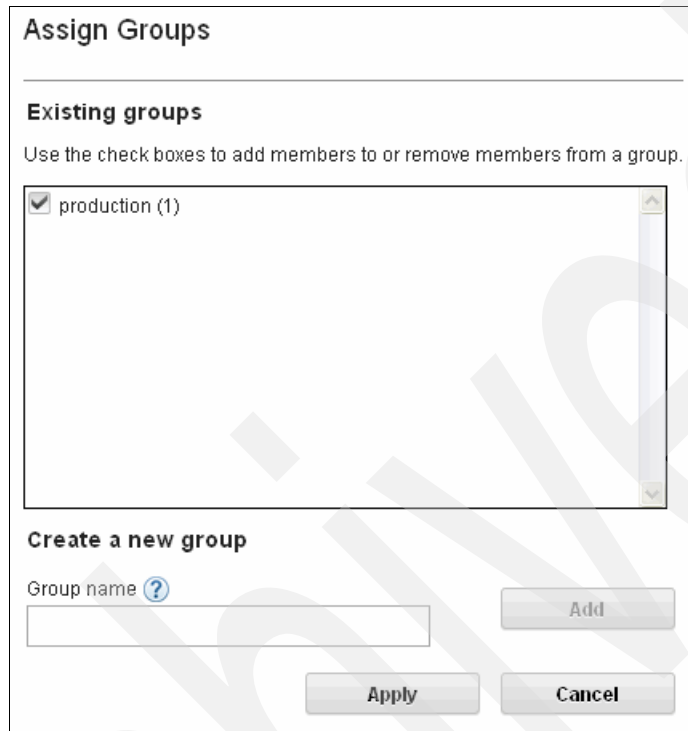


Figure 2-22 Assigning groups

3. In the Assign Groups dialog box (Figure 2-23), add WebSphere DataPower Appliances to groups by using either of the following options:
 - Selecting an existing group from the Existing groups
 - Creating a group by entering a name for the group in the Group name field and clicking **Add**



The image shows a screenshot of the 'Assign Groups' dialog box. The dialog has a title bar 'Assign Groups'. Below the title bar, there is a section titled 'Existing groups' with a subtitle 'Use the check boxes to add members to or remove members from a group.' Below this subtitle is a list box containing one item: 'production (1)' with a checked checkbox. Below the list box is a section titled 'Create a new group'. This section contains a text field labeled 'Group name' with a help icon, an 'Add' button, and an 'Apply' button. At the bottom right of the dialog is a 'Cancel' button.

Figure 2-23 Assign Groups dialog box

4. To add more groups, repeat step 3. After all required changes are made, click **Apply** to save the changes. Then, close the Assign Groups dialog box.

Removing WebSphere DataPower Appliances from a group

To remove WebSphere DataPower Appliances from a group:

1. Log on to WebSphere Appliance Management Center as a user with the system administrator role.
2. On the **Appliances** tab, select the WebSphere DataPower Appliances that you want to remove from a group. Then, click the **Assign groups** icon (Figure 2-22 on page 47).
3. In the Assign Groups dialog box (Figure 2-23), to remove all selected WebSphere DataPower Appliances from a group, find the group in the Existing groups list. Then, clear the check box next to the group name to deselect the group.
4. Repeat step 3 for all groups from which you want to remove the selected WebSphere DataPower Appliances. Click **Apply** to save the changes. Then, close the Assign Groups dialog box.

Filtering WebSphere DataPower Appliances by using groups

To filter the WebSphere DataPower Appliances that are displayed by using a group:

1. Log on to WebSphere Appliance Management Center.
2. On the **Appliances** tab, click the **Define filter** icon (Figure 2-24).

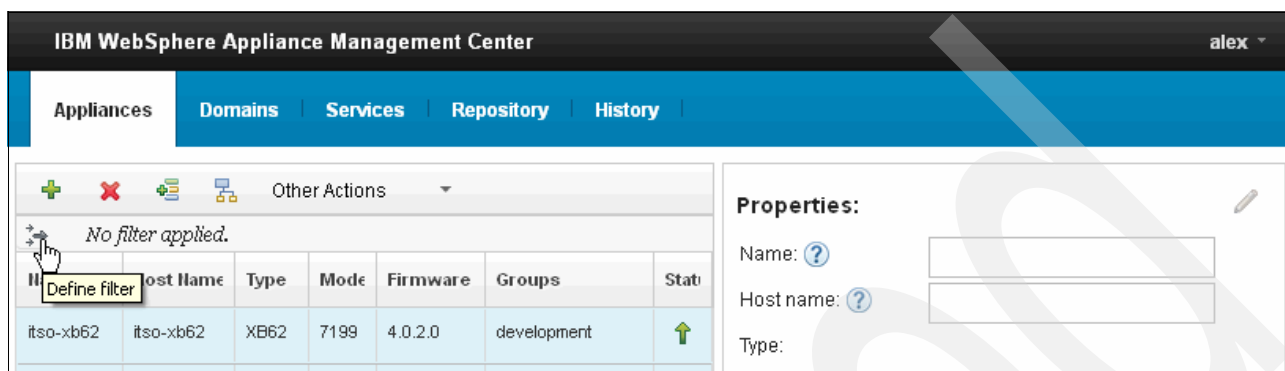


Figure 2-24 Selecting the Define filter icon

3. In the Filter dialog box (Figure 2-25):
 - a. For the Column field, select **Groups**.
 - b. For the Condition field, select an appropriate condition for filtering, for example **contains**.
 - c. For the Value field, select or type the name of a group to filter on.
 - d. Click **Filter** to apply the filter.
 - e. Close the dialog box. The list of displayed WebSphere DataPower Appliances is updated to reflect the filter that is applied.



Figure 2-25 Defining a filter

Archived

Disaster recovery

You can perform a secure backup and restore for IBM WebSphere DataPower Appliances that are managed by IBM WebSphere Appliance Management Center. With a secure backup and restore, you can perform a full backup of a WebSphere DataPower Appliance configuration and then restore the image to another compatible WebSphere DataPower Appliance.

Benefits of a secure backup and restore include disaster recovery and workarounds for appliance problems. Backup files are encrypted and can be stored locally or to an alternate location.

This chapter describes appliance preparation, detailed implementation steps, and post validation. This chapter includes the following sections:

- ▶ Introduction to disaster recovery of WebSphere DataPower Appliances
- ▶ Secure backup
- ▶ Backing up WebSphere DataPower Appliances
- ▶ Secure restore
- ▶ Restoring a WebSphere DataPower Appliance

3.1 Introduction to disaster recovery of WebSphere DataPower Appliances

By using the disaster recovery functions in WebSphere DataPower Appliances, system administrators can create a backup of a WebSphere DataPower Appliance. Then, they can restore it to a compatible WebSphere DataPower Appliance. A compatible WebSphere DataPower Appliance is one with identical firmware level and storage capacity.

The backup files are encrypted so that they can be stored locally or saved to an alternative FTP location. Unlike a standard backup, a secure backup contains certificates, keys, and user passwords that are not included in a standard backup.

No disaster recovery feature: This section does not apply to the following products because they do not provide the disaster recovery feature:

- ▶ IBM WebSphere DataPower XC10 Appliance
- ▶ IBM WebSphere DataPower Blade on zEnterprise
- ▶ Any WebSphere DataPower Appliances with a firmware level before version 3.8.1.0

Secure backup creates a set of files that you can use with a secure restore for multiple purposes:

- ▶ Assure WebSphere DataPower Appliance recovery.
- ▶ At end of life of a WebSphere DataPower Appliance, move the configuration to a replacement WebSphere DataPower Appliance.
- ▶ Use the backup from one WebSphere DataPower Appliance to configure multiple, similar function, and compatible WebSphere DataPower Appliances.

3.1.1 Disaster recovery mode

A system administrator can select only WebSphere DataPower disaster recovery mode at installation time. By using this mode, a system administrator can take a backup of the WebSphere DataPower Appliance. When the appliance is not in disaster recovery mode (instead is in normal mode), the WebSphere DataPower Appliance cannot export cryptography keys. When disaster recovery mode is selected, the WebSphere DataPower Appliance can encrypt the keys and other data. After the disaster recovery mode is set, you cannot change it without reinitializing the WebSphere DataPower Appliance.

Important: You can secure restore a WebSphere DataPower Appliance in normal mode. However, if a WebSphere DataPower Appliance in normal mode is restored, the restore proceeds and permanently changes the WebSphere DataPower Appliance to secure mode during the process.

3.1.2 WebSphere DataPower cryptographic objects

For more information about the WebSphere DataPower Appliance cryptographic objects that are used on a secure backup and restore, see the following IBM WebSphere DataPower Integration Appliance Version 5.0 Information Center topics:

- Creating certificates

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/index.jsp?topic=%2Fcom.ibm.dp.xi.doc%2Fconfiguringdodpki06.htm&path%3D4_6_0_5

- Creating validation credentials

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/index.jsp?topic=%2Fcom.ibm.dp.xi.doc%2Fconfiguringdodpki07.htm&path%3D4_6_0_6

- Creating identification credentials

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/index.jsp?topic=%2Fcom.ibm.dp.xi.doc%2Fconfiguringdodpki08.htm&path%3D4_6_0_7

3.2 Secure backup

By using the secure backup function, system administrators can copy private data from a WebSphere DataPower Appliance. You can use the backup file in various ways, including disaster recovery, appliance end-of-life process, or replicating WebSphere DataPower Appliance settings to other appliances.

3.2.1 Secure backup basics

To use the secure backup command, you must set the WebSphere DataPower Appliance to disaster recovery mode at initialization time. The backup can be saved locally on the WebSphere DataPower Appliance in the `local` or temporary directories. Alternatively, you can save the backup remotely to an alternative location by using FTP or download it by using WebSphere Appliance Management Center.

To perform a secure backup, a public certificate is required for encrypting the backup data. To restore the backup files, the private key that is associated with the public certificate is required.

The backup is a collection of compressed, encrypted files with a *manifest*. The manifest is signed to ensure data integrity. It describes the WebSphere DataPower Appliance firmware level, backup date, settings, and certificate that are used for encryption. The manifest also includes a list of the encrypted files with their size and checksum. No firmware-related files are included in the backup, which enables the backup to be as small as possible. However, at restore time, the WebSphere DataPower Appliance must match the firmware level exactly.

Important: Any attempt to alter the backup files or the manifest renders the backup invalid and unusable.

Data that is user and administrator accessible includes data in the `store`, `config`, and `local` directories and data on the compact flash, iSCSI, or RAID volumes that are included in the backup, if they exist. The data that users and administrators do not have direct access to are keys and password data in the `cert`, `dpcert`, and `sharedcert` directories. Data in hierarchical storage management (HSM) are not backed up, and therefore, are not included as part of the backup.

Although you can perform backups on a working WebSphere DataPower Appliance, you must take the backups carefully to ensure their usability. Backups of appliances with RAID or iSCSI devices and backups of heavily used WebSphere DataPower Appliances might require significant amounts of time. For a complete list of best practices, see 3.2.3, “Considerations for secure backup” on page 54.

3.2.2 Encryption and security

Data that is visible to the user and administrator is encrypted by using an ephemeral symmetric key. This key is encrypted with the public key that is provided on the secure backup command before it is stored in the manifest file. The visible data includes, for example, configuration files, style sheets, and data files. Data from the WebSphere DataPower Appliance that users and administrators cannot view, such as private keys, are encrypted twice. First, the data is encrypted by using an appliance key, and then it is encrypted by using the same ephemeral key as the user visible data.

With the signature of the manifest and the encrypted data files, an administrator can be assured that the backup cannot be manipulated. Without the private key pair of the public certificate that is used on the backup, the files cannot be restored and used.

Important: Because the backup contains private keys and other data, treat it like any other critical data and protect it appropriately.

The idea behind the series of security measures in the secure backup is that a system administrator can determine information about the backup from the manifest, but only users with the private key can decrypt the backup. Any attempt to alter the files or the manifest renders the backup invalid and unusable.

3.2.3 Considerations for secure backup

When you create your backup policy and when you perform secure backups, keep in mind the following practices and considerations:

- ▶ Quiesce the WebSphere DataPower Appliance before the secure backup to ensure that all processing activity is ceased.
- ▶ Before you back up a WebSphere DataPower Appliance, ensure that all configurations are saved. Only saved data is backed up.
- ▶ Ensure that configuration files, style sheets, and other data are not modified during the backup operation.
- ▶ If backups are local, ensure that enough space is available on the WebSphere DataPower Appliance.
- ▶ If backups are remote, ensure that the network bandwidth and space in the target directory are sufficient.
- ▶ Because of the amount of time and space that are required to back up iSCSI and RAID data, use methods other than secure backup. If iSCSI or RAID data can be backed up by using other methods, select the secure backup switch to exclude backing up iSCSI or RAID data.
- ▶ HSM data is not included in the backup.
- ▶ Transient data, such as logs, is not included in the backup.
- ▶ After the backup process, protect the backup files that same as you might do for any other critical data.

- ▶ Keep the private key of the public certificate that is used to create the secure backup. It is required to restore the secure backup.
- ▶ After each firmware upgrade or appliance application modification, create a backup.
- ▶ The firmware at backup time must match the firmware at restore time.
- ▶ You can store the secure backup files locally or remotely. Valid protocols are local, temporary, or FTP. You can also download them by using WebSphere Appliance Management Center.
- ▶ Secure backup overwrites previous backups when writing to the same destination. The exception is for files that are made available for download from WebSphere Appliance Management Center because they contain a timestamp in the file name.
- ▶ You can determine information about the secure backup from the manifest file, but do not attempt to manipulate the .tgz files.

3.3 Backing up WebSphere DataPower Appliances

To guard against the risk of losing important information, back up your WebSphere DataPower Appliances periodically. You must have a good backup policy in place for all the WebSphere DataPower Appliances in your environment. This section explains how to perform a secure backup on your WebSphere DataPower Appliances by using the WebSphere Appliance Management Center.

No disaster recovery feature: This section does not apply to the following products because they do not provide the disaster recovery feature:

- ▶ IBM WebSphere DataPower XC10 Appliance
- ▶ IBM WebSphere DataPower Blade on zEnterprise
- ▶ Any WebSphere DataPower Appliances with a firmware level before version 3.8.1.0

3.3.1 Before you begin

Before you run a secure backup, you must meet the following prerequisites:

- ▶ For a complete list of important points to consider before you begin a secure backup, see 3.2.3, “Considerations for secure backup” on page 54.
- ▶ You must log on to WebSphere Appliance Management Center with a user ID that is assigned the system administrator role.
- ▶ You must add at least one WebSphere DataPower Appliance to the WebSphere Appliance Management Center.
- ▶ You must enable secure backup on the WebSphere DataPower Appliance during initialization of the appliance. Otherwise, the operation will fail. For more information, see 3.1.1, “Disaster recovery mode” on page 52.
- ▶ You must have a cryptographic certificate object defined on the WebSphere DataPower Appliance or have the certificate file on your local server or on a remote HTTP server. For more information to cryptographic objects, see 3.1.2, “WebSphere DataPower cryptographic objects” on page 53.
- ▶ Allow sufficient time for backups of WebSphere DataPower Appliances with RAID or iSCSI devices and backups of heavily used appliances because they might require significant amounts of time.

3.3.2 Performing a secure backup

To perform a secure backup of a WebSphere DataPower Appliance:

1. Log on to WebSphere Appliance Management Center with a user ID that is assigned the system administrator role.
2. On the **Appliances** tab in the IBM WebSphere Appliance Management Center, select the WebSphere DataPower Appliance that you want to perform the secure backup. Click **Other Actions** → **Backup Appliance** (Figure 3-1).

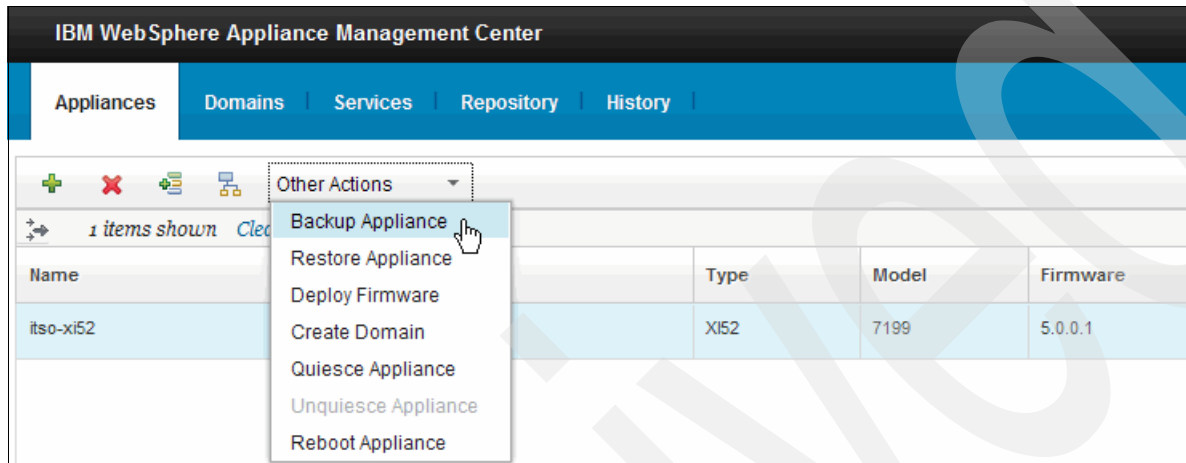


Figure 3-1 Selecting the Backup Appliance option

3. In the Backup Appliance window (Figure 3-2), provide a cryptographic certificate by selecting an option that specifies the location of the cryptographic certificate:
 - If the cryptographic certificate is on the WebSphere DataPower Appliance, select the **Crypto certificate object name** option. Then, enter the cryptographic certificate object name.
 - If the cryptographic certificate object is in a .pem file that is saved locally, select **Local file**. Click **Browse** to specify the location of the .pem file.
 - If you exported the certificate object to a .pem file and saved it on a remote HTTP server, select **Remote location (URL)**. Then, enter the location of the .pem file on the server.

Click **Next**.

The screenshot shows the 'Backup Appliance' window. The title is 'Backup Appliance'. Below the title, there is a section titled 'Provide the crypto certificate:'. The text below this title says: 'Crypto certificates contain a public key that is used to encrypt the secure backup file. Use one of the following options to specify where the crypto certificate is located.' There are three radio button options: 'Crypto certificate object name: ?' (selected), 'Local file:', and 'Remote location (URL): ?'. To the right of the 'Crypto certificate object name' option, there is a text input field containing 'itso-securebackup'. Below the 'Local file:' option, there is a text input field and a 'Browse' button. Below the 'Remote location (URL): ?' option, there is a text input field.

Figure 3-2 Specifying the cryptographic certificate to use for encryption of the secure backup file

Cryptographic certificates contain a public key that is used to encrypt the secure backup file. For more information, see 3.1.2, “WebSphere DataPower cryptographic objects” on page 53.

4. Specify a location in which to save the backup (Figure 3-3):

- To save the backup files onto the computer that you are using to run the web browser, select **File for download**.
- To save the backup files in a subdirectory of the `local://` directory on the WebSphere DataPower Appliance that you are backing up, select **Appliance local file directory**, and then, specify the subdirectory name.
- To save the backup files in a subdirectory of the `temporary://` directory on the WebSphere DataPower Appliance that you are backing up, select **Appliance temporary file directory**, and then, specify the subdirectory name.
- To save the backup files on an FTP server, select **Remote FTP location** and enter the following information for the FTP server:
 - i. In the Host name field, enter the host name or IP address of the FTP server.
 - ii. In the Port field, enter the port number of the FTP server. Typically this port is port 21, but it depends on your network environment.
 - iii. In the Filepath field, enter the name of the directory where you want to save the backup files.
 - iv. In the FTP User ID field, enter the user ID that is used to log on to the FTP server.
 - v. In the FTP User password field, enter the password of the user ID that is used to log on to the FTP server.

Click **Next**.

Backup Appliance

Specify where to save the backup:

☒ File for download ?

☐ Appliance local file directory: local://

☐ Appliance temporary file directory: temporary://

☐ Remote FTP location:

Host name: ?

Port:

Filepath:

FTP user ID:

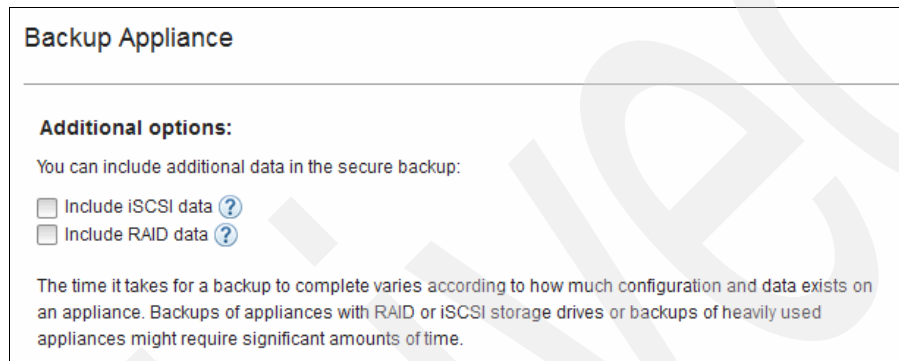
FTP user password:

Figure 3-3 Specifying the location of the secure backup file

5. Optional: If the WebSphere DataPower Appliance that you are backing up contains iSCSI or RAID storage drives, include data from these storage drives in the backup files (Figure 3-4).
 - If the WebSphere DataPower Appliance that you are backing up contains an iSCSI storage drive, select **Include iSCSI data**.
 - If the WebSphere DataPower Appliance that you are backing up contains a RAID storage drive, select **Include RAID data**.

Tip: Because of the amount of time and space that are required to back up iSCSI and RAID data, use methods other than secure backup.

Click **Backup**.



The screenshot shows a dialog box titled "Backup Appliance". Inside, there is a section "Additional options:" with the text "You can include additional data in the secure backup:". Below this text are two checkboxes: "Include iSCSI data" and "Include RAID data", each followed by a question mark icon. At the bottom of the dialog, there is a paragraph of text: "The time it takes for a backup to complete varies according to how much configuration and data exists on an appliance. Backups of appliances with RAID or iSCSI storage drives or backups of heavily used appliances might require significant amounts of time."

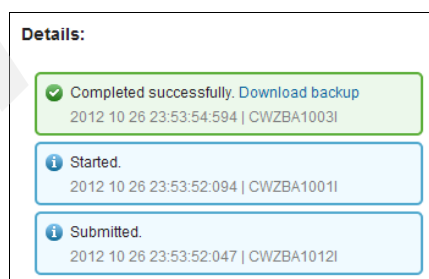
Figure 3-4 Selecting to include iSCSI and RAID data in the backup

6. Check the status of the backup operation on the **History** tab of the IBM WebSphere Appliance Center.
7. If you selected the **File for download** option, download the backup before it expires:

Backup file for download: The backup file for download is automatically deleted from WebSphere Appliance Management Center seven days after it is created.

- a. On the **History** tab in WebSphere Appliance Management Center, select the row that represents this backup operation.
- b. In the Details window (Figure 3-5), in the success message, click **Download backup** to download the compressed file that contains backup files to a location of your choice.

Download link: This download link is also displayed in the message that is shown in the feedback area when the backup completes.



The screenshot shows a "Details:" panel with three status messages in a list. The first message is "Completed successfully. Download backup" with a green checkmark icon, followed by the timestamp "2012 10 26 23:53:54:594 | CWZBA1003I". The second message is "Started." with an information icon, followed by the timestamp "2012 10 26 23:53:52:094 | CWZBA1001I". The third message is "Submitted." with an information icon, followed by the timestamp "2012 10 26 23:53:52:047 | CWZBA1012I".

Figure 3-5 History panel showing the secure backup status

3.4 Secure restore

By using the disaster recovery mode in WebSphere DataPower Appliances, system administrators can restore a WebSphere DataPower Appliance with the backup that was previously created by a secure backup. The secure restore runs on a WebSphere DataPower Appliance that has a valid network configuration and storage definition. However, the secure restore overwrites this valid configuration information with the restored backup files and then restarts the WebSphere DataPower Appliance.

Tip: After the restore operation and before you place the WebSphere DataPower Appliance into service, verify that the configuration information was restored from the backup.

3.4.1 Secure restore basics

To restore a secure backup, you need the private key and public certificate (together called a *crypto identification credential*) that corresponds to the backup files that are being restored. For more information about WebSphere DataPower cryptographic objects, see 3.1.2, “WebSphere DataPower cryptographic objects” on page 53.

The backup is a collection of compressed, encrypted files with a signed manifest. The manifest is signed to ensure data integrity. It describes the WebSphere DataPower Appliance firmware level, backup date, appliance settings, and the certificate that was used for encryption. The manifest also lists the encrypted files with size and checksum. No firmware-related files are included in the backup, which enables the backup to be as small as possible. However, at restore time, the WebSphere DataPower Appliance must match the firmware level.

Secure restore involves the following key factors:

- ▶ The WebSphere DataPower Appliance to restore to must be compatible with the backup files. The same firmware version and level must be installed on the WebSphere DataPower Appliance before the restore process.
- ▶ The WebSphere DataPower Appliance must have enough space to contain the data in the backup files. For example, if the backup contained iSCSI or RAID data, the restoring WebSphere DataPower Appliance must be configured with the same storage.
- ▶ The restored WebSphere DataPower Appliance can have more storage space than the WebSphere DataPower Appliance from which it was backed up.

Important: During the restore process, all data on the WebSphere DataPower Appliance is deleted. The restore process does a complete replacement and does not merge data. Therefore, the WebSphere DataPower Appliance to be restored to must contain only the configuration data that is needed for the restore process.

3.4.2 Considerations for the secure restore process

When you create your backup policy and restore secure backups, keep in mind the following practices and considerations:

- ▶ Quiesce the WebSphere DataPower Appliance before the secure restore to ensure that all processing activity is ceased.
- ▶ Run secure restore only on a clean (reinitialized) WebSphere DataPower Appliance.
- ▶ The cryptographic identification credential, which is based on the public certificate that is used for the secure backup, must exist on the restore WebSphere DataPower Appliance.

- ▶ When the restore process is complete, resolve any differences, such as IP addresses and gateways, between the backup and restored to WebSphere DataPower Appliance.
- ▶ The secure restore process restarts the WebSphere DataPower Appliance. Therefore, quiesce the WebSphere DataPower Appliance before you begin the restore process.
- ▶ The password for the administration user ID is reset to admin after the restore process. You must change it the first time you log in after the restore process.
- ▶ After you begin a secure restore, you cannot recover any existing data on the WebSphere DataPower Appliance.

3.5 Restoring a WebSphere DataPower Appliance

By using the restore appliance function, system administrators can restore a WebSphere DataPower Appliance with a backup that was previously created by a secure backup.

No disaster recovery feature: This section does not apply to the following products because they do not provide the disaster recovery feature:

- ▶ IBM WebSphere DataPower XC10 Appliance
- ▶ IBM WebSphere DataPower Blade on zEnterprise
- ▶ Any WebSphere DataPower Appliances with a firmware level before version 3.8.1.0

3.5.1 Before you begin

Before and after you run a secure restore, you must meet the following prerequisites:

- ▶ For a list of important points to consider *before* you start a secure backup restore, see 3.4.2, “Considerations for the secure restore process” on page 59.
- ▶ For a list of important points that require attention *after* the restore process, see 3.5.3, “What to do next” on page 63.
- ▶ You must log on to WebSphere Appliance Management Center with a user ID that is assigned the system administrator role.
- ▶ You must add at least one WebSphere DataPower Appliance to the WebSphere Appliance Management Center.
- ▶ You can secure restore a WebSphere DataPower Appliance in normal mode. However, if a WebSphere DataPower Appliance in normal mode is restored, the restore proceeds and permanently change the WebSphere DataPower Appliance to secure mode during the process.
- ▶ You must have a cryptographic identification credential object that is defined on the WebSphere DataPower Appliance with the certificate and key that are used to save and encrypt the secure backup that you are now restoring. For more information about WebSphere DataPower cryptographic objects, see 3.1.2, “WebSphere DataPower cryptographic objects” on page 53.

3.5.2 Performing a secure restore

To perform a secure restore of a WebSphere DataPower Appliance:

1. Log on to WebSphere Appliance Management Center with a user ID that is assigned the system administrator role.
2. On the **Appliances** tab in WebSphere Appliance Management Center, select the WebSphere DataPower Appliance for which you want to perform the restore. You must restore one WebSphere DataPower Appliance at a time. Click **Other Actions** → **Restore Appliance** (Figure 3-6).

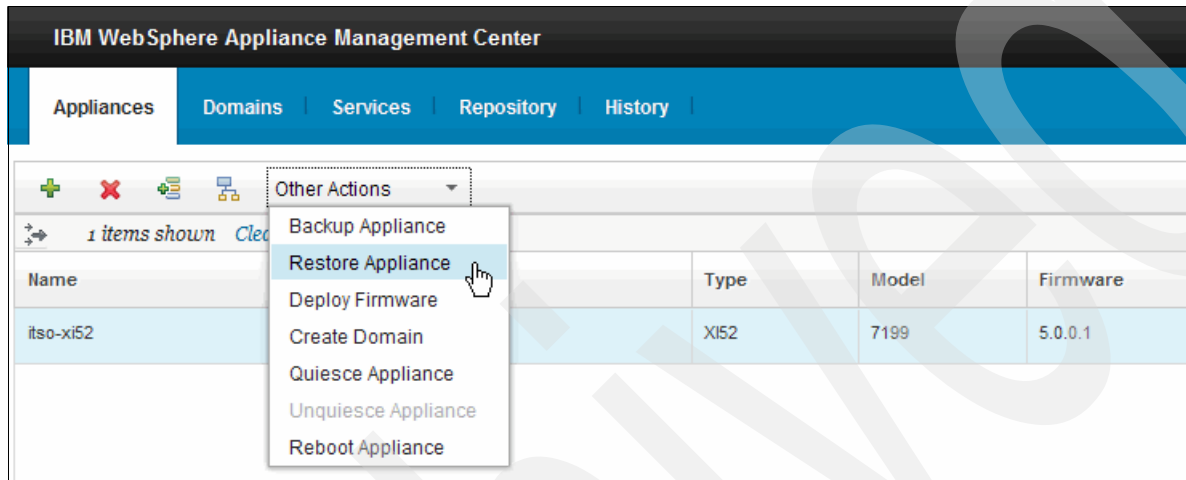


Figure 3-6 Selecting the Restore Appliance option

3. In the Crypto identification credential object name field, enter a cryptographic identification credential object name that corresponds to the secure backup (Figure 3-7). Click **Next**.
For more information about the cryptographic identification credential, see 3.1.2, “WebSphere DataPower cryptographic objects” on page 53.

Restore Appliance

Provide the crypto identification credential:

Crypto certificates contain a public key that is used to encrypt a secure backup file. You must provide the corresponding crypto identification credential to perform this secure restore.

Crypto identification credential object name: [?](#)

[Link to the appliance web GUI](#)

Figure 3-7 Providing the cryptographic identification credential name

4. Specify the directory where the backup is saved by choosing one of the following options (Figure 3-8):
- If the backup files are saved in a directory on the computer that you are using to run the web browser, select **Local file**, and click **Browse**. Then, specify the name of the compressed file that contains the backup files.
 - If the backup files are saved in a subdirectory of the `local://` directory on the WebSphere DataPower Appliance that you want to restore, select **Appliance local file directory**, and specify the subdirectory name.
 - If the backup files are saved in a subdirectory of the `temporary://` directory on the WebSphere DataPower Appliance that you want to restore, select **Appliance temporary file directory**, and specify the subdirectory name.
 - If the backup files are saved on an FTP server, select **Remote FTP location**, and enter the following information for your FTP server:
 - i. In the Host name field, enter the host name or IP address of the FTP server.
 - ii. In the Port field, enter the port number of the FTP server. Typically the port number is port 21, but the number depends on your network environment.
 - iii. In the Filepath field, enter the name of the directory where the backup configuration files are saved.
 - iv. In the FTP user ID field, enter the user ID that is used to log on to the FTP server.
 - v. In the FTP user password field, enter the password of the user ID that is used to log on to the FTP server.

Click **Restore**.

Restore Appliance

Specify where the backup is saved:

☒ Local file:

☐ Appliance local file directory: local://

☐ Appliance temporary file directory: temporary://

☐ Remote FTP location:

Host name:

Port:

Filepath:

FTP user ID:

FTP user password:

Figure 3-8 Specifying the directory where the backup is saved

The WebSphere DataPower Appliance is quiesced and the restore starts. You can check the status of the restore operation on the **History** tab of the IBM WebSphere Appliance Center (Figure 3-9).

Tip: After the restore reports completion, the WebSphere DataPower Appliance is unavailable for some time while the restart completes.

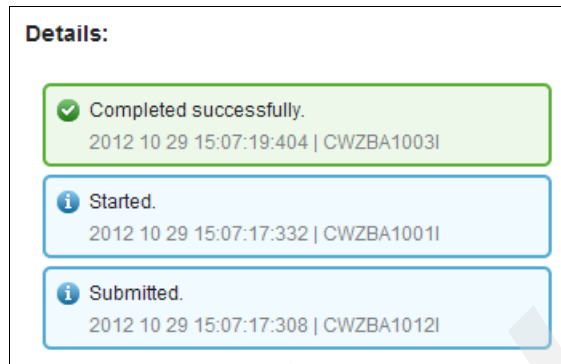


Figure 3-9 History panel showing the restore status

5. Change the password for the administrator user ID the first time you log in after the restore process because it is reset to `admin` after the restore process.
6. Update the WebSphere DataPower Appliance credentials on WebSphere Appliance Management Center. Otherwise, you will be unable to manage it after the restore process.

For more information about changing user passwords in WebSphere Appliance Management Center, see 2.4, “Managing users and roles” on page 32.

Important: Although the restore process is completed, before you enable the restored WebSphere DataPower Appliance, verify that you have handled all procedures that are mentioned in the next section.

3.5.3 What to do next

After the secure restore is complete, the WebSphere DataPower Appliance is restarted and assumes the configuration from the backup. After the restore completes and before you enable the WebSphere DataPower Appliance, consider the topics in this section.

Passwords

After a secure restore, the password for the administrative user is reset to the factory default of `admin`. WebSphere Appliance Management Center is configured to use the administrative user to log on to the WebSphere DataPower Appliance. Therefore, WebSphere Appliance Management Center is unable to implement any actions that require communication with the WebSphere DataPower Appliance until the passwords are modified so that they match. For more information about changing user passwords in WebSphere Appliance Management Center, see 2.4, “Managing users and roles” on page 32.

The system administrator must immediately log in by using the `admin` ID and change the default password then as required. The `admin` ID can then be used to reset any other user or administrator password on the WebSphere DataPower Appliance.

You can use a list of user IDs that are defined on the WebSphere DataPower Appliance to proactively warn users that their passwords have been changed. You can use either of the following methods:

- ▶ WebSphere DataPower command-line interface (CLI)

Issue the following CLI commands to get the users list on the WebSphere DataPower Appliance:

```
config
show usernames
```

- ▶ WebSphere DataPower Web GUI

From the menu on the left side, click **Administration** → **Manage User Account** to access the list of user IDs that are defined on the WebSphere DataPower Appliance.

Network configuration

The network interface information from the backup files is assigned to the restored WebSphere DataPower Appliance. The network configuration after the secure restore does not require any modification in both of the following situations:

- ▶ The secure restore is done on the same WebSphere DataPower Appliance in the same network where the secure backup was done
- ▶ No network changes occurred since the backup

However, if any network changes occurred after the backup was done, or if the secure restore was done on a different WebSphere DataPower Appliance, the network configuration must be changed. For example, if the secure restore is done in a test area or otherwise physically secure location, after the restore restarts the WebSphere DataPower Appliance, the network configuration is incorrect for the test area location.

Therefore, the system administrator must immediately log in to the CLI by using the serial port or Secure Shell (SSH) and confirm that the network configuration is correct for the location of the WebSphere DataPower Appliance. You can do this confirmation by using either of the following options:

- ▶ WebSphere DataPower CLI

Issue the following commands after logging on and authenticating on the WebSphere DataPower Appliance:

```
config
show interface
show name-server
```

- ▶ WebSphere DataPower Web GUI

From the menu on the left side, click **Network** → **Interface** → **Ethernet Interface**.

RAID devices

A secure restore requires that the WebSphere DataPower Appliance have at least as much storage as the WebSphere DataPower Appliance that is backed up. However, if the purpose of the restore is to upgrade a WebSphere DataPower Appliance at end of life or after a disaster, the replacement WebSphere DataPower Appliance most likely has a larger storage capacity than the WebSphere DataPower Appliance that is backed up. If you are using a larger RAID device, the restored configuration might include information that contradicts the new WebSphere DataPower Appliance configuration. The system administrator can verify the configuration data by browsing some files on the RAID device.

For an installation that had an existing backup and restore method for data on the RAID device, the secure backup might have been done without a backup of the RAID device data. In this case, the configuration that is backed up includes definitions for a RAID device, but it does not include the RAID data itself. This situation can result in a RAID device that needs to be reconfigured and then have the RAID data that is restored by using the existing restore method.

To view the directory name that is used for the RAID device and to browse the files, use one of the following methods:

► WebSphere DataPower CLI

Enter the following commands after you log in to and authenticate on the WebSphere DataPower Appliance.

- For directories:

```
config
show raid-volume
```

- For files:

```
config
dir local:///myraidname
```

► WebSphere DataPower web GUI:

- To view the RAID directories, from the menu on the left side, click **Objects** → **System Settings** → **Hard Disk Array**.
- To view the RAID files, click **Control Panel** → **File Management** → **local** → **myraidname**.

iSCSI devices

If multiple iSCSI volumes exist on a WebSphere DataPower Appliance, the secure restore assumes that the volumes are configured identically to the WebSphere DataPower Appliance that is backed up. If a mismatch occurs in the iSCSI volume configuration, the secure restore restores the data to the wrong iSCSI volume, restarts the WebSphere DataPower Appliance, and uses the previous iSCSI configuration information, which points to iSCSI volumes that were not restored.

For example, two iSCSI volumes logical unit numbers (LUNs), LUN 0 and LUN 1, are configured on the WebSphere DataPower Appliance that is being backed up. But, the secure restore was done on a WebSphere DataPower Appliance with LUN 1 and 2. In this case, the data is restored to iSCSI volumes LUN 1 and 2, but the rebooted WebSphere DataPower Appliance points to iSCSI volumes LUN 0 and 1.

The system administrator must immediately log in to the WebSphere DataPower Appliance to browse some data on the iSCSI device to confirm that the iSCSI volumes are configured correctly. To view the directory name of each iSCSI volume, use one of the following methods:

► WebSphere DataPower CLI:

Enter the following commands after you log in to and authenticating in the WebSphere DataPower Appliance:

```
config
show iscsi-volume
```

► WebSphere DataPower Web GUI:

From the menu on the left side, click **Object** → **Network Settings** → **iSCSI Volume**. Clicking each volume name shows the mount point directory name.

IBM Tivoli Access Manager configuration

If you are running the Tivoli Access Manager libraries and have at least one Tivoli Access Manager object that is configured, issues might arise with the Secure Sockets Layer (SSL) keystore if multiple WebSphere DataPower Appliances are using the same files. The Tivoli Access Manager configuration file, keystore, and password stash file should be unique for each object.

The following scenarios illustrate when problems can occur:

- ▶ After the restore process, both WebSphere DataPower Appliances are up and a Tivoli Access Manager object on one of the WebSphere DataPower Appliances refreshes the keystore file. The corresponding object on the other WebSphere DataPower Appliance fails to transition up from the down state because the SSL key no longer matches the version on the policy server.
- ▶ The new WebSphere DataPower Appliance host name is different from the old WebSphere DataPower Appliance, and a Tivoli Access Manager object on the new WebSphere DataPower Appliance attempts to automatically refresh the keystore. The refresh might fail because the distinguished name that is configured for the object does not match the WebSphere DataPower Appliance host name.
- ▶ A Tivoli Access Manager object on the original WebSphere DataPower Appliance refreshed the keystore or password stash file after the secure backup was created. The object does not come up after it is restored, which can affect both the cases where the restore process occurs on the same WebSphere DataPower Appliance or on a different WebSphere DataPower Appliance.

In all cases, generate a unique set of files (including configuration, keystore, and stash files) for each Tivoli Access Manager object.

WebSphere MQ

WebSphere MQ messages are consumed in destructive mode (GET, the default) or in browse mode. The default, destructive mode, causes each message to be dequeued as it is read. Therefore, if the WebSphere DataPower Appliances are doing their WebSphere MQ business this way, each WebSphere DataPower Appliance sees roughly half the messages that arrive on the queue.

The other mode (called *browsing the queue*) lets the application (WebSphere DataPower Appliance in this case) detect the messages, but does not dequeue them. If two applications (or WebSphere DataPower Appliances) are browsing the same queue, each one sees all the messages on that queue.

In either case, review the resulting post-restore WebSphere MQ configuration objects and adjust according to the desired behavior.

Firmware management

IBM WebSphere Appliance Management Center for WebSphere Appliances provides firmware management for IBM WebSphere DataPower Appliances. This chapter highlights the following tasks for system administrators:

- ▶ Identifying and downloading firmware images
- ▶ Procedures to perform before a firmware upgrade
- ▶ Defining a firmware management process based on standard practices
- ▶ Deploying firmware on a single or group of WebSphere DataPower Appliances
- ▶ Solving possible issues that you might encounter when you perform a firmware upgrade

This chapter also includes standard practices to help improve current firmware management. This chapter includes the following sections:

- ▶ Managing the firmware repository
- ▶ Hints and tips before you upgrade the firmware
- ▶ Defining a firmware upgrade policy
- ▶ Deploying the firmware

4.1 Managing the firmware repository

This section provides information about WebSphere DataPower Appliance firmware images and helps system administrators to identify the correct firmware image specific to the WebSphere DataPower Appliance models and types that are in use. This section also shows where to find and download the firmware images from IBM. Finally, this section introduces the WebSphere Appliance Management Center repository and how system administrators can add and remove firmware images from it.

4.1.1 Introducing WebSphere DataPower Appliance firmware

IBM WebSphere DataPower Appliances are purpose-built network appliances that simplify, help secure, and accelerate XML and web services deployments while extending the SOA infrastructure. To get the most out of your WebSphere DataPower Appliances, install the latest compatible firmware releases. By using WebSphere Appliance Management Center, you can centrally manage firmware updates across all the WebSphere DataPower Appliances in your organization.

The latest firmware releases for WebSphere DataPower Appliances introduce new features and technologies, in addition to delivering cumulative maintenance fixes. Consider upgrading to the latest releases to proactively avoid problems that were already resolved.

IBM WebSphere DataPower XC10: The WebSphere DataPower XC10 Appliance runs a specific firmware image that is different from the rest of the WebSphere DataPower Appliances family. The firmware image must match the WebSphere DataPower Appliance model and type. Otherwise, it does not work. The system administrator must manage the WebSphere Appliance Management Center repository so that the correct firmware images match the WebSphere DataPower Appliances that make up their environment.

4.1.2 Identifying and downloading firmware images

For information about identifying and downloading the firmware image file that matches your WebSphere DataPower Appliance, see Knowledge Collection: How to upgrade the firmware on an IBM WebSphere DataPower Appliance at:

<http://www.ibm.com/support/docview.wss?uid=swg27015333>

Complete *Step 1. Read this Important Information* and *Step 2. Identify The Firmware Image File Which Matches Your Appliance*. To download the firmware files from IBM Fix Central after you identify the correct images, complete *Step 3. Download The Image Which Matches Your Appliance*.

4.1.3 Managing firmware images

Managing the WebSphere Appliance Management Center repository includes the tasks of adding a firmware image to the repository and removing a firmware image from the repository.

Adding a firmware image to the repository

You must add firmware images to the WebSphere Appliance Management Center repository so that you can deploy them to a single WebSphere DataPower Appliance or a group of appliances.

Important: The user who performs firmware-related tasks from the WebSphere Appliance Management Center must log on by using a user ID that is assigned the system administrator role. Other roles do not have the required permission to perform firmware upgrades.

To add a firmware image to the WebSphere Appliance Management Center repository:

1. In the WebSphere Appliance Management Center, on the **Repository** tab, click **Add Firmware** (Figure 4-1).

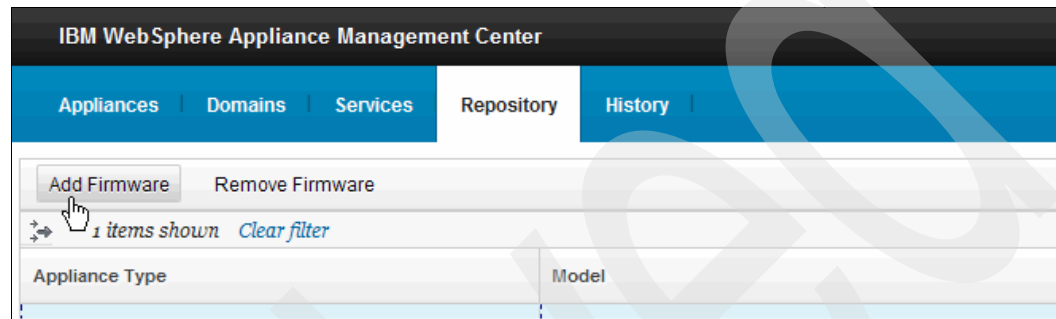


Figure 4-1 Adding a firmware image to the repository

2. Add the firmware images by using local or remote sources:
 - Local file (Figure 4-2)
 - i. After you download the firmware image from IBM Fix Central to your computer (for details, see 4.1.2, “Identifying and downloading firmware images” on page 68), select the **Local file** option and click **Browse**. Specify the firmware image file.
 - ii. Optional: Add a user comment.
 - iii. Click **Add** to upload the firmware image to the repository.

Add Firmware

Specify the source:

☒ Local file:

☐ Remote location URL:

Add a comment to this firmware image (optional):

User comment:

Figure 4-2 Uploading a local firmware image to the repository

- Remote location URL (Figure 4-3)

You can upload firmware images remotely by using the HTTP or HTTPS protocols.

HTTPS protocol: Even though you can use the HTTPS protocol, authentication is not supported.

- Select the **Remote location URL** option, and specify the URL. The HTTP URL takes the following form:
http://IP:Port/directory/firmwareimage
For our example, we use the following URL:
http://192.168.0.21/DP_firmware/xi5001.scrpt2
- Optional: Add a user comment.
- Click **Add** to upload the firmware image to the repository.

Figure 4-3 Uploading a remote firmware image to the repository

The repository should have firmware images that match all of your WebSphere DataPower Appliance types and models (Figure 4-4).

IBM WebSphere Appliance Management Center				
Appliances Domains Services Repository History				
Add Firmware Remove Firmware				
No filter applied.				
Appliance Type	Model	Firmware Version	User Comment	
Xi50	9003	5.0.0.1	v5.0.0.1 firmware Xi50	
Xi52	9005	5.0.0.0	v5.0.0.0 firmware Xi52	
Xi50	9003	4.0.1.5	v4.0.1.5 firmware Xi50	
XC10	9005	2.1.0.1	v2.1.0.1 firmware XC10	

Figure 4-4 WebSphere Appliance Management Center repository

Removing a firmware image from the repository

The system administrator can easily remove a firmware image from the repository. To remove a firmware image, from the **Repository** tab in WebSphere Appliance Management Center, select a firmware image to remove, and then, click **Remove Firmware** (Figure 4-5). After you confirm the deletion, the firmware image is removed.

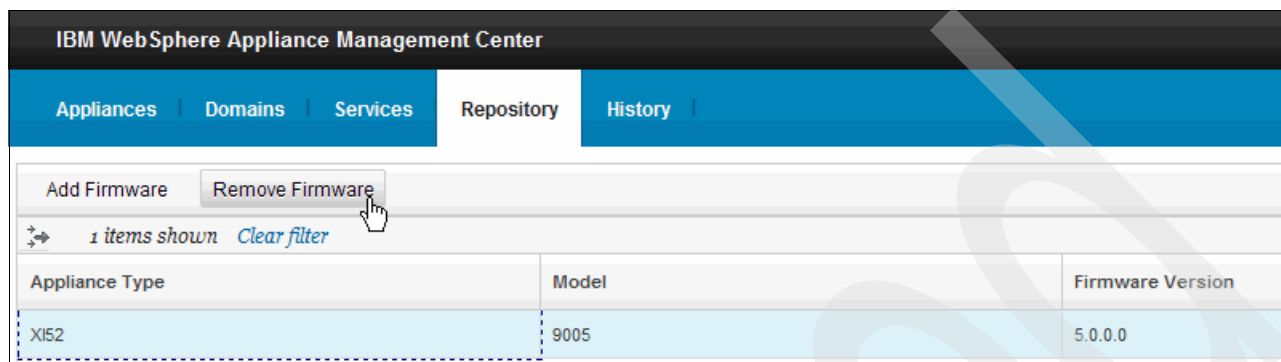


Figure 4-5 Removing a firmware image from the repository

4.2 Hints and tips before you upgrade the firmware

You must perform and validate several procedures before you proceed with a firmware upgrade on a WebSphere DataPower Appliance or environment when using WebSphere Appliance Management Center. These procedures help the system administrator to keep control of the environment and to take action in case of issues or problems.

This section includes the following tasks:

- ▶ Confirming a working WebSphere DataPower administrator user ID
- ▶ Configuration backups
- ▶ Cleaning the file system space
- ▶ Avoiding live traffic and impact

4.2.1 Confirming a working WebSphere DataPower administrator user ID

The WebSphere DataPower admin ID is critical. The only way to recover this ID if it becomes lost is to ship the WebSphere DataPower Appliance back to IBM for a factory reset. Therefore, always have a backup privileged login, which you can use to change the admin ID or to perform administration-related role activities if required.

On the WebSphere DataPower Appliance, enable the *Local Login as Fallback* feature and include the administrator and the backup privileged users. Without configuring the local fallback users properly, a backup privileged user does not work when using role-based management authentication such as Lightweight Directory Access Protocol (LDAP). For more information, see *Configuring role-based management settings* topic in the WebSphere DataPower Integration Appliance version 5.0 Information Center:

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/index.jsp?topic=%2Fcom.ibm.dp.xi.doc%2Fadministratorsguide.xi5039.htm&path%3D4_2_0_3_0_3

Always check the administrator and privileged users credentials by logging in to the WebSphere DataPower Appliance to make sure that they are working and functional.

4.2.2 Configuration backups

Before you upgrade the WebSphere DataPower Appliance firmware, create backups from the current configuration. You can use WebSphere Appliance Management Center to create a secure backup before you proceed with the firmware upgrade. Ensure that you have a good backup policy and process in place when you manage WebSphere DataPower environments. Store backup copies externally in a safe and controlled storage location from the WebSphere DataPower Appliance.

For more information about using WebSphere Appliance Management Center for taking secure backups, see Chapter 3, “Disaster recovery” on page 51.

4.2.3 Cleaning the file system space

On the WebSphere DataPower Appliance, download and save to another location any extra or unneeded files so that you can allow for more space for future upgrades. Delete these files from the WebSphere DataPower Appliance to make room for the upgrade. Always use logging targets to offload the WebSphere DataPower Appliance logs, which you can do for system logs and audit logs. For more information about off-appliance logging, see the *DataPower off-device logging: a configuration example* Technote at:

<http://www.ibm.com/support/docview.wss?uid=swg21269136>

Another option for clearing space on the WebSphere DataPower Appliance is to use the **boot delete** CLI command. This command does not delete the current version firmware. It deletes only the firmware image from the version before the current version. As an example, Figure 4-6 shows and describes how the WebSphere DataPower Appliance caches the current running firmware during a firmware upgrade. The cached firmware is then available for use as a rollback if issues occur with the new upgraded version.

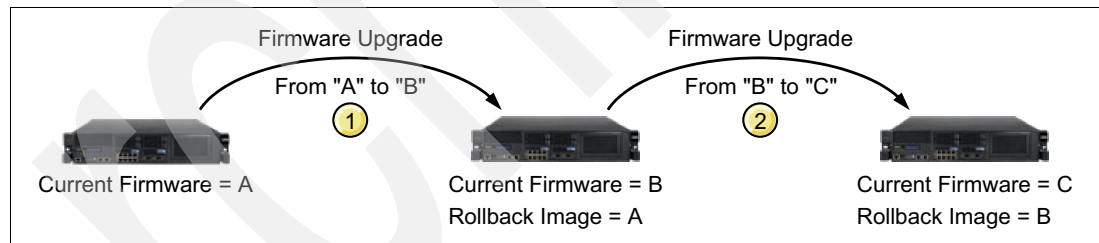


Figure 4-6 WebSphere DataPower Appliance cached firmware

The firmware upgrade scenario in Figure 4-6, which is for instruction purposes only, entails the following process. The WebSphere DataPower Appliance firmware images are represented as letters A, B, and C. In a real scenario, all three letters would be different firmware versions.

1. After upgrading to firmware B, a rollback copy of the previous firmware version A was stored and cached by the WebSphere DataPower Appliance. This cached firmware can be used to roll back from version B to version A. Running the **boot delete** command deletes only cached rollback image A. This task makes more storage space available for the next firmware upgrade.
2. After upgrading to firmware C, a rollback copy of the previous firmware version B was stored and cached by the WebSphere DataPower Appliance. This cached firmware can be used to roll back from version C to version B. Even after you use the **boot delete** command in step 1, you can roll back to version B after you upgrade the firmware. This result is possible because, at the time the **boot delete** command was run, the cached version was still version B, which is no longer used nor required.

The temporary and internal directories in the WebSphere DataPower Appliance are not persisted storage. Also the files in these directories are lost if the WebSphere DataPower Appliance is restarted or powered down. However, these directories are not cleared if you use the Reload option. The temporary and internal directories are used for various processing actions during normal operation. Restarting the WebSphere DataPower Appliance can help to clean the file system before a firmware upgrade.

Tip: Always restart the WebSphere DataPower Appliance after a failed firmware upgrade attempt to free system and disk resources for the next attempt.

4.2.4 Avoiding live traffic and impact

Before you upgrade the WebSphere DataPower Appliance firmware, remove the WebSphere DataPower Appliance from the production, development, or test environment. If traffic is load balanced by a load balancer before it reaches the WebSphere DataPower Appliance, you might want to remove it from the load balancer pool or mark it as inactive to avoid new incoming traffic. Also, quiesce all the domains after traffic to the WebSphere DataPower Appliance is ended. For more information about quiesce, see 5.1.6, “Quiescing and unquiescing domains” on page 96.

Make sure that no changes are in progress and that the configuration is saved. Also, check for active users and disconnect everyone before you proceed with the firmware upgrade. You can easily do this check by using the WebSphere DataPower Appliance GUI and clicking **Status** → **Main** → **Active Users** from the left menu.

As shown in Example 4-1, run the following CLI commands to make sure that no traffic is flowing through the WebSphere DataPower Appliance:

```
show tcp-connections
show int
```

Example 4-1 Checking that no traffic is flowing through the WebSphere DataPower Appliance

```
xi52# show tcp-connection
established: 11
  syn-sent: 0
syn-received: 0
  fin-wait-1: 0
  fin-wait-2: 0
  time-wait: 2
  closed: 0
  close-wait: 0
  last-ack: 0
  listen: 7
  closing: 0

xi52# show int
interface      IP Address      RX (kb/pkts/errs)  TX (kb/pkts/errs)
-----
mgt0           10.1.2.166/16   9803/147896/0      0/4/0
eth0           9.23.237.54/23  3226/43094/0       54091/43817/4383
eth1           0/0/0          0/0/0              0/0/0
eth2           0/0/0          0/0/0              0/0/0
```

You can also use the **show cpu** CLI command to check that the WebSphere DataPower Appliance is not in use as shown on Example 4-2.

Example 4-2 Checking the WebSphere DataPower Appliance CPU usage

```
xi52(config)# show cpu
              10 sec   1 min   10 min   1 hour   1 day
cpu usage (%):      0      0      4      4      4
```

4.3 Defining a firmware upgrade policy

You must take the following critical areas into consideration when you plan and define the firmware upgrade policy and procedure for a WebSphere DataPower Appliance environment:

- ▶ Deciding when to upgrade
- ▶ Firmware support lifecycle for WebSphere DataPower Appliance
- ▶ Upgrading non-critical WebSphere DataPower Appliances first
- ▶ Running service conformity tests after you upgrade the firmware
- ▶ Avoiding impact to the production environment

The following sections present general information and standard practices that can be useful, even when a firmware upgrade policy is already in place. System administrators must ensure that they properly cover the information that is described here in the firmware upgrade procedure and policy.

4.3.1 Deciding when to upgrade

Read the WebSphere DataPower Appliance firmware release notes. Give special attention to enhancements, new features, resolved APARs, and critical updates. Base the final decision about whether to upgrade on the information that is provided and your experience and performance with the current firmware version. Keep in mind the following factors:

- ▶ Stability
- ▶ Performance
- ▶ Enhancement for existing features
- ▶ Requirements for new features

Keep your environment in conformity with the WebSphere DataPower Appliance firmware lifecycle as explained in 4.3.2, “Firmware support lifecycle for WebSphere DataPower Appliance” on page 74.

4.3.2 Firmware support lifecycle for WebSphere DataPower Appliance

A minimum of two years of support is provided for each firmware release, beginning with the general availability (GA) of the release. Releases of the WebSphere DataPower firmware that are older than two years and are not within the three latest levels of firmware are subject to support withdrawal at any time.

To minimize the business impact of changes to customers, IBM created the IBM WebSphere DataPower End of Service policy to help plan firmware upgrades. Customers receive a 12-month notice before the end of service date. A good firmware upgrade policy must ensure that updates are made regularly to conform with the IBM support lifecycle, without any gaps in support.

For more information, see the IBM WebSphere DataPower SOA Appliance Firmware Support Lifecycle website at:

<http://www.ibm.com/support/docview.wss?rs=2362&uid=swg21246298>

4.3.3 Upgrading non-critical WebSphere DataPower Appliances first

A firmware upgrade must start gradually with a low impact environment. More testing can reduce the chances of major problems to the business when you upgrade the production environment. The firmware upgrade policy must have a well-defined starting environment and a period of compliance tests.

The total time that is required for the firmware upgrade depends on how many WebSphere DataPower Appliances you have and on how complex your environment and applications are. Figure 4-7 shows an ideal scenario that you can use as a model when you define your custom firmware upgrade policy.

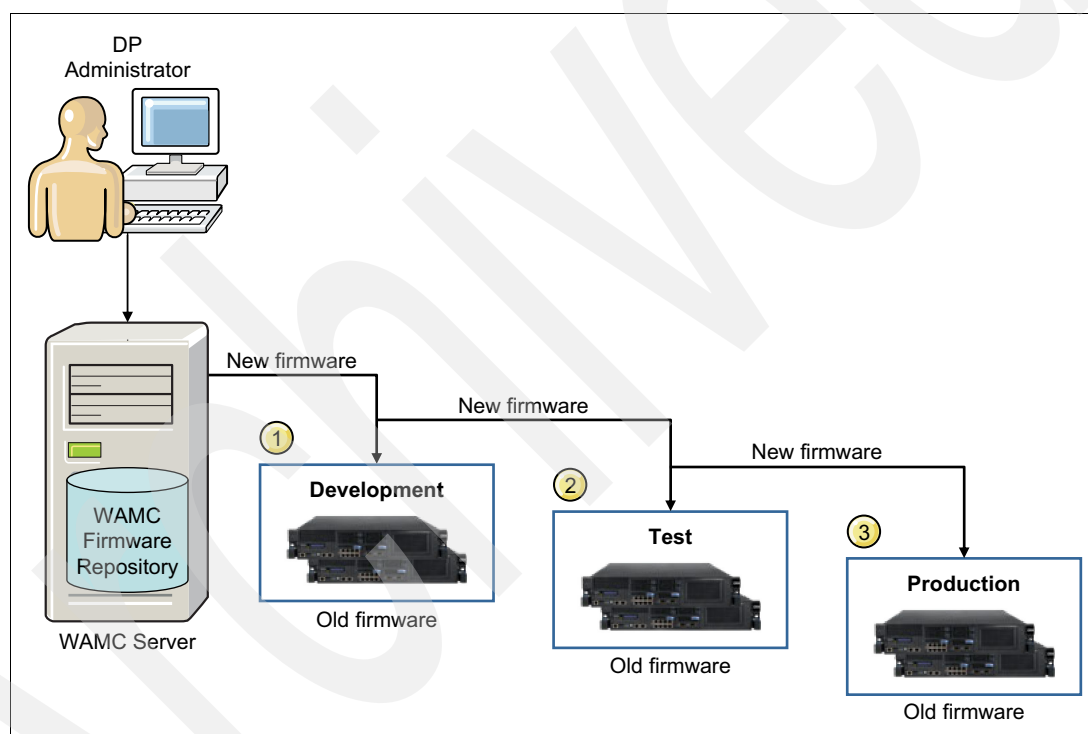


Figure 4-7 Firmware upgrade policy

The scenario in Figure 4-7 entails the following procedure:

1. Development environment

In this scenario, the new firmware is initially deployed to the low priority environment called *Development*. Initial tests on the new firmware are made by the developers to ensure that everything is working as expected. Also, consider how the new firmware will be deployed on this environment. Even in a development environment, people have deadlines to meet and projects to deliver. Therefore, use an approach that can be easily rolled back in case issues arise.

2. Test environment

After you validate the Development environment, you can deploy the new firmware to the next environment. In this scenario, we call it the *Test environment*. In this environment,

tests are run, trying to be as close as possible to the real business production environment. For more information, see 4.3.4, “Running service conformity tests after you upgrade the firmware” on page 76. Plan and architect the firmware deployment in a way that you do not interrupt the usual and current tests.

3. Production environment

After tests are concluded on both previous environments, you can start planning the production upgrade. Production must always be the last environment that is upgraded after everything that is possible has been tested and simulated. With good planning and a battery of tests, the production upgrade tends to be safe.

For more information and standard practices for production upgrades, see 4.3.5, “Avoiding impact to the production environment” on page 76.

4.3.4 Running service conformity tests after you upgrade the firmware

Always run conformity tests after a firmware upgrade. Use automated testing tools or custom scripts to produce enough test cases and to stress the new firmware. Watch carefully for device performance, load, latency, and other areas of importance to your business. Ensure that a regression test procedure is in place so that all aspects of your services are correctly tested. Consider application support teams and customers as resources for these tests.

Sometimes a Request for Comments (RFC) is updated and can affect the default behavior of current services or settings that are implemented on a WebSphere DataPower Appliance. IBM is always in compliance with security standards and RFCs.

The following IBM technote contains information about one case where the Security Socket Layer (SSL) RFC was updated:

<http://www.ibm.com/support/docview.wss?uid=swg21497539>

The update culminated in changing the default behavior of the WebSphere DataPower Appliance when acting as an SSL client that connects to an insecure server.

To access the related RFC, go to:

<http://tools.ietf.org/html/rfc5746>

4.3.5 Avoiding impact to the production environment

Never start a firmware upgrade on the production environment. Make sure that your firmware upgrade policy protects and avoids any impact to the business as first goal. Because of the nature of real data and unpredicted volume, it is difficult to simulate a production environment. Performing a strict load and performance tests on a different environment can help, but it is not a guarantee that no issues will happen on the production environment.

For the production environment, go through a stringent firmware upgrade cycle. Consider upgrading only one WebSphere DataPower Appliance initially. Monitor it closely for the next several days for issues and performance before you upgrade the other production WebSphere DataPower Appliances.

When you plan a firmware upgrade in the production environment, consider redundancy. You do not want to cause a full outage if problems occur. Think about a device where you have at least one or more devices that service the same services and instances. You need to stop traffic to the new upgraded WebSphere DataPower Appliance if problems occur. Make sure that the remaining WebSphere DataPower Appliances can handle and manage the traffic if required.

Use good communication to notify everyone who uses the services that are provided by the WebSphere DataPower Appliance. Everybody must be aware of the firmware upgrade. Most companies have various teams that manage the WebSphere DataPower and Network Appliances. Engage all required people and ask them to be promptly available if needed. You do not want to waste minutes or hours waiting on the engagement of other teams during a firmware upgrade event.

Consider doing the firmware upgrade in the production environment during a quiet period. That is, try to avoid a firmware upgrade on a busy week or month, when you have many code releases and changes happening on the environment. That way, it can be more difficult to identify the real firmware behavior, because new services, settings, or configurations can also affect and mask the performance.

For more information about standard practices for the production environment, see 4.2, “Hints and tips before you upgrade the firmware” on page 71.

4.4 Deploying the firmware

WebSphere Appliance Management Center provides a centralized point to manage your WebSphere DataPower Appliance environment. The firmware repository helps when you plan firmware upgrades across your environment, which can be composed of different WebSphere DataPower models and versions. For the list of supported WebSphere DataPower Appliance types and models, see 1.5, “Supported WebSphere DataPower Appliances” on page 8.

Figure 4-8 on page 78 illustrates the following scenarios about how WebSphere Appliance Management Center can be used to perform firmware upgrades on WebSphere DataPower Appliances. The numbers correspond to the numbers in the figure.

1. Single WebSphere DataPower Appliance. In this scenario, only a single WebSphere DataPower Appliance is upgraded. For more information, see 4.4.1, “Single WebSphere DataPower Appliance upgrade” on page 78.
2. Multiple WebSphere DataPower Appliances in the same model. In this scenario, a group of same model WebSphere DataPower Appliances are upgraded. For more information, see 4.4.2, “Multiple WebSphere DataPower Appliance upgrade” on page 81.
3. Multiple WebSphere DataPower Appliances with different models. In this scenario, a group of different models WebSphere DataPower Appliances is upgraded.

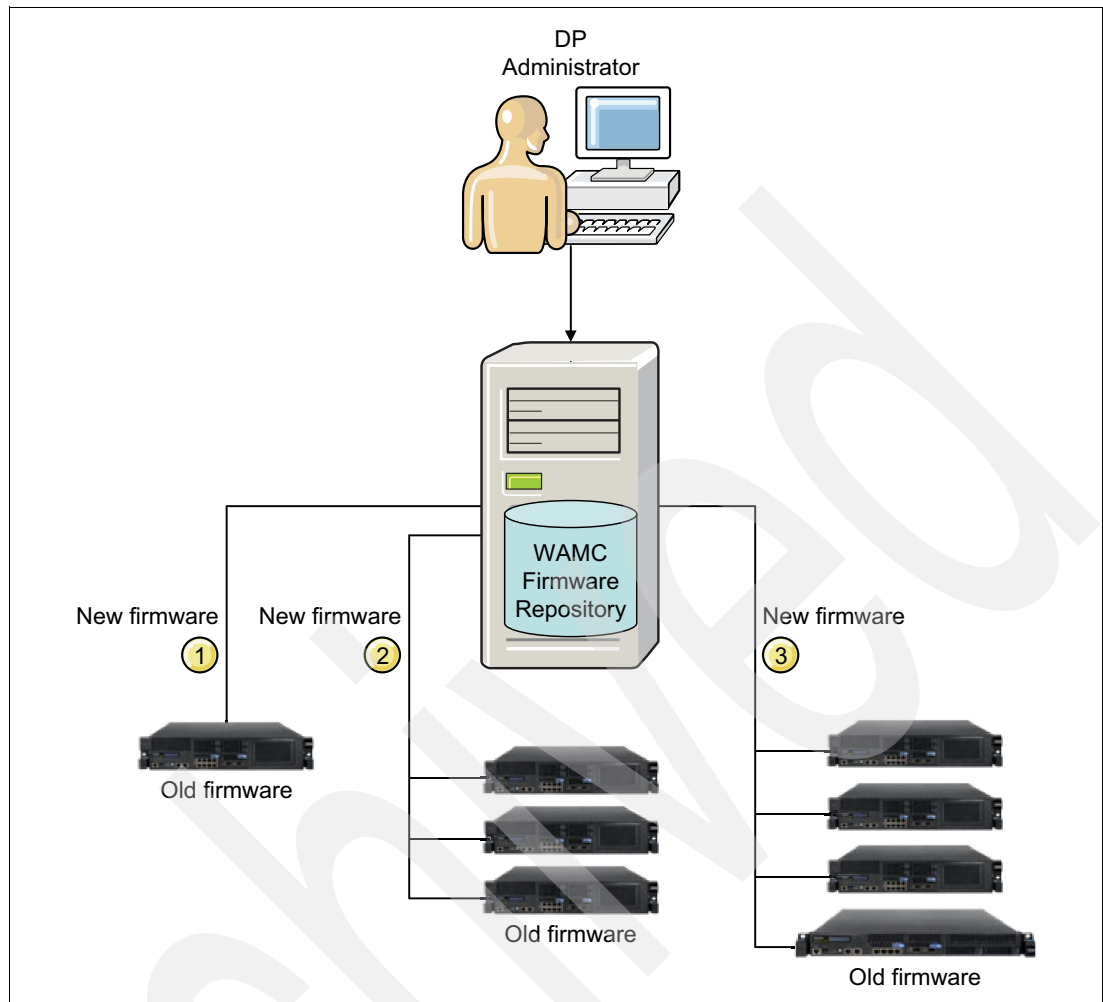


Figure 4-8 Firmware upgrade scenarios using WebSphere Appliance Management Center

4.4.1 Single WebSphere DataPower Appliance upgrade

You can deploy a single WebSphere DataPower Appliance firmware upgrade by using the WebSphere Appliance Management Center.

Important: WebSphere Appliance Management Center assumes that you have handled all requirements, such as for backups and traffic avoidance. Before you read this section, you must read 4.2, “Hints and tips before you upgrade the firmware” on page 71.

To do a firmware deployment on a single WebSphere DataPower Appliance:

1. On the **Appliances** tab, from WebSphere Appliance Management Center (Figure 4-9), select a WebSphere DataPower Appliance, click **Other Actions**, and select **Deploy Firmware**.

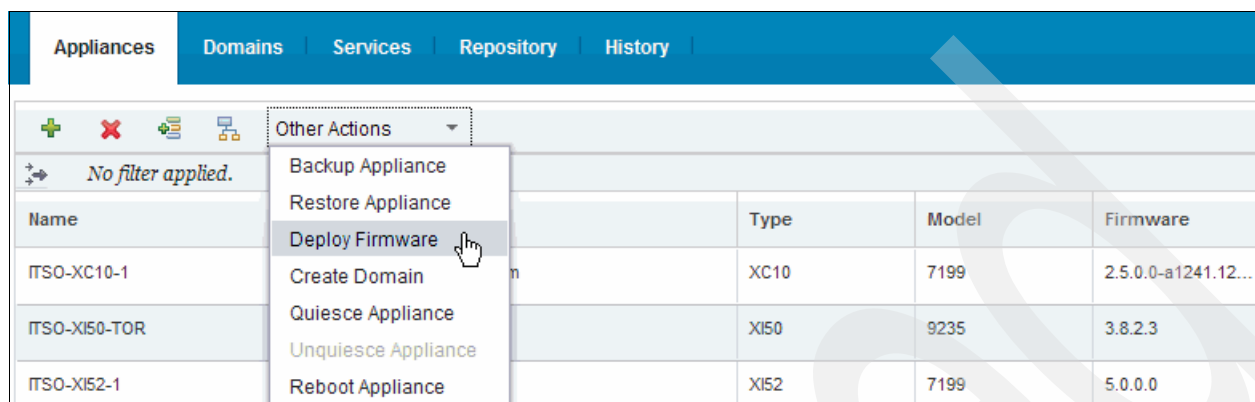


Figure 4-9 Selecting the Deploy Firmware action for a single WebSphere DataPower Appliance

2. In the Deploy Firmware dialog box (Figure 4-10), select the firmware version to be deployed. Two methods are available for selecting the firmware image:

- List upgrades only

This option is the default. By using this option, WebSphere Appliance Management Center automatically selects the latest firmware version that is available in the repository that matches the WebSphere DataPower Appliance model, type, and license. For information about managing the repository, see 4.1, “Managing the firmware repository” on page 68.

Deploy Firmware

Set the target firmware:

☒ List upgrades only
☐ List all compatible firmware versions

Specify the firmware version:

Summary:

Appliance Name	Appliance Type	Appliance Mode	Current Firmware	Target Firmware
ITS0-XI50-TOR	XI50	9235	3.8.2.3	5.0.0.1 details <input checked="" type="checkbox"/>

Figure 4-10 Deploying firmware by using list upgrades only option

- List all compatible firmware versions

By selecting this option (Figure 4-11 on page 80), you can select from a list of firmware versions that are available in the repository that matches your WebSphere DataPower Appliance model, type, and license. This option is preferred when you need to upgrade or downgrade to a specific firmware version rather than to the last available version.

Tip: If WebSphere Appliance Management Center shows no versions available to upgrade, check the firmware images in the repository. Make sure that the right images were downloaded, matching the WebSphere DataPower Appliance model, type, and licenses. For information, see 4.1.2, “Identifying and downloading firmware images” on page 68.

Deploy Firmware

Set the target firmware:

☐ List upgrades only

☒ List all compatible firmware versions

Specify the firmware version: 5.0.0.1

Summary:

Appliance Name	Appliance Type	Appliance Model	Current Firmwar	Target Firmware
ITSO-XI50-TOR	XI50	9235	3.8.2.3	5.0.0.1 details

Figure 4-11 Deploying firmware by using the list all compatible firmware versions option

3. Select the **license agreements** check box, and then, click **Deploy** (Figure 4-12).

☒ accept the terms in the license agreements

Note: After you click **Deploy**, you cannot stop this operation.

Deploy **Cancel**

Figure 4-12 Accepting the license agreements and starting the deployment

The firmware upgrade process starts.

The **History** tab (Figure 4-13) in WebSphere Appliance Management Center shows the status and detailed information about the events that are happening during the firmware upgrade process.

Details:

- Completed successfully.**
2012 10 17 16:44:13:196 | CWZBA1003I
- Started.**
2012 10 17 16:36:48:571 | CWZBA1001I
- Submitted.**
2012 10 17 16:36:48:117 | CWZBA1012I

Figure 4-13 History panel showing details about the firmware upgrade

The WebSphere DataPower Appliance restarts. When the firmware upgrade process is finished, it is available on WebSphere Appliance Management Center again. To verify that the upgrade was successful, see 4.4.3, “Verifying the firmware upgrade” on page 83.

4.4.2 Multiple WebSphere DataPower Appliance upgrade

You can deploy a firmware upgrade on multiple WebSphere DataPower Appliances by using the WebSphere Appliance Management Center.

Important: WebSphere Appliance Management Center assumes that you have handled all requirements, such as backups and traffic avoidance. Before you read this section, you must read 4.2, “Hints and tips before you upgrade the firmware” on page 71.

To do a firmware deployment on multiple WebSphere DataPower Appliances:

1. On the **Appliances** tab in WebSphere Appliance Management Center (Figure 4-14), select the WebSphere DataPower Appliances to be upgraded. Click **Other Actions** → **Deploy Firmware**.

Tip: You can select multiple WebSphere DataPower Appliances by pressing and holding the Control key and selecting the WebSphere DataPower Appliances. Another option is to press and hold the Shift key to select several WebSphere DataPower Appliances.

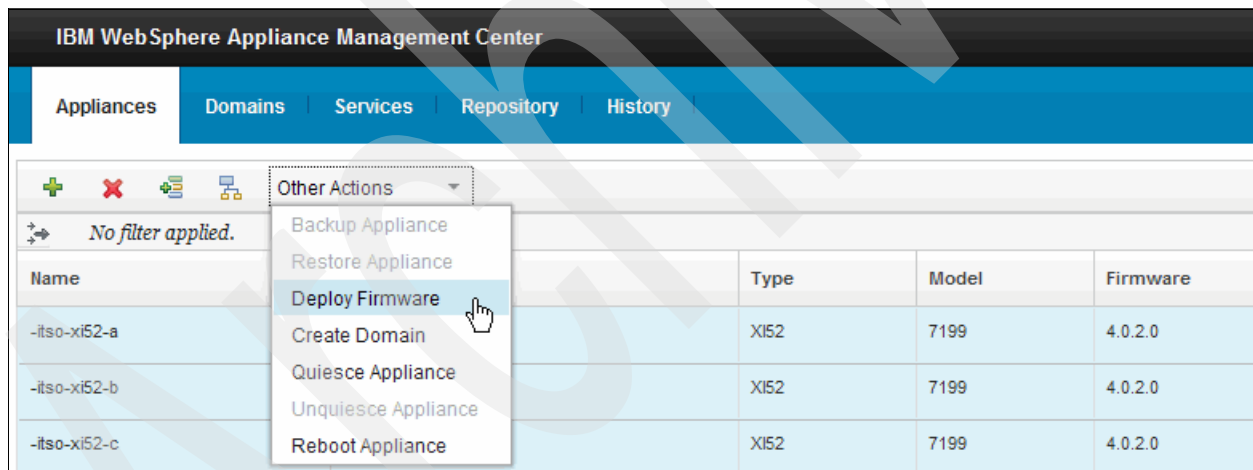


Figure 4-14 Selecting the Deploy Firmware action for multiple WebSphere DataPower Appliances

2. In the Deploy Firmware dialog box (Figure 4-15), select the firmware version to be deployed. Two methods are available to select the firmware image:
 - List upgrades only

This option is the default. By using it, WebSphere Appliance Management Center automatically selects the latest firmware version that is available in the repository that matches the WebSphere DataPower Appliance model, type, and license. For information about managing the repository, see 4.1, “Managing the firmware repository” on page 68.

Deploy Firmware

Set the target firmware:

☒ List upgrades only
☐ List all compatible firmware versions

Specify the firmware version: [?](#)

Summary:

Appliance Name	Appliance Type	Appliance Mod	Current Firmwai	Target Firmware	
-its0-xi52-a	Xi52	7199	4.0.2.0	5.0.0.0 details	✓
-its0-xi52-b	Xi52	7199	4.0.2.0	5.0.0.0 details	✓
-its0-xi52-c	Xi52	7199	4.0.2.0	5.0.0.0 details	✓

Figure 4-15 Deploying firmware for multiple WebSphere DataPower Appliances

- List all compatible firmware versions

By using this option, you can select from a list of firmware versions available in the repository that matches your WebSphere DataPower Appliance model, type, and license. This option is preferred when you need to upgrade or downgrade to a specific firmware version rather than the last available version.

Tip: If WebSphere Appliance Management Center does not show any versions available to upgrade, check the firmware images in the repository. Make sure that the right images were downloaded by matching the WebSphere DataPower Appliance model, type, and licenses. For more information, see 4.1.2, “Identifying and downloading firmware images” on page 68.

3. Select the **license agreements** check box, and then, click **Deploy** (Figure 4-16).

Important: When you upgrade multiple WebSphere DataPower Appliances, the process is sequential. That is, the upgrade process proceeds from one WebSphere DataPower Appliance to the next, regardless of the success or failure of each deployment.

☒ I accept the terms in the license agreements.

Note: After you click **Deploy**, you cannot stop this operation.

Figure 4-16 Accepting the license agreements and starting the deployment

The firmware upgrade process begins.

The **History** tab shows the current status and detailed information about the events during the firmware upgrade process as shown on Figure 4-17.





IBM WebSphere Appliance Management Center		
Appliances	Domains	Services
Repository	History	
No filter applied.		
Status	Action	User ID
	Deploy firmware to appliance 'itso-xi52-b'	wamcadmin
	Deploy firmware to appliance 'itso-xi52-c'	wamcadmin
	Deploy firmware to appliance 'itso-xi52-d'	wamcadmin
	Deploy firmware to appliance 'itso-xi52-a'	wamcadmin


Figure 4-17 History panel showing details about the firmware upgrade to multiple appliances

The WebSphere DataPower Appliances are restarted. When the firmware upgrade process is finished, the appliances are available again on WebSphere Appliance Management Center. To verify that the upgrade was successful, see 4.4.3, “Verifying the firmware upgrade” on page 83.


4.4.3 Verifying the firmware upgrade

You can verify the firmware upgrade by checking the properties of the WebSphere DataPower Appliance that is displayed on the right side of the window on the **Appliances** tab (Figure 4-18).

Properties:

Name: 

itso-xi52

Host name: 

9.42.170.241

Type:

Xi52

Model:

7199


Firmware:


5.0.0.1

Groups:

development, xi52

Status:



Feature list 

MQ, TAM, DataGlue, JAXP-API, PKCS7-SMIME, SQL-ODBC, Tibco-EMS, WebSphere-JMS, RaidVolume, iSCSI, LocateLED, AppOpt, IPMI, DCO, RaidVolumeSr, IntrusionDetection, IPMI-LAN

Serial number:

6803878

Figure 4-18 WebSphere DataPower Appliance properties

4.4.4 Rolling back the firmware

Permissions required for rolling back firmware: An administrator or a privileged user with permission is required to roll back the firmware.

You can roll back the firmware to the previous firmware version before the update if required. Two methods are available methods to roll back the firmware:

- Using the WebSphere DataPower web GUI

To roll back the firmware by using the WebSphere DataPower web GUI, click **Administration** → **Main** → **System Control**. Then, click **Firmware Roll-Back** (Figure 4-19).

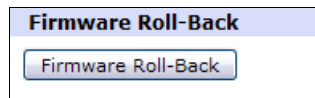


Figure 4-19 Rolling back the firmware using the WebSphere DataPower web GUI

- Using the WebSphere DataPower CLI

To roll back the firmware by using the WebSphere DataPower CLI, issue the commands that are shown in Example 4-3.

Example 4-3 WebSphere DataPower CLI commands to roll back the firmware

```
xi50# conf
Global configuration mode

xi50(config)# flash
Flash configuration mode

xi50(config-flash)# boot switch
Firmware roll-back successful

Device is rebooting now.
```

Managing domains and services

IBM WebSphere Appliance Management Center for WebSphere Appliances can manage application domains and services. Domain management entails exporting required configuration files and knowing how to create, update, and delete domains by using WebSphere Appliance Management Center. The management of services includes creating, updating, and deleting services.

An optional part of creating and updating domains and services is the use of deployment policies. Deployment policies can add flexibility to the process of deploying a configuration.

This chapter includes the following sections:

- ▶ Managing application domains
- ▶ Managing services
- ▶ Deployment policies
- ▶ Automatic synchronization of a configuration

5.1 Managing application domains

You can use WebSphere Appliance Management Center to create, update, and delete application domains across multiple WebSphere DataPower Appliances. This section briefly describes the application domains, their configuration, and how WebSphere Appliance Management Center uses domain configuration backups and domain configuration exports.

5.1.1 Application domains

After initial installation and setup, a WebSphere DataPower Appliance has just one application domain, which is called the *default domain*. Applications and services should not be deployed to the default domain. Default domains are used to store appliance-wide resources, such as network interfaces, users, and access controls. Instead, create additional application domains and deploy services into these domains.

Application domains divide a WebSphere DataPower Appliance into partitions or workspaces. You might divide an appliance this way for the following reasons:

- ▶ Access control. Allowing a user to administer their own domains but preventing them from changing domains that are owned by other users.
- ▶ Workspace separation. Providing application developers with isolated workspaces where they can develop without affecting other applications or services that are running on the same WebSphere DataPower Appliance.
- ▶ Backup and restore. Backing up and restoring the configuration for a whole domain independently of other domains.
- ▶ Migration of configuration between appliances. Exporting a domain configuration and using it to create a domain on a different WebSphere DataPower Appliance.

For more information about application domains, see *DataPower SOA Appliance Administration, Deployment, and Best Practices*, SG24-7901.

5.1.2 Application domain configuration

Application domains are configured to support the services that are deployed to them. An application domain configuration defines settings, including logging, XML managers, services, and host aliases. You can back up or export a domain configuration to a file, which you should do regularly because these exported files function as point-in-time backups of the currently saved configuration.

Two types of domain configuration files are available:

- ▶ Domain configuration backups

A copy of the entire domain configuration that includes all objects (such as services and files, but not certificates) that are part of the domain. A domain configuration backup can include configuration for multiple domains.

- ▶ Domain configuration exports

Similar to a domain configuration backup, an export includes objects and a configuration for a domain. However, domain configuration exports differ from a domain configuration backup in that *selected* configuration objects are exported so that the configuration of individual resources, objects, and services can be exported. A domain configuration export contains configuration for one domain only.

In WebSphere Appliance Management Center, domain configuration files are required when you create a domain or update a domain configuration. The type of configuration file that is used is important as the behavior of WebSphere Appliance Management Center changes depending on the type of configuration file used:

- ▶ When you create a domain by using a domain configuration backup, the name of the new domain must match the name of a domain that the backup file contains. For example, if the configuration was backed up from a domain that is called *development*, the new domain must also be called *development*. If a domain configuration backup contains configuration for two domains that are called *development* and *test*, the newly created domain must be called *development* or *test*.

When you update the configuration of an existing domain by using a domain configuration backup, the name of the domain that is being updated must match a domain name from the configuration backup.

- ▶ When you create a domain by using a domain configuration export, the name of the new domain does not need to match the name of the domain that the export file was created from. For example, if the configuration was exported from a domain that is called *development*, the new domain can be called *development* but can also be called *test*. The same is true when you update the configuration of an existing domain by using a domain configuration export.

5.1.3 Creating domain configuration files

Application domain configuration files are created from the WebSphere DataPower web GUI. It is not possible to create domain configuration backups or domain configuration export files from WebSphere Appliance Management Center. You can create a domain configuration backup and a domain configuration export.

For more information about backing up a domain configuration and exporting application domain configuration and objects from an application domain, see the *Backing up and exporting configuration data* topic of the WebSphere DataPower Integration Appliance version 5.0 Information Center at:

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/topic/com.ibm.dp.xi.doc/administratorsguide.xi50229.htm?path=4_2_0_4_6_3#webgui_backingupexportingconfigdata_task

Creating a domain configuration backup

To back up the configuration of one or more domains:

1. Log in to the WebSphere DataPower web GUI for your WebSphere DataPower Appliance.
2. From the Control panel, select **Administration** → **Configuration** → **Export Configuration**.
3. In the Export Configuration window (Figure 5-1), select **Create a backup of one or more application domains**. Then, click **Next**.

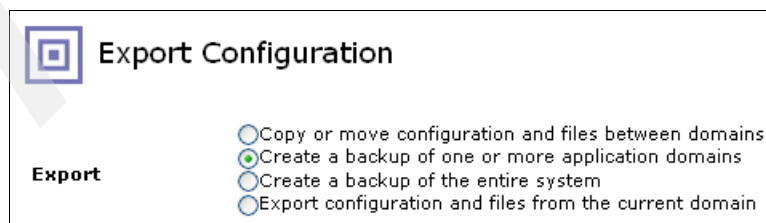
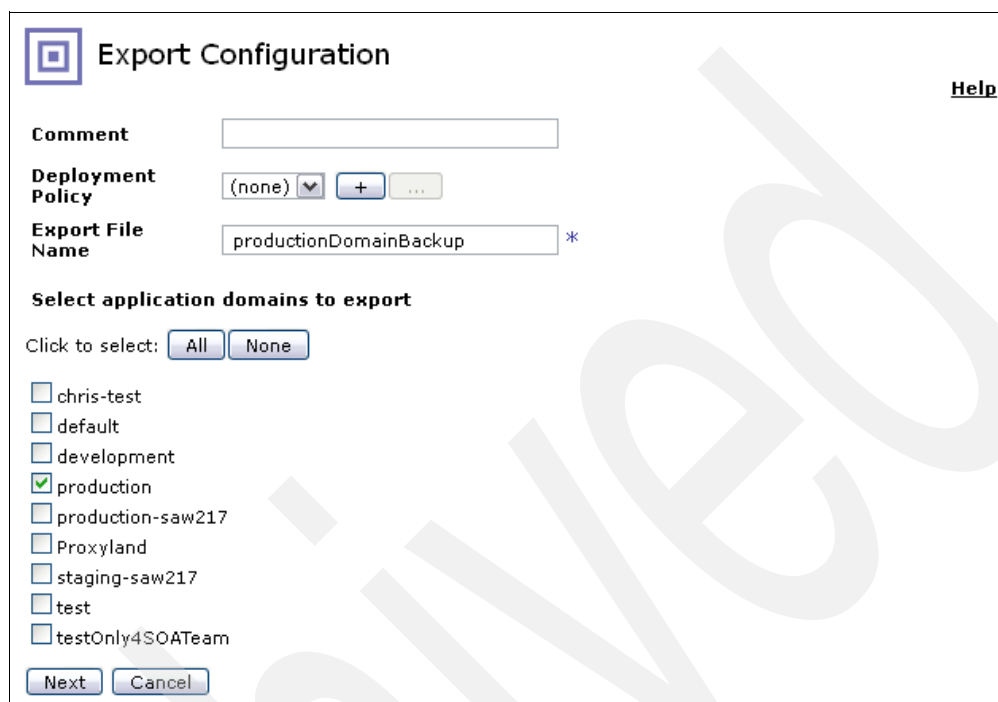


Figure 5-1 Selecting to create a backup of one or more application domains

4. In the next Export Configuration window (Figure 5-2):
 - a. In the Export File Name field, enter a name for the export file.
 - b. Select one or more application domains to back up.
 - c. Click **Next**.



The 'Export Configuration' window features a title bar with a logo and a 'Help' link. It contains several input fields: 'Comment' (empty), 'Deployment Policy' (set to '(none)' with '+' and '-' buttons), and 'Export File Name' (containing 'productionDomainBackup' with an asterisk). Below these is a section titled 'Select application domains to export' with 'Click to select:' buttons for 'All' and 'None'. A list of domains follows, each with a checkbox: 'chris-test', 'default', 'development', 'production' (checked), 'production-saw217', 'Proxyland', 'staging-saw217', 'test', and 'testOnly4SOATeam'. At the bottom are 'Next' and 'Cancel' buttons.

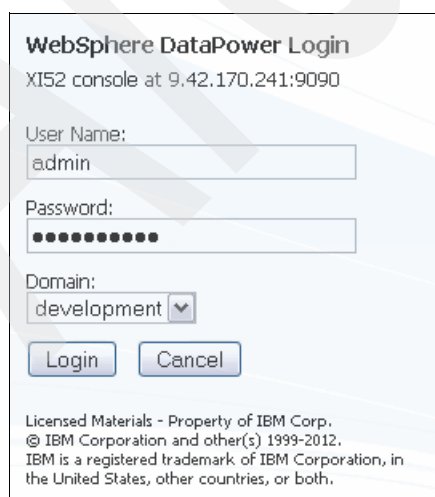
Figure 5-2 Naming the backup and selecting the domains to include

5. Click **Download** to download the backup file.

Creating a domain configuration export

To export the configuration for a domain called *development*:

1. Log in to the WebSphere DataPower web GUI for your WebSphere DataPower Appliance. Figure 5-3 shows the process of logging in to the development domain.



The 'WebSphere DataPower Login' window shows the console address 'XI52 console at 9.42.170.241:9090'. It has fields for 'User Name:' (filled with 'admin'), 'Password:' (masked with dots), and 'Domain:' (a dropdown menu set to 'development'). 'Login' and 'Cancel' buttons are at the bottom. A footer contains copyright information: 'Licensed Materials - Property of IBM Corp. © IBM Corporation and other(s) 1999-2012. IBM is a registered trademark of IBM Corporation, in the United States, other countries, or both.'

Figure 5-3 Logging in to the development domain

2. From the Control panel, select **Administration** → **Configuration** → **Export Configuration**.
3. In the Export Configuration window (Figure 5-4), select **Export configuration and files from the current domain**, and click **Next**.

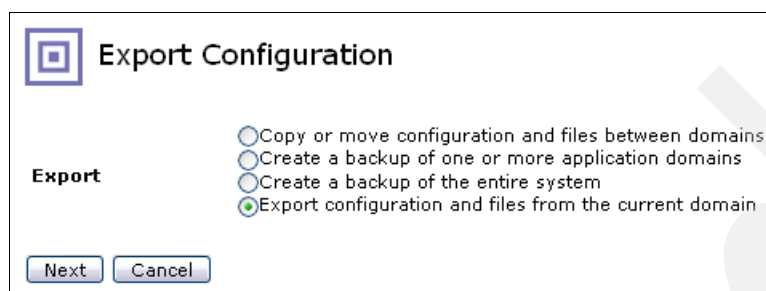


Figure 5-4 Selecting to export configuration from the current domain

4. In the next Export Configuration window, provide the requested information (Figure 5-5):
 - a. In the Export File Name field, enter a name for the export file.
 - b. In the Objects box, select **All Classes**. Then, double-click **All Objects** to add this item to the Selected objects box. Alternatively, click the right arrow to move All Objects to the Selected objects box.
 - c. Verify that the other default options are acceptable and make any changes as required.
 - d. Click **Next**.

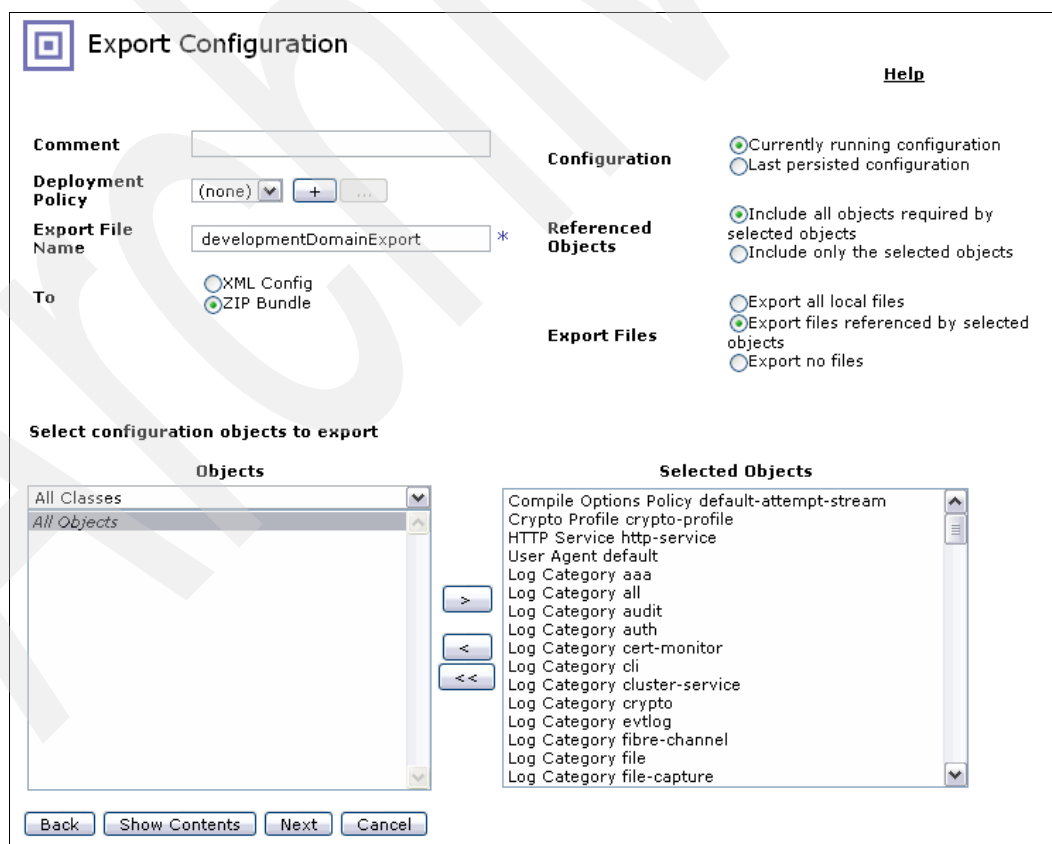


Figure 5-5 Naming the configuration export and selecting the configuration objects to include

5. Click **Download** to download the export file.

5.1.4 Creating domains

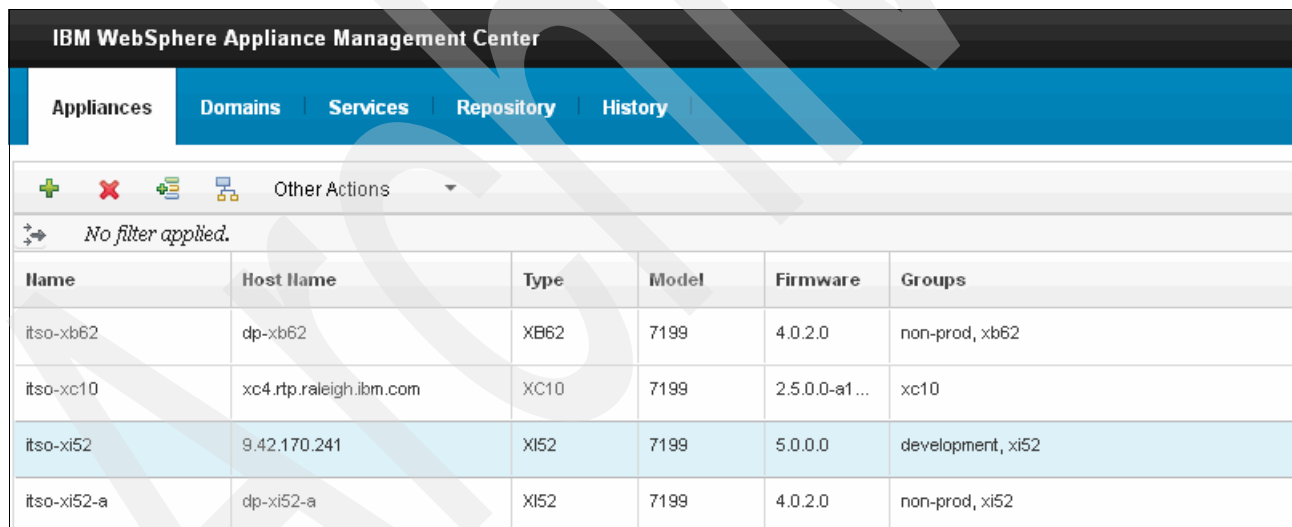
You can create application domains on WebSphere DataPower Appliances directly from WebSphere Appliance Management Center. The creation of a domain requires a domain configuration file. This file can be a domain configuration backup or a domain configuration export. If you are using a domain configuration backup, you must give the newly created domain the same name as the domain that was backed up. If you are using a domain configuration export, you can give the newly created domain any name. Domain configuration exports and backups are created by using the WebSphere DataPower web GUI as explained in 5.1.3, “Creating domain configuration files” on page 87. It is not possible to create domain configuration files by using WebSphere Appliance Management Center.

Required authorization: Creating domains in WebSphere Appliance Management Center requires a user to have the solution deployer role. For more information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

Creating a domain by using a domain configuration export

To create a domain that is called *test* by using a domain configuration export file:

1. Log in to WebSphere Appliance Management Center as a user with the solution deployer role.
2. Locate the target WebSphere DataPower Appliance in WebSphere Appliance Management Center. Click the appliance to select it. Figure 5-6 shows that WebSphere DataPower XI52 Appliance *itso-xi52* is selected in the appliance grid.



The screenshot shows the IBM WebSphere Appliance Management Center interface. The top navigation bar includes 'Appliances', 'Domains', 'Services', 'Repository', and 'History'. Below the navigation bar is a toolbar with icons for adding, deleting, and other actions, followed by a dropdown menu labeled 'Other Actions'. The main area displays a table of appliances. The table has columns for 'Name', 'Host Name', 'Type', 'Model', 'Firmware', and 'Groups'. The row for 'itso-xi52' is highlighted in blue, indicating it is selected.

Name	Host Name	Type	Model	Firmware	Groups
itso-xb62	dp-xb62	XB62	7199	4.0.2.0	non-prod, xb62
itso-xc10	xc4.rtp.raleigh.ibm.com	XC10	7199	2.5.0.0-a1...	xc10
itso-xi52	9.42.170.241	XI52	7199	5.0.0.0	development, xi52
itso-xi52-a	dp-xi52-a	XI52	7199	4.0.2.0	non-prod, xi52

Figure 5-6 Selecting a WebSphere DataPower Appliance in the appliance grid

3. From the toolbar, click **Other Actions** → **Create Domain**.

4. In the Create Domain window (Figure 5-7), enter the name of the new domain. In this example, the new domain is called *test*. Then, click **Next**.

Create Domain

Summary of appliances selected:

Name	Appliance Type
itso-xi52	xi52

New domains are created by using existing configuration. You can either use a backup that contains a domain of the same name, or a configuration export that contains objects to use in the new domain.

* Specify the name for this new domain:

Note: After a domain is created, you cannot change its name.

Figure 5-7 Creating a domain that is called *test* on the *itso-xi52* WebSphere DataPower Appliance

5. Select the domain configuration export to use for creating the domain:
 - If the file is stored on your hard drive, select **Local file**, and use the file browser to select the file. In this example, we select **Local file** (Figure 5-8).

Create Domain

Specify the configuration source for this domain:

The configuration source can be:

- A backup that contains a domain of the same name, or a configuration export that contains objects to include in this domain, loaded from one of the following locations:
 - A local file
 - A remote location accessed through HTTP or HTTPS
- An existing domain of the same name on another appliance

☒ Local file

Select File: **Browse**

☐ Remote location (URL)

Specify URL:

☐ An existing domain of the same name

Select domain:

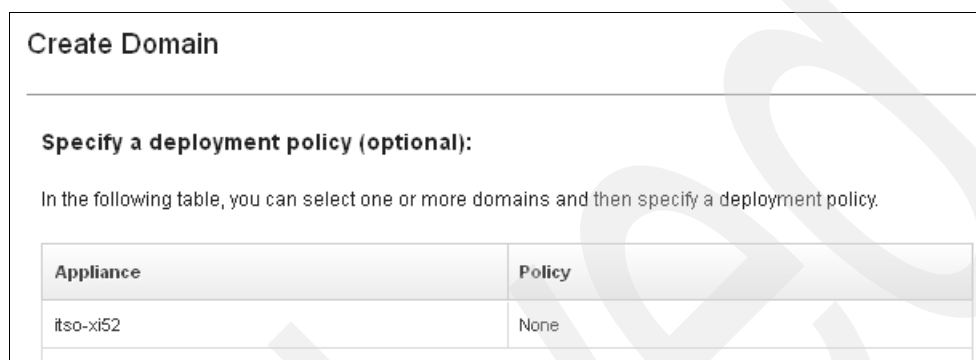
Figure 5-8 Using a local file as the configuration source for the new domain

- If the file is stored on another computer and can be accessed by using HTTP or unauthenticated HTTPS, select **Remote location (URL)** and enter the full URL to the file.

- The domain configuration can be copied directly from another domain without first creating a domain configuration file. To use this option, select **An existing domain of the same name**, and select the domain to use as the domain configuration source. The name of the source domain must match the name of the target domain.

Click **Next**.

6. In the next Create Domain window, select a deployment policy. For more information about using deployment policies, see 5.3, “Deployment policies” on page 113. In this example, we use the default option of setting no deployment policy (Figure 5-9). Click **Next**.



Create Domain

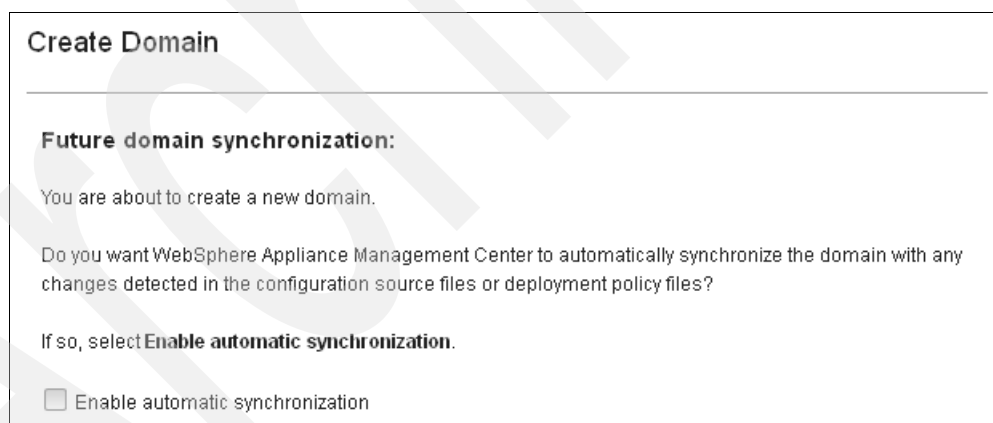
Specify a deployment policy (optional):

In the following table, you can select one or more domains and then specify a deployment policy.

Appliance	Policy
itsa-xi52	None

Figure 5-9 Creating a domain with the default deployment policy option of None

7. To update the domain configuration of the new domain whenever the source of the domain configuration changes, select **Enable automatic synchronization**. In this example, the Enable automatic synchronization is cleared (Figure 5-10). Automatic synchronization is described in detail in 5.4, “Automatic synchronization of a configuration” on page 125.



Create Domain

Future domain synchronization:

You are about to create a new domain.

Do you want WebSphere Appliance Management Center to automatically synchronize the domain with any changes detected in the configuration source files or deployment policy files?

If so, select **Enable automatic synchronization**.

☐ Enable automatic synchronization

Figure 5-10 Selecting not to use automatic synchronization of domain configuration

- Click **Create** to start the domain creation process. A feedback message is displayed to confirm that the domain creation process started. This feedback message changes to green if the domain was created successfully (top of Figure 5-11).

The domain is created by using the domain configuration export file that was provided. You can find the new domain test by going to the **Domains** tab as shown in Figure 5-11.

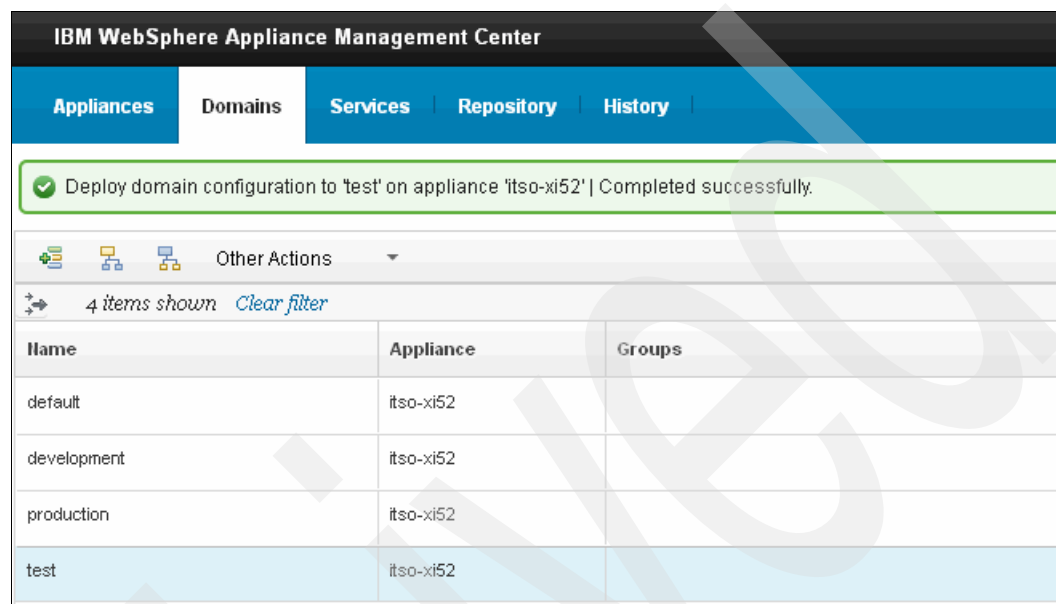


Figure 5-11 Newly created test domain

Creating a domain by using a domain configuration backup

Creating a domain from a domain configuration backup file follows the same process as for creating a domain by using a domain configuration export (see “Creating a domain by using a domain configuration export” on page 90). The difference is that the domain configuration backup file must contain a domain of the same name as the domain that is being created.

For example, when you create a domain called *production*, the domain configuration backup must include configuration for a domain called *production*. The create domain action fails if the configuration backup file does not contain a matching domain. Figure 5-12 shows an example of this error condition.

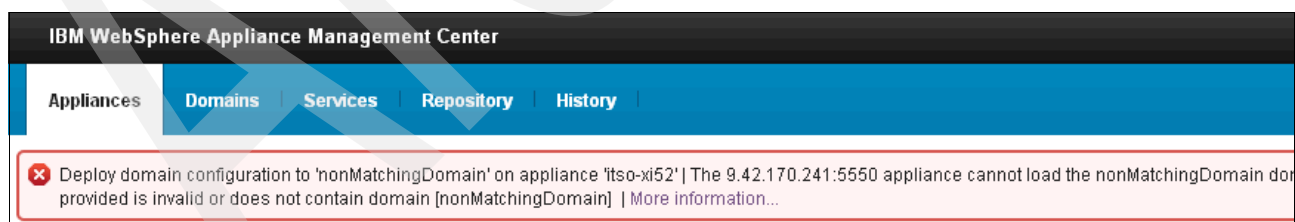


Figure 5-12 A failure when creating a domain

5.1.5 Updating domains

The configuration of an application domain can be updated by using WebSphere Appliance Management Center. The configuration of a domain can be replaced with an updated or changed configuration from a domain configuration export or configuration backup. The process for updating a domain follows a similar process as creating a domain. Domain configuration exports and backups are created by using the WebSphere DataPower web GUI

as described in 5.1.3, “Creating domain configuration files” on page 87. You cannot create domain configuration files by using WebSphere Appliance Management Center.

Required authorization: Updating domains in WebSphere Appliance Management Center requires a user to have the solution deployer role. For information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

Updating a domain by using a domain configuration export

To update a domain that is called *test* with new configuration from a domain configuration export:

1. Log in to WebSphere Appliance Management Center as a user with the solution deployer role.
2. Click the **Domains** tab, and select the domain that you want to update.

Tip: If many domains are listed, you can apply a filter to the list by clicking the **Define filter** icon. For more information, see “Filtering domains by using groups” on page 101.

3. Quiesce a domain before you update its configuration. For more information, see 5.1.6, “Quiescing and unquiescing domains” on page 96.
4. From the toolbar, click **Other Actions** → **Update Domain Configuration**.
5. In the Update Domain Configuration window, select the source of the domain configuration update by using one of the following options:
 - If the file is stored on your hard drive, select **Local file**, and use the file browser to select the file. In this example, we select **Local file** as shown in Figure 5-13.

Update Domain Configuration

Specify the configuration source for this domain:

The configuration source can be:

- A backup that contains a domain of the same name, or a configuration export that contains objects to include in this domain, loaded from one of the following locations:
 - A local file
 - A remote location accessed through HTTP or HTTPS
- An existing domain of the same name on another appliance

☒ Local file

Select file: **Browse**

☐ Remote location (URL)

Specify URL:

☐ An existing domain of the same name

Select domain:

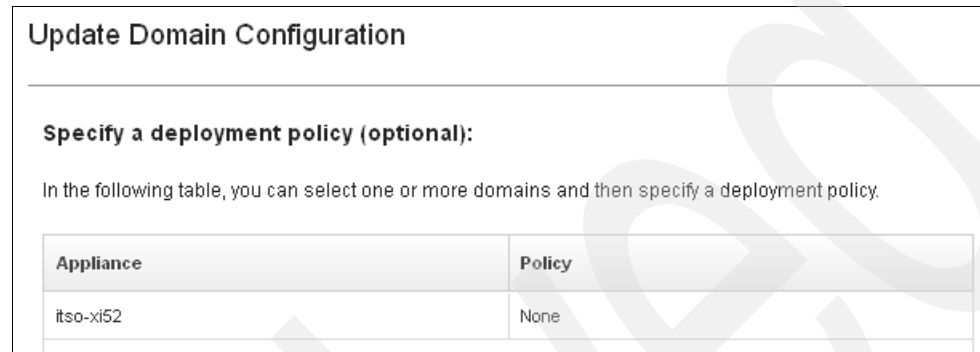
Figure 5-13 Updating domain configuration with a local configuration export

- If the file is stored on another computer and can be accessed by using HTTP or unauthenticated HTTPS, select **Remote location (URL)**, and enter the full URL to the file.

- A domain configuration can be copied directly from another domain without first creating a domain configuration file. To use this option, select **An existing domain of the same name**, and select the domain to use as the domain configuration source. The name of the source domain must match the name of the target domain.

Click **Next**.

- Specify a deployment policy. For information about using deployment policies, see 5.3, “Deployment policies” on page 113. This example uses the default option of setting no deployment policy as shown in Figure 5-14. Click **Next**.

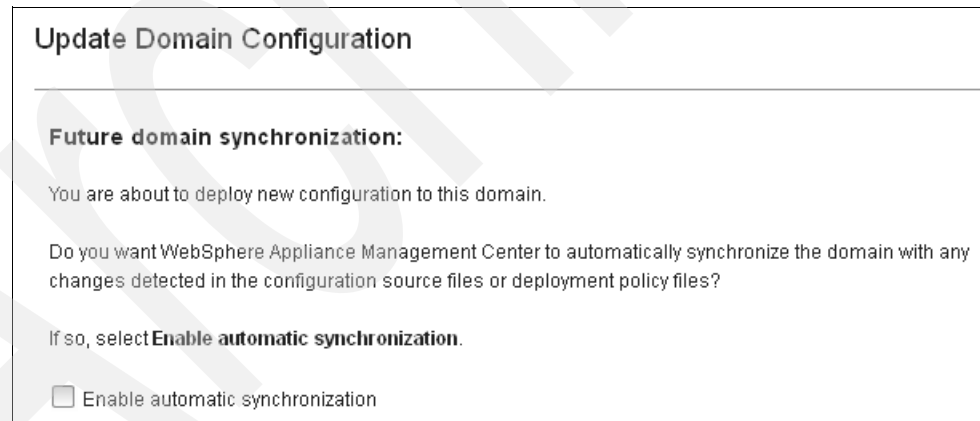


Appliance	Policy
its0-xi52	None

Figure 5-14 Updating domain configuration by using the default deployment policy option of None

- If you want the domain configuration of the domain to be updated whenever the source of the domain configuration changes, select **Enable automatic synchronization**. In this example, automatic synchronization is not enabled as shown in Figure 5-15.

For more information about automatic synchronization, see 5.4, “Automatic synchronization of a configuration” on page 125.



Future domain synchronization:

You are about to deploy new configuration to this domain.

Do you want WebSphere Appliance Management Center to automatically synchronize the domain with any changes detected in the configuration source files or deployment policy files?

If so, select **Enable automatic synchronization**.

☐ Enable automatic synchronization

Figure 5-15 Selecting not to use automatic synchronization of domain configuration

- Click **Finish** to start the update. A feedback message is displayed to confirm that the domain configuration is being updated.

Updating a domain by using a domain configuration backup

Updating a domain from domain configuration backup files follows the same process as for updating a domain by using a domain configuration export (see “Updating a domain by using a domain configuration export” on page 94). The difference is that the domain configuration backup file must contain a domain of the same name as the domain that is being updated.

For example, when you update a domain that is called *test*, the domain configuration backup must include configuration for a domain called *test*. The update domain action fails if the configuration backup file does not contain a matching named domain.

Updating multiple domains in a single action

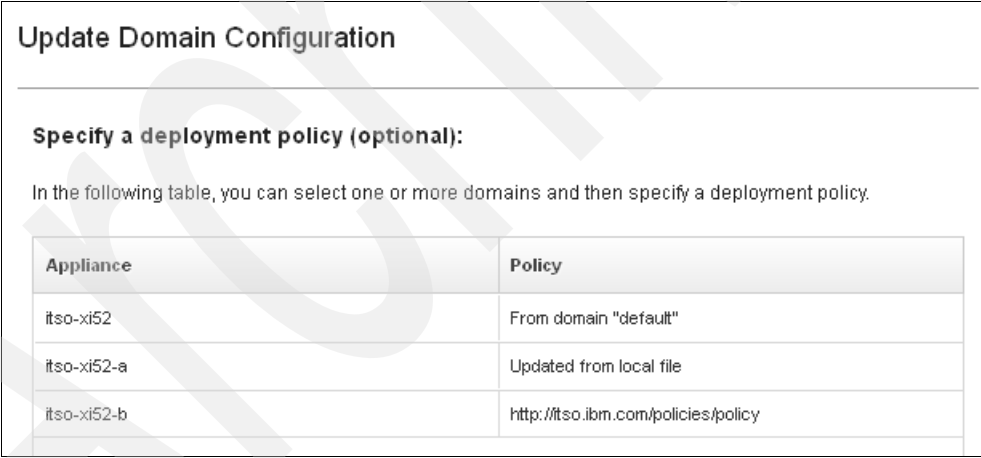
The real power of WebSphere Appliance Management Center is the ability to select multiple application domains across multiple WebSphere DataPower Appliances and to update the configuration of the domains in a single action. This action speeds up the deployment of an updated domain configuration across your WebSphere DataPower environment, reducing downtime and allowing for smaller maintenance windows.

Updating configuration across multiple domains differs from updating configuration for a single domain in the following ways:

- ▶ Multiple domains are selected from the Domains grid. The domains that are selected must all have the same name.
- ▶ Multiple deployment policies can be used for each domain that is being updated.

Use of deployment policies greatly simplifies, and in some cases makes possible, the use of a single domain configuration export to update multiple domains across multiple WebSphere DataPower Appliances. For information about deployment policies, see 5.3, “Deployment policies” on page 113.

Figure 5-16 shows the Update Domain Configuration window that opens from the Deployment Policy page. Each of the target domains on the different WebSphere DataPower Appliances uses a different deployment policy that makes the imported configuration suitable for the target environment.



Update Domain Configuration

Specify a deployment policy (optional):

In the following table, you can select one or more domains and then specify a deployment policy.

Appliance	Policy
its0-xi52	From domain "default"
its0-xi52-a	Updated from local file
its0-xi52-b	http://its0.ibm.com/policies/policy

Figure 5-16 Applying multiple deployment policies to multiple domains

5.1.6 Quiescing and unquiescing domains

Application domains can be quiesced by using WebSphere Appliance Management Center. The domain quiesce feature allows for a domain to be shut down gracefully so that existing operations can complete but no new requests are processed. Quiescing a domain is typically done to allow maintenance activity to be carried out without adversely affecting normal operations. Traffic can be temporarily rerouted to a fallover or backup domain, while the quiesced domain is updated or modified. After the domain is updated, it can be unquiesced again, and normal traffic patterns are restored.

Updating a domain: Updating a domain automatically does a quiesce and unquiesce of the WebSphere DataPower Appliance.

WebSphere Appliance Management Center submits the quiesce instruction to the target domain. The domain is given some time to fully quiesce, which is referred to as the *quiesce timeout*. The default quiesce timeout is 60 seconds, but this value can be set on domains individually if you know that particular domains might take longer to fully quiesce.

Occasionally an error might be reported when quiescing domains. In most cases, the error is that the quiesce did not complete within the timeout period. If this error happens frequently, consider increasing the quiesce timeout.

Required authorization: Quiescing and unquiescing domains in WebSphere Appliance Management Center requires a user to have the solution deployer role. For more information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

Quiescing a domain

To quiesce a domain by using WebSphere Appliance Management Center:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain that you want to quiesce.

Tip: If many domains are listed, you can apply a filter to the list by using the **Define filter** icon. For more information, see “Filtering domains by using groups” on page 101.

3. From the toolbar, click **Other Actions** → **Quiesce Domain** (Figure 5-17).

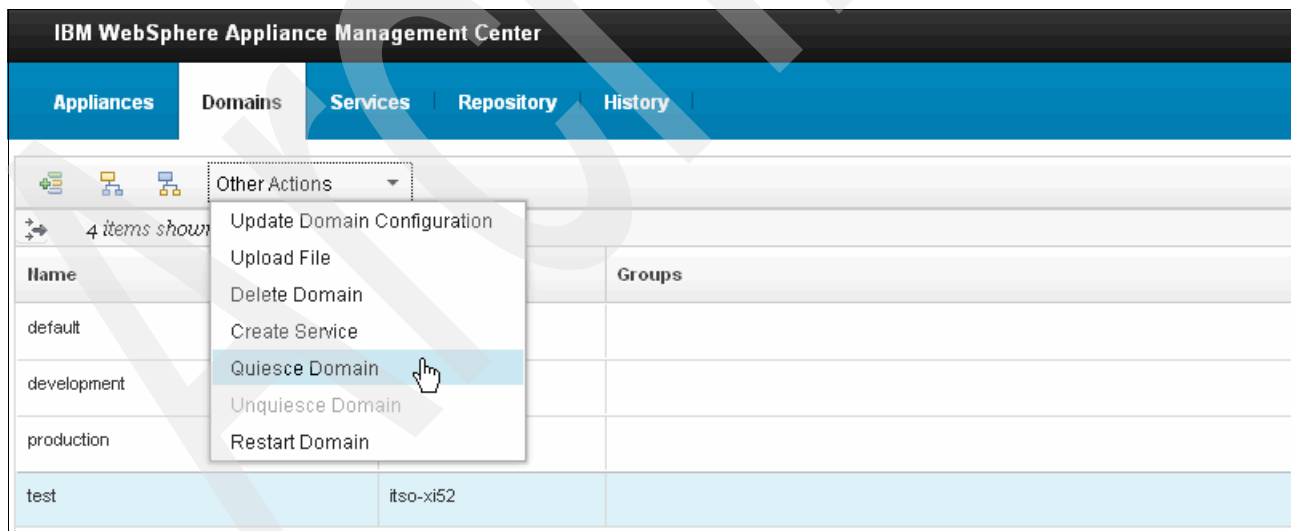


Figure 5-17 Selecting the Quiesce Domain option from the Other Actions menu

4. When you see the confirmation dialog, click **Quiesce** to quiesce the domain. The domain quiesces and stops processing further requests.

Unquiescing a domain

The domain remains in the quiesced state until it is unquiesced again. To unquiesce a domain by using WebSphere Appliance Management Center:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain that you want to unquiesce.

Tip: If many domains are listed, you can apply a filter to the list by using the **Define filter** icon. For more information, see “Filtering domains by using groups” on page 101.

3. From the toolbar, click **Other Actions** → **Unquiesce Domain** (Figure 5-18).

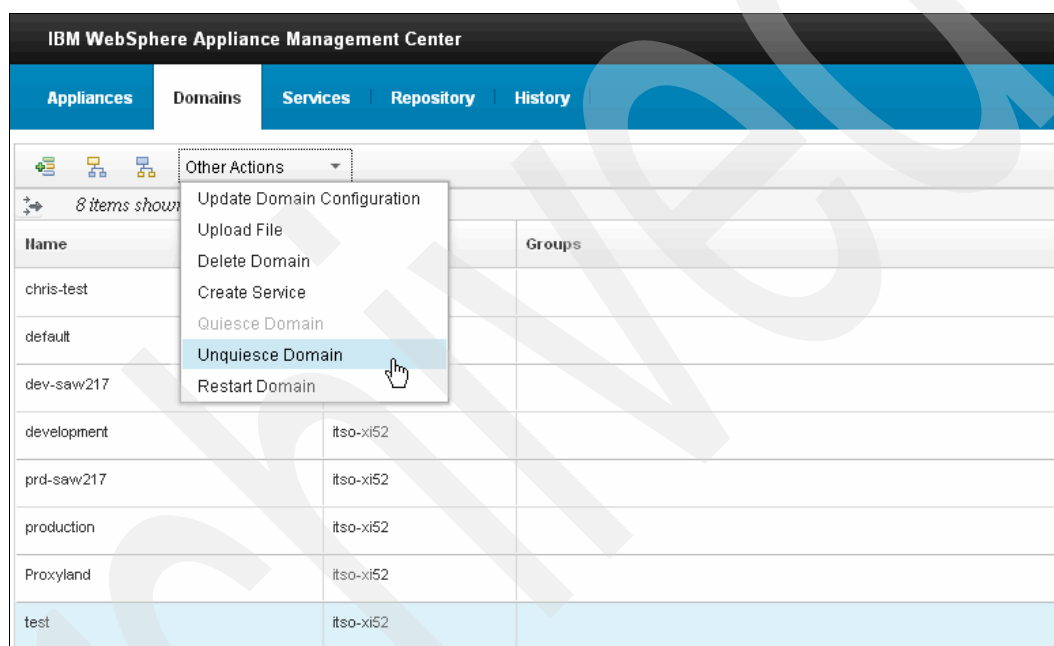


Figure 5-18 Selecting the Unquiesce Domain option from the Other Actions menu

4. In the confirmation window, click **Unquiesce** to unquiesce the domain.

5.1.7 Deleting domains

You can delete domains that are no longer required from WebSphere DataPower Appliances by using WebSphere Appliance Management Center.

Required authorization: Deleting domains in WebSphere Appliance Management Center requires a user to have the solution deployer role. For more information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

Before you delete a domain, you must check the following details:

- ▶ The domain is no longer required.
- ▶ Any active services in the domain are quiesced. For more information, see 5.2.5, “Quiescing and unquiescing services” on page 111.

- The domain is quiesced. For more information, see 5.1.6, “Quiescing and unquiescing domains” on page 96. Quiescing the domain automatically quiesces any services that are running on that domain.

To delete a domain from a WebSphere DataPower Appliance by using WebSphere Appliance Management Center:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain that you want to delete.

Tip: If many domains are listed, you can apply a filter to the list by using the **Define filter** icon. For more information, see “Filtering domains by using groups” on page 101.

3. From the toolbar, click **Other Actions** → **Delete Domain**.
4. In the Delete Domains window (Figure 5-19), confirm that the window shows the domains that you intend to delete.

If the domain or domains that are selected are not quiesced, a warning message is displayed. Quiesce the domains before you delete them, although you can delete unquiesced domains. For more information about quiescing a domain, see 5.1.6, “Quiescing and unquiescing domains” on page 96.

Delete Domains

If you proceed, the domains and all services in the domains are permanently deleted from the specified appliances.

Are you sure you want to delete the following domains?

Name	Appliance	Status
test	its0-xi52	Quiesced

Delete **Cancel**

Figure 5-19 Delete domain confirmation dialog for a quiesced domain

5. Click **Delete** to delete the domain from the WebSphere DataPower Appliance. A success message is displayed, confirming that the delete action completed correctly.

5.1.8 Managing groups of domains

Identifying which application domains belong to which operating environment can become difficult when you add more WebSphere DataPower Appliances to WebSphere Appliance Management Center and the number of application domains on those appliances increases. For example, if a domain configuration update is to be applied to a domain in the test

environment, how can the solution deployer quickly locate all of the domains to be updated? WebSphere Appliance Management Center allows for application domains to be added to groups. The domains grid can then be filtered by using the group name, enabling the solution deployer to find the domains that they need to work with.

Adding domains to a group

To add a domain to a group:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain or domains to add to a group.
3. Click the **Assign Groups** icon from the toolbar (Figure 5-20).

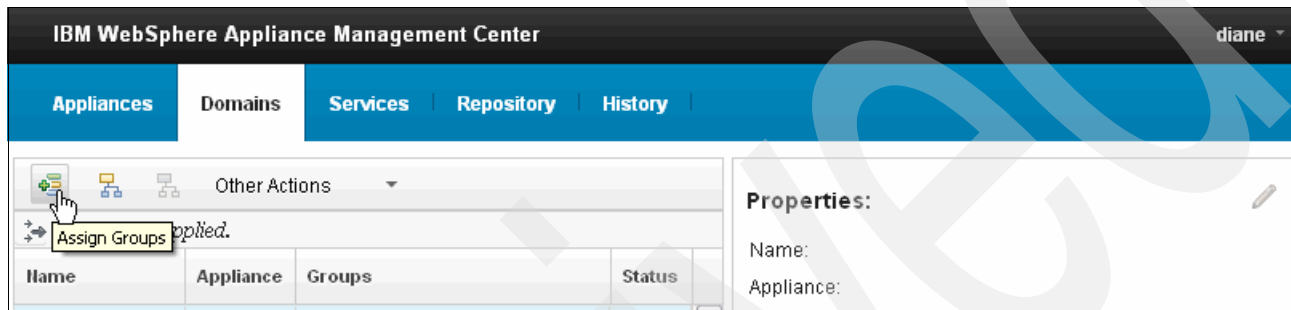


Figure 5-20 The Assign Groups icon on the Domains grid toolbar

4. In the Assign Groups window (Figure 5-21):
 - a. Add the domains to groups by using either of the following methods:
 - Select an existing group from the Existing groups list.
 - Create a group by entering a name for the group in the Group name field, and click **Add**.

Assign Groups

Existing groups

Use the check boxes to add members to or remove members from a group.

☒ production (1)

Create a new group

Group name ?

Figure 5-21 Assigning groups

- b. Optional: Add more groups by repeating step a.
- c. After all required changes are made, click **Apply** to save the changes.
- d. Close the Assign Groups window.

Removing domains from a group

To remove domains from a group or groups:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain or domains that you want to remove from groups.
3. Click the **Assign Groups** icon from the toolbar above the domains grid (Figure 5-20 on page 100).
4. In the Assign Groups window (Figure 5-21 on page 100), to remove all selected domains from a group:
 - a. Find the group in the Existing groups list, and clear the check box for the group name.
 - b. Repeat step a for all groups that you want to remove the selected WebSphere DataPower Appliances from.
 - c. Click **Apply** to save the changes.
 - d. Close the Assign Groups window.

Filtering domains by using groups

To filter the domains grid by using a group or groups:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. From the **Domains** tab, click the **Define filter** icon (Figure 5-22).

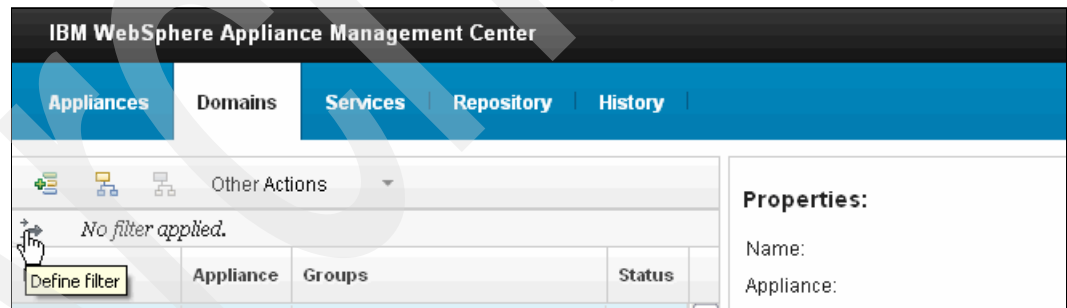


Figure 5-22 The Define filter icon for the Domains grid

3. In the Filter window (Figure 5-23):
 - a. For the Column field, select **Groups**.
 - b. For the Condition field, select an appropriate condition, such as **contains**.
 - c. For the Value field, select or type the name of a group to filter on.
 - d. Click **Filter** to apply the filter.
 - e. Close the Filter window. The Domains grid updates to reflect the filter that is applied.

The image shows a 'Filter' dialog box. At the top, there is a 'Match' dropdown menu set to 'all rules'. Below this, a text input field contains the text 'Groups contains development'. Underneath, there are three stacked dropdown menus: 'Column' is set to 'Groups', 'Condition' is set to 'contains', and 'Value' is set to 'development'. At the bottom of the dialog, there are four buttons: a green plus icon, 'Filter', 'Clear', and 'Cancel'.

Figure 5-23 Defining a filter for groups that contain the word 'development'

5.2 Managing services

Many different services are available on a WebSphere DataPower Appliance, including Multiprotocol Gateway, XML Firewall, and Web Service Proxy. The types of services that are available vary based on the WebSphere DataPower Appliance type. For example, the XB62 appliance offers a B2B Gateway service, and an XI52 appliance does not.

Services are configured and deployed in application domains. An application domain serves as the hosting environment for one or more services. Service configuration can be exported from a WebSphere DataPower Appliance in much the same way that domain configuration can be exported. WebSphere Appliance Management Center can then use this exported configuration to deploy new services or to update existing services. Services can also be deleted by using WebSphere Appliance Management Center.

You can export a service configuration by using the WebSphere DataPower web GUI and then use this configuration to create and update services. You can also delete a service.

5.2.1 Exporting service configuration

The WebSphere DataPower web GUI is used to create a service configuration export. Creating a service configuration export is not possible by using WebSphere Appliance Management Center.

To create a service configuration export file:

1. Log in to the WebSphere DataPower web GUI for your WebSphere DataPower Appliance, and make sure to specify the domain that contains the service or services to export. In this example, for the domain to log in to, we select **development** (Figure 5-24).

A screenshot of the WebSphere DataPower Login dialog box. The title is "WebSphere DataPower Login" and the subtitle is "X152 console at 9.42.170.241:9090". It contains three input fields: "User Name:" with the text "admin", "Password:" with masked characters, and "Domain:" with a dropdown menu showing "development". There are "Login" and "Cancel" buttons at the bottom. A small copyright notice is at the bottom: "Licensed Materials - Property of IBM Corp. © IBM Corporation and other(s) 1999-2012. IBM is a registered trademark of IBM Corporation, in the United States, other countries, or both."

Figure 5-24 Logging in to the development domain

2. From the Control panel, select **Administration** → **Configuration** → **Export Configuration**.
3. In the Export Configuration window (Figure 5-25), select **Export configuration and files from the current domain**. Then, click **Next**.

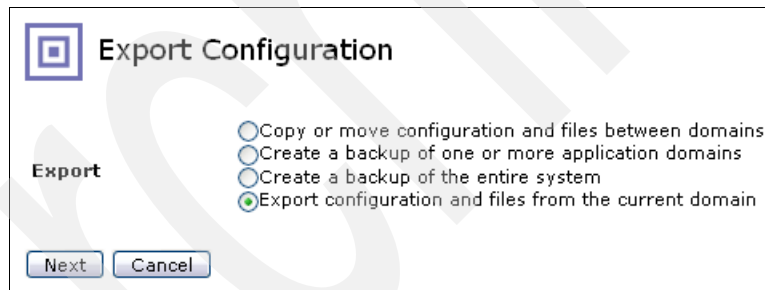
A screenshot of the Export Configuration dialog box. It has a title bar with a square icon and the text "Export Configuration". Below the title bar, there is a section labeled "Export" with four radio button options: "Copy or move configuration and files between domains", "Create a backup of one or more application domains", "Create a backup of the entire system", and "Export configuration and files from the current domain". The last option is selected. At the bottom, there are "Next" and "Cancel" buttons.

Figure 5-25 Selecting to export configuration from the current domain

4. In the next Export Configuration window (Figure 5-26 on page 104):
 - a. In the Export File Name field, enter a name for the export file.
 - b. At the top of the Objects box, select the type of the service to be exported, such as **HTTP Service**.
 - c. In the Object box, select the service or services to export. Then, double-click the service or services to add them to the Selected objects box. Alternatively, click the right arrow to move the services to the Selected objects box.
 - d. For Referenced Objects, verify that **Include all objects required by selected objects** is selected so that any configuration objects that are required by the exported service or services are included in the export file.
 - e. For Export Files, verify that **Export files referenced by selected objects** is selected so that any files that are required by the exported service or services are included in the export file.

- f. Verify that the other default options are acceptable, and make any changes as required.
- g. Click **Next**.

Figure 5-26 Exporting configuration for selected services

5. Click **Download** to download the export file.

For more information about backing up domain configuration and exporting application domain configuration and objects from an application domain, see the *Backing up and exporting configuration data* topic of the WebSphere DataPower Integration Appliance version 5.0 Information Center at:

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/topic/com.ibm.dp.xi.doc/administratorsguide.xi50229.htm?path=4_2_0_4_6_3#webgui_backingupexportingconfigdata_task

5.2.2 Creating services

You can deploy new services to application domains by using WebSphere Appliance Management Center. The creation of a service requires a configuration export that contains an exported configuration for one or more services. You can also create services by using domain configuration backups. If you are using a domain configuration backup, you must create the service on a domain with the same name as the domain that was the source of the backup. Service configuration exports are created by using the WebSphere DataPower web

GUI as described in 5.2.1, “Exporting service configuration” on page 102. You cannot create service configuration files by using WebSphere Appliance Management Center.

Required authorization: Creating a service in WebSphere Appliance Management Center requires a user to have the solution deployer role. For more information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

To create a service from a configuration export:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain in which you want to create a service.

Tip: If many domains are listed, you can apply a filter to the list by using the **Define filter** icon. For more information, see “Filtering domains by using groups” on page 101.

3. From the toolbar, click **Other Actions** → **Create Service**.
4. In the Create Service window (Figure 5-27), select the service configuration file to use for creating the service by using one of the following options:
 - If the file is stored on your hard drive, select **Local file**, and use the file browser to select the file. In this example, we select **Local file** as shown in Figure 5-27.
 - If the file is stored on another computer and can be accessed by using HTTP or unauthenticated HTTPS, select **Remote location (URL)** and provide the full URL to the file.

Click **Next**.

Create Service

Summary of domains selected:

Name	Appliance Name
test	itso-xi52

Specify the configuration source for this service

☒ Local file

Select File: **Browse**

☐ Remote location (URL)

Specify URL:

Next **Cancel**

Figure 5-27 Selecting the local file to use as the source of the service configuration

5. In the next Create Service window (Figure 5-28), select the service to create from the Select the service name and type field:
 - If the service configuration file that you specified contains a single service, it is preselected.
 - If the service configuration file that you specified contains multiple services, select the service that you want to create.

Click **Next**.

Create Service

Summary of domains selected:

Hostname	Appliance Name
test	its0-xi52

* Select the service name and type:

wsproxy-service, Web Service Proxy ▼
 wsproxy-service, Web Service Proxy
 http-service, HTTP Service
 ssl-proxy, SSL Proxy Service

Figure 5-28 Selecting the service to create

6. In the next Create Service window, specify a deployment policy. For information about using deployment policies, see 5.3, “Deployment policies” on page 113. This example uses the default option setting (None) as shown in Figure 5-29. Click **Next**.

Create Service

Specify a deployment policy (optional):

In the following table, you can select one or more service and then specify a deployment policy.

Appliance	Domain	Policy
its0-xi52	development	None

Figure 5-29 Creating a service by using no deployment policy

7. In the last Create Service window, review the list of other services that are affected by the deployment of this new service, which happens if the services share configuration objects or files. Affected services are quiesced during the creation of the new service. Figure 5-30 shows an example of the affected services information where another service is affected by the creation of the new service. Click **Create**.

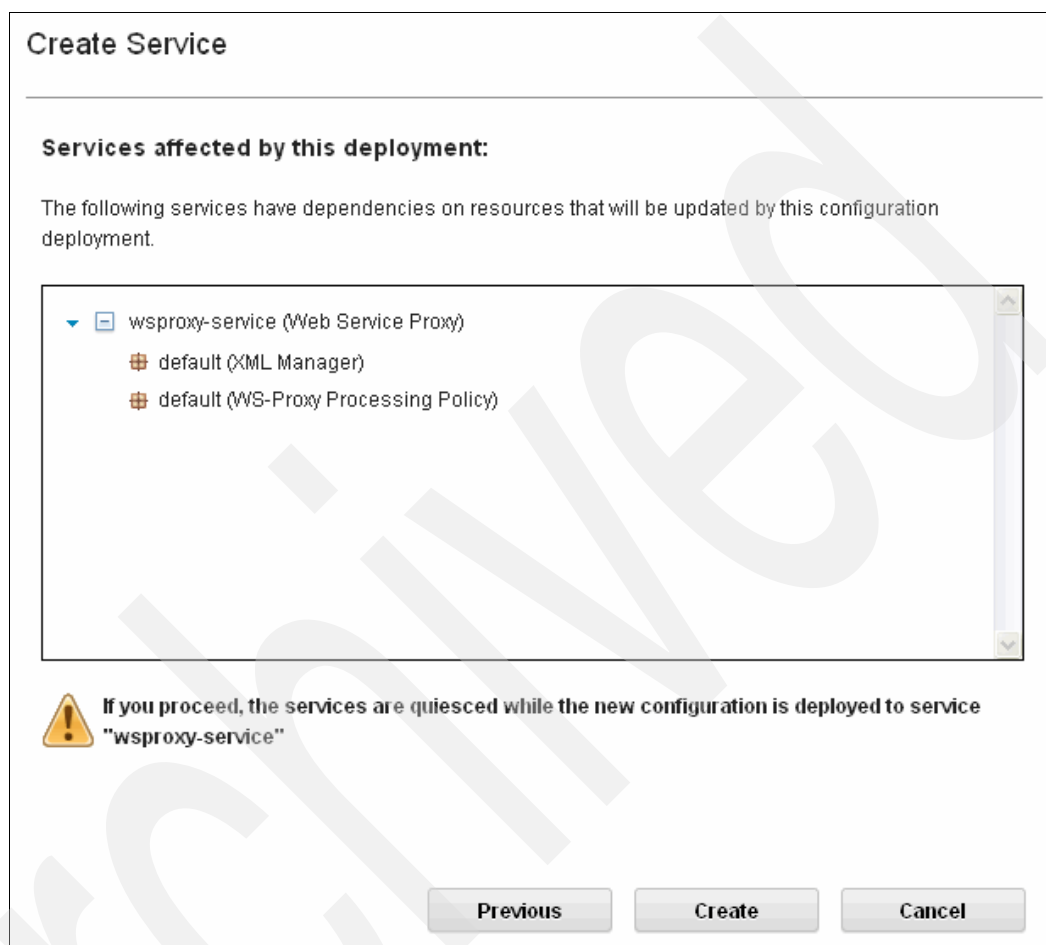


Figure 5-30 Listing of the services that are affected by the creation of the new service

The new service is created on the selected domain.

5.2.3 Updating services

You can update or replace the configuration of a service by using WebSphere Appliance Management Center. You can replace the configuration of a service with a configuration taken from a configuration export file.

The process for updating a service configuration is similar to the process for creating a service. Quiesce a service before you update its configuration. For more information, see 5.2.5, “Quiescing and unquiescing services” on page 111.

Required authorization: Updating a service in WebSphere Appliance Management Center requires a user with the solution deployer role. For information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

To update the configuration of a service:

1. Log in to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Services** tab, select the service that you want to update.

Tip: If many services are listed, you can apply a filter to the list by using the **Define filter** icon.

3. From the toolbar, click **Other Actions** → **Update Service Configuration**.
4. In the Update Service Configuration window (Figure 5-31), select the service configuration export to use for updating the service by choosing one of the following options:
 - If the file is stored on your hard drive, select **Local file**, and use the file browser to select the file. In this example, we use the **Local file** option.
 - If the file is stored on another computer and can be accessed by using HTTP or unauthenticated HTTPS, select **Remote location (URL)** and provide the full URL to the file.

Click **Next**.

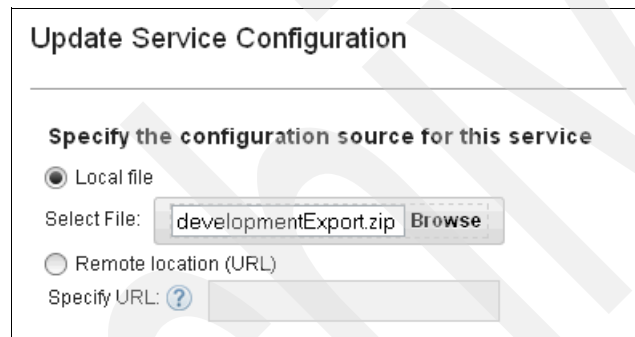
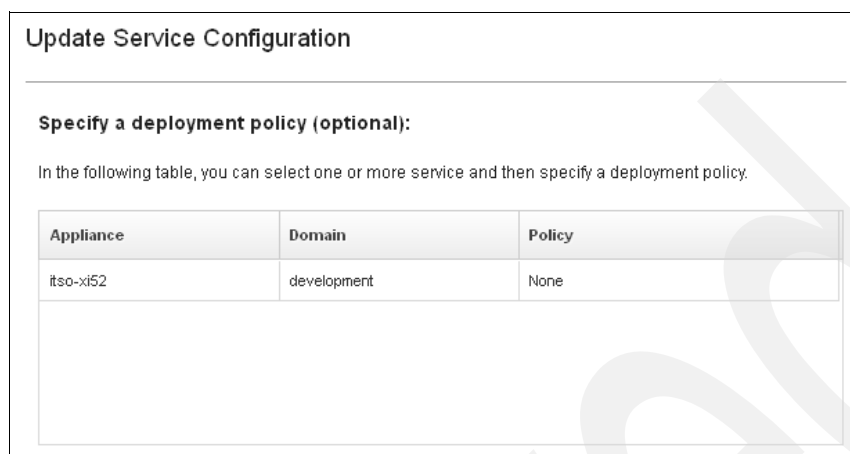


Figure 5-31 Selecting the source of the updated service configuration

5. In the next Update Service Configuration window, specify a deployment policy. For information about using deployment policies, see 5.3, “Deployment policies” on page 113. This example uses the default option setting (None) as shown in Figure 5-32. Click **Next**.



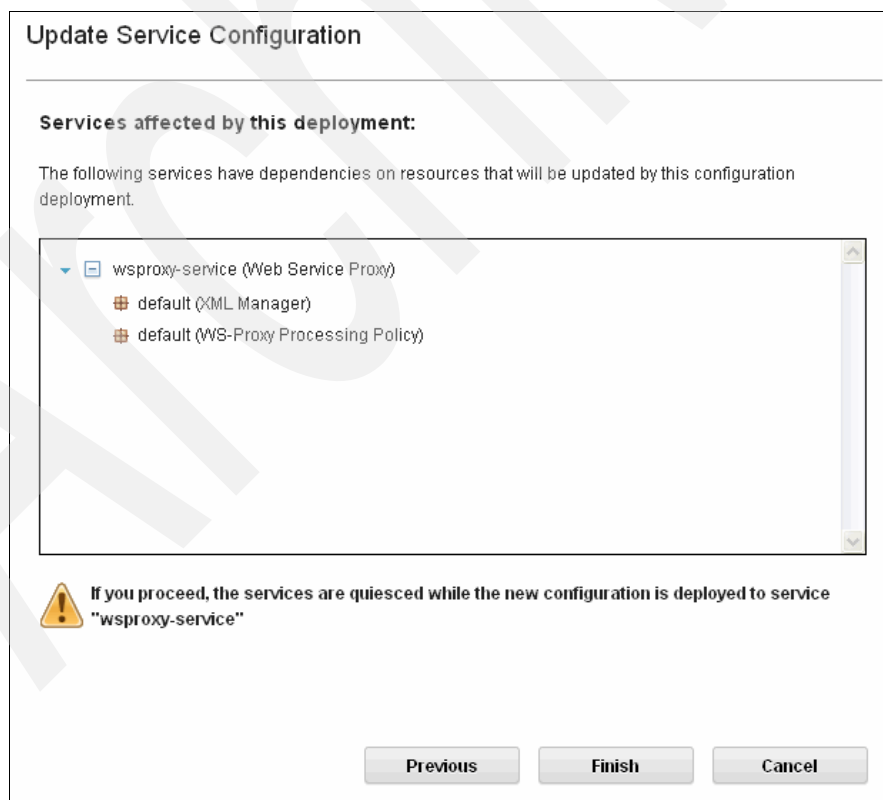
The window is titled "Update Service Configuration". Below the title bar, there is a section titled "Specify a deployment policy (optional):". Under this section, a text label reads: "In the following table, you can select one or more service and then specify a deployment policy." Below the text is a table with three columns: "Appliance", "Domain", and "Policy". The table contains one row with the following values: "its0-xi52" under Appliance, "development" under Domain, and "None" under Policy.

Appliance	Domain	Policy
its0-xi52	development	None

Figure 5-32 Selecting not to use a deployment policy during the update

6. In the last Update Service Configuration window (Figure 5-33), review the list of services that are affected by the updates to the selected service. The list shows other services that share configuration objects or files with the service that is being updated. Any affected services are quiesced, while the update process completes.

Then, click **Finish**. The configuration for the selected service is updated.



The window is titled "Update Service Configuration". Below the title bar, there is a section titled "Services affected by this deployment:". Under this section, a text label reads: "The following services have dependencies on resources that will be updated by this configuration deployment." Below the text is a list box containing the following items: "wsproxy-service (Web Service Proxy)", "default (XML Manager)", and "default (WS-Proxy Processing Policy)". Below the list box, there is a warning icon (a yellow triangle with an exclamation mark) and a text label: "If you proceed, the services are quiesced while the new configuration is deployed to service 'wsproxy-service'". At the bottom of the window, there are three buttons: "Previous", "Finish", and "Cancel".

Figure 5-33 List of services that are affected by the configuration update

Updating multiple services in a single action

Similar to domains, you can update the configuration of multiple services in WebSphere Appliance Management Center in a single action. This approach has the following advantages:

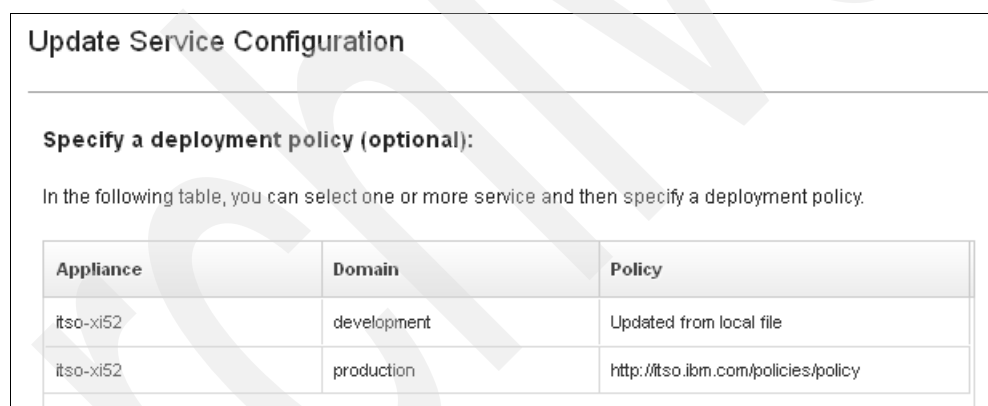
- ▶ It speeds up the deployment of configuration to multiple domains across multiple WebSphere DataPower Appliances.
- ▶ It helps to reduce the amount of time that is required to perform maintenance.

Updating multiple services differs from updating a single service in the following ways:

- ▶ Multiple services are selected from the Services grid. The services that are selected must all be of the same service type, for example XML Firewall or Web Service Proxy.
- ▶ Multiple deployment policies can be used. A deployment policy can be set for each service that is updated.

Use of deployment policies greatly simplifies, and in some cases, makes possible the use of a single service configuration export to update multiple services across multiple domains on multiple WebSphere DataPower Appliances. For more information about deployment policies, see 5.3, “Deployment policies” on page 113.

Figure 5-34 shows the deployment policy page of the Update Service Configuration window. Each service to be updated uses a different deployment policy that makes the imported configuration suitable for the target environment.



The screenshot shows a window titled "Update Service Configuration". Inside, there is a section titled "Specify a deployment policy (optional):" followed by the text "In the following table, you can select one or more service and then specify a deployment policy." Below this is a table with three columns: "Appliance", "Domain", and "Policy".

Appliance	Domain	Policy
itso-xi52	development	Updated from local file
itso-xi52	production	http://itso.ibm.com/policies/policy

Figure 5-34 Using multiple deployment policies to update multiple services on different domains

5.2.4 Updating services by using IBM WebSphere Registry and Repository

You can modify a service configuration by using IBM WebSphere Registry and Repository. You can configure WebSphere DataPower Appliances to automatically make service configuration updates from WebSphere Service Registry and Repository. For more information, see *SOA Policy, Service Gateway, and SLA Management*, SG24-8101.

You can also find more information about using IBM WebSphere Registry and Repository at:

http://www.ibm.com/developerworks/websphere/library/techarticles/1204_burke/1204_burke.html

5.2.5 Quiescing and unquiescing services

Similar to domains, WebSphere Appliance Management Center allows for individual services to be quiesced and unquiesced. This way, configuration changes can be made at the service level without adversely impacting regular application traffic. Requesting a service to quiesce causes the service to stop accepting new requests but allows existing requests to complete.

Unlike a domain-level quiesce, you cannot set a quiesce timeout for an individual service. The domain quiesce timeout is used.

Required authorization: Quiescing and unquiescing services in WebSphere Appliance Management Center requires a user to have the solution deployer role. For information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

Quiescing a service

To quiesce a service by using WebSphere Appliance Management Center:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Services** tab, select the service that you want to quiesce.

Tip: If many services are listed, you can apply a filter to the list by using the **Define filter** icon.

3. From the toolbar, click **Other Actions** → **Quiesce Service** (Figure 5-35).

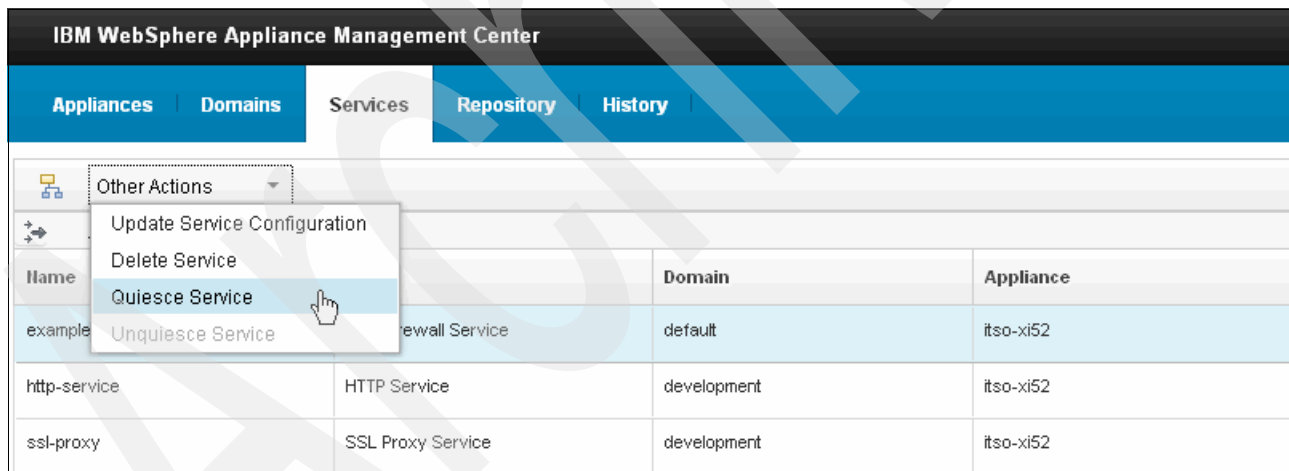


Figure 5-35 Selecting the Quiesce Service option from the Other Actions menu

4. In the confirmation window, click **Quiesce** to quiesce the service. The service quiesces and stops processing further requests.

Unquiescing a service

A service remains in the quiesced state until it is unquiesced again. To unquiesce a service by using WebSphere Appliance Management Center:

1. Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Services** tab, select the service that you want to unquiesce.

Tip: If many services are listed, you can apply a filter to the list by using the **Define filter** icon.

- From the toolbar, click **Other Actions** → **Unquiesce Service** (Figure 5-36).

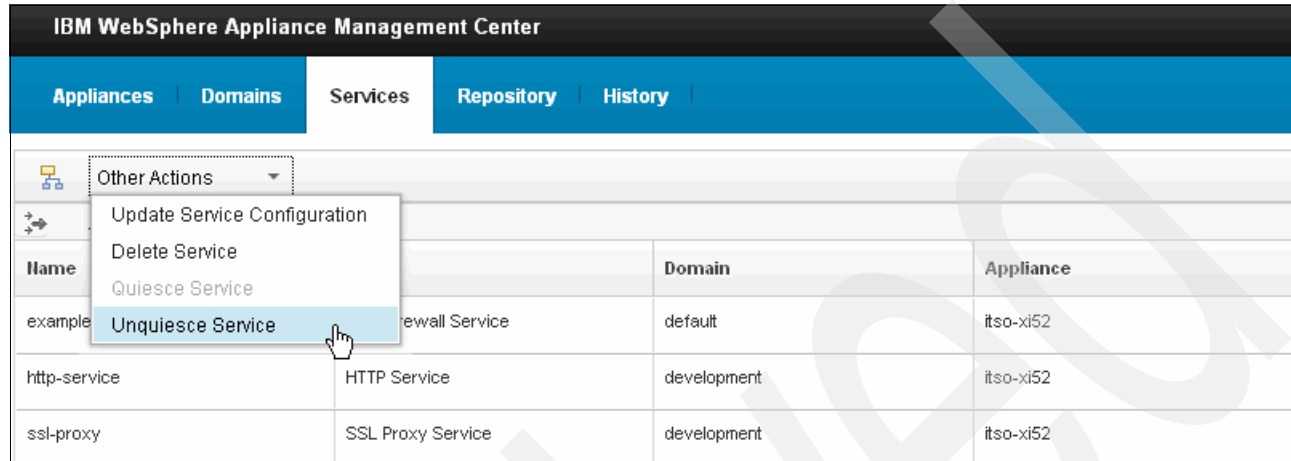


Figure 5-36 Selecting the Unquiesce Service option from the Other Actions menu

- In the confirmation window, click **Unquiesce** to unquiesce the service.

5.2.6 Deleting services

You can delete services by using WebSphere Appliance Management Center.

Required authorization: Deleting services in WebSphere Appliance Management Center requires a user with the solution deployer role. For information about configuring user roles, see 2.4, “Managing users and roles” on page 32.

Before you delete a service, verify the following prerequisites:

- ▶ The service is not required for proper function of other services or applications.
- ▶ The service is quiesced so that any in-flight data traffic can complete its processing. For more information, see 5.2.5, “Quiescing and unquiescing services” on page 111.

To delete a service from an application domain by using WebSphere Appliance Management Center:

- Log on to WebSphere Appliance Management Center as a user with the solution deployer role.
- On the **Services** tab, select the service that you want to delete.

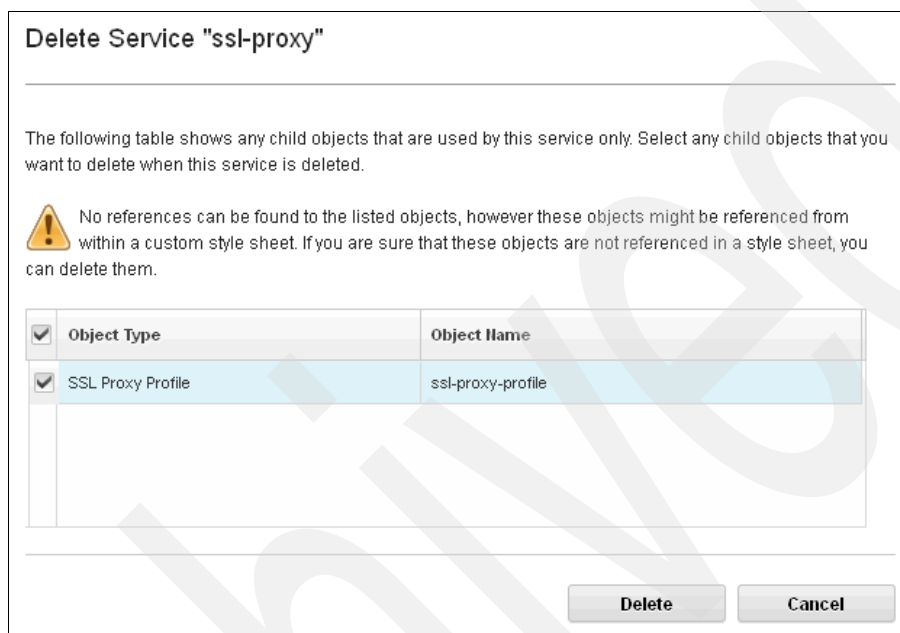
Tip: If many services are listed, you can apply a filter to the list by using the **Define filter** icon.

- From the toolbar, click **Other Actions** → **Delete Service**.

4. In the Delete Service window (Figure 5-37), verify that the reported objects are genuinely not being used. Select any objects that you want to delete along with the service.

This window lists any objects that the service is using that will become orphaned when the service is deleted. These objects can normally be safely removed. The window includes a warning message about certain configurations where an object that is reported as orphaned is still in use.

Click **Delete** to remove the service and any selected child objects that are associated with it.



The dialog box titled "Delete Service 'ssl-proxy'" contains a warning message and a table of child objects. The warning message states: "No references can be found to the listed objects, however these objects might be referenced from within a custom style sheet. If you are sure that these objects are not referenced in a style sheet, you can delete them." The table has two columns: "Object Type" and "Object Name". It lists one object: "SSL Proxy Profile" with the name "ssl-proxy-profile". There are "Delete" and "Cancel" buttons at the bottom right.

<input checked="" type="checkbox"/> Object Type	Object Name
<input checked="" type="checkbox"/> SSL Proxy Profile	ssl-proxy-profile

Figure 5-37 Deleting a service with orphaned child objects

5.3 Deployment policies

Deployment policies are a powerful mechanism that is provided by WebSphere DataPower Appliances to modify the deployment of configuration at deployment time. By using WebSphere Appliance Management Center, deployment policies can be used when you create or update domains and services. You can use deployment policies when you deploy a configuration to domains and services by using WebSphere Appliance Management Center.

5.3.1 Understanding deployment policies

To create configuration files for application domains and services, see 5.1.3, "Creating domain configuration files" on page 87, and 5.2.1, "Exporting service configuration" on page 102. Then, these configuration exports can be used in WebSphere Appliance Management Center to create domains and services or to update the configuration of existing domains and services. The entire contents of the configuration export become the new configuration that is used for the target domain or service.

For example, consider a domain configuration export that contains configuration for an HTTP Service, an SSL Proxy Service, and a Web Service Proxy. Any new domain that is created by using this export file has all three of these services. Consider a situation where a user who creates a domain wants to include the HTTP Service but wants to exclude the other two resources. The user can create the domain with all three services and delete the two services

that they do not want. Alternatively, the user can use a deployment policy to filter out the unwanted resources.

Deployment policies are objects that are created on WebSphere DataPower Appliances. A deployment policy describes simple rules that are applied when configuration is deployed to domains and services. A deployment policy can select objects and a configuration from a configuration export. The policy can define the objects and configuration as one of the following types:

- Accepted (white listed)

Configuration and objects are white listed. Any such objects are included in the deployment target. Figure 5-38 shows a configuration export file that contains three services. The deployment policy that is applied during the configuration import accepts the configuration for one of the services. The other two services are not imported.

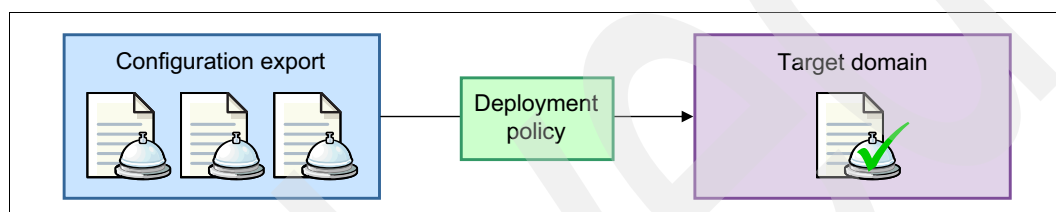


Figure 5-38 A deployment policy that accepts configuration objects

- Filtered (black listed)

Configuration and objects are black listed. Any such objects are always excluded from the deployment target. Figure 5-39 shows a configuration export file that contains three services. The deployment policy that is applied during the configuration import filters out two of the services, preventing them from becoming part of the target domain.

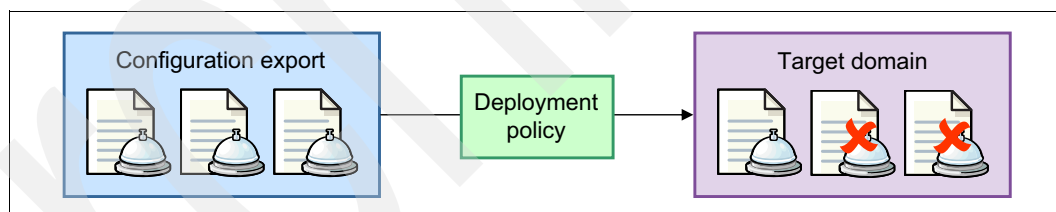


Figure 5-39 A deployment policy that filters configuration objects

- Modified

Configuration and objects can be changed as part of the deployment. Figure 5-40 shows a configuration export file that contains three services, each with a configuration property. The deployment policy that is applied during the configuration import modifies the configuration properties of the three services.

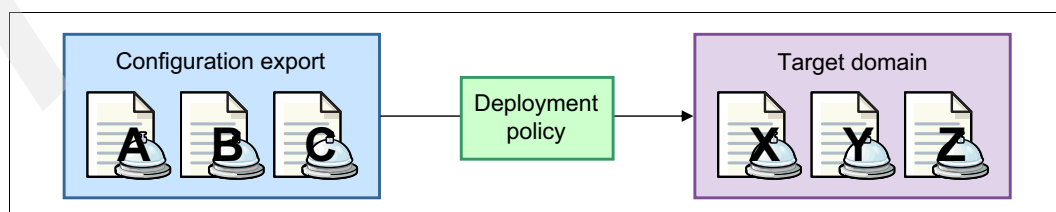


Figure 5-40 A deployment policy that modifies configuration objects

For more information about deployment policies, see the *Deployment policies* topic of the WebSphere DataPower Integration Appliance version 5.0 Information Center at:

http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/topic/com.ibm.dp.xi.doc/administratorsguide.xi50251.htm?path=4_2_0_4_7#deploypol_configuringdeploymentpolicies_concept

5.3.2 Creating deployment policies

Deployment policies are created by using the WebSphere DataPower web GUI. Deployment policies are objects that are created in application domains. A deployment policy can include any combination of accept, filter, and modify rules. This section describes the creation of three deployment policies, one for each of the rule types:

- ▶ Creating a deployment policy to accept configuration
- ▶ Creating a deployment policy to filter configuration
- ▶ Creating a deployment policy to modify configuration

To see how you can use these policies when you create a domain by using WebSphere Appliance Management Center, see 5.3.3, “Using deployment policies” on page 121.

Creating a deployment policy to accept configuration

To create a deployment policy that accepts a configuration that is based on user-defined criteria:

1. Log in to the WebSphere DataPower web GUI for your WebSphere DataPower Appliance.
2. Log in to the application domain where you intend to store the deployment policy object.
3. From the Control panel, select **Objects** → **Configuration Management** → **Deployment Policy**.
4. Click **Add** to create a deployment policy.
5. Give the deployment policy a meaningful name that describes its purpose, for example `accept-http-services`.
6. In the Accepted Configuration section, click **Build**.
7. In the Editing Policy window (Figure 5-41 on page 116), enter the following required information:
 - a. In the Device Address field, to accept configuration only from a certain WebSphere DataPower Appliance, specify the IP address or host name of the management interface of that appliance. To match all WebSphere DataPower Appliances, leave this field blank.
 - b. In the Application Domain field, to accept a configuration only from a certain WebSphere DataPower application domain, select the application domain. Set this field to **(none)** to match all application domains.
 - c. In the Resource Type field, to accept a configuration only for a particular resource type, select the resource type. Set this field to **(all resources)** to match all resource types.
 - d. In the Name Match (PCRE) field, to accept configuration for resources of a particular name, enter a Perl Compatible Regular Expression (PCRE) that matches the name.
 - e. In the Configuration Property field, to accept configuration for resources only if those resources have a certain property, enter the name of the property. If you also set to accept configuration by Resource Type, this field is replaced with a drop-down box from which you can select applicable properties.

- f. In the Configuration Value Match (PCRE) field, to accept configuration for resources only if those resources with a property that has a particular value, enter a PCRE that matches the required value.

The resulting deployment policy accepts configuration from any WebSphere DataPower Appliance and any application domain where the type of the resource is HTTP Service. The name of the HTTP Service must contain the string test and the HTTP Service must have a Port Number setting of 8008.

- g. Click **Save** to save your changes and then close the window.

Editing Accepted Configuration property of **Deployment Policy**

Device Address: [Select Alias](#)

Application Domain: (none) ▼

Resource Type: HTTP Service ▼ *

Name Match (PCRE): .*test,*

Configuration Property: Port Number ▼

Configuration Value Match (PCRE): 8008

[Save](#) [Cancel](#) [Help](#)

Figure 5-41 Editing the accepted configuration for a deployment policy

The deployment policy is updated to show the built match statement. Figure 5-42 shows the built match statement for the example that is shown in Figure 5-41.

Configure Deployment Policy

Main **Modified Configuration**

Deployment Policy

[Apply](#) [Cancel](#)

Name: accept-http-services *

Administrative State: ☒ enabled ☐ disabled

Comments:

Accepted Configuration: */*/services/htpserv?Name=.*test.*&Property=LocalPort&Value=8008 ✕
 //services/htpserv?Name: [Add](#) [Build](#)

Filtered Configuration: (empty)
 [Add](#) [Build](#)

Figure 5-42 The accepted configuration deployment policy

8. Click **Apply** to add the deployment policy to the current domain.
9. Click **Save Config** to save the deployment policy to the current domain.

Creating a deployment policy to filter configuration

To create a deployment policy that filters a configuration that is based on user-defined criteria:

1. Log in to the WebSphere DataPower web GUI for your WebSphere DataPower Appliance.
2. Log in to the application domain where you intend to store the deployment policy object.
3. From the Control panel, select **Objects** → **Configuration Management** → **Deployment Policy**.
4. Click **Add** to create a deployment policy.
5. Give the deployment policy a meaningful name that describes its purpose, for example filter-http-services.
6. In the Filtered Configuration section, click the **Build** button.
7. In the Editing Policy window (Figure 5-43 on page 118), enter the required information:
 - a. In the Device Address field, to filter configuration from a certain WebSphere DataPower Appliance, specify the IP address or host name of the management interface of that appliance. To filter from any WebSphere DataPower Appliance, leave this field blank.
 - b. In the Application Domain field, to filter configuration only from a certain application domain, select the application domain. Set this field to **(none)** to filter from any application domain.
 - c. In the Resource Type field, to filter configuration only for a particular resource type, select the resource type. Set this field to **(all resources)** to match any resource type.
 - d. In the Name Match (PCRE) field, to filter configuration for resources of a particular name, provide a Perl Compatible Regular Expression (PCRE) that matches the name.
 - e. In the Configuration Property field, to filter configuration for resources only if those resources have a certain property, enter the name of the property here. If you also set to filter configuration by Resource Type, this field is replaced with a drop-down box from which you can select applicable properties.
 - f. In the Configuration Value Match (PCRE) field, to filter configuration for resources only if those resources with a property that has a particular value, enter a PCRE that matches the required value.

The resulting deployment policy filters configuration from any WebSphere DataPower Appliance and any application domain where the type of the resource is HTTP Service. HTTP Services are filtered only if they contain the string dev and if they have a Port Number setting of 80. HTTP Services that do not match this filter are not filtered out when the configuration is deployed.

- g. Click **Save** to close the window and save your changes.

Editing Filtered Configuration property of **Deployment Policy**

Device Address: [Select Alias](#)

Application Domain:

Resource Type: *

Name Match (PCRE):

Configuration Property:

Configuration Value Match (PCRE):

[Save](#) [Cancel](#)

Figure 5-43 Editing the filtered configuration for a deployment policy

The deployment policy is updated to show the match statement that is built. Figure 5-44 shows the built match statement for the example that is shown in Figure 5-43.

Configure Deployment Policy

Main **Modified Configuration**

Deployment Policy

[Apply](#) [Cancel](#)

Name: *

Administrative State: ☒ enabled ☐ disabled

Comments:

Accepted Configuration: [Add](#) [Build](#)

Filtered Configuration: [X](#)
 [Add](#) [Build](#)

Figure 5-44 Filtered configuration match statement

8. Click **Apply** to add the deployment policy to the current domain.
9. Click **Save Config** to save the deployment policy to the current domain.

Creating a deployment policy to modify configuration

To create a deployment policy that modifies configuration that is based on user-defined criteria:

1. Log in to the WebSphere DataPower web GUI for your WebSphere DataPower Appliance.
2. Log in to the application domain where you intend to store the deployment policy object.

3. From the Control panel, select **Objects** → **Configuration Management** → **Deployment Policy**.
4. Click **Add** to create a deployment policy.
5. Enter a meaningful name for the deployment policy, such as `modify-http-services`, that describes its purpose.
6. Click **Modified Configuration** to display the Modified Configuration table.
7. Click **Add**.
8. In the Edit Modified Configuration window (Figure 5-45), for the Configuration Match field, click **Build**.

The screenshot shows a dialog box titled "Edit Modified Configuration". It contains the following fields and controls:

- Configuration Match:** A text input field followed by a "Build" button and an asterisk (*).
- Modification Type:** A dropdown menu currently showing "Add Configuration" with a downward arrow, followed by an asterisk (*).
- Configuration Property:** A text input field followed by an asterisk (*).
- Configuration Value:** A text input field followed by an asterisk (*).
- Buttons:** "Apply" and "Cancel" buttons at the bottom left.

Figure 5-45 The Edit Modified Configuration window

9. In the Editing Policy window (Figure 5-46 on page 120), enter the following information:
 - a. In the Device Address, to modify configuration from a certain WebSphere DataPower Appliance, specify the IP address or host name of the management interface of that appliance. To modify configuration from any appliance, leave this field blank.
 - b. In the Application Domain, to modify a configuration only from a certain application domain, select the application domain. Set this field to **(none)** to modify a configuration from any application domain.
 - c. In the Resource Type, to modify configuration only for a particular resource type, select the resource type. Set this field to **(all resources)** to match any resource type.
 - d. In the Name Match (PCRE), to modify configuration for resources of a particular name, enter a Perl Compatible Regular Expression (PCRE) that matches the name.
 - e. In the Configuration Property, to modify configuration for resources only if those resources have a certain property, enter the name of the property here. If you also selected to modify configuration by Resource Type, this field is replaced with a drop-down box from which you can select applicable properties.
 - f. In the Configuration Value Match (PCRE), to filter configuration for resources only if those resources with a property that has a particular value, enter a PCRE that matches the required value.

In this case, the deployment policy matches an HTTP service with a port number value of 80. Click **Save** to save your changes and close the Editing Policy window.

Figure 5-46 A sample configuration match for a deployment policy

10. Select the Modification Type to use for this deployment policy by choosing one of the following options:

- Select **Add Configuration** to create a deployment policy that adds new configuration properties to the configuration that is being deployed.
- Select **Change Configuration** to create a deployment policy that modifies the existing configuration as part of the deployment of configuration.
- Select **Delete Configuration** to create a deployment policy that removes the existing configuration as part of the deployment of configuration.

11. Complete any additional fields. The additional fields that are shown change depend on your selection in step 10.

- For Add Configuration, enter a configuration property and configuration value to add.
- For Change Configuration, enter a configuration value to replace the existing value.
- For Delete Configuration: No further fields need to be completed.

Click **Apply**.

Figure 5-47 shows an example of a modify configuration match statement that changes the configuration value to a new value of 8008.

Figure 5-47 Editing the modified configuration with the Change Configuration option selected

The Modified Configuration table updates to show the modify configuration rule that you created. Figure 5-48 shows the table after you create a modified configuration statement.

Configure Deployment Policy

Main Modified Configuration

Deployment Policy

Apply Cancel

Name

Modified Configuration

Configuration Match	Modification Type	Configuration Property	Configuration Value	
//services/httperv?Property=LocalPort&Value=80	Change Configuration		8008	↑ ↓

Figure 5-48 Final deployment policy showing the modification rule and new configuration value

In the example that is shown in Figure 5-48, the deployment policy matches the configuration from any WebSphere DataPower Appliance and any application domain. The resource type that is matched is an HTTP Service, and the service must have the string dev anywhere in its name. The HTTP Service must have a port number that is set to 80. If all of these criteria match, the deployment policy changes the value of the Port Number property to 8008.

5.3.3 Using deployment policies

You can use deployment policies in WebSphere Appliance Management Center as part of the process of creating and updating of domains and services. WebSphere Appliance Management Center can use deployment policies from the following resources:

- ▶ The machine that is running the web browser client
- ▶ A central store that is accessed by using HTTP or unauthenticated HTTPS
- ▶ Any domain on any WebSphere DataPower Appliance that is managed by WebSphere Appliance Management Center

If you use either of the first two options, the deployment policy objects must first be exported from the WebSphere DataPower Appliance. Deployment policies can be exported individually or as part of a domain configuration export or domain configuration backup. For information about configuration export, see 5.1.3, “Creating domain configuration files” on page 87.

The use of deployment policies when you create or update domains and services by using WebSphere Appliance Management Center is an optional step. The Create Domain, Update Domain Configuration, Create Service, and Update Service Configuration actions all include a panel that allows a deployment policy to be selected.

Figure 5-49 shows this panel as part of the Create Domain action.

Create Domain

Specify a deployment policy (optional):

In the following table, you can select one or more domains and then specify a deployment policy.

Appliance	Policy
its0-xi52	None

Deployment policy option: No policy ▾

Apply Cancel

Previous Next Cancel

Figure 5-49 Specifying a deployment policy as part of creating a domain

To start using deployment policies:

1. From the Specify a deployment policy page, select one or more of the rows in the table that is displayed.
2. In the Deployment policy option drop-down box, select one of the available options:

No policy

Proceed with the creation or update without using a deployment policy.

Policy from a local file

Use a deployment policy that is available on the machine that is running the web browser, which is connected to the WebSphere Appliance Management Center server.

Policy from a remote location

Use a deployment policy from another machine that is accessible by using HTTP or unauthenticated HTTPS.

Policy from another domain

Use a deployment policy that can be found in an application domain on a WebSphere DataPower Appliance that is managed by WebSphere Appliance Management Center.

Figure 5-50 shows these deployment policy options.

The screenshot shows a 'Create Domain' dialog box. It has a section titled 'Specify a deployment policy (optional):' with a sub-instruction: 'In the following table, you can select one or more domains and then specify a deployment policy.' Below this is a table with two columns: 'Appliance' and 'Policy'. The first row shows 'itso-xi52' under 'Appliance' and 'None' under 'Policy'. Below the table, there is a 'Deployment policy option:' label, an 'Apply' button, a 'Cancel' button, and a dropdown menu. The dropdown menu is open, showing four options: 'No policy', 'Policy from a local file', 'Policy from a remote location', and 'Policy from another domain'. The 'Policy from another domain' option is highlighted. At the bottom of the dialog box are three buttons: 'Previous', 'Next', and 'Cancel'.

Appliance	Policy
itso-xi52	None

Deployment policy option:

Figure 5-50 Selecting the type of deployment policy to use

3. Complete the following additional fields, which become available depending on the selection you made in step 2 on page 122:

No policy No additional input is required. Go to step 5 on page 125.

Policy from a local file

Select a file from your local machine by using the file browsing tool, and then, go to step 4 on page 125.

Policy from a remote location

Enter the URL for the remote deployment policy file, and then, go to step 4 on page 125.

Policy from another domain

Select the source WebSphere DataPower Appliance and domain. Enter the name of the deployment policy object to use.

Figure 5-51 shows an example of using a policy from another domain. After you select a WebSphere DataPower Appliance and application domain and enter the name of a deployment policy object, go to step 5 on page 125.

Create Domain

Specify a deployment policy (optional):

In the following table, you can select one or more domains and then specify a deployment policy.

Appliance	Policy
its0-xi52	None

Deployment policy option: Policy from another domain

* Specify the appliance: its0-xi52

* Specify the domain: test

* Specify the policy name: filtering-policy

ApplyCancel

PreviousNextCancel

Figure 5-51 Selecting to use a deployment policy from another domain

- Specify the name of the application domain that contains the deployment policy to use and the name of the deployment policy object in the appropriate fields.

Figure 5-52 shows an example of using a deployment policy from a local file. The file that is used is a domain configuration export from a domain named *development*.

Create Domain

Specify a deployment policy (optional):

In the following table, you can select one or more domains and then specify a deployment policy.

Appliance	Policy
its0-xi52	None

Deployment policy option: Policy from a local file

Specify the file: developmentExport.zip Browse

* Specify the name of the domain that contains the policy: development

* Specify the policy name: modifying-policy

Apply Cancel

Previous Next Cancel

Figure 5-52 Using a deployment policy from a domain configuration export

- Click **Apply** to save your changes.
- Repeat steps 1 on page 122 to step 5 for any additional domains or services.
- Click **Next** to continue with the remainder of the configuration deployment action.

The domain or service is created or updated by using the configuration file that is provided and by applying the deployment policy specified.

5.4 Automatic synchronization of a configuration

When you create or update application domains, the final step of the configuration process in WebSphere Appliance Management Center is to enable automatic synchronization (Figure 5-53 on page 126). This section describes the automatic synchronization feature. It includes usage scenarios and provides information about considerations before you enable automatic synchronization.

Automatic synchronization causes WebSphere Appliance Management Center to periodically check the configuration source of a domain for changes. When changes are detected in the source configuration or in the source deployment policy that is used in the deployment, WebSphere Appliance Management Center automatically updates the domain with the new configuration.

Create Domain

Future domain synchronization:

You are about to create a new domain.

Do you want WebSphere Appliance Management Center to automatically synchronize the domain with any changes detected in the configuration source files or deployment policy files?

If so, select **Enable automatic synchronization**.

☐ Enable automatic synchronization

Figure 5-53 Enabling automatic synchronization as part of domain creation

Automatic synchronization is intended for use when the source of configuration or deployment policy for a domain is a remote location or another domain on another WebSphere DataPower Appliance. Automatic synchronization does nothing when you use configuration from local files.

5.4.1 Understanding the behavior of automatic synchronization

Automatic synchronization entails the following tasks:

- ▶ Triggering a check of the source configuration
- ▶ Checking whether the source configuration changed
- ▶ Updating the configuration of the domain

Triggering a check of the source configuration

Several conditions, such as the following conditions, cause the automatic synchronization to be triggered:

- ▶ At startup of WebSphere Appliance Management Center. When WebSphere Appliance Management Center is started, assume that domains might change when the server is offline. Automatic synchronization is triggered to ensure that any changes are detected.
- ▶ Upon notification from the WebSphere DataPower Appliance. WebSphere Appliance Management Center registers with the managed WebSphere DataPower Appliances listening for, among other things, changes to domain configuration.
- ▶ On a timed schedule. Periodically, WebSphere Appliance Management Center checks the configuration source files for changes.
- ▶ When a configuration source location changes.
- ▶ When enabling automatic synchronization. If automatic synchronization is enabled for a domain where it was previously disabled, the automatic synchronization logic is triggered.

Checking whether the source configuration changed

After the automatic synchronization is triggered, WebSphere Appliance Management Center determines whether a change was made to the source configuration. That is, it determines whether the source configuration is the same as the deployed configuration or whether the source configuration changed. If a change is detected, the deployed configuration is updated with the latest configuration from the source location.

The source configuration or the deployment policy that is used is considered to be changed if any of the following circumstances is true:

- ▶ The configuration of the domain on the WebSphere DataPower Appliance no longer matches the configuration of the source.
- ▶ The timestamp of the configuration source or deployment policy changed since the last deployment.
- ▶ The WebSphere DataPower Appliance reports that the configuration source changed, which can happen when the configuration source is defined as another domain on another appliance.
- ▶ The last attempt to automatically synchronize the configuration failed.

Updating the configuration of the domain

If the deployed configuration is determined to be different than the source configuration (or if the last deployment failed), an update action is started. The target domain is quiesced, the updated configuration is deployed, and the domain is unquiesced again.

5.4.2 Considering the impact of automatic synchronization

Before you enable automatic synchronization, carefully consider whether the automatic synchronization feature is applicable to the environment that you are enabling it for. As explained in 5.4.1, “Understanding the behavior of automatic synchronization” on page 126, automatic synchronization causes domains to be quiesced as part of the deployment of an updated configuration. This deployment is triggered by any one of several possible events that might be outside of your control.

Figure 5-54 shows an example of the process that happens when automatic synchronization is enabled. The test-domain is configured to take its configuration from the dev-domain. The test-domain is initially unquiesced and report as *Up* in WebSphere Appliance Management Center, which shows a green arrow as its status.

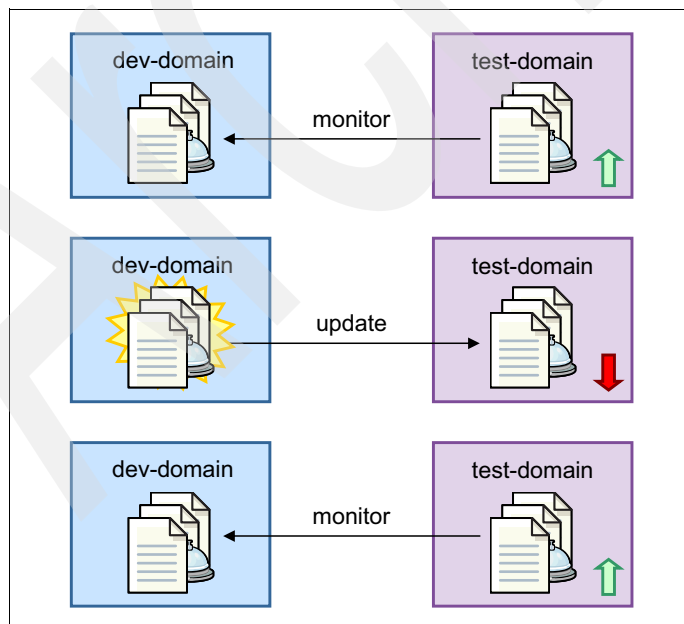


Figure 5-54 Automatic synchronization process

WebSphere Appliance Management Center periodically checks the configuration of the dev-domain. A developer makes a change in the dev-domain as part of developing the next version of their application, which causes WebSphere Appliance Management Center to quiesce the test-domain. The updated configuration is deployed from the dev-domain to the test-domain. After the update complete, the test-domain is unquiesced again, and WebSphere Appliance Management Center returns to periodically checking the dev-domain for configuration updates.

While the test-domain was quiesced, all automated tests that were running at the time failed. The developer had no idea that a change made to the domain might affect anyone else. As explained in 5.1.1, “Application domains” on page 86, application domains can be used as private workspaces that are isolated from all other application domains on the same appliance. Deploying the configuration from the dev-domain to the test-domain by using the option to take the configuration directly from the domain is acceptable by itself. However, the solution deployer who is in charge of looking after the configuration of the test-domain must decide when to update the configuration.

By enabling automatic synchronization, the decision of when to update the configuration is taken away from the solution deployer. Any of the trigger conditions that are listed in 5.4.1, “Understanding the behavior of automatic synchronization” on page 126, can cause the current configuration of the test-domain to be replaced with the configuration of the dev-domain. Always update the application domain configuration in a controlled manner. Include planned downtime so that the domain to be updated can be quiesced. Communicate the downtime to all affected parties so that they are aware that the domain will be unavailable during the update. Automatic synchronization removes the ability of the solution deployer to decide when the configuration update happens.

In this example, automatic synchronization was not a good choice because it took the control for the promotion of domain configuration away from the solution deployer from the test team.

However, in other situations, automatic synchronization is helpful. Consider an environment where several WebSphere DataPower Appliances are configured so that each appliance has an identical domain. For example, the WebSphere DataPower Appliances might be part of a load balancer. When changes are made to one master domain, the configuration for the other domains can be updated automatically. This approach might require rigorous testing before the initial deployment, by using a test WebSphere DataPower Appliance that is not part of the load balancer setup.

This solution must consider the fact that the domains that are configured to take their configuration from the master domain will be quiesced and updated at a time that is not controlled by the solution deployer. If preferred, the solution deployer can maintain control over the deployment schedule by updating multiple domains in a single action. The solution deployer selects the domains within WebSphere Appliance Management Center and clicks **Other actions** → **Update domain configuration**.

5.4.3 Toggling automatic synchronization for existing domains

To enable or disable automatic synchronization for an existing domain at any time:

1. Log in to WebSphere Appliance Management Center as a user with the solution deployer role.
2. On the **Domains** tab, select the domain that you want to modify.

3. In the Properties panel (Figure 5-55), click the **Edit Properties** icon.

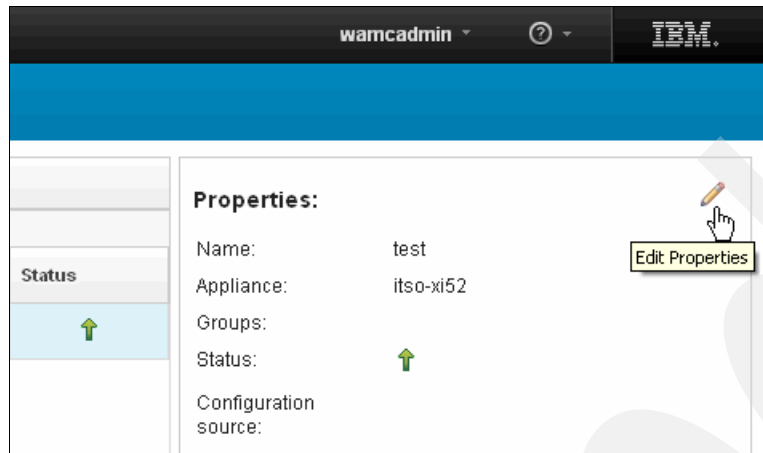


Figure 5-55 The Edit Properties icon on the Domains tab

4. In the Edit Domain window (Figure 5-56), toggle the **Enable automatic synchronization** check box to enable or disable automatic synchronization as required. Click **Save**.

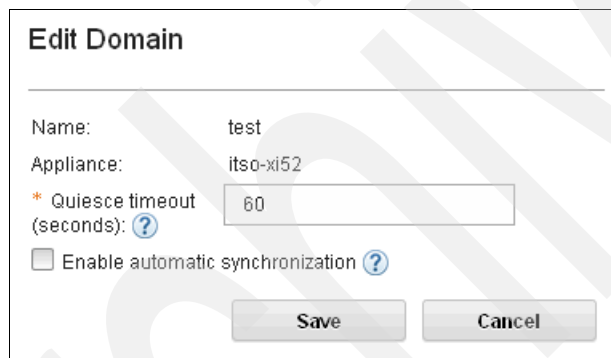


Figure 5-56 Edit Domain window

If you just enabled automatic synchronization for the domain, a check of the source configuration is started as explained in 5.4.1, “Understanding the behavior of automatic synchronization” on page 126.

Archived

Managing the software development lifecycle

When you develop software applications, it is typical to work through a software development lifecycle where code is initially written, tested, and finally deployed into production. When applications use IBM WebSphere DataPower Appliances and services, the configuration objects and services that support applications must also follow the software development process.

This chapter addresses the software development lifecycle and how IBM WebSphere Appliance Management Center can be used to support it. It includes the following sections:

- ▶ The software development lifecycle
- ▶ The development environment
- ▶ Deployment models
- ▶ Promoting configuration

6.1 The software development lifecycle

The general concept behind the software development lifecycle is familiar to most software developers. Any well-managed software project follows a process that sees the product first being scoped with requirements that are being gathered. After the requirements are well-defined and confirmed, development of the product code usually follows. Testing of the product comes next, and after testing completes, the product enters general availability. The development process that you use, whether an older sequential style (such as waterfall) or a newer iterative process (such as agile), is irrelevant in terms of the content in this chapter. The basic idea of a development phase, followed by testing, followed by production, is explored in this chapter.

Applications that use WebSphere DataPower Appliances are typically developed by using a standard software development process. Application code passes from development to test and eventually enters production. The WebSphere DataPower services that an application requires to run correctly must also progress through the same stages of the development lifecycle. For example, an application that is in development uses a Web Service Proxy on a WebSphere DataPower Appliance. The configuration that defines this Web Service Proxy is part of the deliverable that developers send to testers so that they can verify the correct behavior of the application.

For more information about the software development lifecycle and WebSphere DataPower Appliances, see “Development lifecycle” in *DataPower SOA Appliance Administration, Deployment, and Best Practices*, SG24-7901.

6.2 A lifecycle scenario

To help you understand concepts that are described in this chapter, we refer to the scenario of a fictional telecommunications company called *Redbooks Telecoms* that was introduced in 1.6, “A usage scenario” on page 8. This company is creating a customer-facing web service that visitors can use to query information about telephone numbers. This service is made available at no charge to any visitor. As a result, the company wants to restrict access to the service to prevent automated queries from flooding the system. To enable this restricted access, the developers determine that they need to use a Web Service Proxy by using service-level monitoring. The Web Service Proxy is called `telephone-query-wsproxy`.

Redbooks Telecoms owns the following WebSphere DataPower XI52 Appliances:

- ▶ `itso-xi52`
- ▶ `itso-xi52-a`
- ▶ `itso-xi52-b`

The IT operations team for the WebSphere DataPower Appliances uses WebSphere Appliance Management Center to manage these appliances. The WebSphere Appliance Management Center installation is configured with user accounts given appropriate user roles. For more information about users and user roles, see 2.4, “Managing users and roles” on page 32.

6.3 The development environment

To support the software development lifecycle, the development environment must be partitioned so that development resources can be kept separate from test resources, which in turn, are isolated from the production environment. This way, developers can continue to develop new code, and testers can test the latest packaged version of the code. You can achieve this separation of environments by using either of the following basic methods:

- ▶ Partition the environment by using application domains on a single WebSphere DataPower Appliance as shown in Figure 6-1

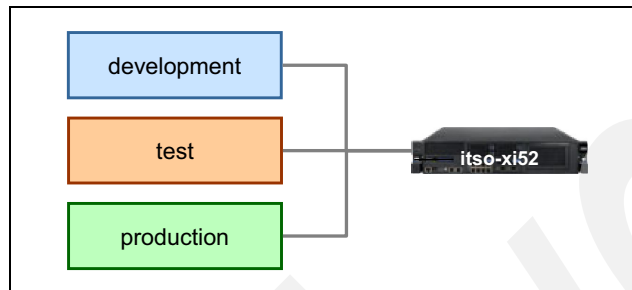


Figure 6-1 Partitioning the environment by using application domains

- ▶ Partition the environment by using separate WebSphere DataPower Appliances as shown in Figure 6-2

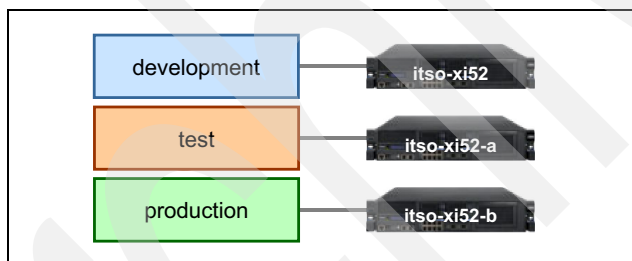


Figure 6-2 Partitioning the environment by using multiple WebSphere DataPower Appliances

6.3.1 Single WebSphere DataPower Appliance

As explained in 5.1.1, “Application domains” on page 86, application domains are an effective way to separate workspace areas and to restrict access to particular users. Redbooks Telecoms can use the `itso-xi52` appliance to create three application domains, called *development*, *test*, and *production*. As development of the application proceeds, the configuration for the `telephone-query-wsproxy` service is migrated or promoted through each of the three domains.

A clear benefit of this configuration is that it requires only one WebSphere DataPower Appliance, which simplifies the amount of setup that required for system configuration. This approach also potentially makes the promotion step easier because host names, IP addresses, and other basic configuration settings for the `telephone-query-wsproxy` service might not need to be changed.

A drawback to this method is that each of the application domains is not isolated from the other domains. All three domains rely on the same shared configuration from the system environment, which has the configuration settings in the *default domain*. Further, if the WebSphere DataPower Appliance must be rebooted, all three domains are unavailable for the duration.

In some situations, the testers might want to test a new firmware version but the production application needs to continue to use the current version. They cannot isolate the *test domain* from the *production domain* if both domains are on the same WebSphere DataPower Appliance. Considering the impact on production-level applications, this method of partitioning the environment is not suitable in many situations.

6.3.2 Multiple WebSphere DataPower Appliances

Alternatively, Redbooks Telecoms can assign one WebSphere DataPower Appliance to each of the software development lifecycle stages:

- ▶ itso-xi52 for development
- ▶ itso-xi52-a for test
- ▶ itso-xi52-b for production

By using this method, all of the environments are isolated from one another. Firmware levels can be updated without affecting any of the other environments. Changes that are made to the *default domain* or to the WebSphere DataPower Appliances themselves do not affect any of the other WebSphere DataPower Appliances. This method is important for the production environment when a change made to help development or test can easily bring production services offline. Isolating each environment on separate WebSphere DataPower Appliances greatly reduces the chances of this happening.

Further, firmware can be upgraded on any of the WebSphere DataPower Appliances independently of the others. The performance of the production WebSphere DataPower Appliance does not depend on the traffic being generated by the test team. Also, the operating environment as a whole is more flexible. For these reasons, separate the development, test, and production domains across multiple WebSphere DataPower Appliances.

Whether the environment is partitioned by using application domains on a single WebSphere DataPower Appliance or across multiple appliances, you can use WebSphere Appliance Management Center as the mechanism for promoting environment configuration. To learn how, see 6.5, “Promoting configuration” on page 142. However, first consider the potential models of deployment and weigh the benefits and drawbacks of each one as explained in the next section.

6.4 Deployment models

When you promote a domain and service configuration through the development environment, consider the scope of the configuration that is being deployed. One aspect is how to partition the development environment. Also consider how to handle the deployment of configuration changes when you promote a domain and service configuration through the development environment.

For example, when developers for Redbooks Telecoms create their domain configuration export to send to the test team, should they export all of the domain configuration or only the telephone-query-wsproxy service and the files that it requires? When the test team uses the configuration export file, should they use it to update the configuration of an existing domain or create a domain from it? Similar considerations apply to the final promotion of the service into the production environment. This section highlights these issues and benefits and drawbacks of the various methods.

6.4.1 Defining the scope of exported configuration

A key consideration when you develop deployment practices is the scope of the deployment configuration. The configuration is promoted through the development, test, and production environments, but at what level do you define the configuration export? You can choose from the following possibilities:

- Work with a configuration for a domain
- Work with a configuration for a service or group of services

Each of possibility has benefits and drawbacks that you must consider carefully before you decide which best suits your needs.

Configuration of domain

Suppose that Redbooks Telecoms decides that the configuration will be promoted from the development environment to the test environment at the level of the domain. The development team creates a domain configuration export or domain configuration backup for the domain that it is developing in. The configuration export includes all of the content of the domain, including all its configuration objects, all of its services, and all files. The whole package is sent to the test team to deploy the package into the test environment. The test team can, therefore, be sure that it is testing the exact configuration that the development team created.

When the code is promoted from test to production, the same configuration is promoted. This approach gives a high level of confidence that the configuration that is in production is the same configuration that was tested and, therefore, should behave as expected.

Figure 6-3 illustrates the export of a whole domain configuration, including the service configuration for telephone-query-wsproxy, and using the exported configuration to deploy to a test environment. As described in 6.3, “The development environment” on page 133, the domains can be on the same WebSphere DataPower Appliance or on separate WebSphere DataPower Appliances.

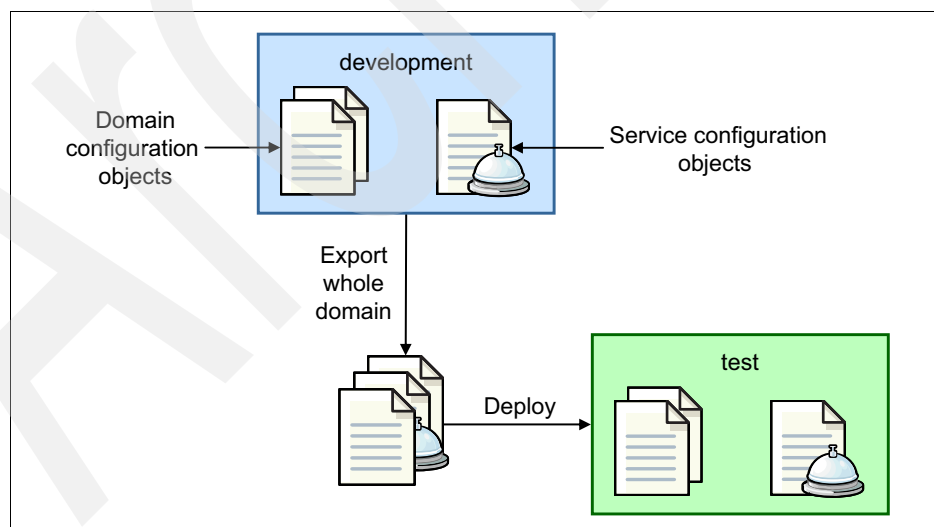


Figure 6-3 Exporting a configuration that includes all configuration objects from the domain

Configuration of a service or group of services

Alternatively, the Redbooks Telecoms team can decide to export configuration at the service level. The developers again create a configuration export file, but this file contains none of the configuration of the development domain. Instead, the file contains only the

telephone-query-wsproxy service and any objects and files that the service requires to function correctly. This way, the test team can deploy the service into an existing domain potentially to test how the service integrates with existing services.

Updating the configuration at the service level also allows for small, incremental updates to be applied to the service without redeploying the entire domain. However, this approach has the risk that you might update shared objects and end up with a service configuration in production that is not tested. Figure 6-4 shows the process of exporting a configuration for the telephone-query-wsproxy service, leaving behind the rest of the configuration for the development domain.

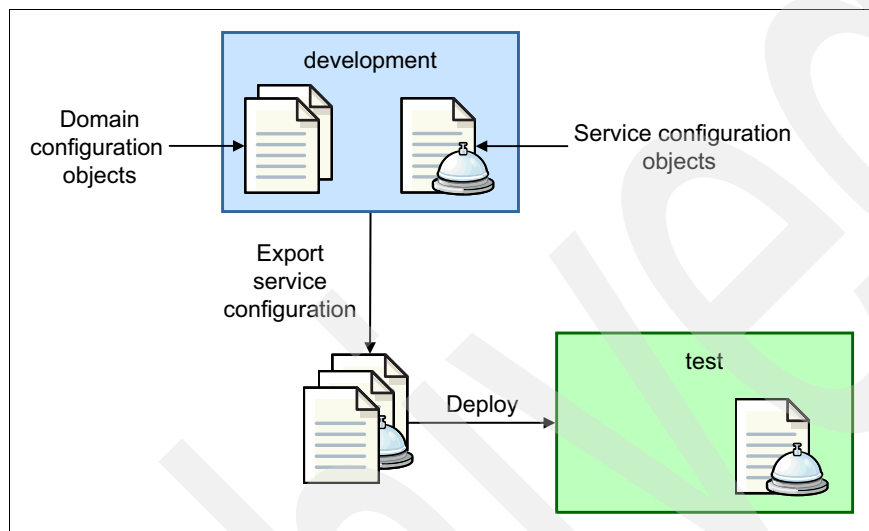


Figure 6-4 Exporting configuration for a service, leaving behind the rest of the domain configuration

As described in 5.1, “Managing application domains” on page 86, and 5.2, “Managing services” on page 102, WebSphere Appliance Management Center provides methods for working with configuration exports at the domain and service levels. The choice of which method to use depends on how you will handle the deployment of the configuration.

6.4.2 Selecting a deployment process

Another important aspect of environment promotion is how you will use the exported configuration files. You can follow several different processes. The choice is potentially limited depending on the decisions that you make when you define the scope of the configuration export. Equally, the choice of deployment process can influence the choice of scope that is used for the configuration export.

This section considers the following possible deployment processes:

- ▶ Deployment of a domain configuration export
All future updates are done at the domain level.
- ▶ Deployment of a domain configuration export with updates to services that use service configuration exports
- ▶ Deployment of an empty or preinitialized domain into which service configuration exports are deployed

Now it becomes clear why the choice of scope affects the choice of process to follow and vice versa. For example, if you do not intend to perform updates to individual services and will work only with domain configuration exports, the deploying a domain configuration export is suitable.

However, you might want to deploy an initial domain configuration file and thereafter make service level updates. In this case, you need to define a process that allows the scope of configuration objects to be both at the domain level and at the individual service level.

Deployment of a domain configuration export

The first deployment model is to always work with full domain configuration exports. Referring to the Redbooks Telecoms example, the development team must always export the entire *development domain* and never export the *telephone-query-wsproxy service* as a stand-alone unit. The test team must always work with a complete domain export and so that it can have increased confidence that the team is testing the configuration as it was developed.

After the test team completes its testing activity, the whole domain configuration can be exported again and is ready for promotion into the production environment. Now, the domain configuration that enters production is the whole unit that was tested, giving confidence that the configuration will work correctly.

Figure 6-5 shows an example of this process. The first configuration export contains the configuration for the whole domain. During the test process, a defect is found. The defect is fixed, and an updated domain configuration export is sent to the test team.

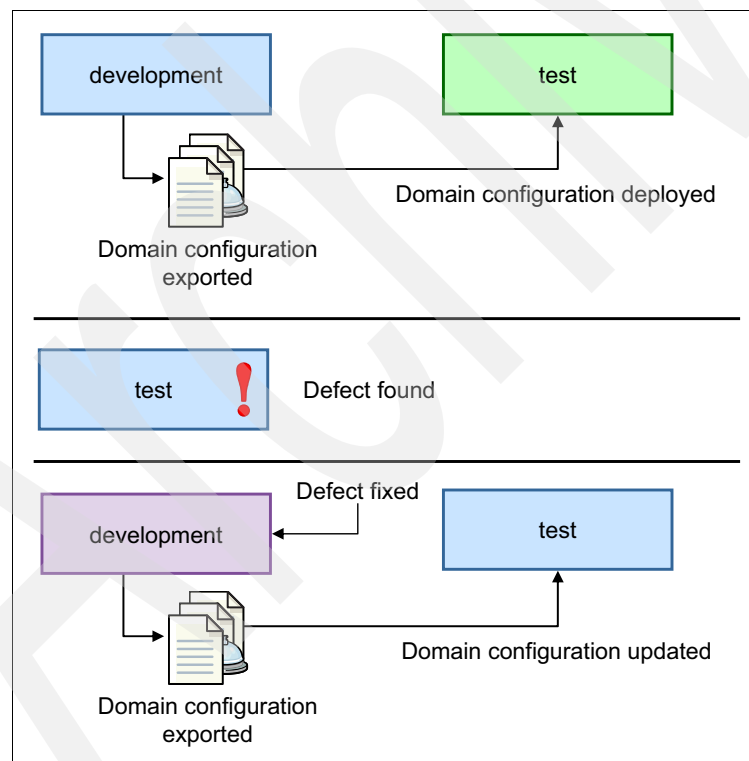


Figure 6-5 Development process with configuration always taken at the domain level

Deployment of domain configuration export with service level updates

An alternative deployment model is to take the initial configuration from a domain level export, but for subsequent updates to be made at the service level. By using this model, the developers at Redbooks Telecoms complete development of their new service and produce a

domain configuration export as before. The package is sent to the test team and deployed to the team's environment.

After some testing is completed, the test team finds an issue and raises a bug with the developers. The developers fix the bug and now need to send an updated configuration to the testers. Rather than send the whole domain configuration, the developers export the configuration for the telephone-query-wsproxy service. The testers apply this configuration update directly to the service. Figure 6-6 shows this process.

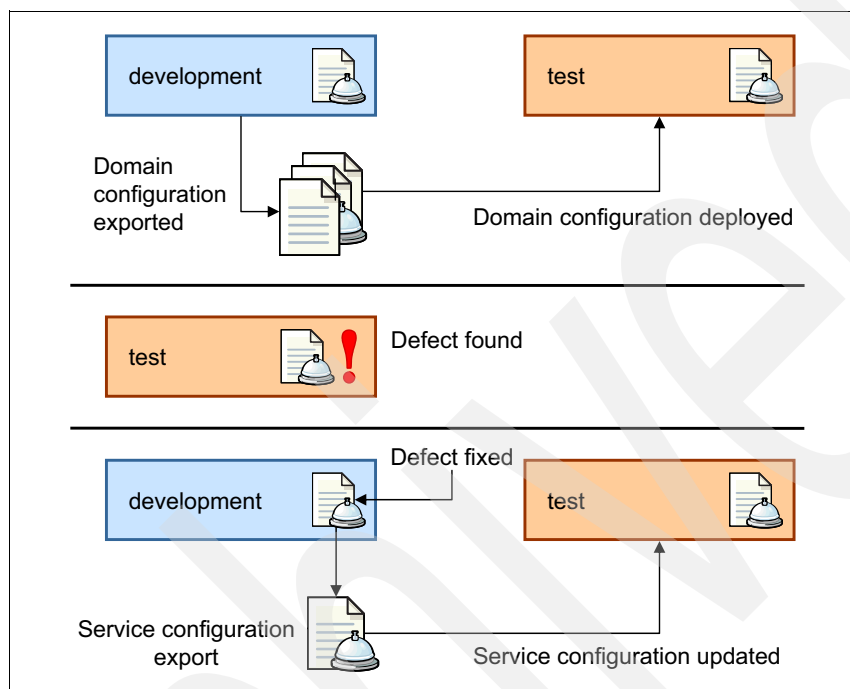


Figure 6-6 Initial configuration that is exported at the domain level and updates at the service level

Deployment of a base domain configuration with service level deployments

Another possibility is to opt for a deployment model where a domain configuration export is created that represents the base configuration for any domain in an organization. For example, Redbooks Telecoms defines a base configuration for all of their domains on all of its WebSphere DataPower Appliances. This base configuration defines logging targets, XML managers, host aliases, and other configuration settings. The base configuration contains no services. When the developers initially start development of the new service, they create a domain by using this base configuration export. They develop services in the domain and, when development is complete, they export the service configuration to a file.

The test team also creates an initialized domain with no services by using the same base configuration export. The team then deploys the service configuration that is provided to it by the developers into this new domain. The same procedure is used when the configuration moves to production.

Figure 6-7 shows a development process where configuration exports are always created at the service level.

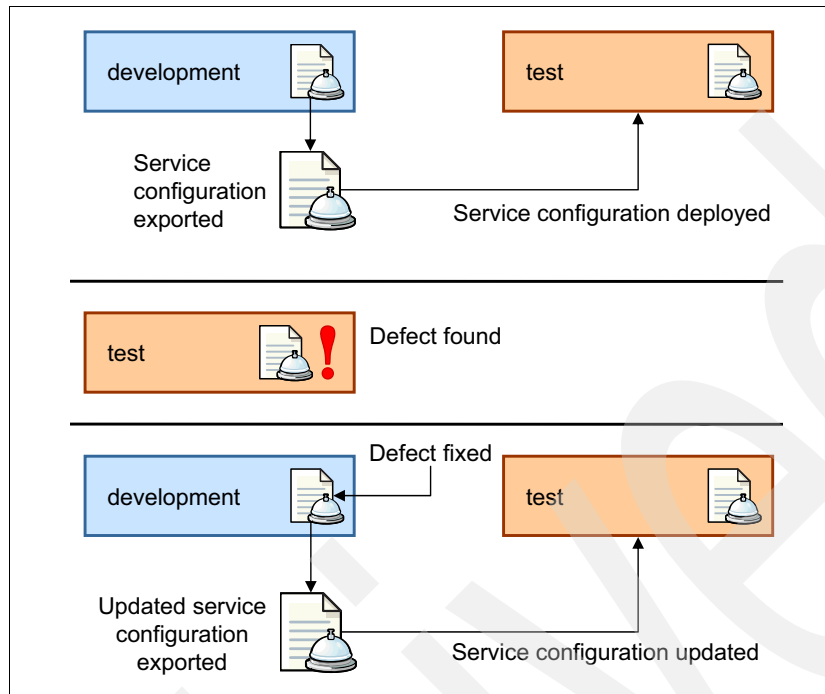


Figure 6-7 Development process with configuration exports always taken at the service level

6.4.3 Updating existing configuration

Another aspect of configuration deployment to consider is whether to deploy updates to existing domains or to start each time with an empty domain. Each approach has advantages, and neither is inherently wrong. For more information about this topic that is not covered in this book, see Chapter 9 in *DataPower SOA Appliance Administration, Deployment, and Best Practices*, SG24-7901. The following summary highlights the main points:

- ▶ Starting with an empty domain ensures that only exported configuration objects are used. No residual objects from previous deployments can contaminate the environment.
- ▶ Deleting or resetting a domain before deployment introduces extra complexity into the deployment process.
- ▶ Some assets are domain-specific and are not included in the configuration export file, such as the public and private key files.
- ▶ There might be substantial differences between the existing domain configuration and the new configuration. In such cases, you might want to start from a new domain.
- ▶ Deploying a new configuration into an existing domain is not as risky as it might seem. Orphaned configuration objects have no effect on the rest of the configuration if the new configuration does not overlap with the configuration that is already in place.

6.4.4 Evaluating the approaches

The combinations of the configuration scope and deployment process has the following benefits and drawbacks:

- Only exporting configuration at the domain level
 - Deployment at the domain level

As shown in Figure 6-8, configuration is always exported at the domain level and is, therefore, always deployed at the domain level.

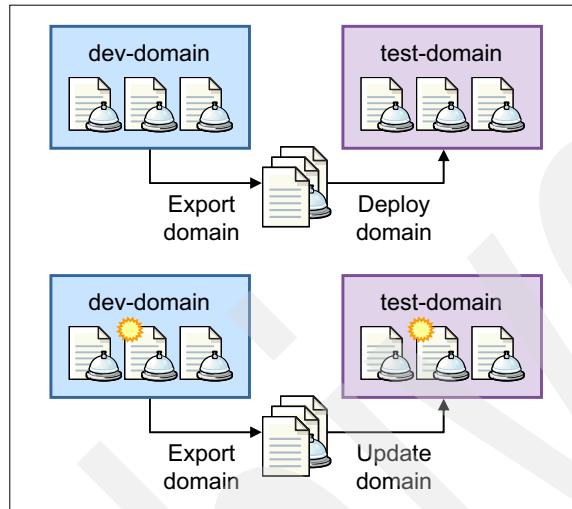


Figure 6-8 Deployment is at the domain level only

The major benefit of this method is that the test team uses an identical configuration as the development team. The configuration that is eventually promoted is a well-defined, well-tested single unit that is confirmed to work correctly.

The biggest drawback of this method is that minor updates at the service level cannot be made. Making an update to a service requires deploying a new configuration to the whole domain. In a production environment, all of the services in that domain become unavailable on that WebSphere DataPower Appliance when the update occurs. This issue is less if the configuration is deployed over the top of an existing domain (domain configuration update). If you deploy into a clean domain each time, more work is required to quiesce traffic and to delete the existing domain.

- Deployment at the service level is not used because the domain configuration is always the scope of the export.
- Combination of exporting configuration at the domain and service level
 - Initial deployment at domain level with subsequent updates at the service level

As shown in Figure 6-9 on page 141, the first configuration export is taken at the domain level. When changes to the services in the domain become necessary, further configuration exports are done at the service level.

The major benefit with this method is that updating the configuration in the target domain affects individual services. The target domain does not need to be quiesced, and other traffic can flow through the domain as normal. The affected service or services are quiesced but is preferable only when the entire domain is unavailable.

The limited scope of this deployment can be an issue. Because only service-level configuration exports are made, changes to the domain configuration cannot be made.

Also, for larger updates that involve multiple services, the extra time of applying updates one service at a time becomes costly.

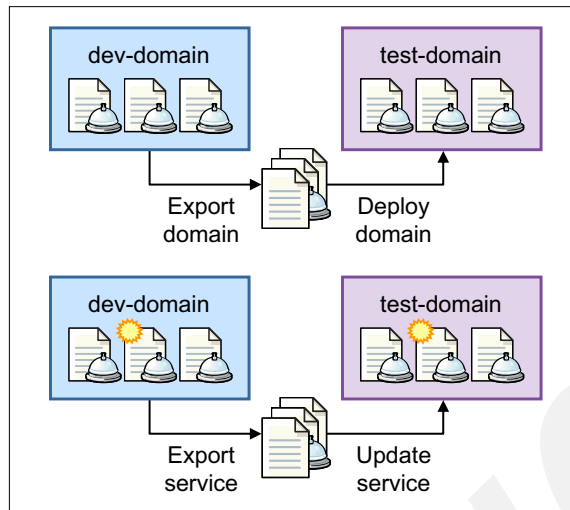


Figure 6-9 Initial deployment at the domain level with subsequent updates at service level

- Initial deployment at the domain level, with small updates made to individual services and larger, less frequent updates that are made at the domain level

The first configuration export is taken at the domain level. Small changes to individual services are made at the service level. If bigger changes are required, a new domain configuration is taken and used for the deployment.

This approach removes the major drawback that is described for the previous method. If multiple services change, a configuration export is made at the domain level, and a single update action is carried out in WebSphere Appliance Management Center at the domain level. This approach negates the benefit of the previous approach in that the target domain must be quiesced, and traffic through the whole domain is suspended.

- Initial deployment of a base domain configuration with an exported configuration at the service level that are deployed to the domain

A base configuration is defined that constitutes the base configuration for all domains across all WebSphere DataPower Appliances. The base configuration is used as the starting point for any newly created domains. Application development takes place in a domain that is created this way. Configuration export is at the service level. Both initial deployment and future updates of services are done at the service level.

This approach is ideal if you have a reasonable amount of base domain configuration that is common to all or most domains in your organization. After the base domain configuration is established, create a configuration export for the whole domain, and use it whenever you create a domain.

As with the other approaches that involve service-level deployment, updating multiple services is done at the extra overhead of updating them one by one.

The flexibility of WebSphere Appliance Management Center allows the usage of any of these approaches. Other approaches that are based on the methods that are presented are equally valid. The key idea is that WebSphere Appliance Management Center allows for updates to be applied either at the domain level or service level. If you combine the possible approaches, you must consider their benefits and drawbacks.

6.5 Promoting configuration

You can choose from two methods to partition the software development lifecycle environment (see 6.2, “A lifecycle scenario” on page 132):

- ▶ One WebSphere DataPower Appliance with development, test, and possibly production domains.
- ▶ Three WebSphere DataPower Appliances, one each for development, test, and production environments.

Configuration exports can have the following scopes (see 6.4.1, “Defining the scope of exported configuration” on page 135):

- ▶ Configuration exported at the domain level
- ▶ Configuration exported at the service level

You can follow the different deployment processes (see 6.4.2, “Selecting a deployment process” on page 136):

- ▶ Deployment always at the domain level
- ▶ Initial deployment at the domain level with updates made at the service level
- ▶ Deployment of a base domain configuration into which services are added

WebSphere Appliance Management Center supports any combination of all of these processes. This section describes some of these processes and how you can realize them by using WebSphere Appliance Management Center.

Further information: The scenarios that are described in this chapter give a basic outline of the procedures that you can follow. For more information about creating and updating domains and services, see Chapter 5, “Managing domains and services” on page 85.

6.5.1 Promoting configuration through a single WebSphere DataPower Appliance

Redbooks Telecoms initially chose to use a single WebSphere DataPower Appliance that is partitioned into three application domains. By using its `itso-xi52` WebSphere DataPower Appliance, the company creates a *development domain* for the developers to work in.

After some time, the Redbooks Telecoms developers complete the initial development of the telephone query application and are ready to send the application to the test team. Along with the built version of the application, the developers send a domain configuration export file for the whole domain. For information about how the developers create a domain configuration export file, see 5.1.3, “Creating domain configuration files” on page 87.

Deploying the configuration to a new domain

The developers send the domain configuration export file to the test team. To create a *test domain*, the test team completes the following steps:

1. Log in to WebSphere Appliance Management Center as a user with the solution deployer role.
2. Check that the `itso-xi52` WebSphere DataPower Appliance is listed in the WebSphere DataPower Appliance table. Click the appliance to select it.

3. Select **Other Actions** → **Create Domain** (Figure 6-10).

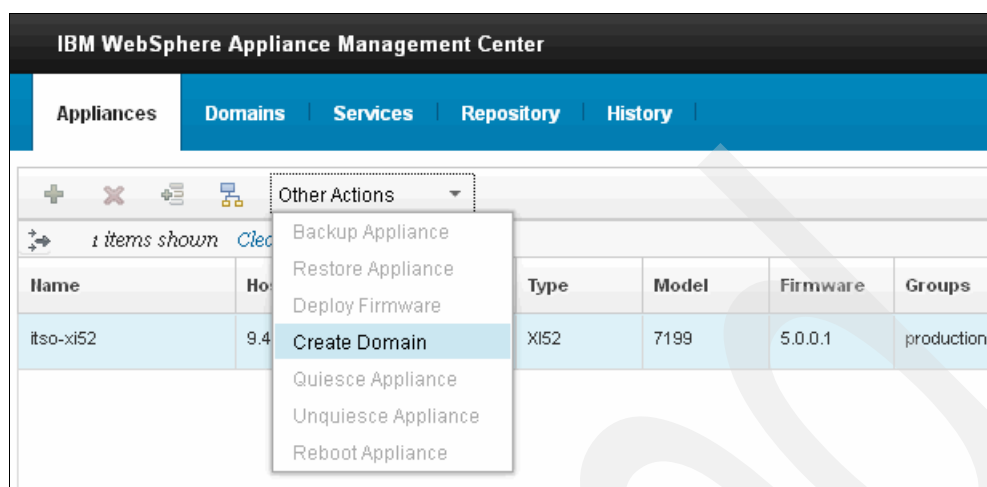


Figure 6-10 Selecting the Create Domain option for the itso-xi52 WebSphere DataPower Appliance

4. In the Create Domain window, enter the name **test** for the domain. Click **Next**.
5. Select the source of the updated configuration as appropriate, such as **Local file**. Then, browse to the location of the configuration export file. Click **Next**.
6. Select a deployment policy to use during the deployment. For information about deployment policies, see 5.3, “Deployment policies” on page 113. In this example, no deployment policy is used. Click **Next**.
7. If required, select **Enable automatic synchronization**. In this scenario, this option is not appropriate. For information about enabling automatic synchronization, see 5.4, “Automatic synchronization of a configuration” on page 125.
8. Click **Finish**. The domain is updated with the information that was provided.

Deploying the configuration to an existing domain

The developers send the domain configuration export file to the test team. In this scenario, the test team already has a test domain that is created and is happy to overwrite the existing configuration with the contents of the domain configuration export. To deploy the configuration into its existing environment, the test team follows these steps:

1. Log in to WebSphere Appliance Management Center as a user with the solution deployer role.
2. Verify that the **itso-xi52** WebSphere DataPower Appliance is listed in the WebSphere DataPower Appliance table. Select the appliance, and click the **View Domains** icon from the toolbar to switch to a view of the existing domains on the WebSphere DataPower Appliance. See Figure 6-11 on page 144.

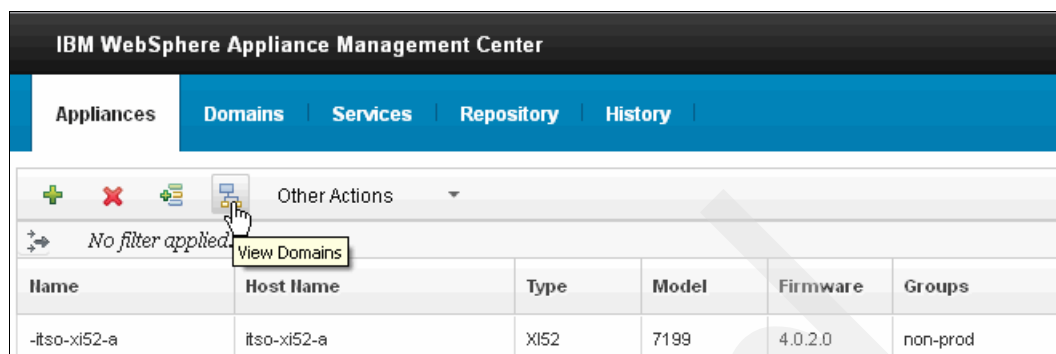


Figure 6-11 Clicking View Domains

3. Locate the **test** domain in the filtered list of domains and select it.
4. Before you apply updates to the domain, ensure that it is first quiesced. Click **Other Actions** → **Quiesce Domain** from the toolbar to quiesce the *test domain*. Figure 6-12 shows the quiesced domain in the domain table.

test	itso-xi52				
------	-----------	--	--	--	--

Figure 6-12 Table row that shows the test domain as quiesced

5. After the domain is quiesced, click **Other Actions** → **Update Domain Configuration**.
6. In the Update Domain Configuration window, select the source of the updated configuration as appropriate, such as **Local file**. Then, browse to the location of the configuration export file. Click **Next**.
7. Select a deployment policy to use during the deployment. For information about deployment policies, see 5.3, "Deployment policies" on page 113. Click **Next**.
8. If required, select **Enable automatic synchronization**. In this scenario, this option is not appropriate. For information about enabling automatic synchronization, see 5.4, "Automatic synchronization of a configuration" on page 125.
9. Click **Finish**. The domain is updated with the information that was provided.

Deploying to production

After all test activities are completed, the telephone query application can be promoted to the production environment. The `telephone-query-wsproxy` service is also promoted. A domain configuration export is taken, and the export file is sent to the team who deployed the code into the production environment. The process for promoting the configuration to the production environment is the same as for promoting from development to test and is as described earlier in this section.

Before you deploy the configuration into production, rigorously test it. After the configuration is exported from the test domain, check the contents of the configuration and validate them before deployment into the production domain.

6.5.2 Promoting configuration through multiple WebSphere DataPower Appliances

Rather than using a single WebSphere DataPower Appliance with separate domains for development, test, and production, Redbooks Telecoms switches to using multiple WebSphere DataPower Appliances. Each appliance is designated to one of the software lifecycle areas. The appliances are assigned in the following way:

- ▶ `itso-xi52` is used for development.
- ▶ `itso-xi52-a` is used for test.
- ▶ `itso-xi52-b` is used for production.

The Redbooks Telecoms developers work on the `itso-xi52` WebSphere DataPower Appliance in a domain that they created for the development of the telephone query application. They call this domain `telephone-query-application`. After some time, development of the application is completed, and the domain configuration is exported.

The test team now follows the same procedure as explained in 6.5.1, “Promoting configuration through a single WebSphere DataPower Appliance” on page 142. However, the team deploys the configuration file to the `itso-xi52-a` WebSphere DataPower Appliance by selecting it from the list of WebSphere DataPower Appliances in WebSphere Appliance Management Center. In this case, however, the test team is likely to use a deployment policy to modify the incoming configuration and make it suitable for the test WebSphere DataPower Appliance. For information about deployment policies and how they can be used in WebSphere Appliance Management Center, see 5.3, “Deployment policies” on page 113.

To promote the code from the test environment to the production environment, the same procedure is repeated once to test the application code and to ensure that the services are completed. The test team exports the domain configuration from the test domain on the `itso-xi52-a` WebSphere DataPower Appliance. The team sends the configuration export to the production deployment team. This team uses WebSphere Appliance Management Center to deploy the configuration to the `itso-xi52-b` production appliance.

Archived

Effective monitoring of WebSphere DataPower Appliances

The monitoring component of IBM WebSphere Appliance Management Center monitors the behavior and status of IBM WebSphere DataPower Appliances, provides useful performance metrics, and can be helpful when you are diagnosing a problem. This chapter explains how to install and use the monitoring component of WebSphere Appliance Management Center for WebSphere Appliances.

This chapter includes the following sections:

- ▶ Monitoring architecture
- ▶ Installing the monitoring component
- ▶ Adding WebSphere DataPower Appliances to ITCAM Agents
- ▶ Monitoring WebSphere DataPower Appliances

7.1 Monitoring architecture

The monitoring component of WebSphere Appliance Management Center includes IBM Tivoli Monitoring and IBM Tivoli Composite Application Manager (ITCAM) Agent for WebSphere DataPower Appliances. IBM Tivoli Monitoring consists of a Tivoli Enterprise Monitoring Server and a Tivoli Enterprise Portal Server. It can display information such as HTTP transaction rate, processor usage, and system load. One or more WebSphere DataPower Appliances can be monitored by an instance of the ITCAM Agent, which polls the WebSphere DataPower Appliance and forwards the data to a Tivoli Enterprise Monitoring Server host.

To allow for failover in an enterprise setting, multiple Tivoli Enterprise Monitoring Server hosts can exist, and each can connect to multiple ITCAM Agents. Tivoli Enterprise Portal Server then pulls data from Tivoli Enterprise Monitoring Server. All of these components can potentially be on different hosts.

Figure 7-1 illustrates the infrastructure that is used for the examples in this chapter. Two hosts are used in our example. One server is used to host Tivoli Enterprise Portal Server (TEPS), Tivoli Enterprise Monitoring Server (TEMS), and an instance of ITCAM Agent. Another server hosts its own instance of an ITCAM Agent, communicating with Tivoli Enterprise Monitoring Server on the first host. A local firewall has opened ports for this server alone. Therefore, it can communicate with a WebSphere DataPower Appliance outside the local area network (LAN).

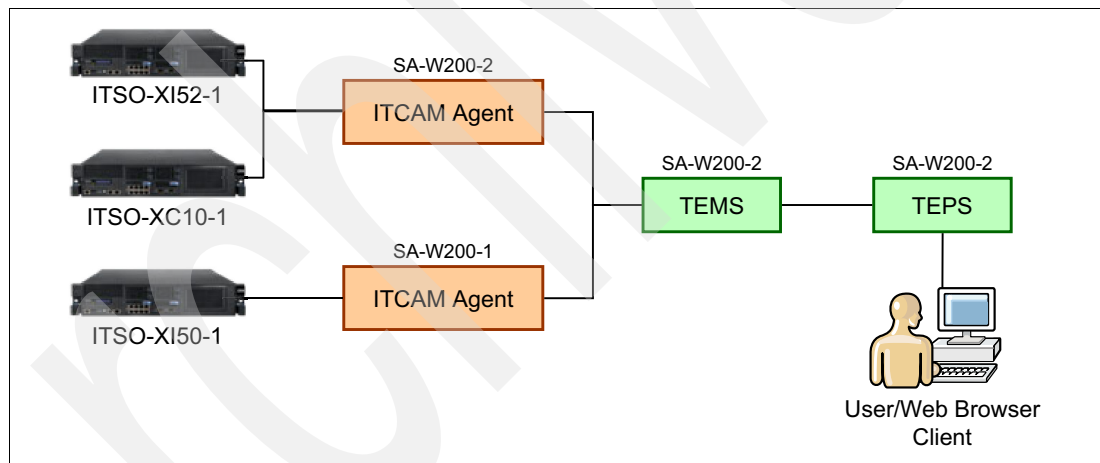


Figure 7-1 Monitoring infrastructure that is used in this chapter

First, you must install IBM Tivoli Monitoring. Then, you must install the ITCAM Agent and set it up for each WebSphere DataPower Appliance.

7.2 Installing the monitoring component

To install the monitoring component of the WebSphere Appliance Management Center, you can obtain the software from the WebSphere Appliance Management Center download site at:

<http://www.ibm.com/software/integration/wamc>

Tip: As with the management component, supported platforms include Windows Server 2008, Linux, and AIX (all 64-bit). In this chapter, only the Windows installation is considered.

This section describes the installation of the monitoring component on a Windows Server 2008 R2 machine. For installation on other platforms, see the *Installing the monitoring component* topic in the WebSphere Appliance Management Center Information Center:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/install_monitoring_component.html

The following versions of the software are used in this chapter:

- ▶ IBM Tivoli Monitoring V6.2.3 Fixpack 1 Base
- ▶ Tivoli Composite Application Manager Agent for WebSphere DataPower Appliance v7.1

Download and extract the monitoring component files to the location on the machine where you will install the monitoring components.

Integration with other Tivoli monitoring agents: The monitoring component that is provided with WebSphere Appliance Management Center is supported only for stand-alone use. It cannot be integrated with other Tivoli monitoring agents or with an existing IBM Tivoli Monitoring Infrastructure. Contact an IBM sales representative if you want to license ITCAM Agent for WebSphere DataPower Appliance for connecting to your enterprise monitoring infrastructure.

7.2.1 Installing IBM Tivoli Monitoring

To install IBM Tivoli Monitoring:

1. Open the directory that you extracted the monitoring component files into and run **setup.exe** in the WINDOWS directory.
2. When the InstallShield wizard opens, click **Next**.
3. Read and accept the license agreement, and click **Next**.
4. Choose a directory to install the files. By default, C:\IBM\ITM is used, but you can select any empty directory if the current Windows user has write privileges to it. Click **Next**.
5. Because Tivoli Enterprise Monitoring Server uses Secure Sockets Layer (SSL) to encrypt its connections, specify a 32-character key. Although you can accept the default of IBMTivoliMonitoringEncryptionKey, consider changing this setting to a random string that contains mixed-case alphanumeric characters. Click **Next**.
6. Select the check boxes to install **Tivoli Enterprise Monitoring Agents**, **Tivoli Enterprise Monitoring Server**, and **Tivoli Enterprise Portal Server** (Figure 7-2 on page 150). In this example, Tivoli Enterprise Portal Desktop Client is not select because the web browser interface is used.

If the component tree of Tivoli Enterprise Monitoring Server, for example, is expanded, agents, which are catalog files, are listed. They describe the data types that agents (such as the ITCAM Agent instances) will send back to Tivoli Enterprise Monitoring Server. The installation asserts that all components will be installed on the same host. However, at this stage, only one component can be installed on this host, with other components of IBM Tivoli Monitoring installed on other hosts.

IBM Eclipse Help Server is selected. You cannot clear it when installing Tivoli Enterprise Portal Server.

Click **Next**.

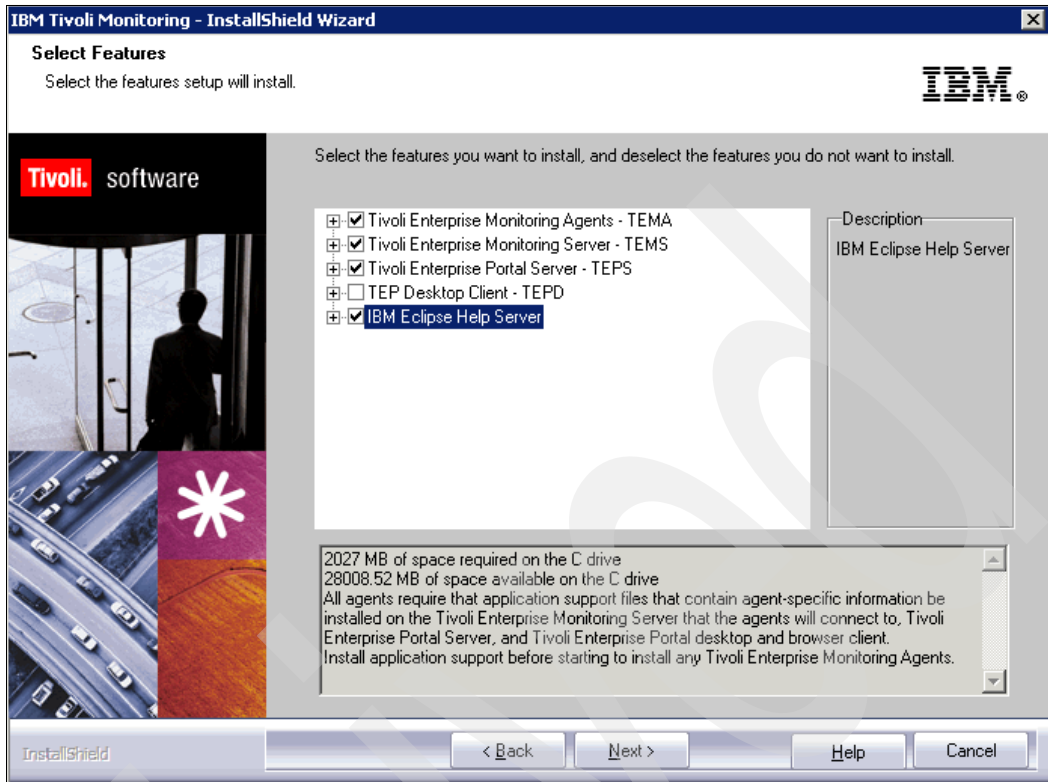


Figure 7-2 IBM Tivoli Monitoring installer page, showing selected components

7. Configure the remote agents. In a production deployment, these agents might be required to be separated from the Tivoli Enterprise Monitoring Server (for example, because of firewalls). These options add the agents into a repository so that many agents can be easily deployed. Tivoli Enterprise Monitoring Server automatically transfers and installs the agent files for each remote host. In this example, only the ITCAM Agent is of interest when monitoring WebSphere DataPower Appliances, which is a separate package. Therefore, leave all items cleared, and click **Next**.
8. Select the folder name (for opening the monitoring software from the **Start** menu) or accept the default value of IBM Tivoli Monitoring. Click **Next**.
9. For users of the Tivoli Enterprise Portal web browser client, enter a user name and password. On Windows, an operating system user is created with the predefined name of *sysadmin*. Therefore, the password must comply with the operating system password requirements.
If a user is already defined with a name of *sysadmin*, you are not prompted to enter a password. During installation, if the option to securely validate users is selected in step 17, the credentials are passed to the Tivoli Enterprise Monitoring Server and are validated.
Click **Next**.
10. In the summary page, click **Next** to install IBM Tivoli Monitoring.
11. After the installation is complete, configure the components of IBM Tivoli Monitoring. You can clear items to defer the configuration, but in this example, we configure the components now. Therefore, ensure that all items are selected, and click **Next**.

12. In the first configuration page, specify the host name of Tivoli Enterprise Portal Server. The host name of the server that is used in this example is SA-W200-2, as shown in Figure 7-3. Because Tivoli Enterprise Portal Server is installed on the same machine as Tivoli Enterprise Monitoring Server, the default value is appropriate.

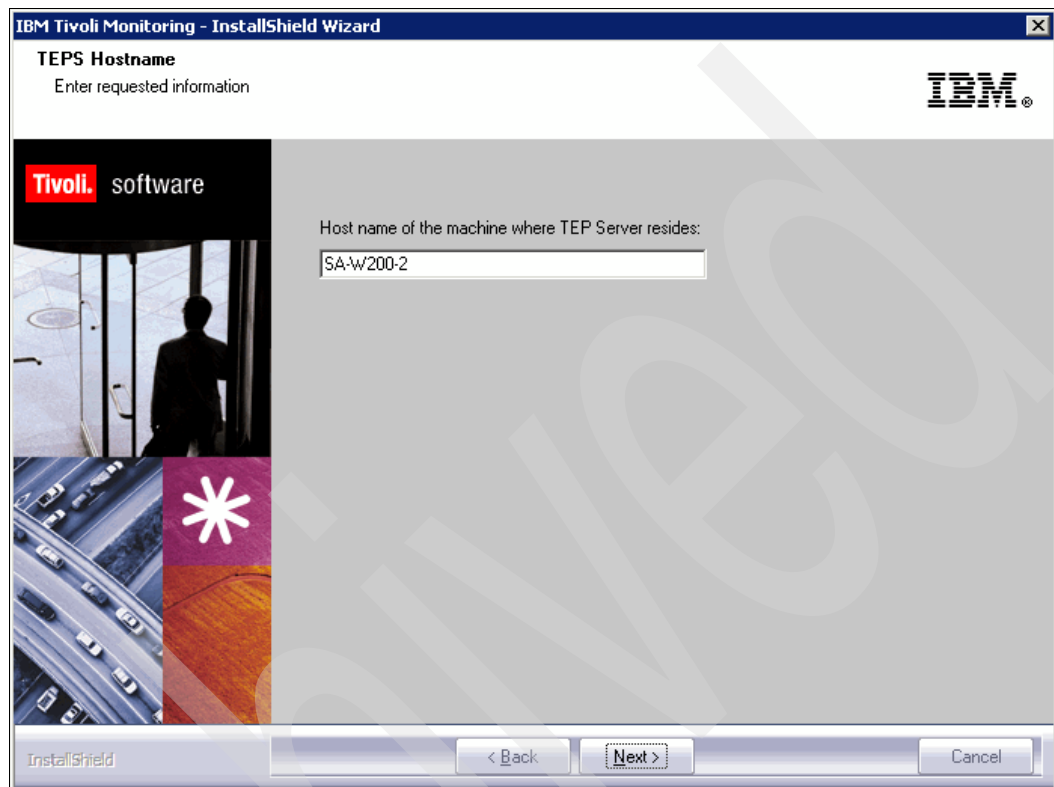


Figure 7-3 Specifying Tivoli Enterprise Portal Server host name

13. Specify the database type for Tivoli Enterprise Portal Server. IBM Tivoli Monitoring supports IBM DB2® and SQL Server, but because they are not installed, only the embedded database is available as shown in Figure 7-4. Click **OK**.

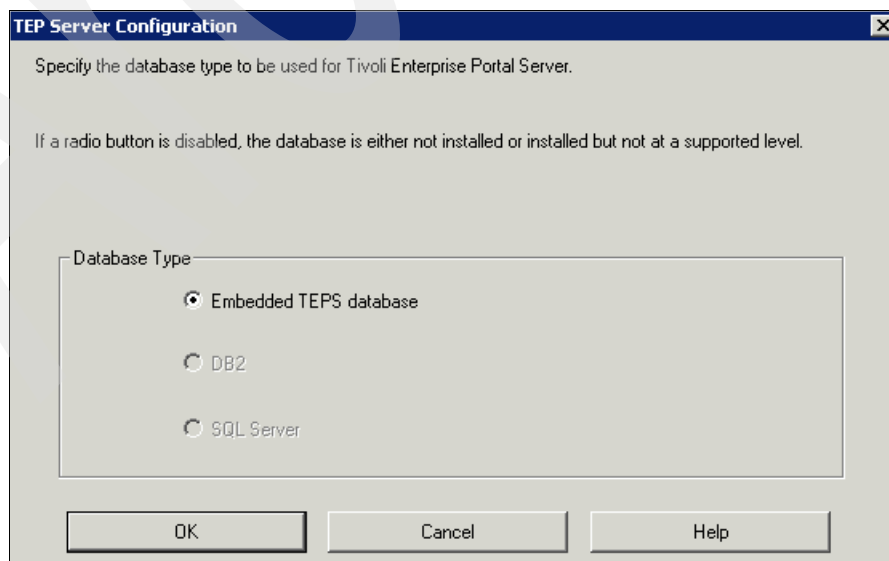


Figure 7-4 Specifying the Tivoli Enterprise Portal Server database configuration

14. In the TEP Server Connection to a Hub TEMS window (Figure 7-5), configure the connection between the Tivoli Enterprise Portal Server and the Tivoli Enterprise Monitoring Server. For Protocol 1, leave the default configuration of **IP.PIPE**. Click **OK**.

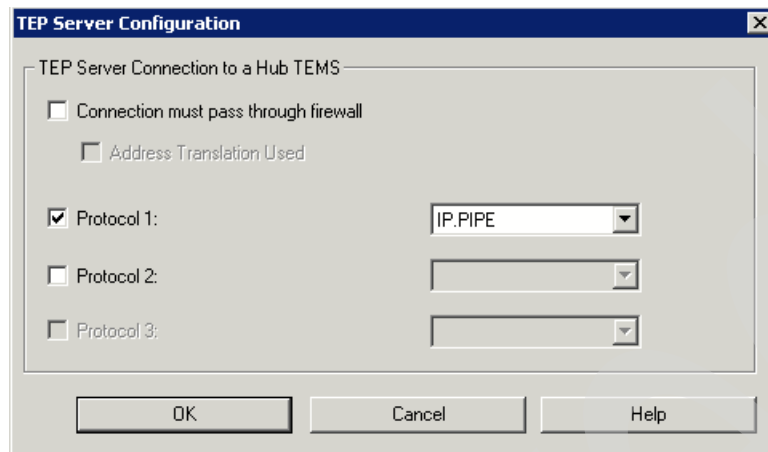


Figure 7-5 Tivoli Enterprise Portal Server to Tivoli Enterprise Monitoring Server connection

15. In the next window, configure the Tivoli Enterprise Portal Server (Figure 7-6):
 - a. Specify the host name of the Tivoli Enterprise Monitoring Server. Because the monitoring infrastructure that is described in this chapter has the Tivoli Enterprise Portal Server and the Tivoli Enterprise Monitoring Server running on the same host, this value matches the value that is used in step 12.
 - b. Verify that the default port for the connection of the Tivoli Enterprise Portal Server and the Tivoli Enterprise Monitoring Server is 1918.
 - c. For the monitoring purposes described in this chapter, leave as cleared the ITM REST or any other service that is not of interest.
 - d. Because LDAP is not considered in this chapter, leave this option as cleared.
 - e. Leave the Entry Options field as the default of **Convert to upper case**.
 - f. Click **OK**.

TEP Server Configuration

IP, UDP Settings of the TEMS

Hostname or IP Address: SA-W200-2

Port number and/or Port Pools: 1918

IP, PIPE Settings of the TEMS

Hostname or IP Address: SA-W200-2

Port number: 1918

IP, SPIPE Settings of the TEMS

Hostname or IP Address: SA-W200-2

Port number: 3660

SNA Settings of the TEMS

Network Name:

LU Name:

LU6.2 LOGMODE: CANCTDCS

TP Name: SNA SOCKETS

Local LU Alias:

(LU Alias is not required if using default)

Entry Options

☐ Use case as typed

☒ Convert to upper case

LDAP Security

☐ Validate User with LDAP ?

☐ Enable Single Sign On

ITM REST service

☐ Enable ITM REST service

NAT Settings

OK Cancel Help

Figure 7-6 Tivoli Enterprise Portal Server configuration

16. When prompted about whether you want to reconfigure the Tivoli Enterprise Portal Server warehouse connection, click **No**.

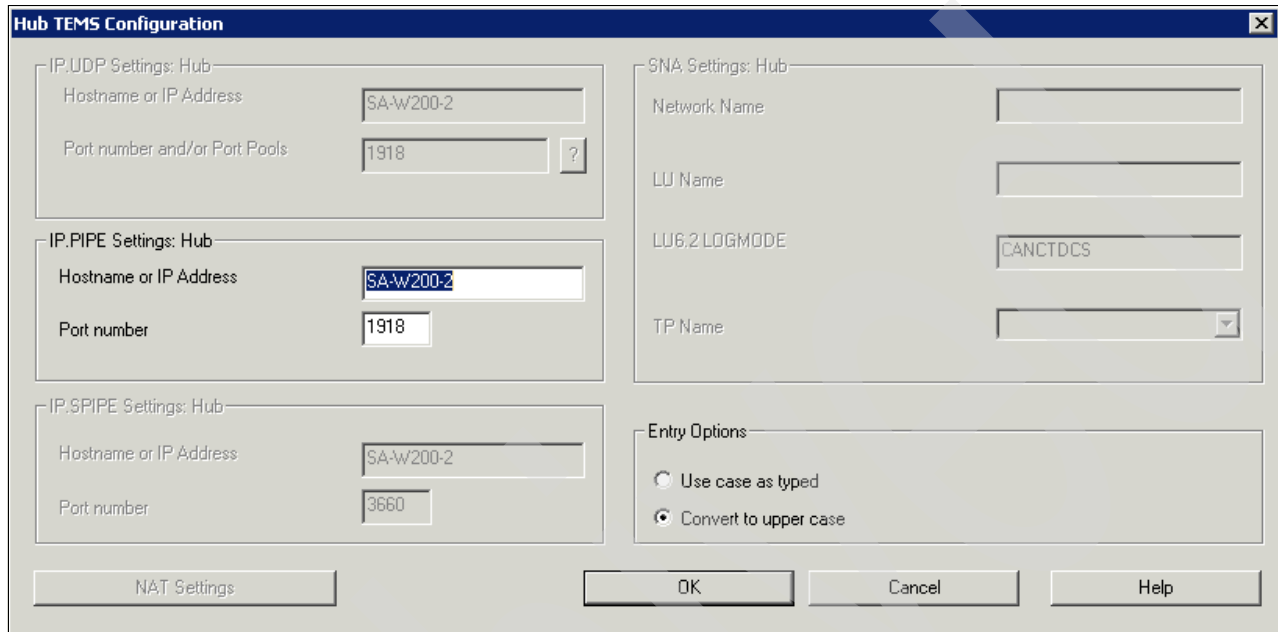
17. After some processing, in the Tivoli Enterprise Monitoring Server Configuration window (Figure 7-7):
- Because this monitoring infrastructure has Tivoli Enterprise Monitoring Server as the central hub of the system, leave the TEMS Type option set to **Hub**.
 - Select **Security: Validate User**. This option ensures that the Tivoli Enterprise Monitoring Server authenticates the user when logging into the TEP browser client by using the password that is specified in step 9.
 - By default, for TEMS Name, use the Tivoli Enterprise Monitoring Server host name that is prefixed with HUB_.
 - In the Protocol for TEMS box, define Protocol 1 as IP.PIPE to match the setting in step 14.
 - Leave all other check boxes cleared, because they are used only in more advanced setups.
 - Click **OK**.

The screenshot shows the 'Tivoli Enterprise Monitoring Server Configuration' dialog box. The 'TEMS Type' section has 'Hub' selected. Under 'Security', 'Validate User' is checked. The 'TEMS Name' is 'HUB_SA-W200-2'. In the 'Protocol for this TEMS' section, 'Protocol 1' is checked and set to 'IP.PIPE'. The 'Configure Hot Standby TEMS' section is empty. The bottom has 'OK', 'Cancel', and 'Help' buttons.

Figure 7-7 Tivoli Enterprise Monitoring Server configuration

Tivoli Enterprise Monitoring Server configuration settings particular to a hub setup are now displayed as shown in Figure 7-8.

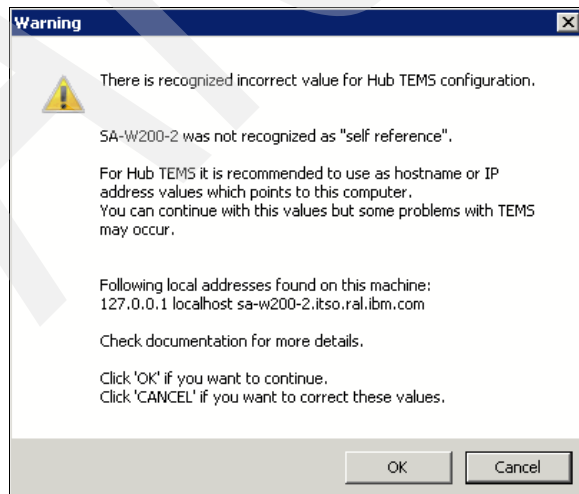
18. Because this instance is the only Tivoli Enterprise Monitoring Server instance, verify that the values for host name and port number match the values that are defined in step 15 on page 153. Click **OK**.



The 'Hub TEMS Configuration' dialog box is divided into several sections. On the left, there are three stacked boxes for 'IP.UDP Settings: Hub', 'IP.PIPE Settings: Hub', and 'IP.SPIPE Settings: Hub'. Each box contains fields for 'Hostname or IP Address' and 'Port number and/or Port Pools'. The 'IP.UDP' and 'IP.SPIPE' sections have a '?' button next to the port field. On the right, there is a 'SNA Settings: Hub' section with fields for 'Network Name', 'LU Name', 'LU6.2 LOGMODE', and 'TP Name'. Below this is an 'Entry Options' section with two radio buttons: 'Use case as typed' and 'Convert to upper case'. At the bottom, there is a 'NAT Settings' button on the left and 'OK', 'Cancel', and 'Help' buttons on the right.

Figure 7-8 Hub Tivoli Enterprise Monitoring Server configuration

Tip: If the installer does not infer that the host name selected in step 18 is a reference to the local machine (localhost), you might receive a warning message (Figure 7-9). If the network setup includes a DNS, and a DHCP client is running on the machine where Tivoli Enterprise Monitoring Server is being set up, you can ignore this warning message. If the host name is static, configure the domain (on Linux) or DNS suffixes (on Windows). If you know that this host name is correct, and can ping the host name from the command line, click **OK**.



The 'Warning' dialog box has a yellow warning icon. The text inside reads: 'There is recognized incorrect value for Hub TEMS configuration. SA-W200-2 was not recognized as "self reference". For Hub TEMS it is recommended to use as hostname or IP address values which points to this computer. You can continue with this values but some problems with TEMS may occur. Following local addresses found on this machine: 127.0.0.1 localhost sa-w200-2.itso.ral.ibm.com Check documentation for more details. Click 'OK' if you want to continue. Click 'CANCEL' if you want to correct these values.' At the bottom are 'OK' and 'Cancel' buttons.

Figure 7-9 Warning message if the host name is not detected as being a reference to localhost

19. Select the Tivoli Enterprise Monitoring Server location for application support. In this example, we select the default value **On this computer**. Then, click **OK**.
20. Select which application support files to add to Tivoli Enterprise Monitoring Server. You set up the agent that is used for monitoring in 7.2.2, “Installing ITCAM Agent for a WebSphere DataPower Appliance” on page 157. Therefore, the only application support to add here is the Tivoli Enterprise Monitoring Server option. Ensure that only this support file is highlighted.

In the Default distribution list settings field, leave the selected option as **New**, because this installation is new. Click **OK**.
21. In the Configuration Defaults for Connecting to a TEMS window (Figure 7-10), review the default configuration options that are used when configuring agents that will connect to this Tivoli Enterprise Monitoring Server instance. Leave Protocol 1 as IP.PIPE. Verify that the host name and port number are the values that are specified in step 18. Click **OK**.

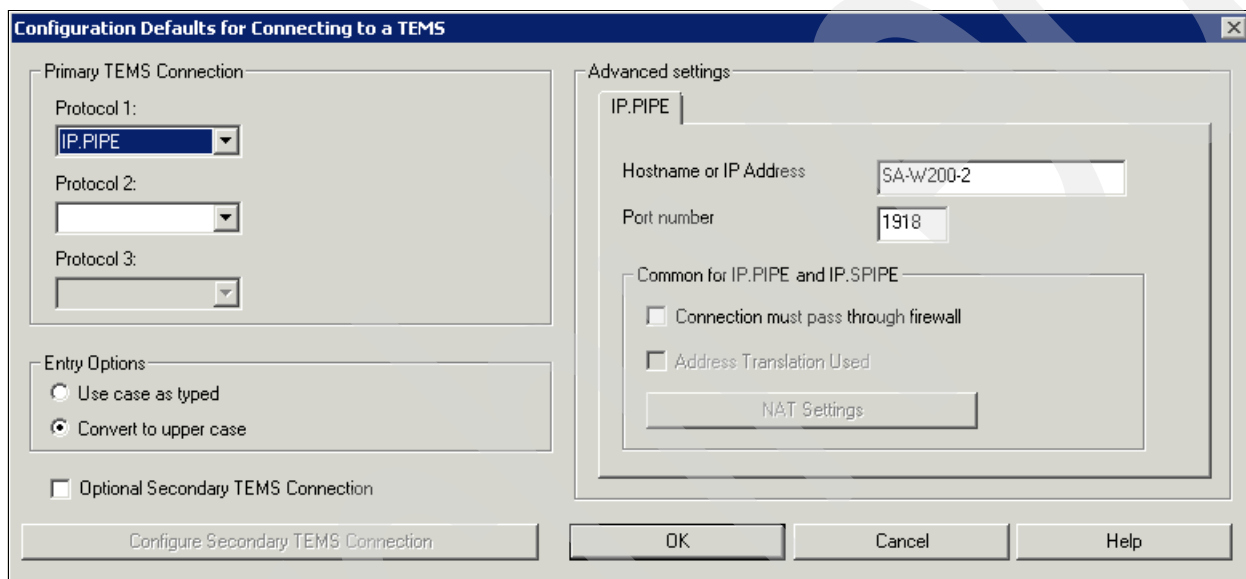


Figure 7-10 Configuration defaults for connecting to a Tivoli Enterprise Monitoring Server

22. In the window where you are prompted to configure Tivoli Performance Analyzer, click **Cancel**. This component is not used in this monitoring infrastructure.
23. After confirmation, in the window where you are prompted to configure the Warehouse Summarization and Pruning Agent, click **Cancel**. Again, this component is not required for monitoring WebSphere DataPower Appliances.
24. If you see a warning message that the Warehouse Proxy must connect to a HUB TEMS, click **OK**.
25. In the Warehouse Proxy: Agent Advanced Configuration window, click **Cancel**.

IBM Tivoli Monitoring services are now *recycled* (restarted).
26. When the InstallShield wizard indicates that the installation is complete, click **Finish**.

The Manage Tivoli Enterprise Monitoring Services application is shown. The central control panel is used to set up new ITCAM Agents, to edit configurations, and to recycle services, including the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server. Close this application and proceed to 7.2.2, “Installing ITCAM Agent for a WebSphere DataPower Appliance” on page 157, to set up the ITCAM Agent.

For important details about the IBM Tivoli Monitoring configuration, see Table 7-1.

Table 7-1 Important IBM Tivoli Monitoring configuration details

Property	Default value
SSL encryption key	IBMTivoliMonitoringEncryptionKey
Tivoli Enterprise Portal Server user name (Windows)	sysadmin
Tivoli Enterprise Portal Server password	Existing sysadmin user password (on Windows) or chosen during installation
Tivoli Enterprise Portal Server → Tivoli Enterprise Monitoring Server connection port	1918

For more information, see the *Installation procedure* topic in the IBM ITCAM for Applications Information Center at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp?topic=%2Fcom.ibm.itm.doc_6.2.2fp2%2Fitm_install131.htm

7.2.2 Installing ITCAM Agent for a WebSphere DataPower Appliance

ITCAM is the second part of the monitoring component for WebSphere Appliance Management Center to install and integrate with the software that you installed in 7.2.1, “Installing IBM Tivoli Monitoring” on page 149.

For the purposes of this example, instances of the ITCAM Agent are installed on two hosts, SA-W200-1 and SA-W200-2. The SA-W200-2 host has the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server running. See Figure 7-1 on page 148.

This section includes the following two scenarios:

- ▶ Installing ITCAM Agent on the same host as the Tivoli Enterprise Monitoring Server
- ▶ Installing ITCAM Agent on a second host and linking to a remote IBM Tivoli Monitoring installation

For more information about installing the ITCAM Agent, see the *Tivoli Composite Application Manager Agent for WebSphere DataPower Appliance Version 6.3 User Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamsoa.doc_6.2.2/DPAgent_UG.htm

Installing ITCAM Agent on the same host as the Tivoli Enterprise Monitoring Server

To install the ITCAM Agent on the same host as the Tivoli Enterprise Monitoring Server (see Figure 7-1 on page 148):

1. Open the directory that you extracted the monitoring component files into and run **setup.exe** in the WINDOWS directory.
2. When the InstallShield wizard is displayed and confirms that IBM Tivoli Monitoring is already installed (Figure 7-11), click **Next**.

Tip: Tivoli Composite Application Manager Agent for WebSphere DataPower Appliance v7.1 is packaged as a tar.gz container. On Windows 2008 R2, to extract the installation files, use a tool such as 7-Zip.

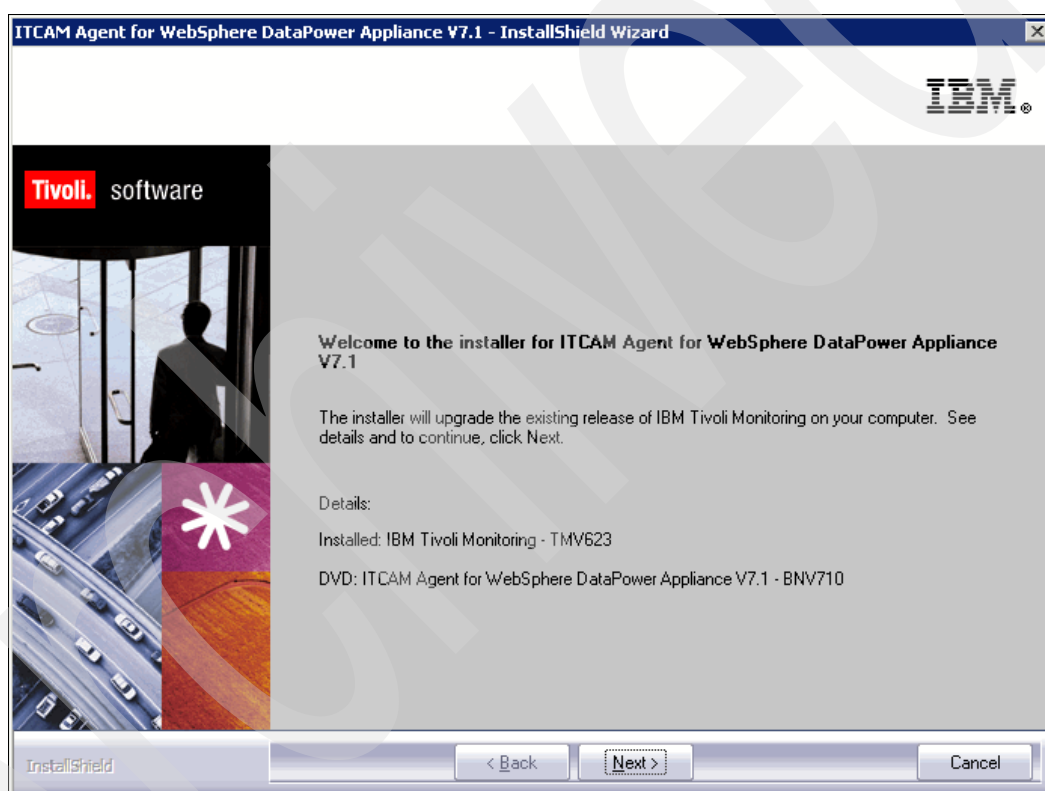


Figure 7-11 ITCAM Agent installer confirming existence of IBM Tivoli Monitoring components

3. Read and accept the license agreement, and then, click **Next**.

4. In the Select Features window, select the features to install. In the hierarchy that is shown in Figure 7-12, the entries for Tivoli Enterprise Monitoring Agents, Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal Server are selected. If the Tivoli Enterprise Portal Desktop client was installed in the previous section, this option is also selected.

Because only 64-bit environments are supported, the ITCAM Agent for WebSphere DataPower Appliance (x86-64 only) option is selected under Tivoli Enterprise Monitoring Agents. The selection of the Tivoli Enterprise Monitoring Agents subtree installs the agent.

The Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server subtrees are selected to install supporting catalog files as explained in step 6 on page 149.

Click **Next**.

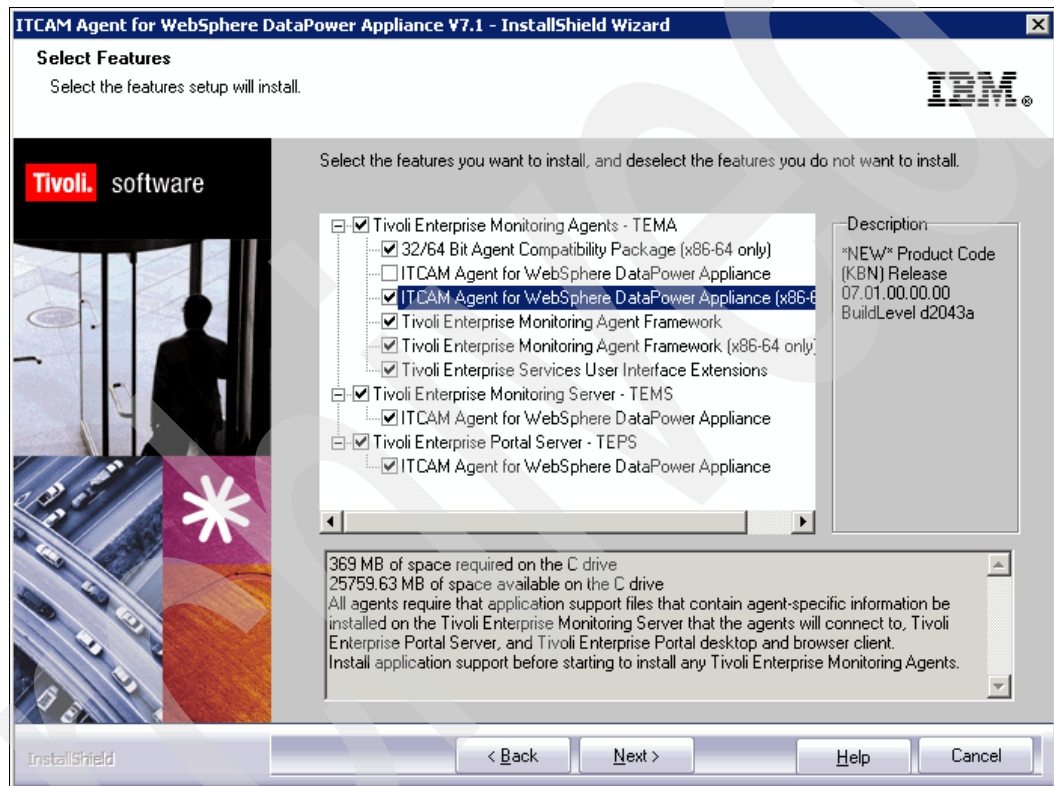


Figure 7-12 ITCAM Agent installer showing selected features to install

5. In the Agent Deployment window (Figure 7-13), because the ITCAM Agent is installed manually, do not select any items. Click **Next**.

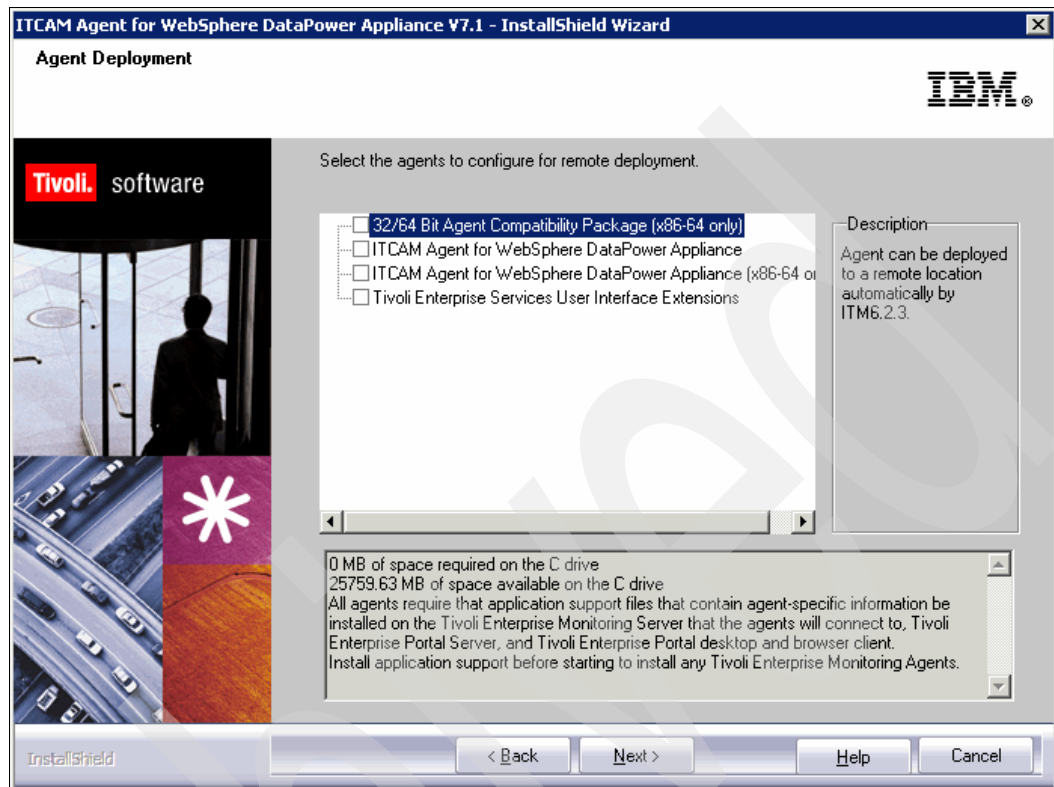


Figure 7-13 ITCAM Agent installer with no remote agents selected

6. In the summary window, click **Next**.

7. After the installation is complete, configure the components of IBM Tivoli Monitoring (Figure 7-14). To defer configuration, clear those items. In this example, we configure the components now. Therefore, ensure that all items are selected. Then, click **Next**.

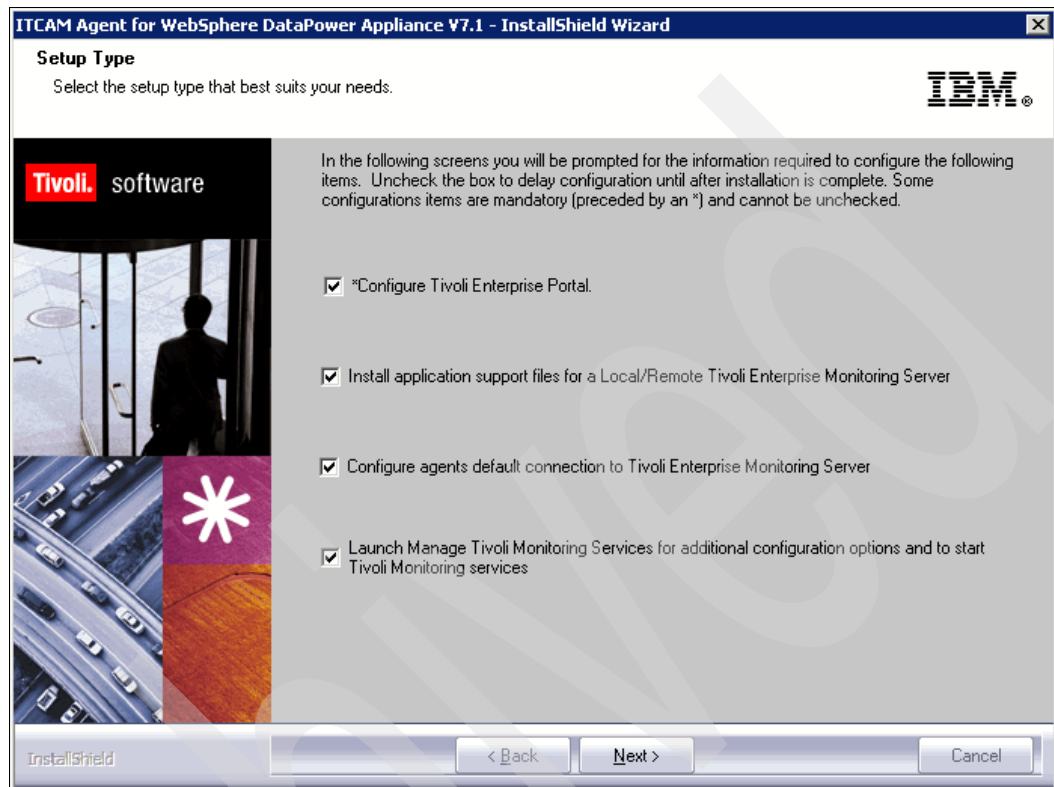


Figure 7-14 Configuration options during ITCAM Agent installation

8. In the TEPS Hostname window (Figure 7-15), enter the host name of the Tivoli Enterprise Portal server. For this example, we enter SA-W200-2. Click **Next**.

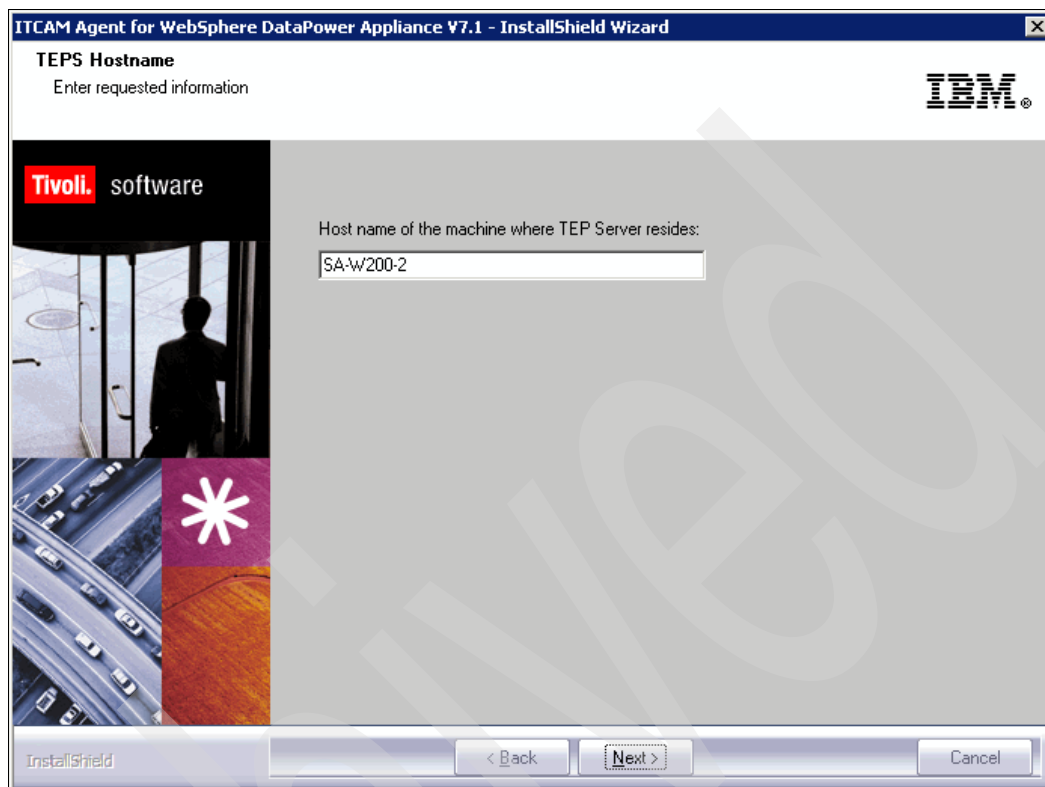


Figure 7-15 ITCAM Agent installer prompt for the Tivoli Enterprise Portal Server host name

9. Add application support to the Tivoli Enterprise Monitoring Server (Figure 7-16). Leave the default of **On this computer**, and click **OK**.

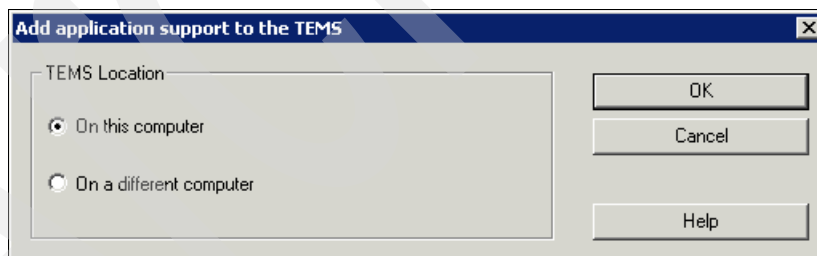


Figure 7-16 Adding application support for Tivoli Enterprise Monitoring Server

10. Select which application support files to add to the Tivoli Enterprise Monitoring Server (Figure 7-17). Because only one agent is set up here (ITCAM Agent), select the **ITCAM Agent for WebSphere DataPower Appliance** option, which is the only application support to add here. Ensure that this support file is highlighted.

In the Default distribution list settings field, leave the selected option as **All** because this installation is new. Click **OK**.

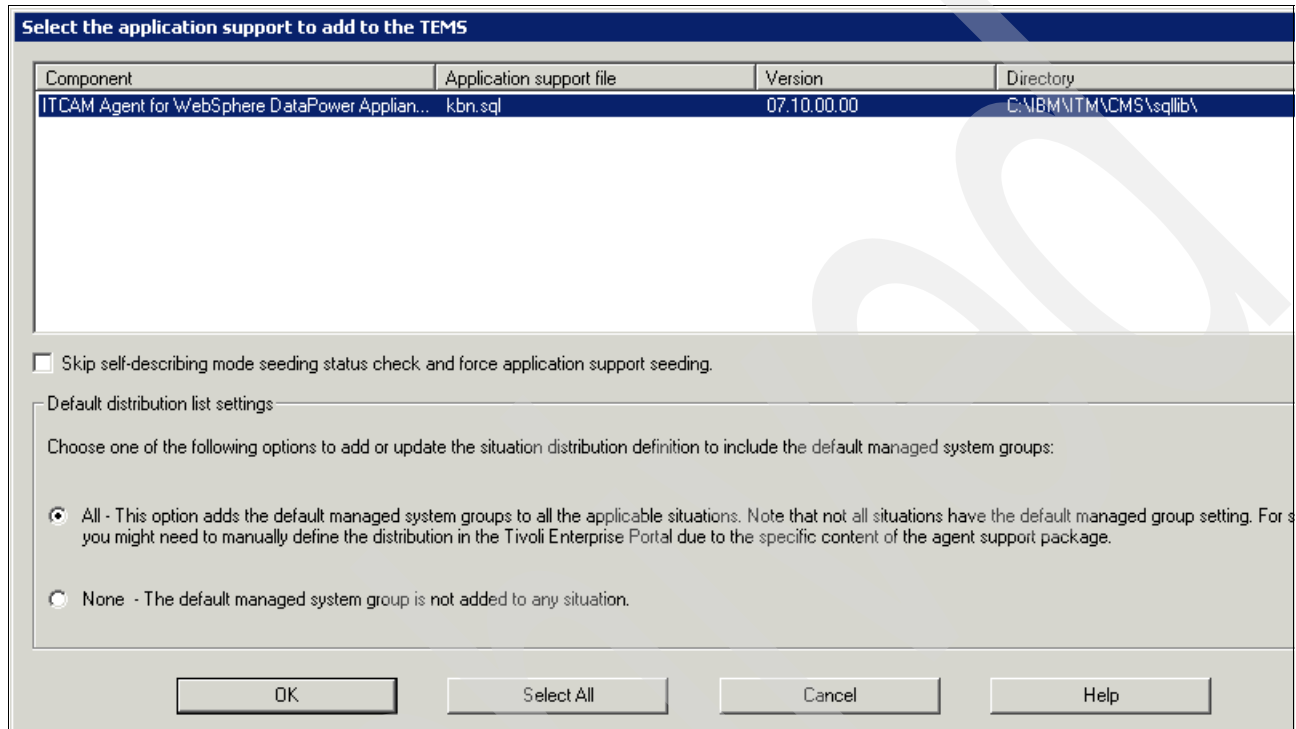


Figure 7-17 Adding ITCAM Agent to the Tivoli Enterprise Monitoring Server

11. Set the configuration details for connecting ITCAM Agent instances to a Tivoli Enterprise Monitoring Server (Figure 7-18). Leave Protocol 1 as IP.PIPE. Set the host name and port number to the same values that you entered in step 15 on page 153. Click **OK**.

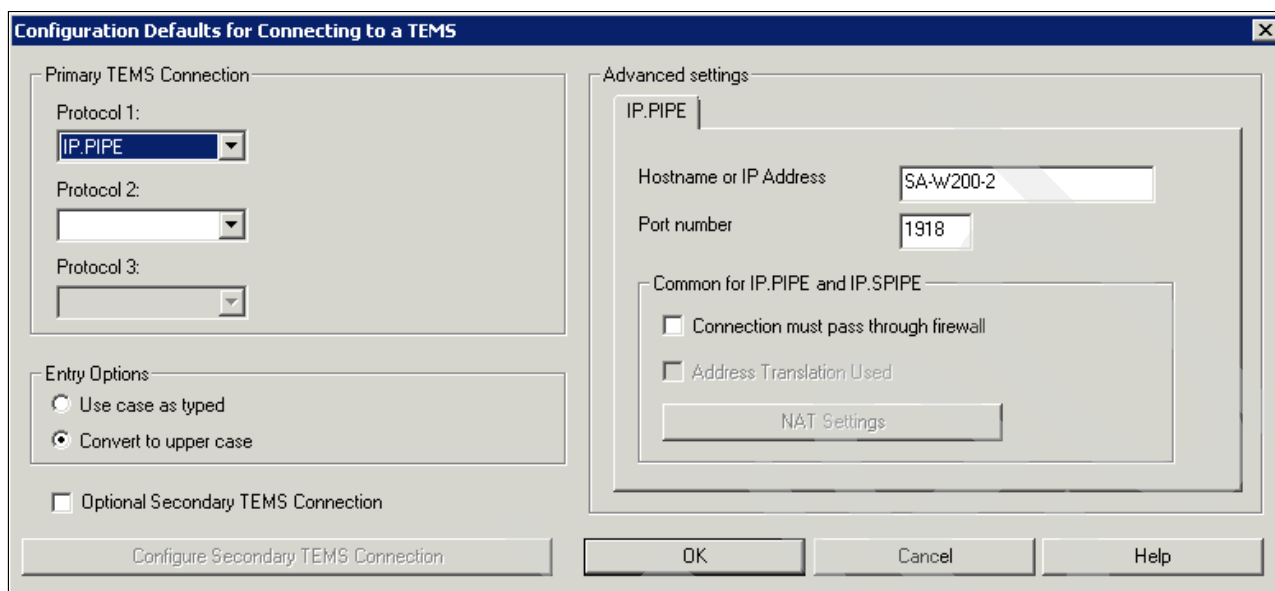


Figure 7-18 Connecting ITCAM Agents to a Tivoli Enterprise Monitoring Server

12. When the InstallShield wizard indicates that the installation is complete, click **Finish**.

The Manage Tivoli Enterprise Monitoring Services application (Figure 7-19) now lists ITCAM Agent, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server. You can now configure this instance of ITCAM Agent to monitor your WebSphere DataPower Appliances.

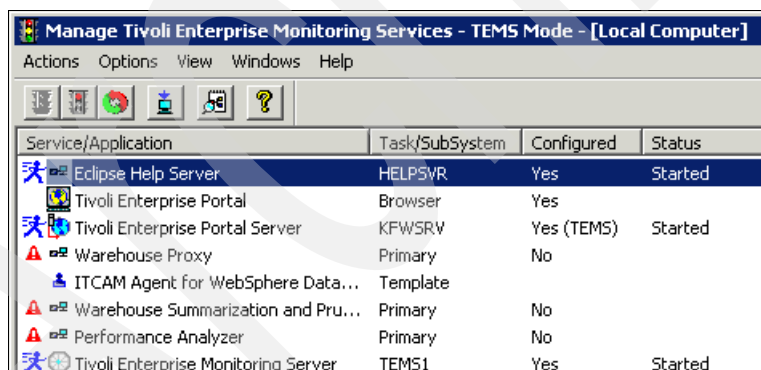


Figure 7-19 Tivoli Enterprise Monitoring Services application

To complete the monitoring infrastructure that is described at the beginning of this chapter, another instance of ITCAM Agent is installed on host SA-W200-1. To use only a single host, skip to 7.3, “Adding WebSphere DataPower Appliances to ITCAM Agents” on page 168.

Installing ITCAM Agent on a second host and linking to a remote IBM Tivoli Monitoring installation

To monitor another WebSphere DataPower Appliance, ports on a firewall are opened to another host, SA-W200-1. This host runs only the ITCAM Agent, which communicates with the Tivoli Enterprise Monitoring Server on SA-W200-2. See Figure 7-1 on page 148.

To set up ITCAM Agent on this machine, use the following steps, which are mostly the same as in “Installing ITCAM Agent on the same host as the Tivoli Enterprise Monitoring Server” on page 158:

1. To run the installer, double-click **setup.exe** in the WINDOWS directory.
2. When you see the prerequisites message about knowing the host name and IP address of the Tivoli Enterprise Management Server the ITCAM Agent is connecting to (Figure 7-20), click **Next**.



Figure 7-20 Installing ITCAM Agent on a host not running Tivoli Enterprise Monitoring Server

3. In the Select Features window (Figure 7-21), select only **Tivoli Enterprise Monitoring Agents** (64-bit version) for the installation. The other packages that make up the monitoring component are installed on a different host. Click **Next**.

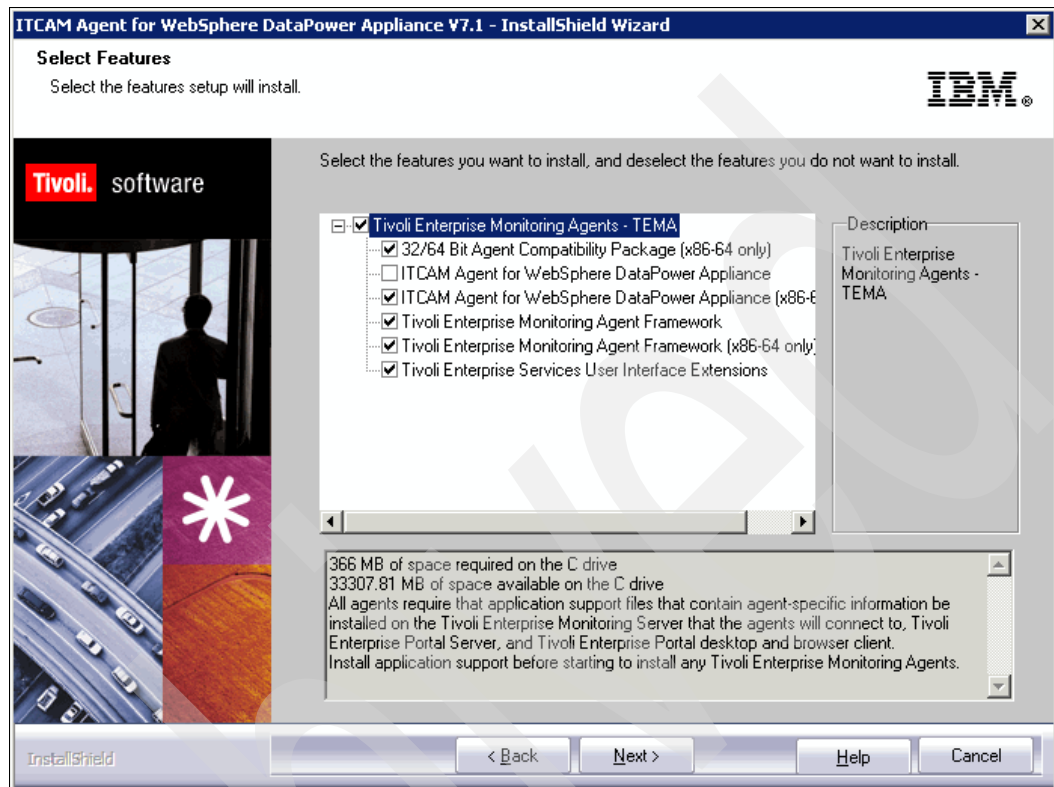


Figure 7-21 Selecting the Tivoli Enterprise Monitoring Agents option

4. In the summary window, click **Next** to start the installation.
5. When you see the warning message about not stopping the installation, click **Yes**.
6. After the installation is complete, leave selected the options to configure the default connection settings for the agent and to start Manage Tivoli Monitoring Services. Then, click **Next**.

7. Verify the configuration defaults for connecting to a Tivoli Enterprise Monitoring Server (Figure 7-22). Protocol 1 must be IP.PIPE, and the host name and port must be for the Tivoli Enterprise Monitoring Server. For this example, the host name is SA-W200-2, and the port number is 1918. Click **OK**.

Figure 7-22 Configuration details for connecting to the Tivoli Enterprise Monitoring Server

8. In the window to configure an instance of the ITCAM Agent (Figure 7-23), click **Cancel**. For more information about these settings to link the agent to WebSphere DataPower Appliances, see 7.4, “Monitoring WebSphere DataPower Appliances” on page 174.

Figure 7-23 Configuration page for the ITCAM Agent

9. In the message window that opens, click **Yes** to confirm. The installation is now complete,
10. Click **Finish**.

The Manage Tivoli Enterprise Monitoring Services application is shown listing the ITCAM Agent template (Figure 7-24).

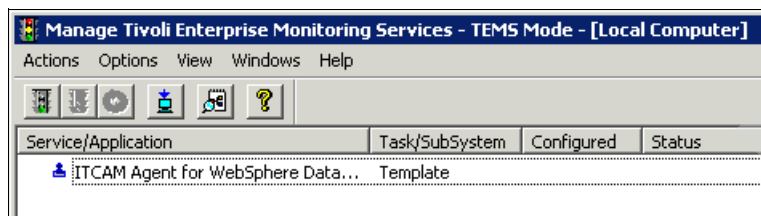


Figure 7-24 Manage Tivoli Enterprise Monitoring Services listing the ITCAM Agent template

The next step is to link the ITCAM Agents and the WebSphere DataPower Appliances as explained in 7.3, “Adding WebSphere DataPower Appliances to ITCAM Agents” on page 168.

7.3 Adding WebSphere DataPower Appliances to ITCAM Agents

In this section, the monitoring component of WebSphere Appliance Management Center is installed. You can set up one or more instances of the ITCAM Agent by providing them with the login details of one or more WebSphere DataPower Appliances. Do not assign any more than 10 WebSphere DataPower Appliances to each instance of the ITCAM Agent. However, you can set up multiple agents on one machine.

The ITCAM Agent uses SOAP Configuration Management (SOMA) or syslog to monitor most WebSphere DataPower Appliances. The exception is the WebSphere DataPower XC10 Appliance, for which it uses Simple Network Monitoring Protocol (SNMP).

Tip: SNMP is a set of protocols for monitoring systems and devices. Although most WebSphere DataPower Appliances support this method to allow ITCAM Agents to poll WebSphere DataPower Appliances, SOMA is easier to set up and is preferred, by allowing monitoring data to pass over the XML management interface. For more information, see *WebSphere DataPower SOA Appliance: The XML Management Interface*, REDP-4446. WebSphere DataPower Appliances can also be polled by reading the system logs directly (by using syslog).

To link an ITCAM Agent to a WebSphere DataPower Appliance:

1. Open the Manage Tivoli Enterprise Monitoring Services application.
2. Locate the ITCAM Agent template. This template contains the default configuration setup information that was provided in the previous sections and is used to create an instance of the ITCAM Agent.

3. Right-click the **ITCAM Agent Template**, and select **Configure Using Defaults** (Figure 7-25).

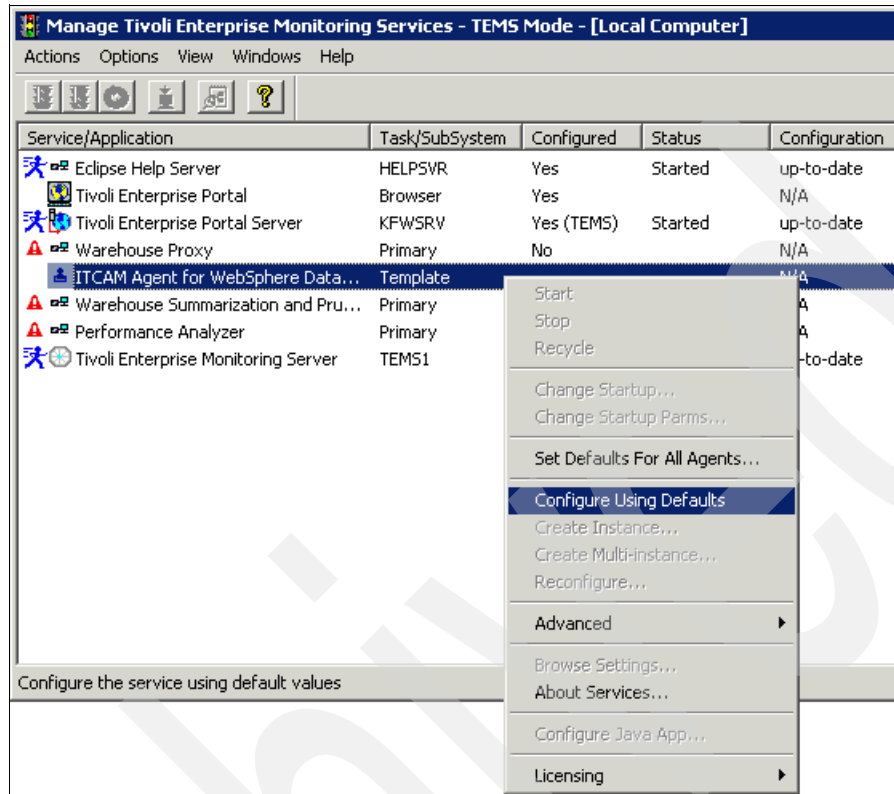


Figure 7-25 Configuring an instance of the ITCAM Agent

4. In the message window (Figure 7-26), enter a unique name for this instance of the ITCAM Agent. In this example, we use the host name of this machine with a prefix of `AGENT_`, which results `AGENT_SA-W200-2`. Click **OK**.

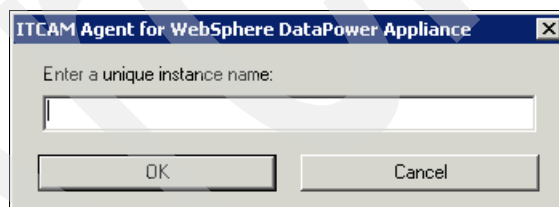


Figure 7-26 Specifying the ITCAM Agent instance name

5. In the Configure ITCAM Agent for WebSphere DataPower Appliance window (Figure 7-27), click **Next** to accept the default values, including the default values for Security Level, Authentication, and Privacy.

Configure ITCAM Agent for WebSphere DataPower Appliance

☐ SNMP Events
☐ DataPower Appliances
☐ DataPower XC10 Appliances

SNMP properties for receiving events

*Instance Name: AGENT_SA-W200-2

*Port Number: 162

*Security Level: Authentication, Privacy

*SNMP User Name: admin

*SNMP Authentication Protocol: SHA

SNMP Authentication Secret:

Confirm SNMP Authentication Secret:

*SNMP Privacy Protocol: DES

SNMP Privacy Secret:

Confirm SNMP Privacy Secret:

Back Next Home OK Cancel

Figure 7-27 Configuring an instance of ITCAM Agent

Managed System Details has two sections: one for general WebSphere DataPower Appliances, and one for the WebSphere DataPower XC10 Appliance. The first section is for general WebSphere DataPower Appliances.

6. Next to Managed System Details, click **New**.

7. In the Remote Managed System section (Figure 7-28), enter the details for a WebSphere DataPower Appliance and administrator user account (host name, XML management interface port, user ID, and password) on that appliance. You can enter the appliance's IP address instead of the host name. The agent communicates with the WebSphere DataPower Appliance by using SOMA.

If you want the agent to monitor the WebSphere DataPower Appliance by using syslog, click **Browse** to select the log file. You must use the full path, with single-byte characters.

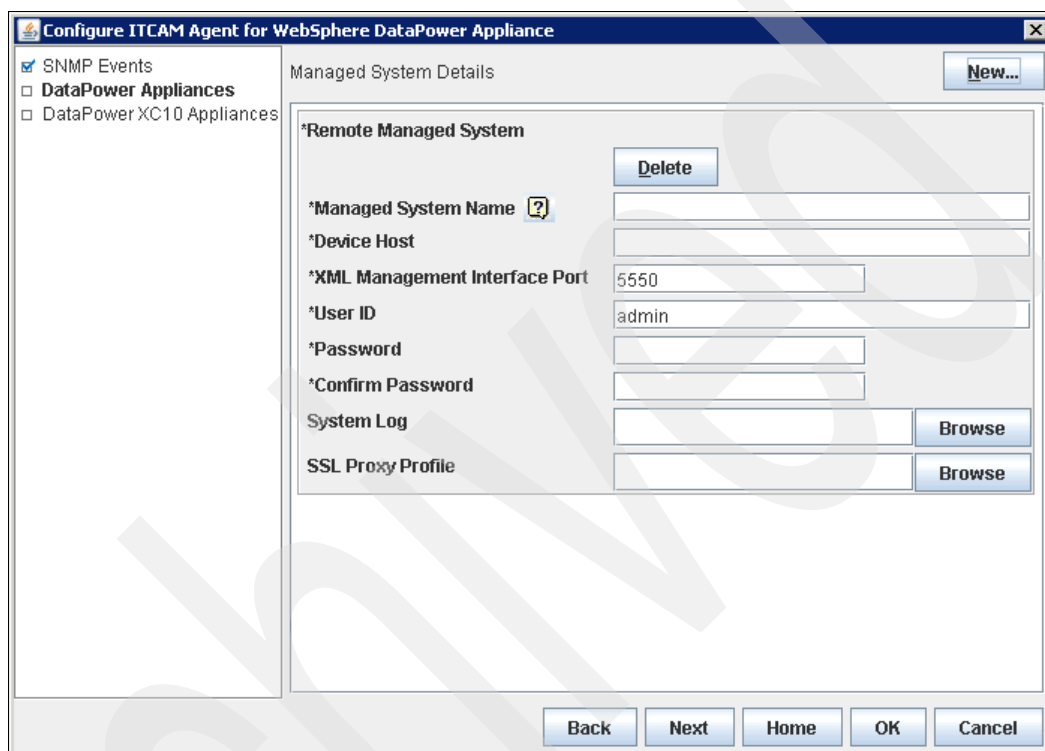


Figure 7-28 Entering WebSphere DataPower Appliance details during ITCAM Agent instance configuration

For more information about configuring a syslog target on the WebSphere DataPower Appliance, see the *Tivoli Composite Application Manager Agent for WebSphere DataPower Appliance Version 6.3 User Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamsoa.doc_6.2.2/DPAgent_UG.htm

8. If you have more WebSphere DataPower Appliances that you want to monitor by this agent, repeat steps 6 on page 170 and 7. Alternatively, you can configure an instance of the ITCAM Agent for each WebSphere DataPower Appliance. When you are finished, click **Next**.
9. In the section for adding remote WebSphere DataPower XC10 Appliances:
 - a. Because the user ID and password of an administrator account on the WebSphere DataPower Appliance are not required, you do not need to enter them.
 - b. Ensure that SNMP port 161 is open between the ITCAM Agent host and the WebSphere DataPower XC10 Appliance.
 - c. If you want to monitor a WebSphere DataPower XC10 Appliance, click **New**. The ITCAM Agent monitors WebSphere DataPower XC10 Appliances by using SNMP. Otherwise, skip to step 12.

10. Enter the host name (or IP address) of the WebSphere DataPower XC10 Appliance and the name of an SNMP community on the appliance (Figure 7-29). Click **OK**.

The screenshot shows a Windows-style dialog box titled "Configure ITCAM Agent for WebSphere DataPower Appliance". On the left is a tree view with three items: "SNMP Events" (checked), "DataPower Appliances" (checked), and "DataPower XC10 Appliance" (unchecked). The main pane is titled "Managed System Details" and contains a "New..." button in the top right. Below this is a section for a "Remote Managed System" with a "Delete" button. The fields are: "*Managed System Name" (with a help icon), "*SNMP VERSION" (set to "snmpv2"), "*Device Host", "*SNMP Port Number" (set to "161"), "*SNMP Community", and "*Confirm SNMP Community". At the bottom are "Back", "Next", "Home", "OK", and "Cancel" buttons.

Figure 7-29 Setting up the monitoring of a WebSphere DataPower XC10 Appliance

Tip: To confirm the name of an SNMP community or to create an SNMP community, log in to your WebSphere DataPower XC10 Appliance:

`https://hostname`

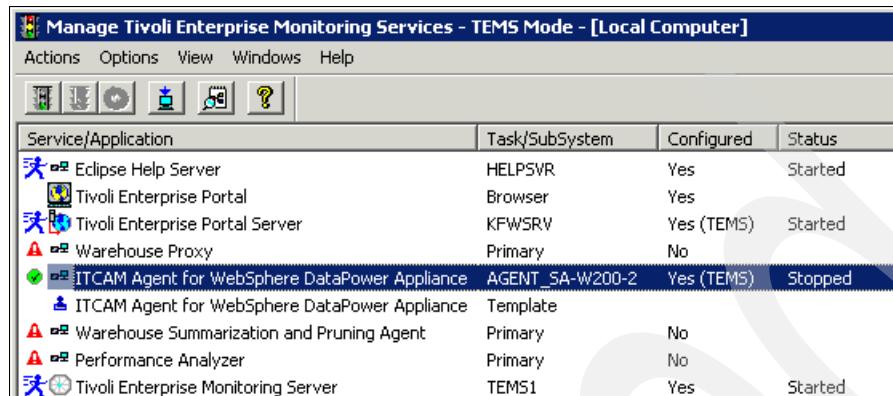
Select **Appliance** → **SNMP Settings**. Then, ensure that **Enable SNMP** is selected, and click **SNMP Communities**.

To create a community, click **Create community**. Hosts can be restricted if required.

11. To monitor more WebSphere DataPower XC10 Appliances, repeat steps 9 and 10.

An instance of ITCAM Agent is created and shown in the Manage Tivoli Enterprise Monitoring Services application (Figure 7-30). Currently, the status is *Stopped*.

12. To start the agent, right-click the agent, and click **Start**.



Service/Application	Task/SubSystem	Configured	Status
Eclipse Help Server	HELPSVR	Yes	Started
Tivoli Enterprise Portal	Browser	Yes	
Tivoli Enterprise Portal Server	KFWSRV	Yes (TEMS)	Started
Warehouse Proxy	Primary	No	
ITCAM Agent for WebSphere DataPower Appliance	AGENT_SA-W200-2	Yes (TEMS)	Stopped
ITCAM Agent for WebSphere DataPower Appliance	Template		
Warehouse Summarization and Pruning Agent	Primary	No	
Performance Analyzer	Primary	No	
Tivoli Enterprise Monitoring Server	TEMS1	Yes	Started

Figure 7-30 Newly created instance of an ITCAM Agent

7.3.1 Editing the configuration settings of an ITCAM Agent instance

If you decide to monitor other WebSphere DataPower Appliances with an existing ITCAM Agent or otherwise modify its configuration:

1. Locate the ITCAM Agent in the Manage Tivoli Enterprise Monitoring Services application, right-click the application, and select **Reconfigure** (Figure 7-31).

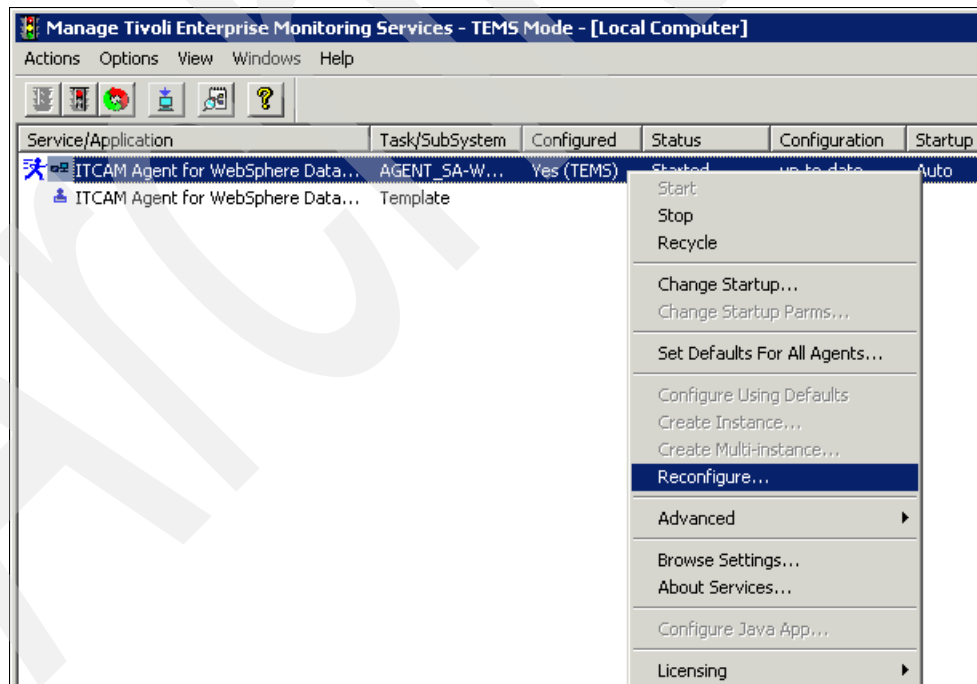


Figure 7-31 Reconfiguring an ITCAM Agent instance

2. In the first window, change the agent's connection settings to Tivoli Enterprise Monitoring Server. Click **OK**.

3. In the standard ITCAM Agent configuration window (Figure 7-27 on page 170), click **Next** to view the WebSphere DataPower Appliances that are being monitored by this agent. For each WebSphere DataPower Appliance that is listed, click **Delete** to remove it from the agent. Similarly, click **New** to monitor another WebSphere DataPower Appliance (Figure 7-32). When your changes are complete, click **OK**.

Figure 7-32 Configuring a new ITCAM Agent instance

4. When prompted if you want to restart the agent, click **Yes**. To force a recycle, right-click the agent, and select **Recycle**.

7.4 Monitoring WebSphere DataPower Appliances

Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server are also running on this host, and their statuses are reported as *started* in the Manage Tivoli Enterprise Monitoring Services application (Figure 7-30 on page 173). Therefore, you can visit the Tivoli Enterprise Portal Server browser client in a web browser.

To connect to the browser client:

1. Go to the following address:

`http://TEPS-hostname:15200/cnp.html`

Alternatively, you can connect by using SSL:

`https://TEPS-hostname:15201/cnp.html`

Here *TEPS-hostname* is *localhost*.

2. Log in with the user name and password that you specified when you installed IBM Tivoli Monitoring (step 9 on page 150).

You see a window similar to the example in Figure 7-33. The panes in this window make up the *workspace*.

Tip: If `cnp.html` is omitted in the web link, a web browser check is performed, which might assert that your web browser is not supported. If you are using a web browser that is supported by WebSphere Appliance Management Center (see 1.4.3, “Supported web browsers” on page 8), go to `cnp.html`.

Tivoli Enterprise Portal Server browser client is a Java applet. Therefore, you might be prompted to install or update your Java plug-in. Click **Run** to download and install **ibm-java6.exe**.

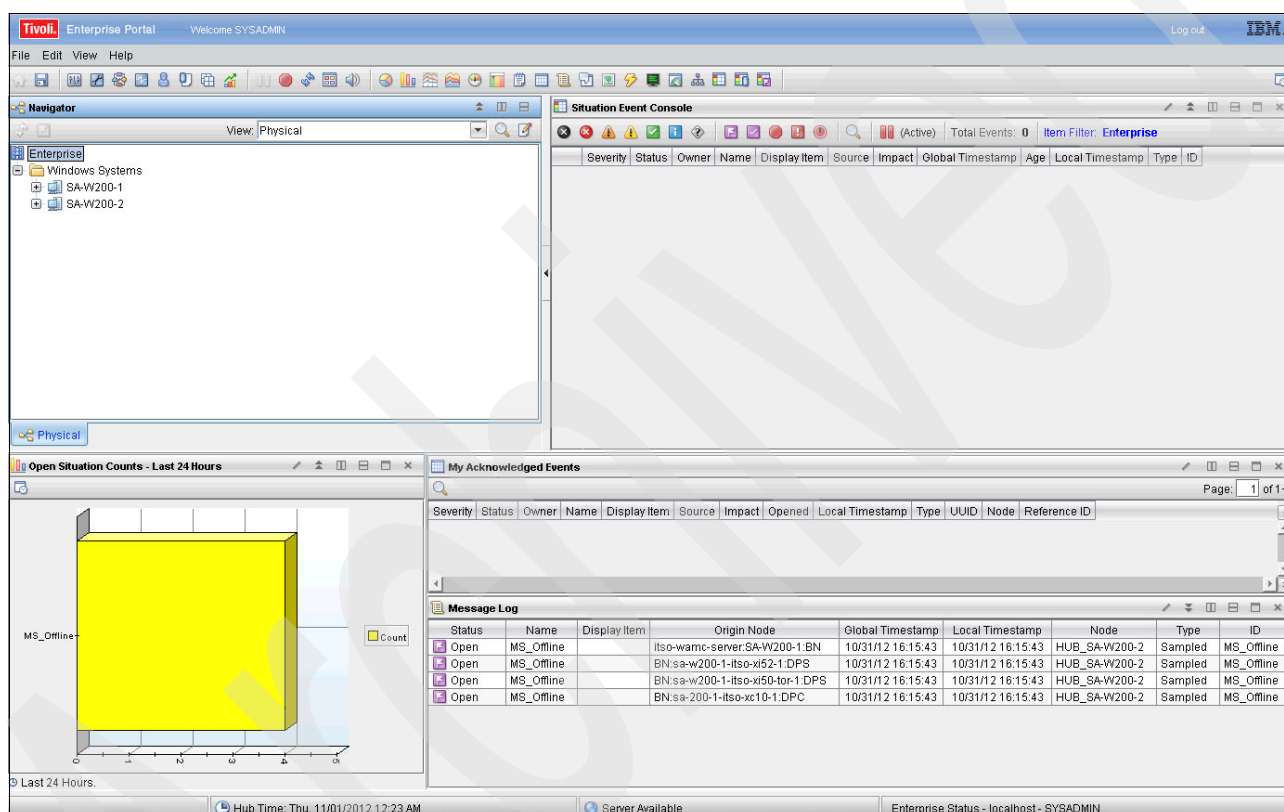


Figure 7-33 Tivoli Enterprise Portal Server web browser client window after login

The *Message Log pane* is in the lower-right corner in Figure 7-33. By using the Navigator pane, you can select which agent to view and which WebSphere DataPower Appliance you want to monitor:

1. Expand **Windows Systems** to see a listing of the hosts that are running instances of ITCAM Agent.
2. Expand one of the hosts, and click **DataPower Monitoring Agent**.

A window opens similar to the example in Figure 7-34.

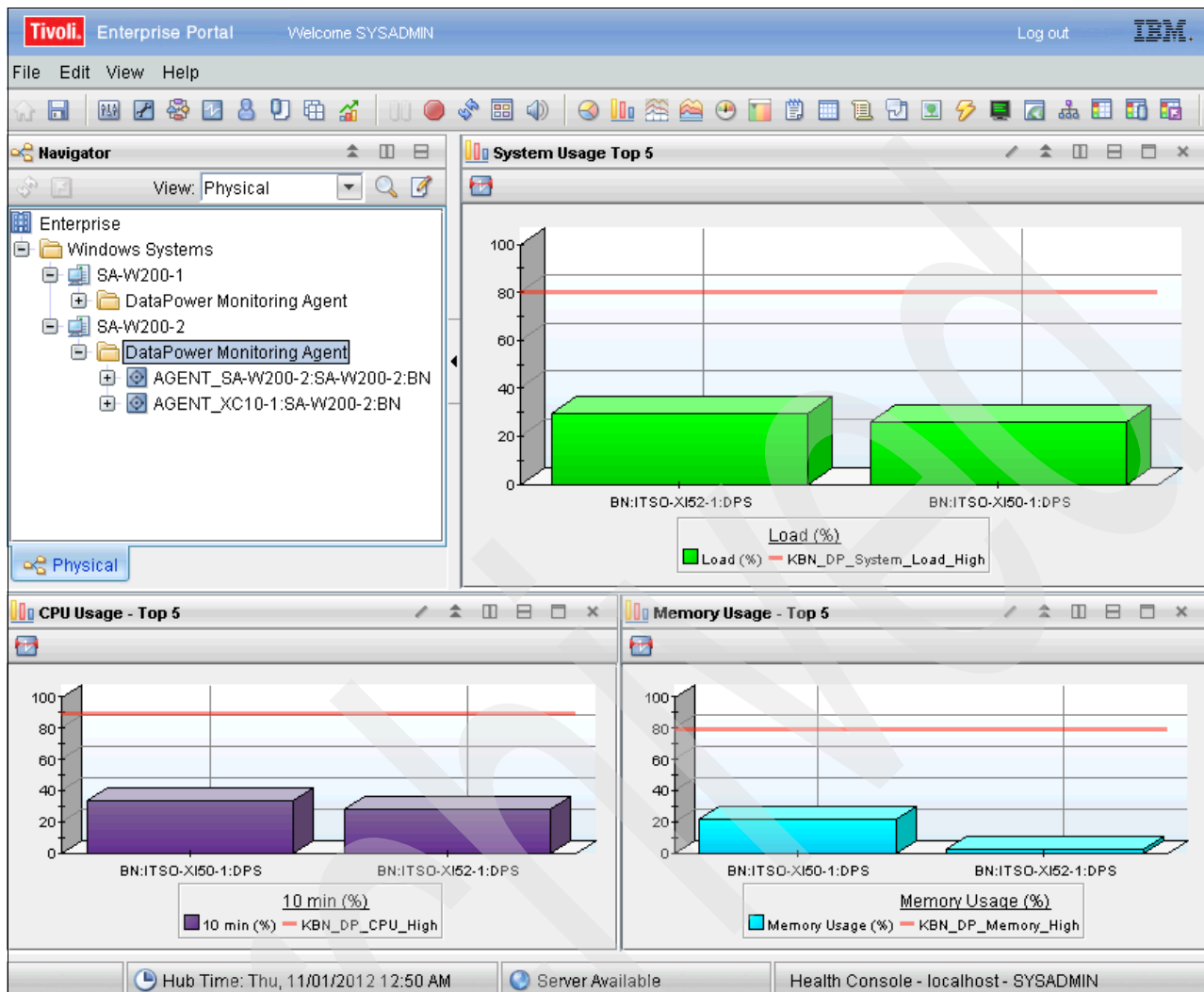


Figure 7-34 Overview of WebSphere DataPower Appliances being monitored by IBM Tivoli Monitoring

The window in Figure 7-34 shows an overview of the WebSphere DataPower Appliances that are being monitored by this instance of Tivoli Enterprise Monitoring Server. System usage (load), CPU usage, and memory usage are shown for the top five WebSphere DataPower Appliances (that is, those appliances that are reporting the highest values). Threshold values are indicated by red lines.

When you expand the tree for a particular WebSphere DataPower Appliance and select the appliance listing, you see a summary page for that WebSphere DataPower Appliance (Figure 7-35).

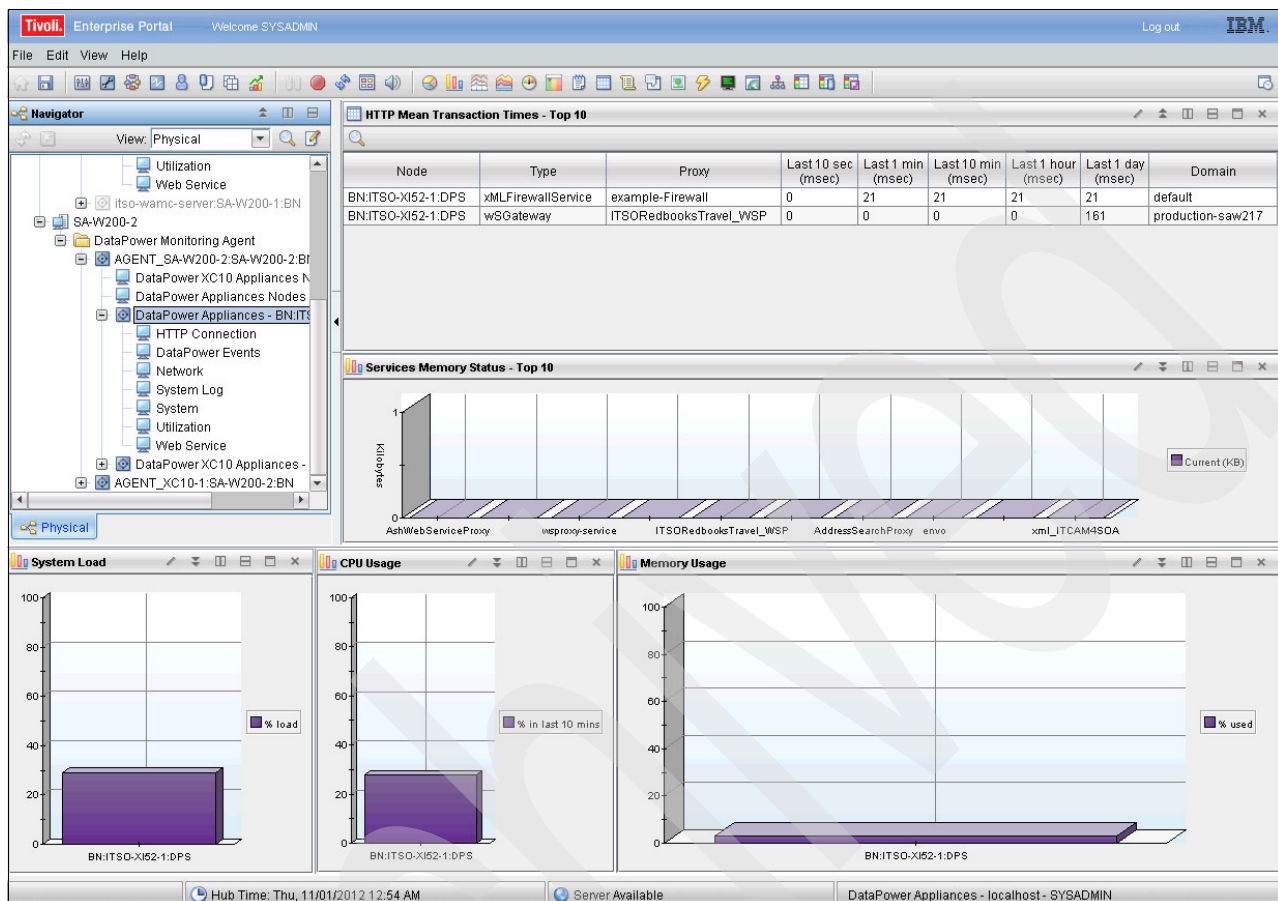


Figure 7-35 Summary workspace for a monitored WebSphere DataPower Appliance

Figure 7-35 shows at a glance the HTTP mean transaction times (top 10), services memory status (top 10), in addition to the system load, CPU usage, and memory usage. You can access workspaces with more detailed information for this WebSphere DataPower Appliance by using the Navigator pane.

Click **HTTP Connection**.

The HTTP Connection Requests (Top 10) and HTTP Connection Statistics are shown, with the HTTP Connection Statistics split by domain (Figure 7-36). Here, the requests mostly involve the default domain.

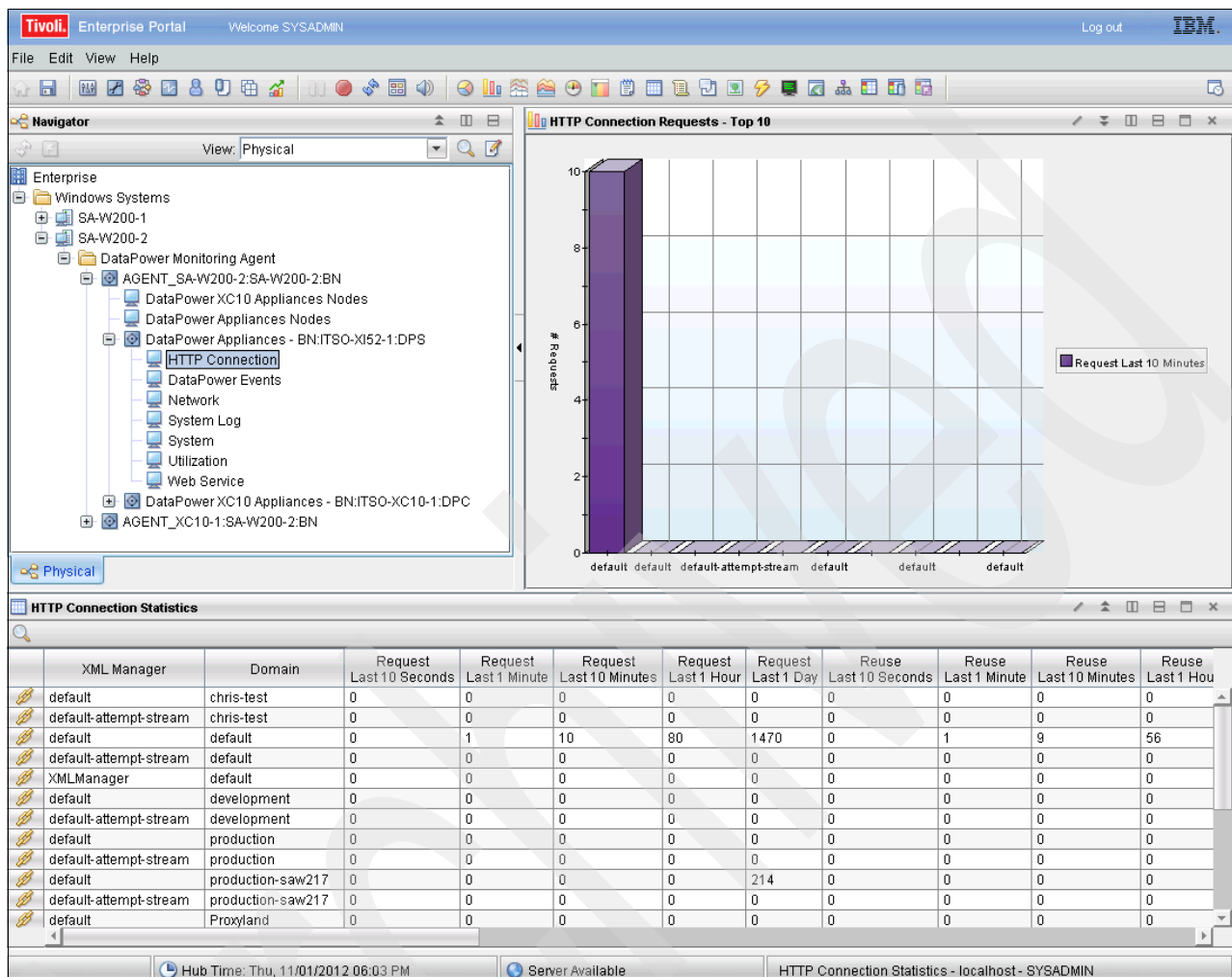


Figure 7-36 HTTP connection workspace for a monitored WebSphere DataPower Appliance

The HTTP connection statistics, which are sorted by domain, have link icons on the left side of the bottom pane.

Figure 7-37 shows the link icons more clearly. Select a domain by clicking one of the link icons.

HTTP Connection Statistics									
	XML Manager	Domain	Request Last 10 Seconds	Request Last 1 Minute	Request Last 10 Minutes	Request Last 1 Hour	Request Last 1 Day	Reuse Last 10 Seconds	Reus Last 1 M
	default	chris-test	0	0	0	0	0	0	0
	default-attempt-stream	chris-test	0	0	0	0	0	0	0
	default	default	0	1	10	80	1470	0	1
	default-attempt-stream	default	0	0	0	0	0	0	0
	XMLManager	default	0	0	0	0	0	0	0
	default	development	0	0	0	0	0	0	0
	default-attempt-stream	development	0	0	0	0	0	0	0
	default	production	0	0	0	0	0	0	0
	default-attempt-stream	production	0	0	0	0	0	0	0
	default	production-saw217	0	0	0	0	214	0	0
	default-attempt-stream	production-saw217	0	0	0	0	0	0	0
	default	Proxyland	0	0	0	0	0	0	0

Figure 7-37 HTTP connection statistics for a monitored WebSphere DataPower Appliance

For this domain (in this example **default** is chosen), a bar chart shows the HTTP connection statistics from the last 10 minutes (Figure 7-38).

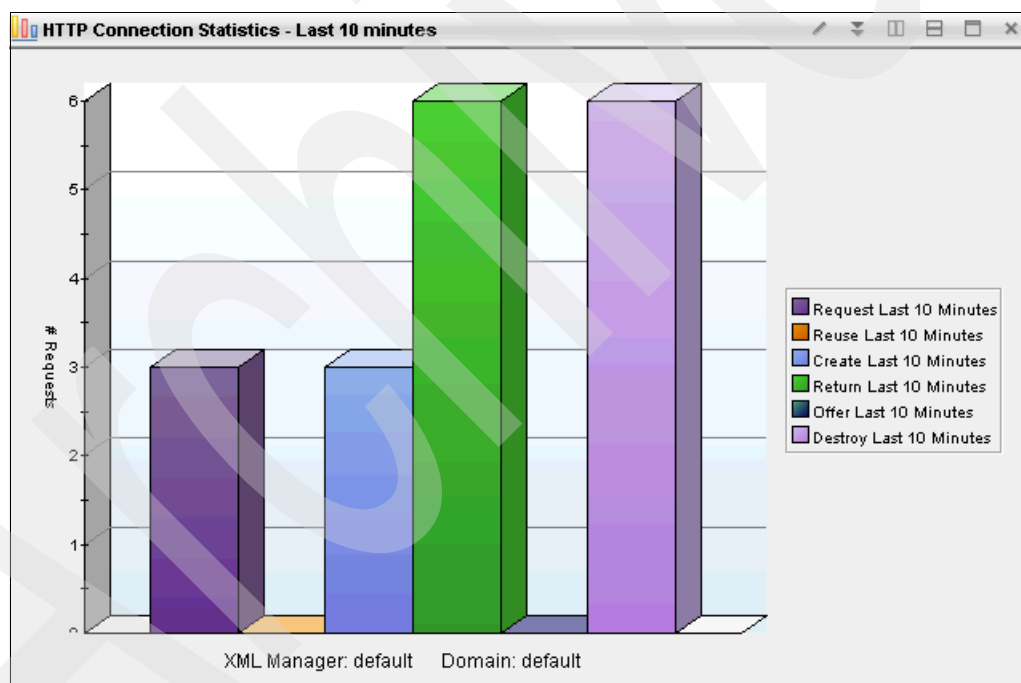


Figure 7-38 HTTP connection statistics (last 10 minutes) for a monitored WebSphere DataPower Appliance

For detailed TCP port information, click **Network** in the Navigator pane. Then, you see a workspace similar to the example in Figure 7-39.

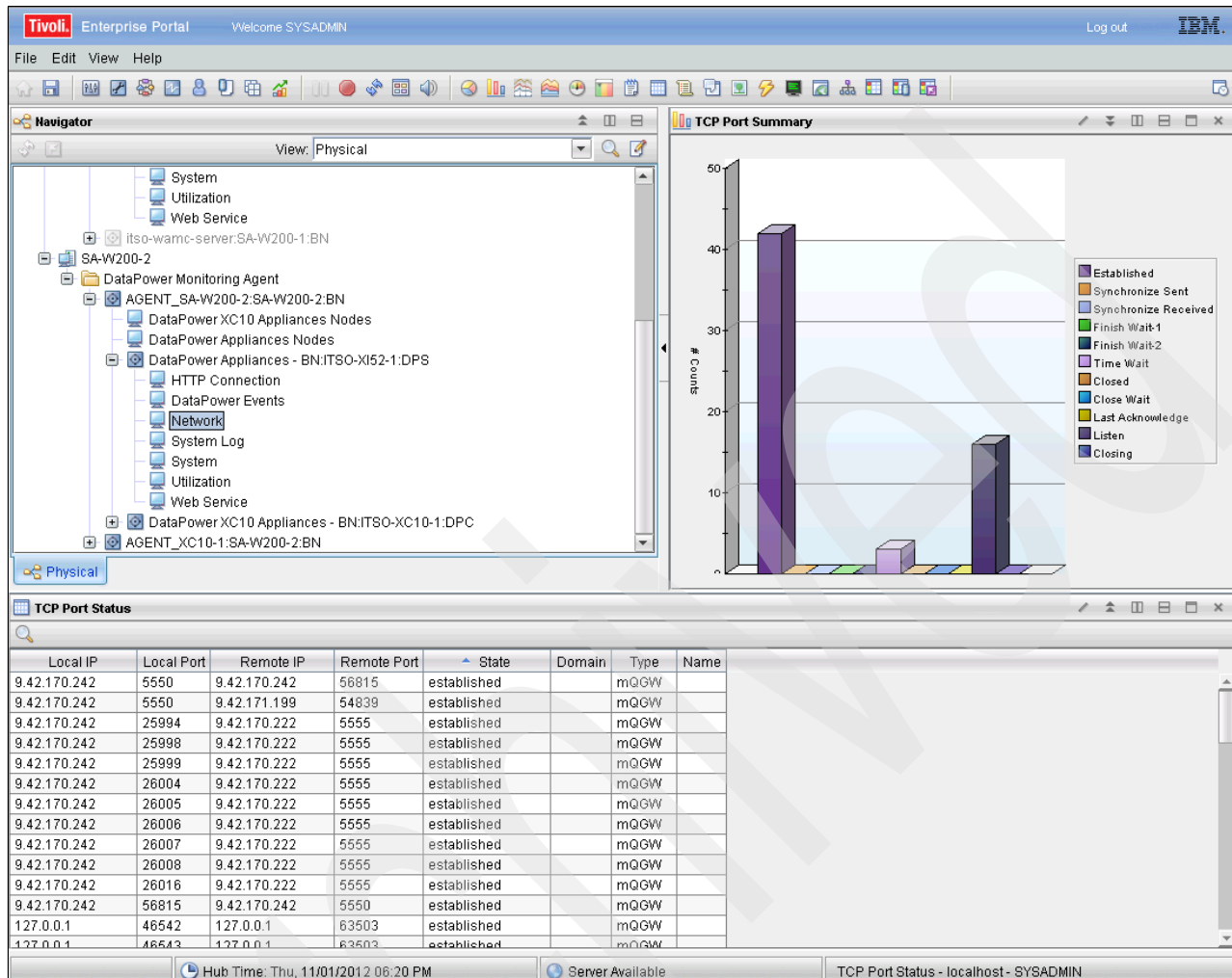


Figure 7-39 Network overview workspace for a monitored WebSphere DataPower Appliance

TCP port status is displayed as a bar chart (Figure 7-40).

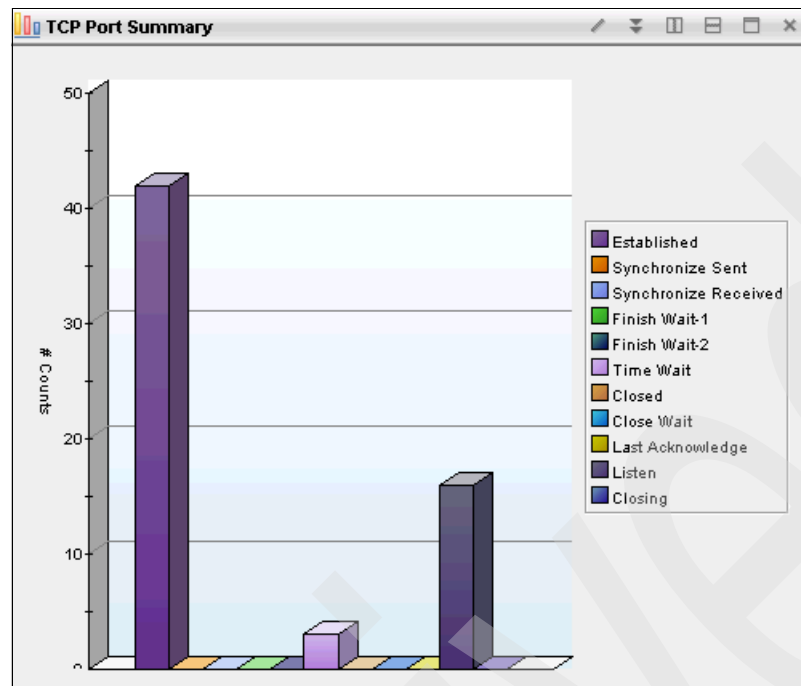


Figure 7-40 TCP port summary panel for a monitored WebSphere DataPower Appliance

A detailed table shows IP addresses and ports, locally and remote (Figure 7-41). The System Log workspace shows log messages, if ITCAM Agent was set up to monitor the logs for this WebSphere DataPower Appliance.

Local IP	Local Port	Remote IP	Remote Port	State	Domain	Type	Name
9.42.170.242	5550	9.42.170.242	56815	established		mQGw	
9.42.170.242	5550	9.42.171.199	54839	established		mQGw	
9.42.170.242	25994	9.42.170.222	5555	established		mQGw	
9.42.170.242	25998	9.42.170.222	5555	established		mQGw	
9.42.170.242	25999	9.42.170.222	5555	established		mQGw	
9.42.170.242	26004	9.42.170.222	5555	established		mQGw	
9.42.170.242	26005	9.42.170.222	5555	established		mQGw	
9.42.170.242	26006	9.42.170.222	5555	established		mQGw	
9.42.170.242	26007	9.42.170.222	5555	established		mQGw	
9.42.170.242	26008	9.42.170.222	5555	established		mQGw	
9.42.170.242	26016	9.42.170.222	5555	established		mQGw	
9.42.170.242	56815	9.42.170.242	5550	established		mQGw	
127.0.0.1	46542	127.0.0.1	63503	established		mQGw	

Figure 7-41 TCP port status for a monitored WebSphere DataPower Appliance

To view detailed information about a domain, click the **System** item in the Navigator pane. Then, you see information similar to the example in Figure 7-42.

Domains Memory Status

Domain	Current (KB)	1 min (KB)	1 to 5 min (KB)	5 to 10 min (KB)	10 to 60 min (KB)	1 to 12 hours (KB)	12 to 24 hours (KB)
Proxyland	0	0	0	0	0	0	0
chris-test	0	0	0	0	0	0	0
default	0	355	361	917	973	973	973
development	0	0	0	0	0	0	0
dfgdfg	0	0	0	0	0	0	0
production	0	0	0	0	0	0	0
production-saw217	0	0	0	0	0	0	5441
staging-saw217	0	0	0	0	0	0	0
test	0	0	0	0	0	0	0
testOnly4SOATeam	0	0	0	0	0	0	0
tutorial-domain	0	0	0	0	0	0	0
versioning-saw217	0	0	0	0	0	0	0

Domain Status

Name	Save Needed	Trace Enabled	Debug Enabled	Probe Enabled	Diag Enabled	Current Command	Quiesce State	Device
Proxyland	off	off	on	off	off			9.42.170.241
chris-test	off	off	off	off	off			9.42.170.241
default	off	off	off	off	off			9.42.170.241
development	off	off	off	off	off			9.42.170.241
dfgdfg	off	off	off	off	off			9.42.170.241
production	off	off	off	off	off			9.42.170.241
production-saw217	off	off	on	on	off			9.42.170.241
staging-saw217	off	off	off	off	off			9.42.170.241
test	off	off	on	off	off			9.42.170.241
testOnly4SOATeam	off	off	off	on	off			9.42.170.241
tutorial-domain	off	off	off	off	off			9.42.170.241
versioning-saw217	off	off	off	off	off			9.42.170.241

Hub Time: Thu, 11/01/2012 06:29 PM Server Available Domain Status - localhost - SYSADMIN

Figure 7-42 System workspace for a monitored WebSphere DataPower Appliance

Figure 7-43 shows the domain memory status table.

Domains Memory Status								
	Domain	Current (KB)	1 min (KB)	1 to 5 min (KB)	5 to 10 min (KB)	10 to 60 min (KB)	1 to 12 hours (KB)	12 to 24 hours (KB)
	Proxyland	0	0	0	0	0	0	0
	chris-test	0	0	0	0	0	0	0
	default	0	355	361	917	973	973	973
	development	0	0	0	0	0	0	0
	dfgdfg	0	0	0	0	0	0	0
	production	0	0	0	0	0	0	0
	production-saw217	0	0	0	0	0	0	5441
	staging-saw217	0	0	0	0	0	0	0
	test	0	0	0	0	0	0	0
	testOnly4SOATeam	0	0	0	0	0	0	0
	tutorial-domain	0	0	0	0	0	0	0
	versioning-saw217	0	0	0	0	0	0	0

Figure 7-43 Domains memory status

Figure 7-44 shows the domain status. Again, you see link icons next to each domain.

Domain Status							
	Name	Save Needed	Trace Enabled	Debug Enabled	Probe Enabled	Diag Enabled	Current Command
	Proxyland	off	off	on	off	off	
	chris-test	off	off	off	off	off	
	default	off	off	off	off	off	
	development	off	off	off	off	off	
	dfgdfg	off	off	off	off	off	
	production	off	off	off	off	off	
	production-saw217	off	off	on	on	off	
	staging-saw217	off	off	off	off	off	
	test	off	off	on	off	off	
	testOnly4SOATeam	off	off	off	on	off	
	tutorial-domain	off	off	off	off	off	
	versioning-saw217	off	off	off	off	off	

Hub Time: Thu, 11/01/2012 06:29 PM
 Server Available
Domain Sta

Figure 7-44 Domain status

For more information about the services in a domain, click a **link** icon in the Domains Memory Status table (pane in the upper right corner in Figure 7-42 on page 182). Here, the default domain is selected, which changes the view to the Utilization window, for this particular domain.

The memory status of each service (top 10) is shown as a bar chart with detailed statistics for each service (Figure 7-45).


Services Memory Status by Domain										
	Type	Name	Current (KB)	1 min (KB)	1 to 5 min (KB)	5 to 10 min (KB)	10 to 60 min (KB)	1 to 12 hours (KB)	12 to 24 hours (KB)	Lifetime (KB)
	XMLFirewallService	example-Firewall	0	355	917	361	973	973	973	1095

Figure 7-45 Services memory status by domain

Click the **link** icon for a service. Here, an XML firewall service that is called **example-Firewall** is selected. The services memory status for this service is displayed as a bar chart (Figure 7-46).

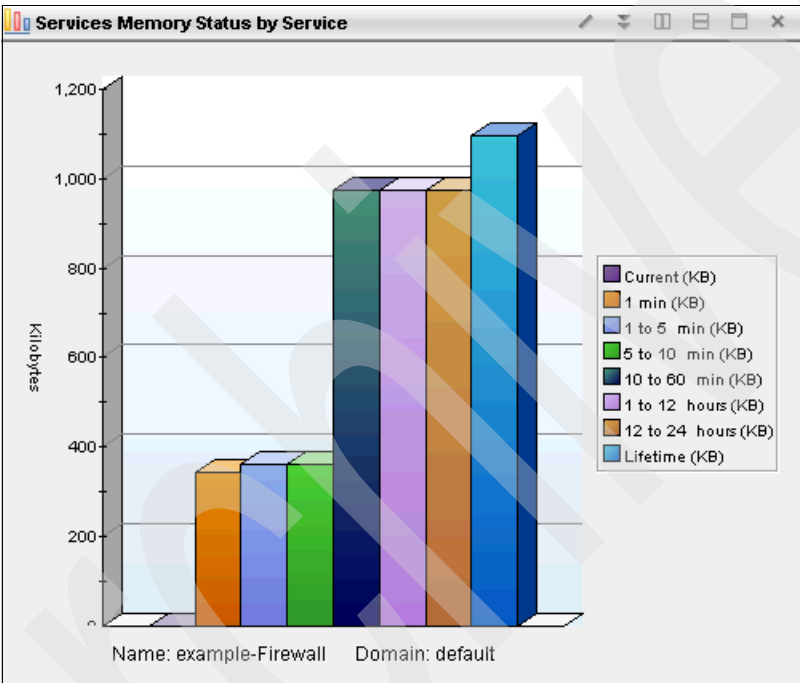


Figure 7-46 Services memory status by service

If a link icon is clicked in the Domain Status table (for a particular domain), the Active Services and Object Status tables are displayed. Figure 7-47 shows the table for the default domain.

Of note are the default ports for the XML management interface, which the management component of WebSphere Appliance Management Center connects on, and 9090 for the web GUI. The objects that are listed include cryptographic certificates and keys and Ethernet ports on the WebSphere DataPower Appliance. Therefore, the status of these ports on the WebSphere DataPower Appliance can be determined.

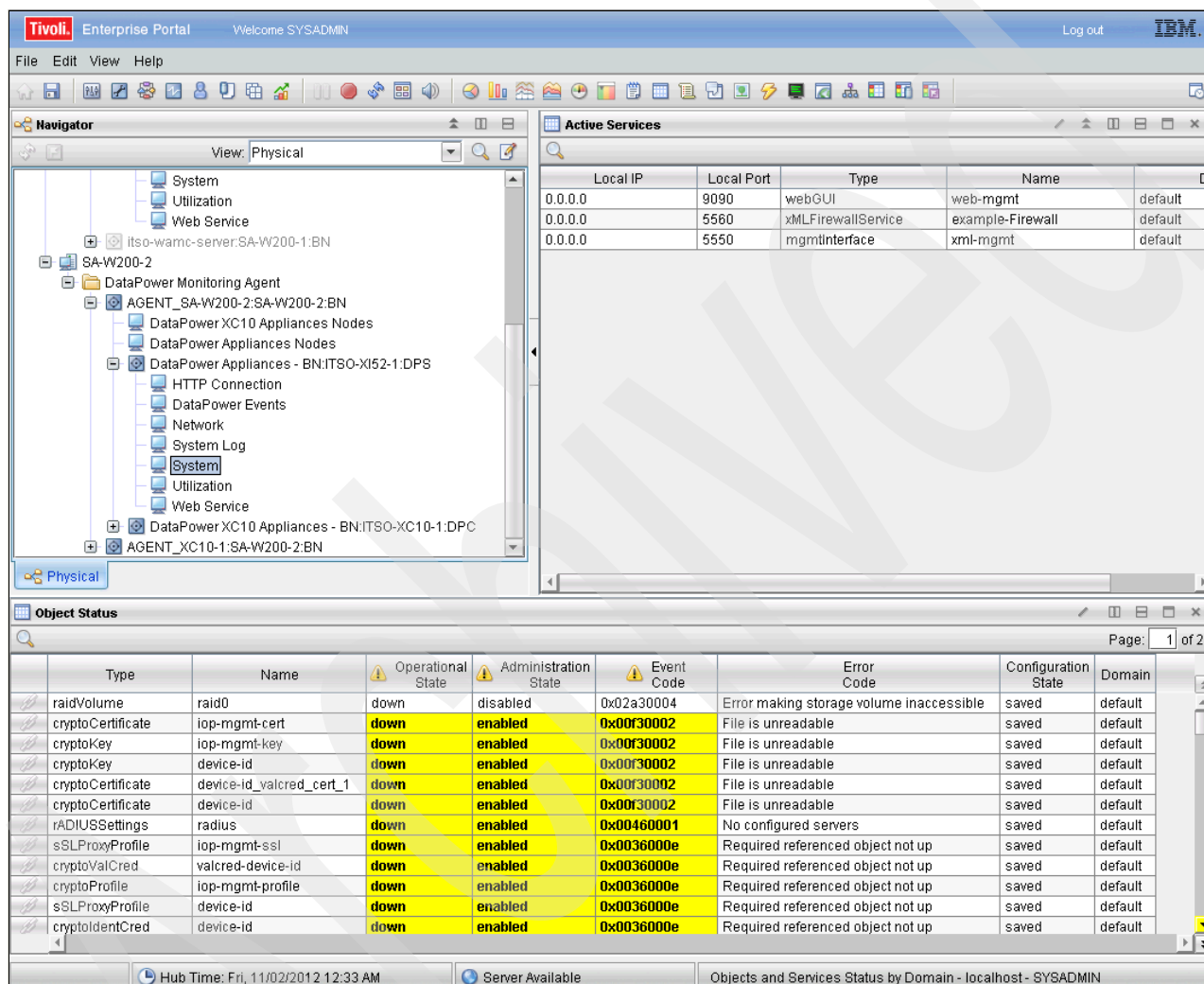


Figure 7-47 System workspace for a domain that shows object status and active services

By selecting the Utilization workspace directly, in addition to system usage and CPU usage for that WebSphere DataPower Appliance, filesystem usage is also shown (Figure 7-48).

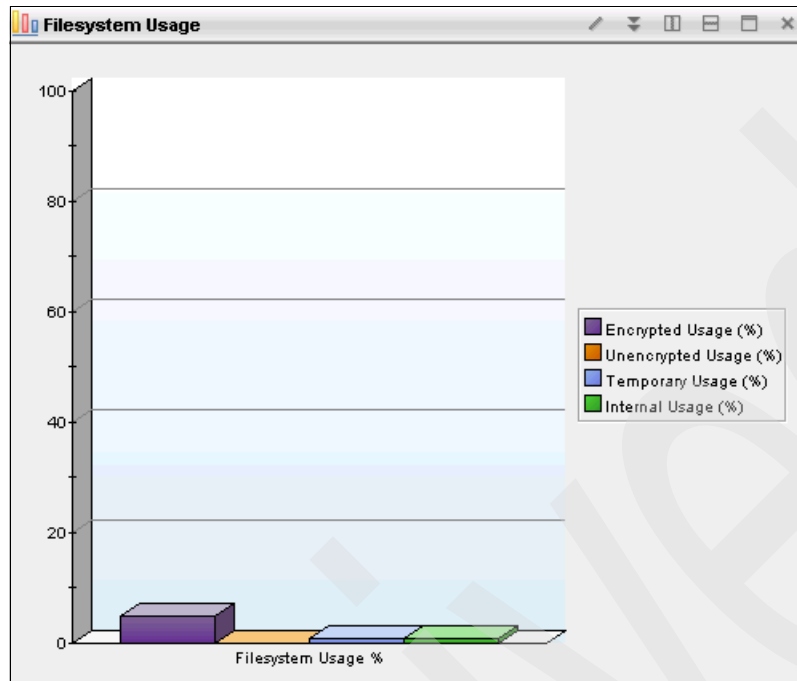


Figure 7-48 Filesystem Usage panel for a monitored WebSphere DataPower Appliance

Troubleshooting

As with all software, occasionally you might experience issues when you use IBM WebSphere Appliance Management Center for WebSphere Appliances. This chapter highlights some of the most common issues and provides information about how to resolve them. This chapter also includes hints and tips included to assist with day-to-day usage of WebSphere Appliance Management Center.

This chapter includes the following sections:

- ▶ Issues with the installer
- ▶ Issues with the graphical user interface
- ▶ Issues with WebSphere DataPower Appliances
- ▶ Issues with firmware
- ▶ Logging and trace
- ▶ Technotes
- ▶ Other hints and tips

8.1 Issues with the installer

This section covers issues that can occur when you install WebSphere Appliance Management Center. Follow the guidance in this section if you are experiencing the following situations:

- ▶ Unable to install WebSphere Appliance Management Center
- ▶ Looking for more information about the installation process
- ▶ Unable to uninstall WebSphere Appliance Management Center

8.1.1 Problems running the installer

As listed in 1.7, “Ordering information” on page 16, WebSphere Appliance Management Center is supported on multiple platforms and operating systems. All supported platforms are 64-bit. If you attempt to install on a 32-bit platform, you see one of the following messages based on your environment:

- ▶ On Linux and AIX, the installer fails to start with an error message similar to the following example:

```
./install.bin: line 3320:  
/tmp/install.dir.9187/Linux/resource/jre/jre/bin/java: cannot execute binary  
file
```
- ▶ On Windows, the installer fails to start with an error message similar to the following example:
Windows error 216 occurred while loading the Java VM

Ensure that you downloaded the correct version of WebSphere Appliance Management Center for your operating system. Table 8-1 lists the supported operating systems and the correct installation archive to use.

Table 8-1 Operating systems and matching installation archive file

Operating system	Install archive file
Windows	WAMC_YYYY-MM-DD_Win64.zp
Linux on x86	WAMC_YYYY-MM-DD_LinuxX64.tar.gz
Linux on System Z (mainframe)	WAMC_YYYY-MM-DD_Linux_z64.tar.gz
AIX	WAMC_YYYY-MM-DD_AIXPC64.tar.gz

8.1.2 Installer log files

If the installation of WebSphere Appliance Management Center fails, a log file is created in the one of the following directories based on your environment:

- ▶ Microsoft Windows Server:
`<user_home>\desktop\WebSphere_Appliance_Management_Center_Install_<date>.log`
- ▶ AIX and Linux:
`<temp_dir>\WebSphere_Appliance_Management_Center_Install_<date>.log`

When the installation of WebSphere Appliance Management Center is successful, an installation log file is created in the `<WAMC_install_dir>\Installer\Logs` directory. In this directory, `<WAMC_install_dir>` is the location where WebSphere Appliance Management Center was installed.

8.1.3 Problems running the uninstaller

You can uninstall WebSphere Appliance Management Center by using the uninstaller program in the <WAMC_install_dir>/Installer directory.

In some situations, the uninstaller might fail to function correctly. For information about how to manually uninstall the product, see the WebSphere Appliance Management Center Information Center at:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/uninstall_management_component_manual.html

8.2 Issues with the graphical user interface

This section deals with issues loading the WebSphere Appliance Management Center graphical user interface (GUI). Follow the guidance in this section if you are unable to perform the following tasks:

- ▶ Load the WebSphere Appliance Management Center GUI
- ▶ Log in to the GUI

When you start the WebSphere Appliance Management Center server, you see a message, which confirms that the server is started. If you attempt to access the GUI, you see an error message, which states that the page cannot be found. This error occurs because, while the application server that hosts WebSphere Appliance Management Center is started, the application is not yet fully deployed. Wait a few minutes, and then try to load the page again.

8.2.1 Verifying the server address that is used

You can access the management component of WebSphere Appliance Management Center through your web browser by going to the following server address:

`https://servername:9443/wamc`

Where `servername` is the hostname alias or IP address that uniquely identifies the machine that is running your WebSphere Appliance Management Center installation.

The default port that the WebSphere Appliance Management Center server runs on is 9443. This port is configurable when you install WebSphere Appliance Management Center. If you forget which port you specified at installation time, you can find the port number in the <WAMC_install_dir>/server/usr/servers/runtime/bootstrap.properties file.

Attention: The `bootstrap.properties` file contains important configuration settings for WebSphere Appliance Management Center and is *not* intended to be modified. All modifiable configuration settings are in the `config` directory under the top-level WebSphere Appliance Management Center installation directory.

WebSphere Appliance Management Center is accessed by using HTTPS. If you attempt to connect to WebSphere Appliance Management Center by using HTTP, you see “The connection was reset” error message (Figure 8-1).

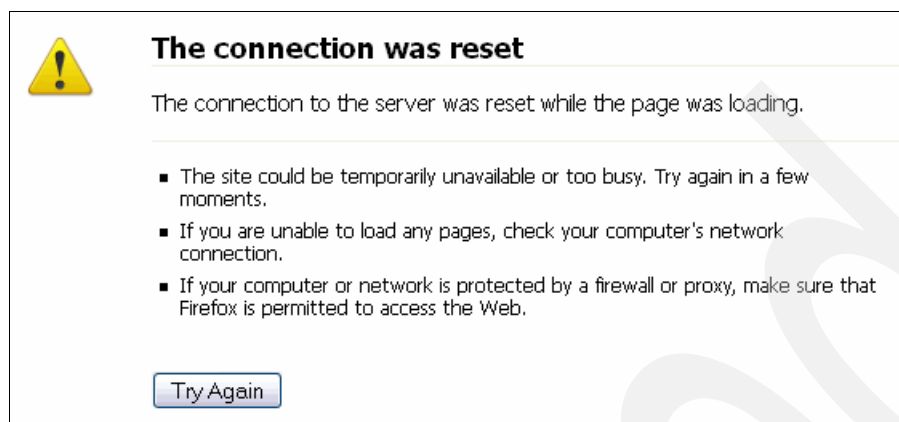


Figure 8-1 Failure to connect to WebSphere Appliance Management Center when using HTTP

8.2.2 Checking the state of the server

Attention: The actions that are described in this section require direct login access to the server that hosts WebSphere Appliance Management Center. If you do not have access to this server, contact the administrator of the server for assistance.

On the server that hosts your WebSphere Appliance Management Center installation, check to see if the server process is still running. Choose one of the following options, depending on your server:

- ▶ On Windows Server 2008 and Windows Server 2008 R2:
 - a. Start the Task Manager.
 - b. Select **View** → **Select columns**.
 - c. Ensure that **Command Line** is selected, and click **OK**.
 - d. Look for a Java process with a command line that ends with **ws1aunch.jar runtime**. This part is the WebSphere Appliance Management Center server process.
- ▶ On Linux, Linux on System z, and AIX:
 - a. Locate the server process by using one of the following options:
 - When the server is running, a file that contains the process ID of the server process is written to the `<WAMC_install_dir>/server/usr/servers/.pid/runtime.pid` file. Use the **ps <process id>** command to see if the process is still running.
 - Obtain a list of running processes. For example, enter the **ps -ax** command.
 - b. Look for a Java process with a command line that ends with **ws1aunch.jar runtime**. This part is the WebSphere Appliance Management Center server process.

If you cannot find a WebSphere Appliance Management Center process, the server process is no longer running. Use the **start-wamc** command in the installation directory of WebSphere Appliance Management Center to start the server again.

If the WebSphere Appliance Management Center server is still running, the server logs might contain information or error messages that can help determine the cause of the problem.

when connecting to the server. For information about logging and trace, see 8.4, “Issues with firmware” on page 197.

If the server logs do not show any obvious errors, check the status of the server process. Locate the WebSphere Appliance Management Center server process, and check to see whether the process is using large amounts of CPU time or memory resource.

Figure 8-2 shows the Task Manager on a Windows 2008 R2 server where the WebSphere Appliance Management Center process is using no CPU resource and around 570 MB of memory. In this case, the server was not under load. These values are not typical values. The values that are reported by your server might vary.

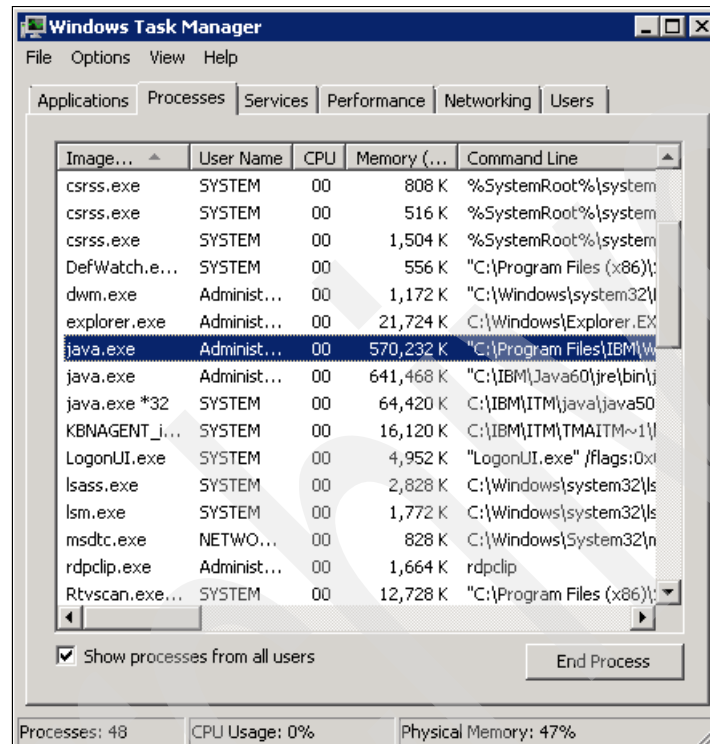


Figure 8-2 WebSphere Appliance Management Center server process

If the server is using excessive amounts of CPU time or memory, this reason might be because of an increased load on the server. If so, CPU usage should decrease as existing requests are completed. Memory usage also naturally fluctuates over time and is capped at 2 GB. If all of the 2 GB of allocated memory is used and no memory can be freed, the Java process reports an error to the WebSphere Appliance Management Center log and creates Java diagnostic files. This error is referred to as an *Out Of Memory (OOM)* error. If this situation happens, use the log files and the diagnostic files to open an issue with IBM Support.

Excessive CPU usage and OOM issues cause the WebSphere Appliance Management Center to become unresponsive. In most cases, you can stop the server and start it again to resolve the problem. If the issue continues, contact IBM Support for more support.

8.2.3 Web browser problems

Check whether your web browser is supported by WebSphere Appliance Management Center. You can find a list of supported browsers in the WebSphere Appliance Management Center Information Center at:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/software_reqs.html

In some cases, the user interface fails to process requests correctly. For example, you might complete the field in the Create Domain window, but do not receive any feedback that indicates that the process of creating the domain started. This issue is rare. However, if you experience an issue where the user interface fails to respond to an action or appears to accept input, but then fails to complete the selected action, check your web browser's JavaScript error console.

The web browser JavaScript error console might contain further information but is typically not human readable. Nevertheless, a WebSphere Appliance Management Center developer can use the error message from the console, the information about the action that is attempted, and the web browser version information to track down and fix problems of this kind. In rare cases where a JavaScript error occurs that prevents you from using WebSphere Appliance Management Center correctly, contact IBM support for further assistance.

JavaScript errors: In most cases, JavaScript errors indicate that an unsupported web browser is being used. If you see JavaScript errors, verify that your web browser is supported. Some web browsers, particularly Mozilla Firefox, might periodically automatically update.

8.2.4 Checking the login credentials

If you are unable to log in to WebSphere Appliance Management Center because your password was rejected, you might need to reset your password. You can reset your password by using either of the following methods, depending on the configuration of your WebSphere Appliance Management Center installation:

- ▶ If you are using LDAP as the user registry, reset your password by using the standard mechanism that is defined by your organization.
- ▶ If you are using the simple file-based user registry, request a password reset. The administrator of the WebSphere Appliance Management Center can set up a new password for you. For information about the file-based user registry, see 2.4.1, "Managing users by using the local repository" on page 33.

If you are unable to log in to WebSphere Appliance Management Center with your correct user name and password, you might not be assigned to one of the standard user groups. A user cannot log in to WebSphere Appliance Management Center if the user is not assigned to the SystemAdministrators, SolutionDeployers, or SystemOperators groups. For information about adding a user to a user group, see 2.4, "Managing users and roles" on page 32.

If the user name and password are correct, the user is a member of a group, and the problem still persists, you can go back to a previous version of the `userRegistry.xml` and `roleMapping.xml` (from your backup). Then, try to start the WebSphere Appliance Management Center again.

In a worst-case scenario, you can import the default file, either `userRegistry.xml` and `roleMapping.xml`, when the WebSphere Appliance Management Center is installed.

As shown in Example 8-1, you can see the default `userRegistry.xml` file. Make a backup copy of your current version of this file.

Example 8-1 Default userRegistry.xml file

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
  <basicRegistry id="wamcRegistry">
    <group name="SystemAdministrators">
      <member name="wamcadmin"/>
    </group>
    <group name="SystemOperators">
      <member name="wamcadmin"/>
    </group>
    <group name="SolutionDeployers">
      <member name="wamcadmin"/>
    </group>
    <user name="wamcadmin" password="need2change"/>
  </basicRegistry>
</server>
```

Default userRegistry.xml file: When you use the default `userRegistry.xml` file to log in to the console, you must use `wamcadmin` as the user name and `need2change` as the password. If required, you can change this password as explained in “Changing a user password” on page 37.

As shown in Example 8-2, you can see the default `roleMapping.xml` file. Make a backup copy of your current version of this file.

Example 8-2 Default roleMapping.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
  <application id="wamc" location="wamc.war">
    <application-bnd>
      <security-role name="SolutionDeployer">
        <group name="SolutionDeployers" />
      </security-role>
      <security-role name="SystemAdministrator">
        <group name="SystemAdministrators" />
      </security-role>
      <security-role name="SystemOperator">
        <group name="SystemOperators" />
      </security-role>
    </application-bnd>
  </application>
</server>
```

After you set WebSphere Appliance Management Center to use the default XML files, start WebSphere Appliance Management Center (see 2.2, “Starting and stopping WebSphere Appliance Management Center” on page 29). Then, try to log in again.

8.3 Issues with WebSphere DataPower Appliances

This section addresses common issues with the connection between WebSphere DataPower Appliances and WebSphere Appliance Management Center. Follow the guidance in this section if you are experiencing the following situations:

- ▶ Unable to add WebSphere DataPower Appliances to WebSphere Appliance Management Center
- ▶ Unable to retrieve the properties of WebSphere DataPower Appliances or properties, such as status or firmware level, are displayed as a blank or with question mark symbols
- ▶ Unable to perform actions on WebSphere DataPower Appliances

8.3.1 Checking the WebSphere DataPower Appliance and firmware support

Many WebSphere DataPower Appliance models and types are available, but not all of them are supported by WebSphere Appliance Management Center, particularly for much older models and newer models. Support for a new WebSphere DataPower Appliance model is typically added to the next release of WebSphere Appliance Management Center after the WebSphere DataPower Appliance model is shipped. For the current complete list of supported WebSphere DataPower Appliances, see the WebSphere Appliance Management Center Information Center at:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/supported_appliances.html

Similarly, many versions of WebSphere DataPower firmware are available. For information about firmware versions that are supported by WebSphere Appliance Management Center, see the WebSphere Appliance Management Center Information Center at the previous web address.

Some actions in the WebSphere Appliance Management Center GUI are available only when you use certain WebSphere DataPower Appliances or firmware versions:

- ▶ When managing the IBM WebSphere DataPower XC10 Appliance, the only available actions in the WebSphere Appliance Management Center GUI are deploying the firmware and rebooting the appliance.
- ▶ All service-level actions require a WebSphere DataPower Appliance to run firmware version 5.0.0.0 or later. Services that are running on WebSphere DataPower Appliances with older firmware versions cannot be managed from the WebSphere Appliance Management Center GUI.

8.3.2 Checking the connection to the WebSphere DataPower Appliance

If an error occurs when you add a WebSphere DataPower Appliance to WebSphere Appliance Management Center, you can find more information about the error by clicking the **Show detail** link. This link provides an error message that gives hints about the problem and how to solve it. If more technical information is required, for example to see the stack trace of the root cause of the issue, click **Additional technical information**.

Figure 8-3 shows an error message when adding a WebSphere DataPower Appliance.

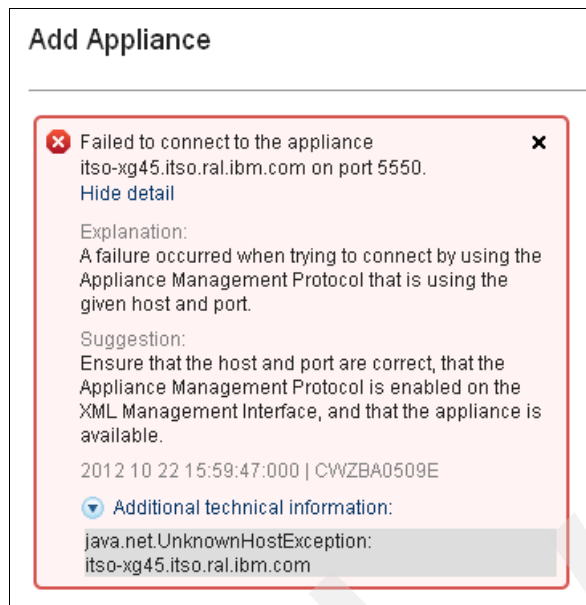


Figure 8-3 Error message when adding a WebSphere DataPower Appliance

In Figure 8-3, the error was that the WebSphere DataPower Appliance host name was invalid. If the host name that is entered is correct, verify that you can access the WebSphere DataPower Appliance from the machine that hosts WebSphere Appliance Management Center. Open a terminal or shell on the machine that hosts WebSphere Appliance Management Center and try to use the **ping** command to ping the WebSphere DataPower Appliance. If the **ping** command works normally:

- ▶ On Windows, try to access the WebSphere DataPower Appliance web GUI by using your web browser.
- ▶ On UNIX, try to use Secure Shell (SSH) to access the WebSphere DataPower Appliance command-line interface (CLI).

If you can connect to the WebSphere DataPower Appliance by using either method from the machine that is hosting WebSphere Appliance Management Center, the issue is not with the connection between the server host and the WebSphere DataPower Appliance.

Communication between WebSphere Appliance Management Center and the WebSphere DataPower Appliance might be blocked by firewalls. If your network environment contains firewalls, for information about firewall configuration settings, see 8.3.5, "Setting up firewalls" on page 197.

Finally, the system log on the WebSphere DataPower Appliance might contain more information as described in 8.5.3, "The WebSphere DataPower Appliance system log" on page 205.

8.3.3 Checking the configuration of the XML management interface

WebSphere Appliance Management Center uses the XML management interface of the WebSphere DataPower Appliances. If the XML management interface is disabled, WebSphere Appliance Management Center cannot communicate with the WebSphere DataPower Appliance.

To check the status of the XML management interface:

1. Log on to the WebSphere DataPower web GUI for the WebSphere DataPower Appliance. You must log on to the *default domain*.
2. From the Control panel, select **Objects** → **Device Management** → **XML Management Interface**.
3. In the Configure XML Management Interface window (Figure 8-4):
 - a. Make sure that the Administrative State of the XML management interface is set to **enabled**.

Tip: Also check that the AMP Endpoint is enabled.

- b. Check that the Port Number setting matches the port number that was entered in the Add Appliance window in WebSphere Appliance Management Center. The default port number is 5550.
 - c. Apply and save any changes.

Configure XML Management Interface

main Advanced SLM

XML Management Interface [up]

Apply Cancel Undo

Administrative State ☒ enabled ☐ disabled

Local IP Address 0.0.0.0 Select Alias *

Port Number 5550 *

Access Control List xml-mgmt + ...

Comments

Enabled Services

- ☒ SOAP Management URI
- ☒ SOAP Configuration Management
- ☒ SOAP Configuration Management (v2004)
- ☒ AMP Endpoint
- ☒ SLM Endpoint
- ☒ WS-Management Endpoint
- ☐ WSDM Endpoint
- ☐ UDDI Subscription
- ☒ WSRR Subscription

Figure 8-4 Configuring the XML Management Interface in the WebSphere DataPower web GUI

- d. If the basic XML management interface configuration appears to be correct, check whether a custom SSL proxy profile is being used to secure the communication with

the XML management interface. From the configuration window (Figure 8-4 on page 196), click the **Advanced** tab.

If Custom SSL Proxy Profile is set to **(none)**, no SSL proxy profile is being used and no further configuration is required. If an SSL Proxy is being used, for instructions about how to create a custom truststore, see the WebSphere Appliance Management Center Information Center at:

http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/topic/com.ibm.wamc.doc/truststore_config.html

8.3.4 Checking the login credentials

Incorrect login credentials can also prevent WebSphere Appliance Management Center from establishing a connection to a WebSphere DataPower Appliance. Make sure that you can log on to the web GUI for the WebSphere DataPower Appliance by using the same user name and password that WebSphere Appliance Management Center is using.

The password for the admin user is reset to a default value after a WebSphere DataPower Appliance level restore operation. If you are using the admin user in WebSphere Appliance Management Center, log on to the WebSphere DataPower Appliance web GUI and change the password. Make sure that the password that is defined in WebSphere Appliance Management Center matches the password that is used on the WebSphere DataPower Appliance.

8.3.5 Setting up firewalls

The WebSphere Appliance Management Center server uses the basic ports as described in 2.3, “Default ports” on page 31. The network administrator must grant communication between the basic ports.

Important: The network administrator must grant the port communication according to the flow (source and destination).

If changes occurred on the default ports during the installation of WebSphere Appliance Management Center or during the configuration of WebSphere Appliances the WebSphere Appliance Management Center, the administrator must inform the network administrator about the correct ports to open.

8.4 Issues with firmware

WebSphere DataPower Appliance firmware is refreshed regularly and is updated to include fixes and updates to appliance functionality. As described in Chapter 4, “Firmware management” on page 67, changing the level of the firmware that is deployed to a WebSphere DataPower Appliance can introduce new issues. This section describes issues that can occur when you use WebSphere Appliance Management Center to manage the firmware upgrade process for your WebSphere DataPower Appliances.

Follow the guidance in this section if you are experiencing the following situations:

- ▶ Unable to add firmware to the WebSphere Appliance Management Center repository
- ▶ Unable to find applicable firmware for your WebSphere DataPower Appliance
- ▶ Unable to deploy firmware to a WebSphere DataPower Appliance

8.4.1 Problems adding firmware to the repository

As explained in Chapter 4, “Firmware management” on page 67, firmware images are downloaded from IBM Fix Central and added to the repository in WebSphere Appliance Management Center. The repository stores uploaded firmware images on a disk on the server that hosts your WebSphere Appliance Management Center installation. The **Repository** tab in the WebSphere Appliance Management Center user interface provides a view of the firmware images that are stored in the repository.

When you add firmware images to WebSphere Appliance Management Center, a possible problem is that insufficient disk space is available to store the firmware images. WebSphere DataPower firmware image files can be large. If WebSphere Appliance Management Center is used to store many firmware files, the repository can grow to fill all of the available space on the disk. Figure 8-5 shows the error message in WebSphere Appliance Management Center when you attempt to add firmware to the repository when the disk is full.

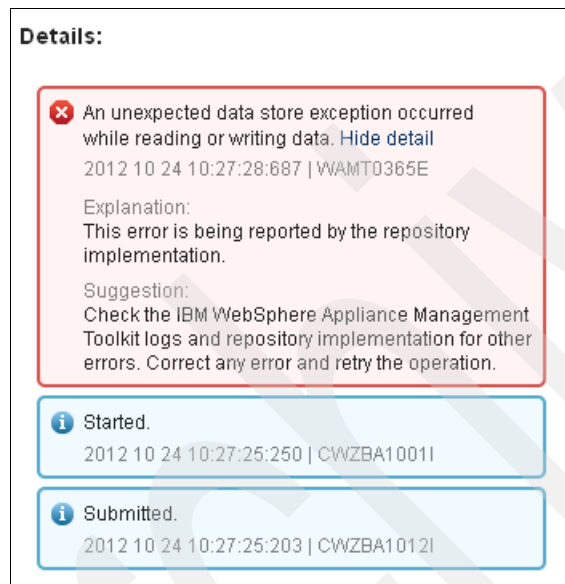


Figure 8-5 Error message when you add a firmware to the repository when the disk is full

The error message that is displayed is generic and directs you to examine the WebSphere Appliance Management Center logs for further information. For information about these logs, see 8.5, “Logging and trace” on page 203.

If this error occurs, the trace log contains the additional information that you need to diagnose the problem. Example 8-3 shows the relevant section of the trace log for this error.

Example 8-3 Trace log for adding a firmware image to the repository when the disk is full

```
[10/24/12 10:27:28:343 EDT] 00000061 id=
m.ibm.datapower.wamt.dataAPI.local.filesystem.RepositoryImpl 2 saveBlobToFile THROW
java.io.IOException: There is not enough space on the disk.
    at sun.nio.ch.FileDispatcherImpl.write0(Native Method)
    at sun.nio.ch.FileDispatcherImpl.write(FileDispatcherImpl.java:83)
    at sun.nio.ch.IOUtil.writeFromNativeBuffer(IOUtil.java:101)
    at sun.nio.ch.IOUtil.write(IOUtil.java:72)
    at sun.nio.ch.FileChannelImpl.write(FileChannelImpl.java:207)
    at com.ibm.datapower.wamt.dataAPI.local.filesystem.RepositoryImpl.saveBlobToFile(RepositoryImpl.java:1254)
```

```

at
com.ibm.datapower.wamt.dataAPI.local.filesystem.StoredFirmwareVersionImpl.<init>(StoredFirmwareVersionImpl.
java:104)
at
com.ibm.datapower.wamt.dataAPI.local.filesystem.RepositoryImpl.createFirmwareVersion(RepositoryImpl.java:819)
at com.ibm.datapower.wamt.clientAPI.FirmwareVersion.<init>(FirmwareVersion.java:186)
at com.ibm.datapower.wamt.clientAPI.AddFirmwareTask.execute(AddFirmwareTask.java:159)
at com.ibm.datapower.wamt.clientAPI.QueueProcessor.process(QueueProcessor.java:451)
at com.ibm.datapower.wamt.clientAPI.QueueProcessor.run(QueueProcessor.java:145)
at java.lang.Thread.run(Thread.java:777)

```

8.4.2 Problems matching firmware to a WebSphere DataPower Appliance

As described in 4.4, “Deploying the firmware” on page 77, when deploying firmware to a WebSphere DataPower Appliance by using WebSphere Appliance Management Center, the repository is searched for images that match the selected WebSphere DataPower Appliance. When you use the Deploy Firmware function in WebSphere Appliance Management Center, you might be informed that no firmware images match the chosen WebSphere DataPower Appliances. Figure 8-6 shows the WebSphere Appliance Management Center user interface in this situation.

Deploy Firmware

Set the target firmware:

☐ List upgrades only

☒ List all compatible firmware versions

Specify the firmware version: [?](#) (None available) ▼

Summary:

Appliance Name	Appliance Type	Appliance Mode	Current Firmware	Target Firmware
itso-xb62	XB62	7199	4.0.2.0	(None available) ❌

☐ I accept the terms in the license agreements.

Note: After you click **Deploy**, you cannot stop this operation.

Deploy **Cancel**

Figure 8-6 No matching firmware images for the selected WebSphere DataPower Appliance

In this situation, check the following items:

1. Is the WebSphere DataPower Appliance supported?

For a list of supported WebSphere DataPower Appliance types and models, see 1.5, “Supported WebSphere DataPower Appliances” on page 8.

2. Is the firmware level supported?

For a list of supported firmware versions, see 1.5, “Supported WebSphere DataPower Appliances” on page 8.

3. Is the firmware image a match for the WebSphere DataPower Appliance?

For information about finding the correct firmware image for your WebSphere DataPower Appliance, see 4.1.2, “Identifying and downloading firmware images” on page 68. Pay attention to feature licenses because WebSphere Appliance Management Center does not consider a firmware image to match your WebSphere DataPower Appliance unless the feature licenses match correctly. In particular, you cannot deploy firmware with fewer features than the WebSphere DataPower Appliance.

If checking the previous items does not resolve the problem, enable trace logging as explained in 8.5.2, “Trace in WebSphere Appliance Management Center” on page 204, and start the Deploy Firmware action again. Example 8-4 shows an excerpt from the trace log immediately after opening the Deploy Firmware window.

Example 8-4 Trace log excerpt that shows firmware matching being attempted

```
[10/24/12 10:54:50:172 EDT] 00006cb1 id=
com.ibm.datapower.wamt.clientAPI.Firmware                > assertCompatibility
ENTRY
Firmware[XI50:9003:SQL-ODBC_6.0;Tibco-EMS_5.1.5;:DataGlue;JAXP-API;PKCS7-SMIME;HSM
;XG4;Compact-Flash;iSCSI;RaidVolume;LocateLED;IPMI;AppOpt;MQ_7.0.1.1;TAM_6.0;WebSp
here-JMS_1.2.3;] null DeviceType[XB62] ModelType[7199]
StringCollection[MQ,DataGlue,JAXP-API,PKCS7-SMIME,SQL-ODBC,WebSphere-JMS,RaidVolum
e,iSCSI,LocateLED,IPMI,RaidVolumeSr,IntrusionDetection,IPMI-LAN]
[10/24/12 10:54:50:172 EDT] 00006cb1 id=
com.ibm.datapower.wamt.clientAPI.Firmware                2 assertCompatibility
THROW
com.ibm.datapower.wamt.clientAPI.DeviceTypeIncompatibilityException: WAMT0047E:
The XI50 appliance type for the firmware does not match the XB62 appliance.
```

When the Deploy Firmware window is opened, WebSphere Appliance Management Center searches the repository. It attempts to determine whether each of the firmware images that is stored there is compatible with any of the WebSphere DataPower Appliances that are selected for the firmware deployment. All firmware images in the repository are checked for each WebSphere DataPower Appliance that is selected.

With trace enabled, each firmware compatibility check is printed to the log file so that you can determine why the firmware is not considered a match for the WebSphere DataPower Appliance. As shown in Example 8-4, the firmware image match fails because the WebSphere DataPower Appliance type of the firmware, XI50, does not match the WebSphere DataPower Appliance type of the appliance, XB62.

8.4.3 Problems deploying firmware

Occasionally, you might experience issues with deploying a firmware image to the target WebSphere DataPower Appliance. For suggestions about predeployment actions to take to ensure that the firmware deployment works correctly, see 4.2, “Hints and tips before you upgrade the firmware” on page 71. Pay attention to ensuring that sufficient space is available on the file system of the WebSphere DataPower Appliance to accommodate the firmware image.

A bug is in some older versions of the WebSphere DataPower firmware that prevents the firmware deployment process from working correctly in WebSphere Appliance Management Center. See the following technote, which describes this issue and provides a worked around:

<http://www.ibm.com/support/docview.wss?uid=swg21567828>

8.4.4 Unable to connect to web GUI or SSH after upgrading firmware

If you are using a custom certificate or authentication for the management services and any of the associated certificates are expired, you might be unable to connect to a WebSphere DataPower Appliance with the web GUI or SSH after upgrading the firmware. In firmware upgrade situations, expired pubcert:/// certificates are not part of the upgrade image.

Expired certificates: Certificates that have expired in the pubcert: directory are not included in the image.

To verify that the network is functioning correctly, enter the following WebSphere DataPower Appliance commands:

```
# show int
# show int mode
# show route
```

These commands show you whether any network activity is occurring and the Ethernet link speed. After the network is confirmed, the quickest way to recover the web management and SSH services is to delete and recreate them with the default settings by using the serial console.

Use the WebSphere DataPower CLI commands that are shown in Example 8-5 to reset the RBMs, ACLs, web GUI, and SSH services to the default settings.

SSH: If SSH is working, you might want to omit any commands that are associated with the SSH.

Example 8-5 Resetting the RBMs, ACLs, web GUI, and SSH services to the default settings

```
config
no web-mgmt
no ssh
rbm
reset
exit
acl web-mgmt
reset
exit
acl ssh
reset
exit
write mem (key step to remove the current settings)
y
web-mgmt <ip to listen on or 0.0.0.0 for all> <port to use default is 9090>
ssh <ip to listen on or 0.0.0.0 for all> <port to use default is 22>
write mem
y
```

After the default settings are reset, test the service and confirm that you can now access the WebSphere DataPower Appliance. You can then configure any custom certificates or authentication settings that are required.

8.4.5 Management Information Base changes in firmware

Changes to the Simple Network Management Protocol (SNMP) Management Information Base (MIB) files can occur between firmware versions. Certain SNMP MIBs become obsolete between firmware versions because of incompatible SNMP changes. The SNMP MIB files document the obsolete entries, replacements, and other changes. Check the description that is provided in the enterprise MIB files on the WebSphere DataPower Appliance.

Example 8-6 shows an obsolete network status that changed with WebSphere DataPower firmware 5.0.0.0.

Example 8-6 Obsolete SNMP network status

```
dpStatusNetworkInterfaceStatusRxKbytes OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
        "The amount of data successfully received on this interface, including MAC
        framing overhead. Obsoleted in release 5.0.0.0 due to incompatible SNMP
        changes in release 4.0.1.0. When read via SNMP, the value type improperly
        returns Counter64 from release 4.0.1.0 to release 4.0.1.7 and from release
        4.0.2.0 to release 4.0.2.3."

 ::= { dpStatusNetworkInterfaceStatusEntry 9 }
```

To view any changes, check the enterprise MIB files from the WebSphere DataPower web GUI:

1. From the Control Panel, select **Administration** → **Access** → **SNMP Settings**.
2. On the **Enterprise MIBs** tab (Figure 8-7), click any MIB file that is listed to view its details.

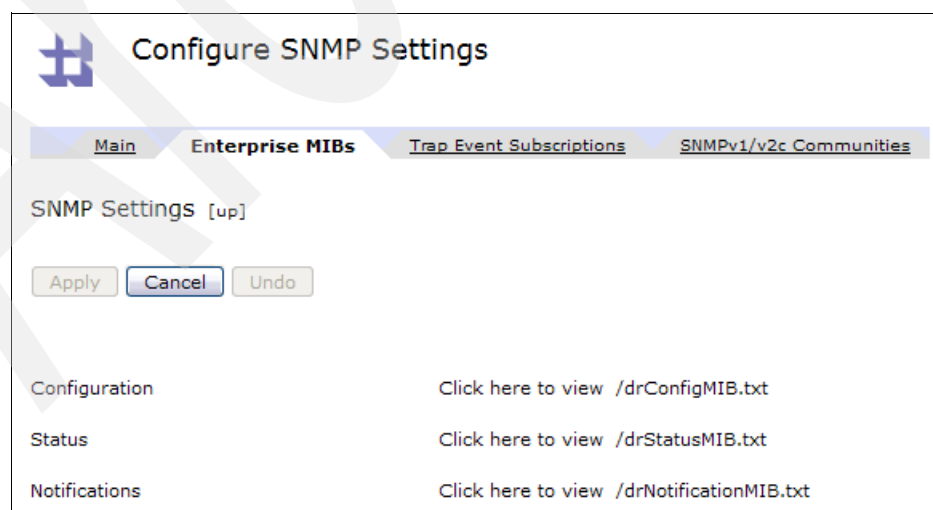


Figure 8-7 Checking the SNMP settings

8.5 Logging and trace

As you use WebSphere Appliance Management Center, you might run actions that result in an error. These errors can be caused by a range of problems from failure, to communication with a WebSphere DataPower Appliance, to invalid input or configuration. The WebSphere Appliance Management Center logs often contain information that can help determine the root cause of a problem. In some cases, the default log files might not provide enough information, but more trace options can be enabled for further help. The WebSphere DataPower Appliance system log file can also be a valuable source of more information.

8.5.1 Logging in WebSphere Appliance Management Center

To help with debugging errors and failures, WebSphere Appliance Management Center logs server output that is related to the actions that users perform in the user interface. The default logging options log most errors and warnings at a sufficient level of detail to allow for most common problems to be diagnosed.

More detailed trace-level logging can be enabled when required. Trace-level logging is typically needed listed when debugging more complex issues or when requesting product support from IBM.

The default logging is in the <WAMC_install_dir>/logs directory.

This directory has the following files and subdirectory:

- ▶ The console.log file
Error messages from WebSphere Appliance Management Center are logged to the console.log file but contain less detail than the messages.log file.
- ▶ The messages.log file
The messages.log file contains more detailed logging information. Stack traces from errors and exceptions are listed in this log.

Multiple messages.log file: The messages.log file gets cycled and split into separate files over time. You might see several messages.log files with files names that are stamped with different dates and times.

- ▶ The history directory
The history directory contains a store of the history that is displayed on the **History** tab in WebSphere Appliance Management Center. Do *not* modify the files in this directory.

If an error message in the WebSphere Appliance Management Center user interface directs you to check the log files, check the console.log and messages.log files.

In some cases, more error logs are created in the logs directory. First-failure data capture (FFDC) logs are generated for some types of errors. When an FFDC log is created, a new directory, called ffdc, is in the logs directory. These FFDC log files contain more information about the cause of the FFDC. FFDC files are related to errors in the application server container that are not fatal to the operation of WebSphere Appliance Management Center.

8.5.2 Trace in WebSphere Appliance Management Center

The default logging options do not always provide enough information about an error to determine the root cause of the problem. In these situations, you can enable more logging options that cause WebSphere Appliance Management Center to output more detailed information about the actions it is running. Trace-level logging is often requested when you contact IBM for product support.

Important: Enabling trace causes extra logging information to be generated, which can lead to generating large log files. Trace-level logging can also impact the performance of the WebSphere Appliance Management Center server. For these reasons, do not enable trace-level logging by default.

Enable trace logging only when you are reproducing a problem. After the problem is diagnosed, disable trace to avoid adversely affecting the performance of WebSphere Appliance Management Center.

You can enable and disable trace without stopping the WebSphere Appliance Management Center server.

Enabling trace

To enable WebSphere Appliance Management Center trace logging:

1. On the server where WebSphere Appliance Management Center is installed, browse to the configuration directory. The default directory is `<WAMC_install_dir>/config`.
2. Rename the `trace.disabled` file to the `trace.xml` file.

Trace logging is shown in the `log` directory as a new file called `trace.log`.

Disabling trace

To disable WebSphere Appliance Management Center trace logging:


1. On the server where WebSphere Appliance Management Center is installed, browse to the configuration directory. The default directory is `<WAMC_install_dir>/config`.
2. Rename the `trace.xml` file to the `trace.disabled` file.

Trace-level logging stops. No further messages are added to the `trace.log` file.

8.5.3 The WebSphere DataPower Appliance system log


In some situations, an error message in WebSphere Appliance Management Center directs you to check the system log on the WebSphere DataPower Appliance. Figure 8-8 shows an example of one of these error messages from the **History** tab.

Details:

 An error occurred when the DataPower appliance manager attempted to backup the device from the 9.42.170.242:5550 appliance.
[Hide detail](#)
2012 10 23 17:16:46:328 | WAMT0512E

Explanation:
A status = ERROR was returned in the response to the backup device request.

Suggestion:
Ensure that the disaster recovery mode is enabled on the device. Examine the IBM WebSphere Appliance Management Toolkit logs and the System logs on the device for more information.

 Started.
2012 10 23 17:16:46:265 | CWZBA1001I




 Submitted.
2012 10 23 17:16:46:203 | CWZBA1012I

Figure 8-8 Error message indicating to check the system log on the WebSphere DataPower Appliance

The error condition shown in Figure 8-8 happened when attempting to use the backup appliance function in WebSphere Appliance Management Center. Figure 8-9 shows an excerpt of the system log for the WebSphere DataPower Appliance. The root cause of the failure is clear from the WebSphere DataPower system log. The backup request failed because the no-such-cert certificate could not be found on the WebSphere DataPower Appliance.



System Log

 Refresh Log

Target:

default-log

Filter:

(none)

(none)

(none)

Help

current time: 17:21:36 on 2012-10-23

time	category	level	domain	tid	direction	client	msgid	message	Show last 50 100
Tue Oct 23 2012									
17:16:49	cli	error		27373895			0x81000224	=== Line 2: secure-backup "no-such-cert" "xa35://temporary//temp_dir_05414" "off" "of	
17:16:49	cli	error		27373895			0x810002b8	Certificate 'no-such-cert' not found	

Figure 8-9 WebSphere DataPower system log showing details of an error condition

8.6 Technotes

Occasionally, issues that cannot be resolved easily are discovered when using WebSphere Appliance Management Center or WebSphere DataPower Appliances. In these cases, the WebSphere Appliance Management Center development or technical support team might choose to create a technote on the IBM Support website. A technote describes an issue with the product, including symptoms that help to identify the problem. The technote also describes suggested workarounds and can include information about fixes that are available.

For a link to a prefiltered view of the technotes that exist for WebSphere Appliance Management Center on the IBM Support website, go to:

http://www.ibm.com/support/entry/portal/search_results/software/websphere/websphere_datapower_soa_appliances?q=%22WebSphere%20Appliance%20Management%20Center

8.7 Other hints and tips

You might find the following hints and tips helpful in troubleshooting:

- ▶ In addition to being available online, the WebSphere Appliance Management Center Information Center is also bundled within the GUI. In the upper-right corner of the GUI, click ? → **Help** to open the bundled WebSphere Appliance Management Center Information Center.
- ▶ If you do not see the feedback that you expected or for more information about an error, check the **History** tab of WebSphere Appliance Management Center.
- ▶ You can select multiple WebSphere DataPower Appliances, domains, or services in WebSphere Appliance Management Center by holding down the Ctrl key and clicking multiple table rows in the GUI. You can also select ranges of rows by clicking the row at the start of the range by holding down the Shift key and clicking the row at the end of the range.

Related publications

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

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications in this list might be available in softcopy only.

- ▶ *DataPower Architectural Design Patterns: Integrating and Securing Services Across Domains*, SG24-7620
- ▶ *DataPower SOA Appliance Administration, Deployment, and Best Practices*, SG24-7901
- ▶ *DataPower SOA Appliance Service Planning, Implementation, and Best Practices*, SG24-7943
- ▶ *SOA Policy, Service Gateway, and SLA Management*, SG24-8101
- ▶ *IBM WebSphere DataPower SOA Appliances Part I: Overview and Getting Started*, REDP-4327
- ▶ *IBM WebSphere DataPower SOA Appliances Part IV: Management and Governance*, REDP-4366
- ▶ *SOA Policy, Service Gateway, and SLA Management*, SG24-8101
- ▶ *WebSphere DataPower SOA Appliance: The XML Management Interface*, REDP-4446

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following IBM Redbooks website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- ▶ IBM WebSphere Appliance Management Center for WebSphere Appliances
<http://www.ibm.com/software/integration/wamc>
- ▶ IBM WebSphere Appliance Management Center for WebSphere Appliances Information Center
<http://pic.dhe.ibm.com/infocenter/wamcinfo/v5r0m0/index.jsp>
- ▶ WebSphere Appliance Management Center for WebSphere Appliances download
<http://www.ibm.com/support/docview.wss?uid=swg24032265>
- ▶ IBM WebSphere DataPower Integration Appliance Version 5.0 Information Center
<http://pic.dhe.ibm.com/infocenter/wsdatap/v5r0m0/topic/com.ibm.dp.xi.doc/welcome.htm>
- ▶ How to upgrade the firmware on an IBM WebSphere DataPower Appliance Technote
<http://www.ibm.com/support/docview.wss?uid=swg27015333>

- ▶ DataPower off-device logging: a configuration example Technote
<http://www.ibm.com/support/docview.wss?uid=swg21269136>
- ▶ IBM WebSphere DataPower SOA Appliance Firmware Support Lifecycle
<http://www.ibm.com/support/docview.wss?rs=2362&uid=swg21246298>
- ▶ Tivoli Composite Application Manager Agent for WebSphere DataPower Appliance Version 6.3 User Guide
http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamsoa.doc_6.2.2/DPAgent_UG.htm

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



IBM WebSphere Appliance Management Center for WebSphere Appliances



Learn about centralized administration of IBM WebSphere DataPower Appliances

Discover best practices for managing WebSphere DataPower Appliances

See how to monitor appliance status with IBM Tivoli Monitoring

IBM WebSphere Appliance Management Center for WebSphere Appliances simplifies the management and monitoring of environments that consist of multiple IBM WebSphere DataPower Appliances. This web-based application provides centralized multi-appliance administration to support daily WebSphere DataPower Appliance operation. WebSphere Appliance Management Center for WebSphere Appliances provides the following key services:

- ▶ Centralized firmware management
- ▶ Disaster recovery
- ▶ Domain and service configuration
- ▶ Configuration life cycle deployment
- ▶ Monitoring multiple appliances, collecting key metrics, and presenting them in a central location

This IBM Redbooks publication helps administrators of WebSphere DataPower Appliances to perform daily administration tasks by using WebSphere Appliance Management Center. The topics in this book include health monitoring of an environment, disaster recovery (secure backup and restore), firmware management, and environment promotion. This book also includes best practices, tips and techniques, and general recommendations for administrators of WebSphere DataPower Appliance deployments.

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