

Progress Fathom Management Standard Edition

Resource Monitoring Guide

Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. This manual is also copyrighted and all rights are reserved. This manual may not, in whole or in part, be copied, photocopied, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Progress Software Corporation.

The information in this manual is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear in this document. The references in this manual to specific platforms supported are subject to change.

Allegrix, A [Stylized], ObjectStore, Progress, Powered by Progress, Progress Fast Track, Progress Profiles, Partners in Progress, Partners en Progress, Progress en Partners, Progress in Progress, P.I.P., Progress Results, ProVision, ProCare, ProtoSpeed, SmartBeans, SpeedScript, and WebSpeed are registered trademarks of Progress Software Corporation or one of its subsidiaries or affiliates in the U.S. and/or other countries. AccelEvent, A Data Center of Your Very Own, Allegrix & Design, AppsAlive, AppServer, ASPen, ASP-in-a-Box, BusinessEdge, Business Empowerment, Empowerment Center, eXcelon, Fathom, Future Proof, IntelliStream, ObjectCache, OpenEdge, PeerDirect, POSSE, POSSENET, Progress Business Empowerment, Progress Dynamics, Progress Empowerment Center, Progress Empowerment Program, Progress for Partners, Progress OpenEdge, Progress Software Developers Network, PSE Pro, PS Select, SectorAlliance, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Technical Empowerment, WebClient, and Who Makes Progress are trademarks or service marks of Progress Software Corporation or one of its subsidiaries or affiliates in the U.S. and other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Any other trademarks or service marks contained herein are the property of their respective owners.

Fathom Management includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation. All rights reserved (Xalan XSLT Processor) and Copyright © 2000-2002 The Apache Software Foundation. All rights reserved (Jakarta-Oro). The names “Apache,” “Xerces,” “Jakarta-Oro,” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. Products derived from this software may not be called “Apache” or “Jakarta-Oro,” nor may “Apache” or “Jakarta-Oro” appear in their name, without prior written permission of the Apache Software Foundation. For written permission, please contact apache@apache.org. Software distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License agreement that accompanies the product.

Fathom Management includes software developed by ACME Labs. Copyright © 2000 by Jef Poskanzer <jef@acme.com>. All rights reserved. Software distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License agreement that accompanies the product.

Fathom Management includes software developed by Sun Microsystems, Inc. Copyright © 2003 Sun Microsystems, Inc. All Rights Reserved. Software distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License agreement that accompanies the product.

Fathom Management includes the Jetty Package Copyright © 1998 Mort Bay Consulting Pty. Ltd. (Australia).

Fathom Management includes software developed by the ModelObjectsGroup (<http://www.modelobjects.com>). Copyright © 2000-2001 ModelObjects Group. All rights reserved. The name “ModelObjects” must not be used to endorse or promote products derived from the SSC Software without prior written permission. Products derived from the SSC Software may not be called “ModelObjects”, nor may “ModelObjects” appear in their name, without prior written permission. For written permission, please contact djacobs@modelobjects.com.

Fathom Management includes files that are subject to the Netscape Public License Version 1.1 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at (<http://www.mozilla.org/NPL>). Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License. The Original Code is Mozilla Communicator client code, released March 31, 1998. The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by Netscape are Copyright © 1998-1999 Netscape Communications Corporation. All Rights Reserved.

Fathom Management contains copyright material licensed fromAdventNet, Inc. <http://www.adventnet.com>. All rights to such copyright material rest with AdventNet.

Fathom Management includes the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

August 2004



Product Code: 4496

Release: V3.0A

Contents

Preface	Preface–1
1. Resource Monitoring with Fathom Management	1–1
Configuring Fathom	1–2
Understanding Fathom terminology	1–3
Commonly used terms.	1–3
Using the Fathom Management console	1–6
Identifying resources you can monitor	1–7
Monitoring a resource	1–8
Viewing resource monitor performance details	1–9
Creating and scheduling Fathom jobs	1–10
Exporting and importing Fathom monitoring components	1–11
2. Using the Fathom Management Console	2–1
Starting Fathom Management	2–2
Logging on.	2–2
Using the console	2–4
Viewing the contents of a container	2–6
Accessing Fathom functions from the menu bar	2–7
Viewing additional details	2–8
Navigating the console	2–9
Sorting in the console list frame	2–11
Checking resource status	2–12

Changing the console display	2-14
Refreshing the console	2-15
Expanding or collapsing resource categories	2-15
Returning to the previous Fathom page	2-15
Displaying a page in a new window	2-16
Accessing help	2-16
Additional console details	2-16
3. Creating Collections and Collection Views in Fathom	3-1
The My Fathom Home page	3-2
How do collections and collection views differ?	3-4
Collections	3-4
What is a collection?	3-4
Collection terminology and hierarchy	3-5
Sample collection scenario	3-6
Working with collections	3-8
Creating a collection	3-8
Editing a collection	3-13
Deleting a collection	3-14
Collection views	3-14
What is a collection view?	3-14
Working with collection views and viewlets	3-15
Viewlet characteristics	3-18
Creating a collection view	3-19
Customizing the view layout	3-21
Editing a collection view	3-22
Deleting a collection view	3-23
Customizing a viewlet	3-24
4. Setting up Resource Monitoring	4-1
Before you begin	4-3
Monitoring remote resources	4-3
Naming conventions	4-4
Monitoring a system, network, or file resource: an overview	4-4
Monitoring a database or an OpenEdge resource	4-5
Working with CPU and memory resources	4-6
Selecting a system, network, or file resource to monitor	4-8
Creating a resource monitoring plan	4-10
Trending considerations	4-11
Choosing a schedule for the monitoring plan	4-12
Adding rules to the monitoring plan	4-17
Sharing rules and rule sets	4-18

Calculating meaningful thresholds with the Configuration Advisor	4-22
Configuration Advisor baselining guidelines	4-22
Using the Configuration Advisor with a disk, CPU, or file system resource	4-23
Reviewing the recommended threshold settings	4-26
Comparing and selecting threshold settings	4-28
Submitting your threshold setting selections	4-28
Determining the effectiveness of your selections	4-29
Understanding alerts	4-29
Determining Fathom's action in response to an alert	4-30
Using default actions	4-31
Creating an e-mail action	4-32
Creating a log action	4-36
Creating a compound action	4-37
Creating a Simple Network Management Protocol (SNMP) trap action	4-39
Updating and deleting actions	4-41
Editing or copying a resource monitor	4-42
Deleting a resource monitor	4-43
Working with default values	4-43
Reviewing and changing global settings	4-44
Reviewing and changing resource type defaults	4-45
Using job and report templates	4-46
Sharing monitoring components using the Fathom Library	4-46
 5. Monitoring System Resources	 5-1
System resource monitoring overview	5-2
Reviewing system resource default values	5-2
Reviewing system resource monitoring plans	5-4
Reviewing the CPU resource monitoring plan	5-4
Reviewing the memory resource monitoring plan	5-9
Reviewing a disk resource monitoring plan	5-13
Reviewing the file system resource monitoring plan	5-14
 6. Monitoring Network Resources	 6-1
Network resource monitoring overview	6-2
Trending considerations for network resources	6-3
Reviewing network resource default values	6-3
Discovering and monitoring TCP and UDP ports	6-5
Reviewing the list of well-known ports	6-6
Discovering network resources	6-8
Adding resource monitors for discovered machines and ports	6-11
Creating a TCP or UDP resource monitor	6-13

Creating a PING (ICMP) resource monitor	6-15
Using the HTTP resource monitor to determine Web site status	6-17
General considerations	6-17
Creating an HTTP resource monitor	6-18
7. Monitoring File Resources	7-1
File resource monitoring overview	7-2
Log file monitor features	7-2
File monitor features	7-3
Verifying mapped network drives	7-4
Reviewing log file and file resource default values	7-5
Creating a log file monitor	7-7
Defining properties	7-7
Using a bookmark	7-9
Creating a monitoring plan	7-13
Adding log file rules	7-15
Adding log file rule sets	7-16
Associating rule sets with log file monitors	7-20
Specifying search criteria	7-25
Creating search criteria	7-28
Enabling the log file monitor	7-35
Editing, copying, or deleting a log file monitor	7-36
Creating a file resource monitor	7-37
Trending performance data for file monitor resources	7-37
Creating a file monitor	7-38
8. Creating Jobs and Job Templates	8-1
Jobs overview	8-3
Creating a custom job	8-3
Creating a job template	8-4
Using a predefined database maintenance job template	8-4
Creating a job instance	8-5
Setting up job completion actions and alerts	8-8
Updating job completion actions and alerts	8-11
Job chaining	8-11
Using environment variables	8-14
Editing a job	8-19
Copying a job	8-20
Deleting a job	8-20
Running a job immediately	8-21

Scheduling a job	8-21
Using cron-based scheduling	8-22
Scheduling a job instance or a job template	8-24
Duration Execution Policy	8-26
Single Execution Policy	8-27
Job Execution Policy over time	8-27
Monthly By Date Execution Policy	8-28
Viewing scheduled jobs	8-29
Viewing running jobs	8-30
Viewing job history	8-31
Viewing database maintenance job instances associated with an individual database	8-33
Working with job templates	8-34
Additional characteristics of job templates	8-35
Creating a job template	8-36
Accessing existing job templates	8-42
Viewing debug details about jobs	8-42
 9. Exporting and Importing in Fathom	 9-1
Exporting and importing overview	9-2
General export and import considerations	9-2
Exporting Fathom Library components	9-3
Exporting referenced items	9-6
Importing Fathom Library components	9-7
 Index	 Index-1

Figures

Figure 2-1:	Fathom Resources page	2-5
Figure 2-2:	Container view in the detail frame	2-6
Figure 2-3:	Fathom user name details	2-8
Figure 2-4:	Collapsed Library categories in list frame	2-9
Figure 2-5:	Expanded Library categories in list frame	2-10
Figure 2-6:	Email actions in Library→Actions	2-10
Figure 2-7:	Parent Folder icon	2-11
Figure 2-8:	Actions category	2-11
Figure 2-9:	Resources sorted by status	2-12
Figure 2-10:	Resource statuses	2-12
Figure 3-1:	My Fathom page	3-2
Figure 3-2:	Sample resource viewlets	3-15
Figure 3-3:	Sample Standard viewlet	3-16
Figure 3-4:	View panel viewlets	3-17
Figure 3-5:	CPU viewlet	3-18
Figure 3-6:	Customize Viewlet icon	3-24
Figure 3-7:	Customizing a viewlet	3-24
Figure 3-8:	Customized viewlet	3-27
Figure 4-1:	Schedules	4-12
Figure 4-2:	Predefined schedules	4-14
Figure 4-3:	Sample rule definition	4-17
Figure 4-4:	Recommended threshold values for disk resource	4-26
Figure 4-5:	Threshold calculation details	4-27
Figure 4-6:	Expanded Actions category	4-30
Figure 4-7:	Fathom Component Library page	4-47
Figure 5-1:	Editing the CPU monitoring plan defaults	5-8
Figure 5-2:	Editing the Memory monitoring plan defaults	5-12
Figure 6-1:	Editing the content rule definition for an HTTP monitor	6-23
Figure 6-2:	HTTP Monitor resource summary	6-24
Figure 7-1:	Log file monitoring plan	7-13
Figure 8-1:	Sample job chaining scenario	8-12
Figure 8-2:	Sample job chaining with flow control scenario	8-13
Figure 8-3:	Using a job as an action	8-16
Figure 8-4:	Selecting Cron expression as the Repeat interval	8-22
Figure 8-5:	Sample cron expression	8-23
Figure 8-6:	Sample of two cron expressions	8-24
Figure 8-7:	Scheduled Jobs page	8-29
Figure 8-8:	Running Jobs page	8-30
Figure 8-9:	New job template in Create Custom Job page	8-37
Figure 8-10:	Job template schedule	8-41
Figure 8-11:	Create Custom Job page	8-42
Figure 9-1:	Implicit and explicit components selected for export	9-6
Figure 9-2:	Implicit and explicit components export confirmation	9-7

Tables

Table 1–1:	Resources for local and/or remote monitoring	1–7
Table 1–2:	Fathom Management actions	1–8
Table 2–1:	Resource status legend	2–13
Table 2–2:	Console control bar icons	2–14
Table 3–1:	Moving the viewlets	3–22
Table 4–1:	Predefined schedules	4–14
Table 4–2:	CPU, disk, and file system rules and formulas	4–23
Table 4–3:	Variables for an e-mail action	4–34
Table 4–4:	Alert details obtained from the fmalertTable	4–40
Table 4–5:	Additional Fathom Library features	4–48
Table 6–1:	Well-known ports and their associated names	6–7
Table 7–1:	Perl 5 regular expressions	7–30
Table 7–2:	Examples using the Perl 5 regular expressions	7–32
Table 8–1:	Environment variables common to all jobs	8–14
Table 8–2:	Environment variables for jobs with associated database resources	8–16
Table 8–3:	Alert environment variables for job actions	8–17
Table 8–4:	Environment variables for jobs associated with the FathomTrendDatabase	8–18

Preface

This Preface contains the following sections:

- [Purpose](#)
- [Audience](#)
- [Fathom Management with OpenEdge or Progress](#)
- [Organization](#)
- [Typographical conventions](#)

Purpose

This guide introduces resource monitoring with Fathom™ Management. The guide provides an introduction to monitoring resources and describes how to use the Fathom Management console; create collections and views; monitor system, network and file resources; use jobs and job templates; and import and export Fathom monitoring components.

Audience

This guide is designed for database administrators and end users of the Fathom Management product. This includes IT managers, ASP hosting companies, and others who are responsible for the day-to-day management and monitoring of resources and OpenEdge™ databases.

Fathom Management with OpenEdge or Progress

This version of Fathom Management runs against the following:

- OpenEdge 10.0B.
- Progress® Version 9.1D and the 9.1D09 service pack.

For the sake of simplicity, the procedures and screen shots provided in this manual refer to running Fathom against OpenEdge 10.0B. However, be assured that unless indicated otherwise, the procedures are the same for both Progress Version 9.1D with the 9.1D09 service pack and OpenEdge 10.0B. For example, if a procedure refers to an OpenEdge database, the procedure applies to a Progress database as well.

Organization

[Chapter 1, “Resource Monitoring with Fathom Management”](#)

Provides an overview of resource monitoring and Fathom terminology.

[Chapter 2, “Using the Fathom Management Console”](#)

Introduces the Fathom Management console and describes its navigation and features.

[Chapter 3, “Creating Collections and Collection Views in Fathom”](#)

Describes the My Fathom Home page and provides information about creating collections of resources and collection views that focus specifically on Fathom monitoring data you find most valuable.

Chapter 4, “Setting up Resource Monitoring”

Describes how to set up a resource monitor, including its properties, monitoring plan, schedule, and rules. The chapter also touches briefly on Fathom alerts and then describes Fathom actions that occur in response to alerts. Also included is information about default resource monitor values and using the Configuration Advisor with a disk, CPU, memory, or file system resource.

Chapter 5, “Monitoring System Resources”

Describes the default values Fathom provides for system resources and the resource rules.

Chapter 6, “Monitoring Network Resources”

Describes the default values Fathom provides for network resources and how to create network resource monitors.

Chapter 7, “Monitoring File Resources”

Describes how to create a log file resource monitor (to monitor file contents) and a file resource monitor (to monitor file characteristics).

Chapter 8, “Creating Jobs and Job Templates”



Describes how to create, edit, copy, schedule, run, or delete a Fathom job. The chapter provides information about creating job templates, reviewing scheduled jobs, reviewing running jobs, and reviewing job history.

Chapter 9, “Exporting and Importing in Fathom”

Describes how to export and import sharable Fathom Library components, which can help reduce duplication of effort and improve consistency among machines.

Typographical conventions

This manual uses the following typographical conventions:

Convention	Description
Bold	Bold typeface indicates commands or characters the user types, or the names of user interface elements.
<i>Italic</i>	Italic typeface indicates the title of a document, provides emphasis, or signifies new terms.
SMALL, BOLD CAPITAL LETTERS	Small, bold capital letters indicate OpenEdge™ key functions and generic keyboard keys; for example, GET and CTRL .
KEY1-KEY2	A hyphen between key names indicates a <i>simultaneous</i> key sequence: you press and hold down the first key while pressing the second key. For example, CTRL-X .
KEY1 KEY2	A space between key names indicates a <i>sequential</i> key sequence: you press and release the first key, then press another key. For example, ESCAPE H .
Syntax:	
Fixed width	A fixed-width font is used in syntax statements, code examples, and for system output and filenames.
<i>Fixed-width italics</i>	Fixed-width italics indicate variables in syntax statements.
Fixed-width bold	Fixed-width bold indicates variables with special emphasis.
UPPERCASE fixed width	Uppercase words are Progress® 4GL language keywords. Although these always are shown in uppercase, you can type them in either uppercase or lowercase in a procedure.
	This icon (three arrows) introduces a multi-step procedure.
	This icon (one arrow) introduces a single-step procedure.

Resource Monitoring with Fathom Management

Fathom™ Management Standard Edition provides you with the means to monitor your network resources and local and remote system, file, database, and OpenEdge™ server (AppServer™, NameServer, and WebSpeed® Transaction server) resources. You receive feedback on each resource Fathom is monitoring, based on performance criteria that you establish. If a resource's performance does not meet the criteria you set, you determine what action Fathom takes.

This chapter provides an introduction to Fathom Management resource monitoring. Specifically, the chapter provides details about the following:

- [Configuring Fathom](#)
- [Understanding Fathom terminology](#)
- [Using the Fathom Management console](#)
- [Identifying resources you can monitor](#)
- [Viewing resource monitor performance details](#)
- [Creating and scheduling Fathom jobs](#)
- [Exporting and importing Fathom monitoring components](#)

Configuring Fathom

When you first install Fathom Management, you select some initial configuration settings, such as the password you want to use for the management console and whether you want Fathom to start automatically when the AdminServer starts. You decide where you want the FathomTrendDatabase to be and what Web server port number to use. You also specify an e-mail server and a default operator who receives e-mail if Fathom generates an alert and you have set the Default_Action as the alert action. The alert action is the action that should occur, by default, when an alert triggers. Other initial configuration choices you make affect SNMP adapter settings (if you have installed the adapter), and whether you want Fathom to monitor and trend file systems and disks.

Once you make these initial configuration decisions, you can configure Fathom to monitor remote resources. You also add Fathom users in one of two roles: administrator, with access to all Fathom functionality, and operators, with access to more limited functionality.

You work with Fathom through the browser-based Fathom Management console. If your user role in Fathom is that of an operator, you might find that some management console links or options are gray and unavailable to you. Note that all descriptions and graphics provided in this guide are presented with the assumption that you have full access to Fathom functionality.

Fathom also provides a command-line interface that allows you to:

- Start, query, and stop Fathom.
- Dump the contents of the Fathom configuration database to a readable form (an XML file) and, in the event of a catastrophic failure, use the backup dump file to restore the database.
- Enable and disable polling.
- Work with alert commands.
- Access command-line help.

Understanding Fathom terminology

As you work with Fathom Management, there are several terms with which you will become familiar.

Commonly used terms

Terms commonly used in Fathom resource monitoring include:

- Resource.
- Container.
- Collection.
- Monitor and schedule.
- Rules, alerts, and actions.
- Resource monitoring plan.
- FathomTrendDatabase.

Resource

A *resource* is a specific component of your configuration. A resource might be:

- A database or database log file.
- A system resource, such as CPU, memory, disk, or file system.
- A network resource, such as TCP or UDP port, Ping (ICMP), or HTTP communication.
- A file resource, such as a log file or other file you identify for monitoring.
- An OpenEdge server component, such as an AppServer, NameServer, or WebSpeed Transaction Server.

Note: Fathom Management supports monitoring and managing the WebSpeed® Transaction Server product. Throughout this guide, references to the WebSpeed Transaction Server and WebSpeed are used interchangeably.

When you install Fathom Management, Fathom automatically creates resource monitors for your CPU resource and memory resource and assigns default values, which you can change. Fathom also creates monitors for resources registered with the AdminServer; these resources include databases, AppServers, NameServers, and WebSpeed Transaction Servers.

Container

A *container* represents a named instance of an AdminServer that is either running Fathom or has been configured to be monitored by Fathom. There is typically a 1:1 relationship between the host name and container name unless there are multiple AdminServers running Fathom on the same host.

Collection

A *collection* is a user-defined group of resources.

You can create and use a collection to better organize and operate on resources. For example, you might create a collection, known as Collection A, that includes all resources on which a particular application depends. You might then create another collection, known as Collection B, that is also dependent on one of the resources in Collection A. If the resource common to both Collection A and Collection B fails, the failure is reflected in the status of both collections, enabling you to determine quickly the extent and the impact of the failure.

An administrator can create a private or a shared collection. An operator can create a private collection and see, but not create, a shared collection.

A collection can include any number of the following resources:

- Monitored resources, such as CPU, disk, memory, and database.
- Jobs.
- Reports.
- Other collections.

Monitor, schedule, rules, and rule sets

A *monitor* in Fathom is defined as the combination of a resource, schedules, and rules. The *schedule* defines a block of monitoring time in Fathom, and the *rules* determine how a resource's performance is judged while it is being monitored. Each rule verifies whether a resource complies with its performance criteria. Rules are considered broken when a resource is not in compliance with the criteria that you set up. When you are working with database, log file, AppServer, NameServer, and WebSpeed monitors, you can also use *rule sets* when monitoring performance.

When you monitor a resource, you set up criteria by which you can keep track of the resource's performance. As necessary, you can adjust the criteria (against which performance is measured) to meet your expectations. For example, you might want to monitor a database twenty-four hours per day, seven days a week, and receive notification if the database shuts down abnormally.

Alerts and actions

A broken rule generates an *alert*, which notifies you that some criteria have been violated.

Fathom Management allows you to set up *actions* that trigger automatically in response to alerts. For example, you can establish that the system administrator receive an e-mail if a database experiences an abnormal shutdown.

Resource monitoring plan

A *resource monitoring plan*, also known more simply as a *monitoring plan*, defines a block of time in which a specific resource is monitored and identifies the rules to be checked during the defined time frame. Any resource that you create in Fathom must have one or more monitoring plans before Fathom can perform any monitoring.

Fathom uses monitoring plans to determine when to monitor a resource and which rules and criteria to use when evaluating a resource's compliance within these defined parameters. By defining more than one monitoring plan, you can specify different criteria (rules) for different times. For example, you might evaluate the rules for a database resource every five minutes Monday through Friday and only every thirty minutes on weekends.

FathomTrendDatabase

Fathom allows you to store trend data, which is the monitoring information Fathom collects, in either a local or remote FathomTrendDatabase. If you choose to send trend data to a local database (the default), you specify the trend database location and the port used to connect to that database. If you choose to use a remote database, you specify the hostname and Web server port of the remote Fathom Web server. The trend database must be locally configured at the remote location. All values you enter for either option are validated.

Using the Fathom Management console

Once you install Fathom, you can access the management console, which is the graphical user interface to Fathom.



To access the management console once you install Fathom, you can do any of the following:

- To access Fathom from a Web browser, enter the URL `http://host:port` in the address or location field. The *host* is the name of a machine on which Fathom is installed, and *port* is the Fathom Web server port (by default, this port is 9090). A logon window appears.
- Click the **Management Console** icon on your desktop (if you installed Fathom on Windows and chose to install the shortcut icon).
- Choose **Start→Programs→Fathom Management→Management Console** on the Windows platform.

The first time you log on to Fathom, you use the default user name of **admin** and the default password of **admin**.

Using the console, you can set up monitoring for each of the Fathom resources whose performance you want to follow.

Identifying resources you can monitor

With Fathom Management, you can monitor the performance of local and/or remote resource types (provided you have run the Fathom Remote Configuration Utility to set up monitoring of remote resources) as indicated in [Table 1–1](#).

For details about the Fathom Remote Configuration Utility, see the [Installation and Configuration Guide](#).

Table 1–1: Resources for local and/or remote monitoring

Resource	Local	Remote
Log file	√	–
Other file	√	√
Network components (TCP, UDP, PING, HTTP)	√	√
CPU	√	√
Memory	√	√
OpenEdge server components (AppServer brokers, NameServers, WebSpeed Transaction Servers)	√	√
Disks	√	√
File systems	√	√

You can also monitor managed databases (recognized by the AdminServer and Fathom), and you can migrate scripted databases so that they, too, become managed and available for monitoring.

Monitoring a resource

You select the resource you want to monitor and create its monitoring plan. Provided here are the overall steps, which are covered in greater detail throughout this guide.

Once you install Fathom and set initial configuration options, you can configure Fathom to monitor certain remote resources as well as local ones.



To monitor a resource in Fathom:

1. Create a resource monitor (for a database, file, network component, OpenEdge server component, or system component).
2. Create a monitoring plan for the resource monitor. The monitoring plan defines all the criteria you want to use in assessing the resource’s performance and consists of the following parts:
 - One or more schedules that identify what portion of time you want monitoring to encompass.
 - One or more rules that identify the performance standards you expect the resource to meet. If a standard established by a rule is not met, the rule is considered broken and Fathom generates an alert as notification of the performance issue.
 - An action that occurs when Fathom generates an alert about a performance issue. See [Table 1–2](#) for a list of available actions.

Table 1–2: Fathom Management actions (1 of 2)

In response to this action...	Fathom...
Default action	Contains the e-mail action.
Email action	Generates an e-mail to a recipient you identify, notifying the recipient about the alert.
Log action	Records details about the alert in a log file.
SNMP trap action	Sends notification of the alert to your SMNP management console.

Table 1–2: Fathom Management actions (2 of 2)

In response to this action...	Fathom...
Compound action	Executes one action that consists of one or more other actions.
Job action	Executes a job in response to an alert.

Viewing resource monitor performance details

You can acquire information about resource performance in the following ways:

- Create a collection of resources. The collection functions as a group, and each resource is a member. When you create a collection, you typically choose resources with a common characteristic; for example, you might create a collection of databases that span multiple hosts but support one particular application.
- Create one or more custom, collection views that display only the details you want to see. For example, you can create a custom view of all monitoring plans you have in place, or find out any number of specifics about a particular database. The details that the custom view contains are determined by you and appear in individual panes known as *viewlets*. Each viewlet provides details in a graphical format and allows you to get a quick status of only those pieces of information you find key at any particular time.

Fathom provides you with a default custom view, known as the **My Fathom** Home page.

- Create and run a report that includes performance data (in both graphical and HTML formats) about one or more resources. When you create a report, you can use one of the report templates that Fathom provides, or you can create your own report template. Creating a report and running it need not be done at the same time; you can create a number of reports and schedule them to run at a particular time. You can review a list of reports you have scheduled to run and a list of reports that are currently running.

You can also run a real-time report with a specific focus, such as a database summary or statistics about open alerts (in detail or summary format) by using the **Realtime Reports** option.

See the *Reporting Guide* for details about creating and running Fathom reports.

Creating and scheduling Fathom jobs

As you monitor resources with Fathom, you can define tasks for execution at intervals you determine. Each task is known as a job.

Fathom supports three kinds of jobs:

- **Custom job** — A task that you define for execution at a scheduled interval.
- **Job template** — A set of default values that you use when creating a job instance.
- **Predefined database maintenance job template** — A tailored template that performs a maintenance activity for an OpenEdge database.

Exporting and importing Fathom monitoring components

You can export or import certain Fathom resource monitoring components among machines, which allows you to establish common monitoring guidelines without having to recreate manually the monitoring structure you want. These exportable and importable components reside in the Fathom Library, making them available for sharing.

You can export or import the following monitoring components:

- Actions.
- Report templates.
- Job templates.
- Database rule sets.
- Log file rule sets.
- NameServer rule sets.
- AppServer rule sets.
- WebSpeed rules sets.
- Log file search criteria.

Using the Fathom Management Console

This chapter provides an introduction to the browser-based Fathom Management console, which is the graphical user interface you use when working with Fathom Management Standard Edition, as outlined in the following sections:

- [Starting Fathom Management](#)
- [Using the console](#)
- [Navigating the console](#)
- [Changing the console display](#)
- [Additional console details](#)

Starting Fathom Management

The Fathom Management console is the Web-based graphical user interface that you use to work with Fathom Management. You access the console from any browser that Fathom Management supports. (See the *Installation and Configuration Guide* for specifics about which browsers are supported.)

You use the management console to access all of Fathom's functionality.

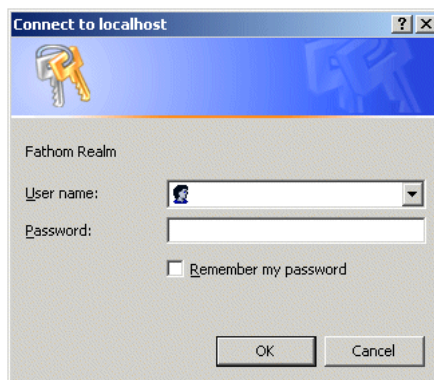
Logging on

After you log on to Fathom Management for the first time, you must establish some initial configuration settings before you can use Fathom.



To access the logon window and open the Fathom Management console:

1. Choose one of the following methods, depending on whether you are accessing the management console from a Web browser or locally:
 - To access Fathom from a Web browser, enter the URL `http://host:port` in the **Address** or **Location** field. The *host* is the name of a machine on which Fathom is installed, and *port* is the Fathom Web server port (by default, this port is 9090). A logon window appears.
 - To access Fathom locally from the Windows Desktop, select **Start→Programs→Fathom→Management Console**. The default browser appears in the background and the logon window, shown below, appears in the foreground:



(Depending on how Fathom Management was installed at your site, there might also be a **Management Console** shortcut icon available from the Windows Desktop. If so, clicking the icon displays this same logon window.)

Note that the specific appearance of the logon window depends on the browser you are using.

2. If you are logging on for the first time, type the user name **admin** and the password **admin** in the appropriate fields, and click **OK**. The **Fathom Management Configuration** page appears when the console opens.

When you log on at any point after the first time, you use a new password you have created. The console opens to **My Fathom**:

Menu bar

Detail menu

List frame

Detail frame

Detail control bar

List control bar

Resource	First Alert	Last Alert	Total
nbaspauldixp.Disk-0-C...	May 13, 2004 8:47:44 AM	May 13, 2004 9:27:54 AM	1
nbaspauldixp.Fathom	May 13, 2004 8:47:44 AM	May 13, 2004 9:27:54 AM	1
nbaspauldixp.FileSys-C...	May 13, 2004 8:47:44 AM	May 13, 2004 9:27:54 AM	2

Resource	Status
nbaspauldixp.Disk-0-C...	Pass
nbaspauldixp.Fathom	Fail
nbaspauldixp.FileSys-C...	Not Checked
	Not Running
	Disabled
	Inactive
	Offline

Alert	Severity
	Severe
	Warning
	Error
	Information

Using the console

The console consists of the following components:

- **Menu bar** — Identifies the host Fathom is running on and provides access to these Fathom features: **My Fathom**, **Alerts**, **Resources**, **Library**, **Reports**, **Jobs**, **Options**, and **Help**.
- **Detail menu** — A dynamic HTML menu available on each detail page in the Fathom Management console. The content of the menu varies depending on where it appears, and its commands enable you to perform a number of common Fathom tasks.
- **List frame** — The left pane in the console. The list frame provides access to different areas within Fathom by presenting a collapsible and expandable tree-like structure and a sort feature.
- **List control bar** — Allows you to work with the contents of the list frame by refreshing the list frame display, expanding the list frame categories, or collapsing the list frame categories.
- **Detail frame** — The right pane in the console. The detail frame displays the Fathom component you select in the list frame.
- **Detail control bar** — Allows you to work with the contents of the detail frame by returning to the previous Fathom page, refreshing the page, displaying the page in a new window, or accessing online help.

Figure 2–1 shows how the management console appears if you select **Resources** in the menu bar and then click the **Container** name in the list frame. The list frame displays existing resource-related information (in this case, for the container **nbaspauldixp**), with a **Sort by** option, and the detail frame displays the **Fathom Resources** page.

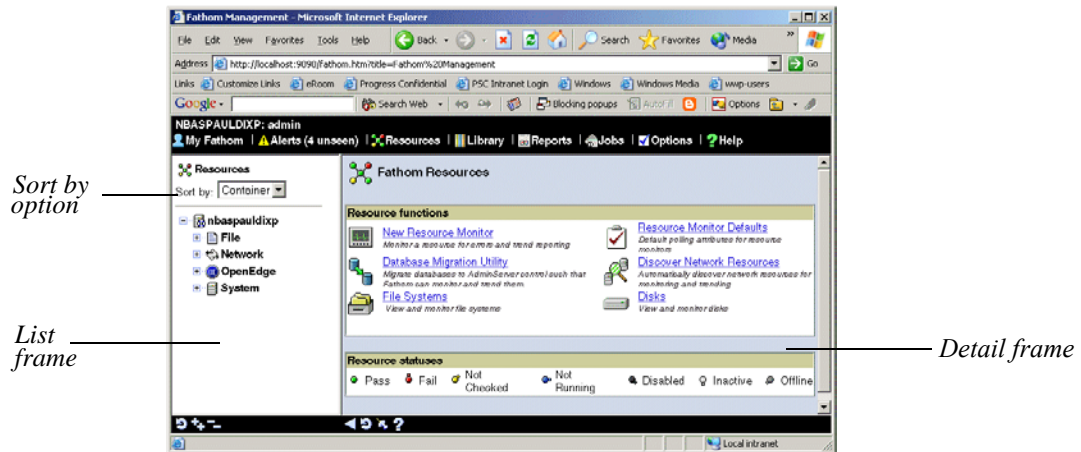


Figure 2–1: Fathom Resources page

Viewing the contents of a container

If you click the container name in the list frame, the **Container** page appears in the detail frame.

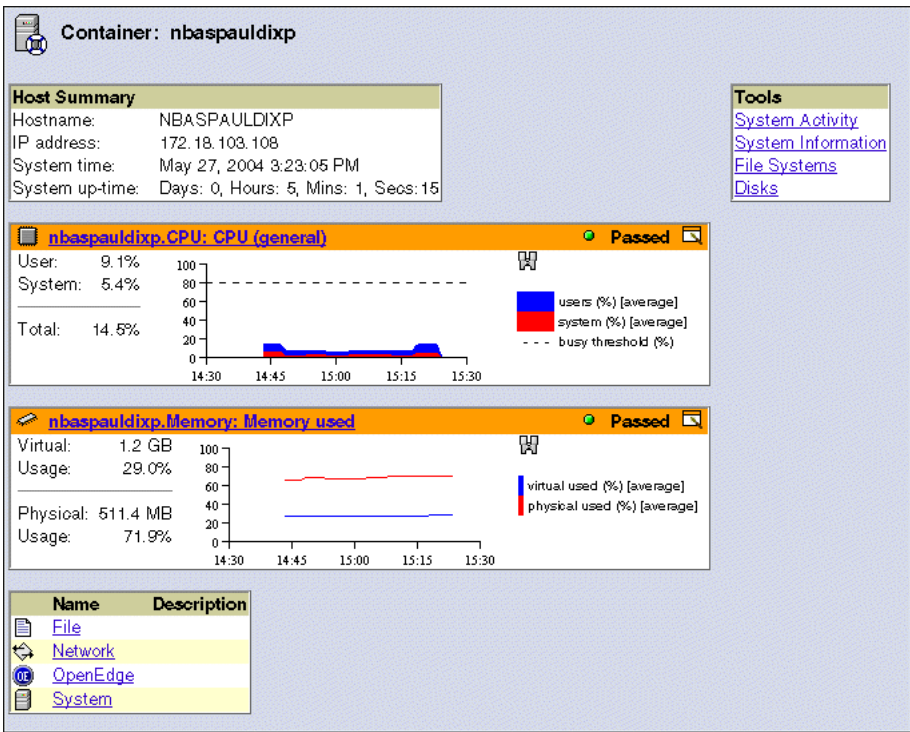


Figure 2–2: Container view in the detail frame

As shown in [Figure 2–2](#), the **Container** page includes summary information about the host machine; viewlets that illustrate CPU and memory performance details; and access to the different resource categories, such as **File** and **Network**, for example.

The **Container** page also provides access to the following details:

- **System Activity** — The System Activity report, which identifies host information, CPU utilization, and memory utilization.
- **System Information** — The System Information report, which provides details about the host, the operating system, the Fathom Management installation, the OpenEdge installation, and startup information (such as Java classpath setting, the library path setting, and system path setting).
- **File Systems** — Tabular and graphical details about the the container's file systems, including the systems' overall capacity, free space, current usage, and other statistics.
- **Disks** — A list of the container's disks and access to details about each one.

Accessing Fathom functions from the menu bar

You can access the following Fathom functions from the menu bar:

- **My Fathom** — Customizable private or shared collections of resources that include views of Fathom components.
- **Alerts** — Open alerts.
- **Resources** — The resources being monitored by Fathom: database, file, network, OpenEdge server, and system.
- **Library** — Functions you use to centrally define components for sharing and reuse among resources. Library functions include actions, search criteria, rule sets, schedules, and templates.

You can also perform various export and import activities related to resource distribution and management from the Library.

- **Reports** — Reporting functions, such as creating, scheduling, and running reports.
- **Jobs** — Job functions, such as creating, scheduling, and running jobs.
- **Options** — Administrative and user management functions.
- **Help** — Various help resources, such as Fathom documentation, support, and Knowledge Base access.

Viewing additional details

The name of the Fathom-hosting machine and your user name also appear in the menu bar; in [Figure 2–3](#), the machine name is **nbaspauldixp**. If you click the user name, you see details about the user, such as the user name, a description of the user (if available), and the user’s role (either administrator or operator).

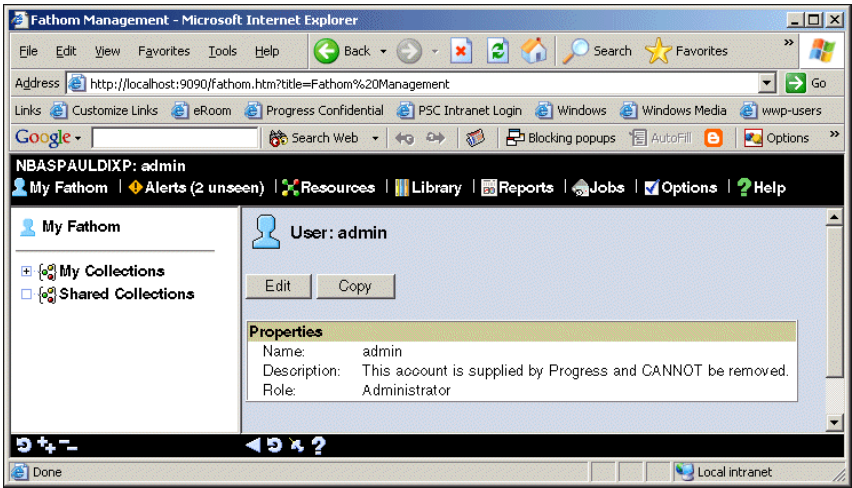


Figure 2–3: Fathom user name details

Navigating the console

When you open the management console you see a list of private (**My Collections**) and shared collections (**Shared Collections**) in the list frame. As you select different features in the Fathom menu bar, the contents of the management console change.

For example, if you click **Library**, you see the library-related components in the list frame, as shown in Figure 2–4.



Figure 2–4: Collapsed Library categories in list frame

If a plus sign (+) precedes a category in the list frame, as shown in Figure 2–4, you can click the plus sign to expand the collapsed category and see its contents. If a minus sign (-) precedes a category, the category has been fully expanded and all its contents are in view. If an empty box precedes a category, the category has no contents.

If you were to click the plus sign preceding each of the collapsed main **Library** categories shown in [Figure 2–4](#), for example, the expanded view would look like that shown in [Figure 2–5](#).

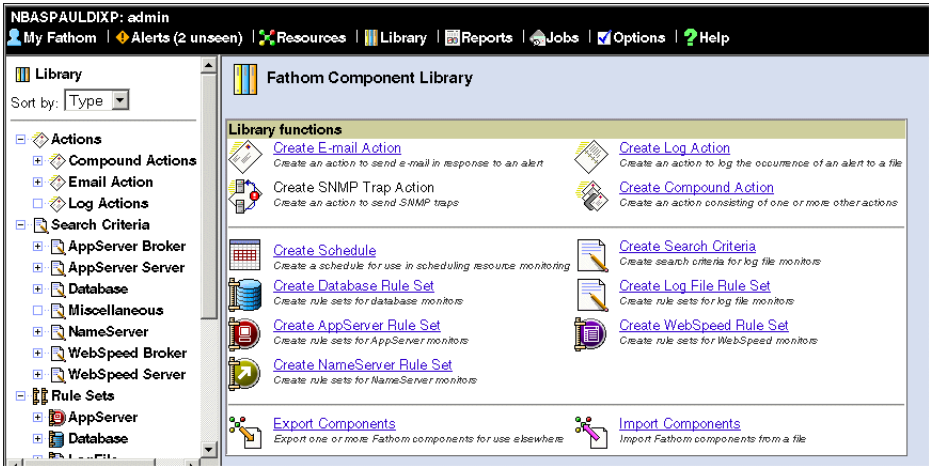


Figure 2–5: Expanded Library categories in list frame

When you click a category in the list frame, a list of items in that category appears in the detail frame. For example, if you click **Email Action** under the **Actions** category, a list of email actions you can choose from appears, as shown in [Figure 2–6](#).

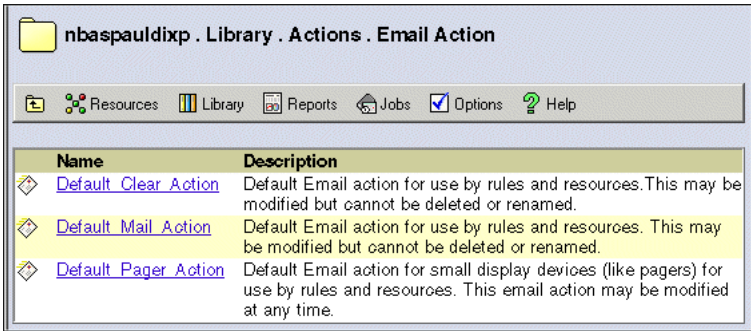


Figure 2–6: Email actions in Library→Actions

Note also that a dynamic HTML menu bar, known as the *detail menu bar*, appears in [Figure 2–6](#). As you navigate throughout the console, you will notice the menu on certain Fathom pages; the options available from the menu differ, depending on where you are in the application. Included in the detail menu bar is the **Parent Folder** icon, shown in [Figure 2–7](#).



Figure 2–7: Parent Folder icon

You can click the **Parent Folder** icon to navigate to a level above the page being shown in the console.

In the example shown in [Figure 2–6](#), the parent folder is **Actions**, so the detail frame would change to display the **Actions** category’s contents, as shown in [Figure 2–8](#).



Figure 2–8: Actions category

Sorting in the console list frame

By using the Fathom **Sort by** feature, you can sort alerts, library components, and resource categories in the list frame in one or more of the following ways (depending on the component):

- **Container** — In alphanumeric order by container name.
- **Resource Name** — In alphanumeric order by *<container name> . <resource name>*.
- **Alert Name** — In alphanumeric order by alert name.
- **Last Date** — By date in descending date, from most recent to least recent.
- **Severity** — By severity: **Severe**, **Error**, **Warning**, or **Information**.
- **Type** — By type, such as actions or rule sets in the **Library**.

- **Name** — In alphanumeric order by name.
- **Status** — By the following statuses: **Pass**, **Fail**, **Not Checked**, **Not Running**, **Disabled**, **Inactive**, and **Offline**, as shown in [Figure 2–9](#).

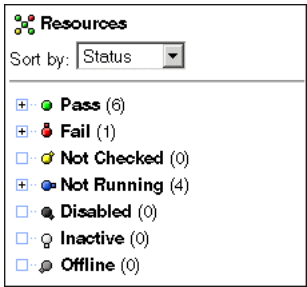


Figure 2–9: Resources sorted by status

The number in parentheses that follows each status category indicates how many resources the category currently includes.

See the “[Checking resource status](#)” section on page 2–12 for details about the significance of the colored bullet that precedes each category.

- To sort resources in the list frame, choose the **Sort by** category in the drop-down list.

Checking resource status

Once you set up resources, Fathom gives you a visual indication as to the general status of each resource monitor by using one of seven, small, colored icons. Each of the icons in the **Resource statuses** legend, shown in [Figure 2–10](#), corresponds to a particular status.

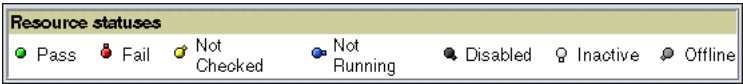


Figure 2–10: Resource statuses

Table 2–1 briefly describes what each status/color combination represents.

Table 2–1: Resource status legend

Status	Color	Description
Pass	Green	The resource monitor is currently working.
Fail	Red	<p>The most recent test involving the resource failed. This includes statuses such as tardy, timeout, unreachable, and so forth. Check the Alert Summary page or the specific monitor for possible alert details.</p> <p>This status can also identify an internal error that prevents the resource from being monitored.</p>
Not Running	Blue	<p>The resource is currently not running. This status is particularly informative as it applies to resources such as databases that must be operating before you can monitor them.</p> <p>For example, databases have operational dependencies. The state of the AdminServer, database broker, or agent can cause a Not Running status to be generated for a database or off-line container.</p>
Not Checked	Yellow	The resource monitor's status is currently unknown. For example, at system startup, it is possible that the resource has not yet been polled.
Disabled	Black	The resource monitor has been disabled and is not currently monitoring a resource.
Inactive	White	There is no active monitoring plan at this time.
Offline	Gray	The resource is currently offline.

How outstanding alerts can affect resource statuses

If there are outstanding alerts on a resource, the icon that indicates the most severe alert status displays to the left of the status icon. If there are no alerts on the resource, only the status icon appears. The presence of the alert icon helps you to easily see if there are any outstanding alerts on a resource.







Note that it is possible for a resource to have a **Pass** status, as indicated by a green status icon, when the resource still has open alerts. In such a case, the status is indicating that the resource passed on the last poll but failed at some point in the past.

Changing the console display

You can use the management console control bars to change or update the console display. The two adjoining control bars appear horizontally across the bottom of the management console: the list control bar appears across the bottom of the list frame, and the detail control bar appears across the bottom of the detail frame.

Each control bar contains a set of icons, as listed in [Table 2–2](#), that you can use to perform a particular task on the information within the frame.

Table 2–2: Console control bar icons

Icon	Description
	Refresh.
	Expand all.
	Collapse all.
	View previous page.
	Display page in new window.
	Access context-sensitive help.

Refreshing the console

As you work with Fathom, be sure to refresh or reload (depending on the browser) the management console often so that the console display is always the most current.



To refresh or reload all or part of the console:

- Select **View**→**Refresh** from Internet Explorer's tool bar to refresh the entire console.
- Select **View**→**Reload** from Netscape's tool bar to reload the entire console.
- To refresh either the list frame or the detail frame, click the **Refresh** icon, shown in [Table 2-2](#), in either the list frame control bar or the detail frame control bar.

Expanding or collapsing resource categories

Your ability to expand the categories can be very useful when you have a large number of categories and subcategories in the list frame that you want to review.



To expand all existing categories and subcategories in the list frame, click the **Expand All** icon shown in [Table 2-2](#).



To collapse all categories and focus on a more condensed view, click the **Collapse All** icon shown in [Table 2-2](#).

Returning to the previous Fathom page

You might want to go back to the Fathom page you just viewed.



To return to the most recent Fathom page you reviewed, click the **Previous Page** icon, shown in [Table 2-2](#), in the detail control bar.

Displaying a page in a new window

You can display a page in a new window in the management console, which provides an easy way for you to view different components simultaneously.



To open the current detail frame in a new window, click the **Display Page in New Window** icon, shown in [Table 2–2](#), in the detail control bar.

Accessing help

You can access Fathom Management help in two different ways:

- From the detail control bar, click the **Help** icon, shown in [Table 2–2](#), to see context-sensitive help directly related to the active Fathom Management page.
- From the Fathom menu bar, choose **Help**→**Fathom Documentation** for an online version of the Fathom Management guides.

Additional console details

Keep the following details in mind as you work with the management console:

- All required fields in the management console appear in red by default. If you are reading this document in .pdf file format through a browser, notice that the required fields shown in the screen captures also display in red.

Depending on your printer and printer options, it is possible that the required fields will not print in red if you print the .pdf file.

- The management console presents some initial default values for Fathom that you can either retain to get Fathom up and running quickly or change to suit your own particular needs.
- When you select a resource, the management console provides summary information at the top of the detail frame to help you assess—at a glance—name, polling, and status information such as last poll, last failure, and percent of failure.

- The management console includes ToolTips that save you from clicking on each Fathom alert to see the contents of the alert message. ToolTip information that summarizes alert details for a resource can be displayed on alert icons in the list frame and on the specific alert as it appears on the resource monitor summary page. To display a ToolTip, place your cursor over either of these alert icons; the summarized alert message appears after a few moments.
- Fathom does not asynchronously updates pages, except when you are starting or stopping OpenEdge servers or databases. Therefore, periodically refresh the management console to be sure that you are looking at the most up-to-date data.

You can also set the pages to refresh automatically. (By default, this option is disabled.) Click **Options** on the console menu bar, and then select **User Preferences**. You can then choose how often you want Fathom to automatically refresh the pages.

- To display session context data in more than one browser, you should launch a separate browser. Creating a new browser window simply using the browser's functionality can lead to an unreliable display of information.

Creating Collections and Collection Views in Fathom

You can create one or more groups of resources, known as *collections*, in Fathom. When you create a collection, you typically group together resources that have a common element: for example, all the database resources used by one division in your company, or all resources that support one particular application. When you group resources, you can more easily examine their details and assess their status.

You can also optionally create one or more custom views within a collection and specify exactly what types of information you want to see. The information provides a customized view, sometimes in a graphical format, of your various resources' status.

This chapter provides the following information about collections and custom views:

- [The My Fathom Home page](#)
- [Collections](#)
- [Collection terminology and hierarchy](#)
- [Sample collection scenario](#)
- [Working with collections](#)
- [Collection views](#)
- [Working with collection views and viewlets](#)

The My Fathom Home page

Fathom creates a default private home collection for each Fathom user. It is this collection, named **My Collections.Home** and consisting of a default view named **Default**, that you see after you click **My Fathom** on the management console menu bar.

In the **My Fathom** page shown in [Figure 3–1](#), the list frame shows two categories: **My Collections** and **Shared Collections**. The detail frame contains a default view of the **Home** collection.

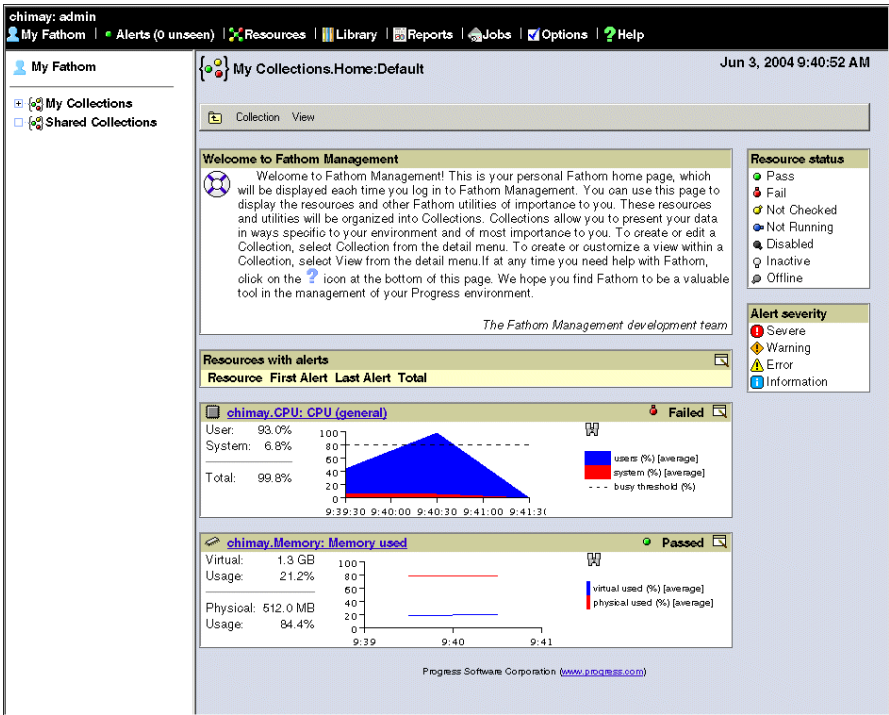


Figure 3–1: My Fathom page

The detail frame consists of the following individual groups of data, known as *viewlets*:

- **Welcome to Fathom Management** — Describes how you can customize the page. This viewlet appears each time you open the **My Fathom** page until you create your own view and select its viewlet contents.
- **Resources with alerts** — Provides the following information about each resource that currently has one or more alerts: the name of the resource (preceded by the container name), when the first alert was fired, when the last alert was fired, and the total number of alerts the resource has. In [Figure 3–1](#), there are no alerts listed.
- **CPU** — Provides the CPU usage.
- **Memory** — Provides the memory usage.
- **Resource status legend** — Describes what the resource status icons on the page represent.
- **Alert severity legend** — Identifies the different icons used to indicate the severity of an alert.

The **My Fathom** page also provides a dynamic HTML menu bar known as the *detail menu bar*. The detail menu bar includes two options: **Collection** and **View**.

From the **Collection** menu, you can:

- Create a new collection.
- Edit a collection.
- Delete a collection.

From the **View** menu, you can:

- Create a new collection view.
- Customize a collection view by modifying either or both of the following:
 - **Content**
 - **Layout**
- Delete a view.

How do collections and collection views differ?

A collection is a logical grouping of resources and views, and a view is a display of user-selected data. The visualization of any collection is one or more views.

Collections extend the more limited **My Fathom** views available previously in Fathom Management; views are now incorporated into collections.

Collections and collection views also differ in the following ways:

- You can create a collection with an arbitrarily large number of members; however, displaying them all in a single Fathom page might not be practical. Instead, you can create multiple views of a collection; each view can focus on a different aspect of the collection.
- A collection is hierarchical. You choose the parent for each collection when you create it, thereby allowing you further flexibility in isolating specific performance data.
- You can create views that include nonresource viewlets, such as resources with alerts or active monitoring plans. Neither of these views corresponds to a single resource and would not, then, equate to a member in a collection, which consists of a group of individual resources.

Collections

You create, edit, and delete collections from the **My Fathom** page.

What is a collection?

A collection is a group of resources (known also as members) that you define. You group resources into a collection based on criteria that you find valuable when grouped and viewed together.

You can include the following resources in a collection:

- All monitored resources, such as CPU, disks, databases, or WebSpeed Transaction servers. A resource can be a member of multiple collections.
- Jobs.

- Reports.
- Other collections.

When you create a collection, you assign it a name and provide its definition. You can identify the collection members when you create the collection, and you can later add or remove members. You can include resources from multiple containers in a collection.

When you select members for a collection, you can use a wildcard feature that enables you to select all resources, all resources of a particular type, or all resources on all containers, etc. Using the wildcard is a powerful way to manage the members of a collection; for example, if you select all databases on all containers as members of a collection, databases added to containers after you created the collection are automatically added as members of the collection. Likewise, any database that is removed from a container is also removed automatically from the collection.

When you look at the status of a collection, you see a rollup of the status of all members of the collection. For example, consider a scenario in which you host an application that is used by multiple customers. The application uses multiple databases and OpenEdge brokers, and it spans several hosts. If your customers contract for premium services that include dedicated hosts, databases, and/or brokers, you can group resources based on which customers use them. In so doing, you can quickly assess the status of the application for any of the supported customers.

Collection terminology and hierarchy

Collections are categorized as follows:

- **My Collections** — Private collections that you create and that are available only to you.
- **Shared Collections** — Collections that are created by administrator users. Administrator users can view, reference, edit, and delete shared collections; operator users can view and reference shared collections.
- **Referenceable collection** — Any collection that you tie as a child to either **My Collections** or **Shared Collections** as a parent. When tied to **My Collections**, the collection becomes a private referenceable collection. When tied to **Shared Collections**, the collection becomes a shared referenceable collection.

The advantage of creating a referenceable collection is that you can reference the collection from more than one place. Consider, for example, the case of a system resources collection whose members include CPUs, memory, and file systems for three different containers. You can create this system resources collection once, and tie it to a Shared Collection and a private collection. It is unnecessary to create the collection twice; you create it once, in one collection, and create a reference to it from another collection.

The referenceable collection can be referenced without being copied, thereby providing a single point of collection maintenance.

- **Child collection** — A collection whose parent was chosen through the **Parent** property. For details, see the “[Creating a collection](#)” section on page 3–8.

Sample collection scenario

When you create a collection, consider which resources it makes sense to group. Remember that a resource can be a member of more than one collection, so you have significant flexibility in how you organize collection members.

Consider the case of a large company that has Fathom Management monitoring multiple OpenEdge-based applications, such as Payroll, Finance, Accounts Receivable, and Shipping, that also span multiple hosts. In some instances, the applications also share resources.

By using Fathom’s collections feature, an administrator at the company could group resources based on the applications that use them, as follows:

- Payroll Collection:
 - Finance database on Host A.
 - Payroll database on Host B.
 - WebSpeed Broker on Host B.
 - System resources on Hosts A and B.

- Finance Collection:
 - Finance database on Host A.
 - Accounts Receivable database on Host C.
 - AppServer Broker on Host A.
 - System resources on Hosts A and C.
- Accounts Receivable Collection:
 - Accounts Receivable database on Host C.
 - AppServer Broker on Host C.
 - System resource on Host C.
- Shipping Collection:
 - Shipping database on Host D.
 - Accounts Receivable database on Host C.
 - WebSpeed Broker on Host D.
 - System resources on Hosts C and D.

By looking at a particular collection, an administrator could easily determine the status of any application. Each application collection contains the set of resources that the application depends on, and a failure in a resource is reflected in the status of the collections that use that resource.

Working with collections

You can create, edit, or delete a collection.

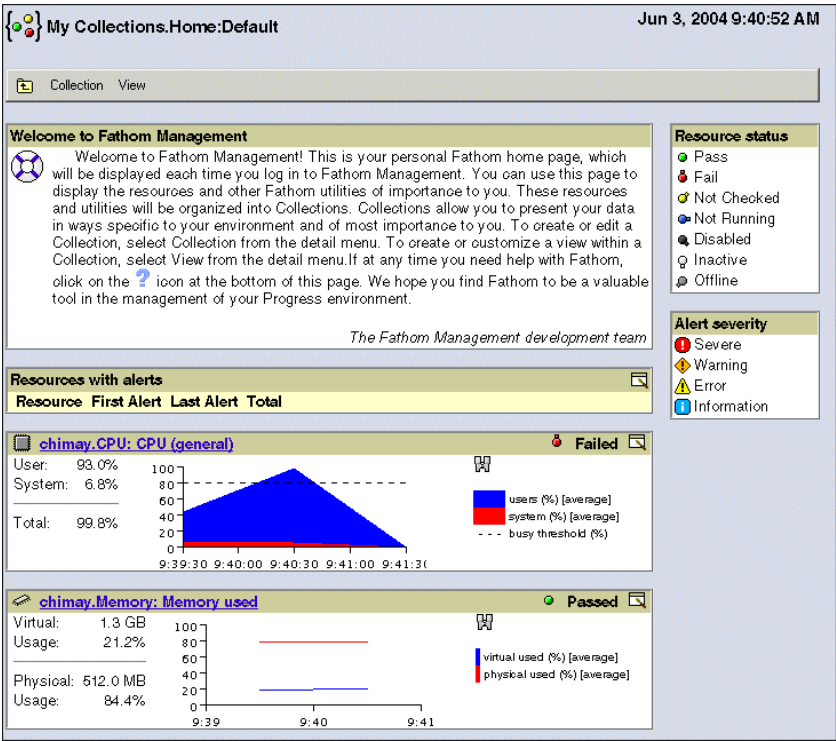
Creating a collection

An administrator can create a private or shared collection. An operator can create only a private collection.



To create a collection of Fathom resources:

1. Click **My Fathom** on the Fathom menu bar. The **My Collections.Home** page appears in the detail frame:



2. From the detail menu, choose **Collection**→**New Collection**. The **Create Collection** page appears:

3. Provide the following properties:
- **Name** — Type the name of the collection.
 - **Parent** — From the dropdown list, choose the parent collection (thereby making the newly created collection a child):

My Collections	Collections that are private and available only to you.
My Collections Home	A collection created by default for a user.
Shared Collections	Collections available to all other users of Fathom.

- **Description** — An optional description of the collection.

4. Select the members of the collection by following these steps:
- a. In the **List resource of type** field, you can choose resource types either by choosing from the available resources or by choosing the wildcard (*). If you choose the wildcard, all resource types are selected. In addition, any newly created resource will automatically be added as a member of the collection, and any deleted resource will automatically be deleted from the collection.
 - b. In the **for container** field, you can choose the containers either by choosing from those available or by choosing the wildcard. If you choose the wildcard, all containers are selected. Any newly created container will automatically be added as a member of the collection, and any deleted container will automatically be deleted from the collection.
- Note that you can also choose all available referenceable collections by choosing **collections** in the **for Container** field.
5. Click **Apply Filter**. The list of collections that match the filter specifications appear in the **Available** list, as shown in the following database resources example:

Create Collection:

Save

Cancel

Properties

Name:

Invntry_and_Bkordr_DBs

Parent:

My Collections.Home

Description:

A collection of databases related to inventory and backorders.

Members

Available

Filter

List resource of type:

Database

for container:

nbaspauldixp

Apply Filter

Available

nbaspauldixp.Database.*

nbaspauldixp.Database.Backorders

nbaspauldixp.Database.FathomTrendDatabase

nbaspauldixp.Database.Inventory

Select All

Selected

Select All

6. Select the resources:

- To select all the databases, for example, as members of the collection, click **Select All**. Then click the right arrow.
- To choose one or more individual databases, highlight and click each database you want to include; then click the right arrow.

The databases appear in the **Selected** list:

Create Collection:

Save Cancel

Properties

Name: Invntry_and_Bkordr_DBs

Parent: My Collections.Home

Description: A collection of databases related to inventory and backorders.

Members

Available Filter

List resource of type: Database


for container: nbaspauldixp

Apply Filter


Available	Selected
nbaspauldixp.Database.*	nbaspauldixp.Database.Backorders
nbaspauldixp.Database.FathomTrendDatabase	nbaspauldixp.Database.Inventory


Select All Select All

7. Click **Save**. The default view page for that new collection appears:







 **My Collections.Home.Invntry_and_Bkordr_DBs:Default**
A collection of databases related to inventory and backorders.

May 31, 2004 5:28:33 PM

 Collection

 View

Resources with alerts

Resource	First Alert	Last Alert	Total
  nbaspauldixp.Backorders	May 31, 2004 8:07:59 AM	May 31, 2004 5:28:32 PM	3
  nbaspauldixp.Fathom	May 31, 2004 8:07:59 AM	May 31, 2004 5:28:32 PM	1
  nbaspauldixp.Inventory	May 31, 2004 8:07:59 AM	May 31, 2004 5:28:32 PM	3





Running jobs

Name	PID	Start Time	Command
No jobs running			

Running reports

Name	PID	Start Time
No reports running		

Collection members

Name	Description
  nbaspauldixp.Backorders	
  nbaspauldixp.Inventory	

Editing a collection

You can edit a private collection (and a shared collection, if you are an administrator).



To edit a collection:

1. From the **My Fathom** page list frame, choose the collection you want to edit from the private **My Collections** list or the **Shared Collections** list.
2. From the detail menu, choose **Collection**→**Edit Collection**. The **Edit Collection** page appears:

The screenshot shows the 'Edit Collection' dialog box for a collection named 'nbaspauldixp.DBCollection'. The dialog has a title bar with a small icon and the text 'Edit Collection: nbaspauldixp.DBCollection'. Below the title bar are 'Save' and 'Cancel' buttons. The main area is divided into two sections: 'Properties' and 'Members'.

Properties section:

- Name:** A text field containing 'DBCollection'.
- Parent:** A dropdown menu showing 'Shared Collections'.
- Description:** A large text area with a small icon and a dropdown arrow on the right.

Members section:

- Available Filter:** A section with two dropdown menus: 'List resource of type:' (showing '*') and 'for container:' (showing '*'). Below these is an 'Apply Filter' button.
- Available:** A list box containing two items, each with a blue circular arrow icon next to it.
- Selected:** An empty list box.
- At the bottom of each list box are 'Select All' buttons.

3. Edit the collection as you want. When you finish, click **Save**.

Deleting a collection

You can delete a collection you no longer need.



To delete a collection:

1. From the **My Fathom** page list frame, choose the collection you want to delete from the private **My Collections** list or the **Shared Collections** list.
2. From the detail menu, choose **Collection→Delete Collection**. A message appears asking you if you want to delete the collection.
3. Click **OK**. The collection is deleted.

Collection views

You can create, edit, and delete a collection view from the detail menu bar.

What is a collection view?

A collection view consists of individual viewlets. Each viewlet summarizes particular content, such as which resources have alerts or which active monitoring plans exist.

Working with collection views and viewlets

Each collection view contains one or more viewlets. There are three types of viewlets: resource, standard, and view panel.

Resource viewlets

A resource viewlet is specific to a single instance of a resource. In [Figure 3–2](#), for example, each viewlet shows information about the FathomTrendDatabase resource.

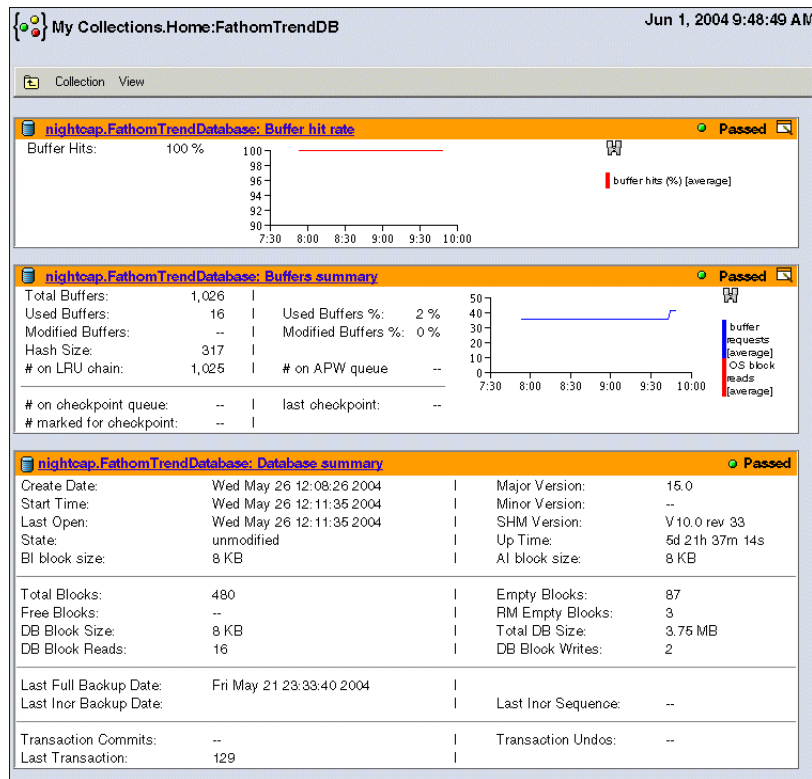


Figure 3–2: Sample resource viewlets

Standard viewlets

A standard viewlet is predefined by Fathom for displaying content about multiple resources or other aspects of Fathom.

For example, as shown in [Figure 3–3](#), you can set up a viewlet of active monitoring plans.

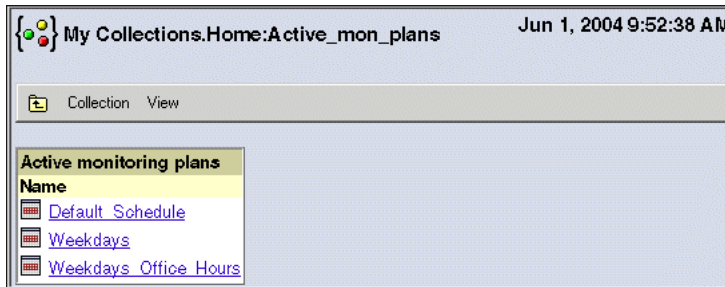


Figure 3–3: Sample Standard viewlet

The viewlet displays the currently active monitoring plans (or schedules).

Other standard viewlets that Fathom provides are as follows:

- **Collection members** — A list of all members of the collection, including other collections. A description of the member also appears, if available.
- **Active monitoring plans** — A list of all active resource monitoring plans.
- **Running reports** — The currently running reports, shown in tabular format. You can customize the view by selecting the fields to display for each report.
- **Alert severity legend** — An explanation of the different icons used to indicate the severity of an alert.
- **Resources with alerts** — A list of resources with open alerts as well as summary information, such as the date and the time of the last occurrence. Each resource name is preceded by its container name.

You can customize the view by selecting the fields to display for each resource.

- **Running jobs** — The currently running jobs, shown in tabular format. You might want to customize the view by selecting fields to display for each job, or by limiting the display to jobs running greater than some period of time.
- **Resource status legend** — An explanation of what certain data in the viewlet represents.

View panel viewlets

A view panel viewlet displays a view for any other collection being referenced by the active collection. Your ability to define views in one collection that you can display in another collection contributes to centralized, streamlined maintenance while also eliminating the need to create duplicate viewlets of the same data.

Figure 3–4 shows the **sample** view in the **My Collections.Home.DBs** collection. The **sample** view contains viewlets showing the **View left panel** and the **View right panel** of the **Default** view in the **DBs.OEserver** collection.

My Collections.Home.DBs:sample All dbs Jun 7, 2004 9:38:30 AM

Collection View

DBs: OEserver: Default: View left panel

Resources with alerts

Resource	First Alert	Last Alert	Total
nbaspauldixp.Fathom	Jun 7, 2004 9:20:48 AM	Jun 7, 2004 9:20:48 AM	1

Running jobs

Name	PID	Start Time	Command
No jobs running			

DBs: OEserver: Default: View right panel

Collection members

Name	Description
nbaspauldixp.asbroker1	
nbaspauldixp.NS1	
nbaspauldixp.wsbroker1	

Running reports

Name	PID	Start Time
No reports running		

Collection members

Name	Description
nbaspauldixp.OEserver	OEserver
nbaspauldixp.Backorders	
nbaspauldixp.FathomTrendDatabase	
nbaspauldixp.Inventory	

Figure 3–4: View panel viewlets

Viewlet characteristics

Note the following facts about viewlets:

- The title bar of a resource viewlet provides basic status information about the resource. This includes the most recent polling status (**Passed** or **Failed**, for example) as well as whether the resource has any outstanding alerts. In [Figure 3–5](#), the CPU has passed its last poll and has no outstanding alerts.

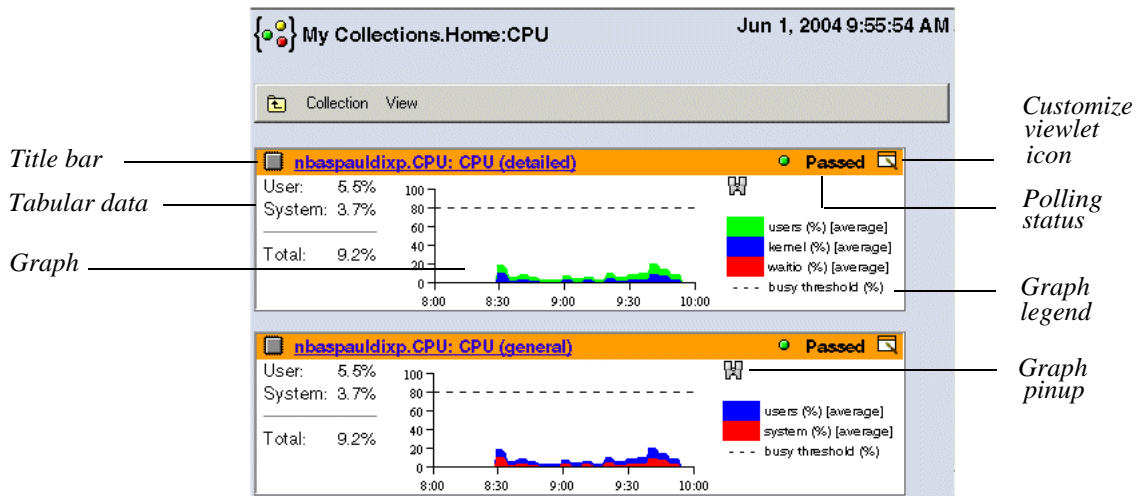


Figure 3–5: CPU viewlet

- If the resource has any outstanding alerts, the title bar color is set to the worst-case severity of the open alerts for the resource. For example, if a resource has an outstanding alert with a severity of **Error**, the title bar is yellow as you view it in your browser. Note that it is possible for a resource to have a status of **Passed** but still have outstanding alerts.
- The viewlet provides information in both tabular and graphical format.
- The legend indicates that the graph is showing the percentage of time the resource is busy for the represented time frame.
- The **Customize Viewlet** icon allows you to choose how the viewlet displays data. For details, see the [“Customizing a viewlet”](#) section on page 3–24.

Creating a collection view

Fathom provides a default **My Fathom** page for each user. You can use the **My Fathom** page to create collection views and choose exactly what kinds of information you want to see.



To create a new collection view in My Fathom:

1. From the detail menu, click **View→New Collection View**. The **Create** page appears.
2. Type the name of the collection in the **Name** field.
3. Choose the standard viewlets you want to display in the view by selecting one or more of the options in the **Standard viewlets to show** area:

Standard viewlets to show	
<input type="checkbox"/> Collection members	<input type="checkbox"/> Resources with alerts
<input type="checkbox"/> Active monitoring plans	<input type="checkbox"/> Running jobs
<input type="checkbox"/> Running reports	<input type="checkbox"/> Resource status legend
<input type="checkbox"/> Alert severity legend	

4. Choose the resource viewlets you want to display for each individual database resource by selecting one or more of the options in the **Viewlets to show** area, as shown in the following example for the **Backorders** database resource in the container **nbaspauldixp**:

nbaspauldixp.Backorders	<input type="checkbox"/> Database summary	<input type="checkbox"/> User summary
	<input type="checkbox"/> Open transactions	<input type="checkbox"/> Open transactions (active)
	<input type="checkbox"/> Buffer summary	<input type="checkbox"/> Transaction activity
	<input type="checkbox"/> Checkpoint activity	<input type="checkbox"/> Buffer hit rate
	<input type="checkbox"/> Record wait/read ratio	<input type="checkbox"/> Record activity
	<input type="checkbox"/> APW performance	<input type="checkbox"/> BIW performance
	<input type="checkbox"/> BIW writes percent	<input type="checkbox"/> AIW performance
	<input type="checkbox"/> AIW writes percent	<input type="checkbox"/> APW summary
	<input type="checkbox"/> Checkpoint summary	<input type="checkbox"/> BI summary
	<input type="checkbox"/> BI buffer waits (actual)	<input type="checkbox"/> BI busy buffer waits
	<input type="checkbox"/> BI empty buffer waits (percent)	<input type="checkbox"/> BI partial writes (percent)
	<input type="checkbox"/> BI partial writes (actual)	<input type="checkbox"/> AI summary
	<input type="checkbox"/> AI busy buffer waits	<input type="checkbox"/> Area Space Usage
	<input type="checkbox"/> Area Space Utilization	<input type="checkbox"/> Area Space Total
	<input type="checkbox"/> Area reads	<input type="checkbox"/> Area writes

Each of these viewlets supplies detailed information about some aspect of a database.

5. Choose any other resource viewlets you want to include in the collection view.

6. Choose the view panel viewlets you want to appear (if available). For example, you might have one referenced collection whose views are available:

DBs: OEservers		
Default	<input type="checkbox"/> View left panel	<input type="checkbox"/> View right panel
OEserversview	<input type="checkbox"/> View left panel	<input type="checkbox"/> View right panel

7. Click **Save** when you finish making your selections. The resource and standard viewlets you chose for display appear:

My Collections.Home:Backorders

Jun 1, 2004 11:21:51 AM

CollectionView

nbaspauldixp.Backorders: Database summary

Passed

Create Date:	Tue May 11 11:03:20 2004	Major Version:	15.0
Start Time:	Tue Jun 01 11:21:34 2004	Minor Version:	--
Last Open:	Tue Jun 01 11:21:34 2004	SHM Version:	V10.0 rev 33
State:	unmodified	Up Time:	0m 17s
BI block size:	8 KB	AI block size:	8 KB
Total Blocks:	904	Empty Blocks:	16
Free Blocks:	116	RM Empty Blocks:	3
DB Block Size:	4 KB	Total DB Size:	3.53 MB
DB Block Reads:	23	DB Block Writes:	3
Last Full Backup Date:			
Last Inor Backup Date:		Last Inor Sequence:	--
Transaction Commits:	--	Transaction Undos:	--
Last Transaction:	169		

Collection members

Name	Description
nbaspauldixp.Invntry_and_Bkordr.DBs	A collection of databases related to inventory and backorders.
Monthly_Compaction	
nbaspauldixp.asbroker1	
nbaspauldixp.Backorders	
nbaspauldixp.CPU	Default CPU resource
nbaspauldixp.Disk-0_C_	Default disk resource
nbaspauldixp.FathomTrendDatabase	
nbaspauldixp.FileSys-C_	Default file system resource
nbaspauldixp.idrepos	
nbaspauldixp.Inventory	
nbaspauldixp.logfile12	
nbaspauldixp.Memory	Default memory resource
nbaspauldixp.NS1	
nbaspauldixp.SMTP_MAIL	Default operator e-mail monitor.
nbaspauldixp.test	
nbaspauldixp.wsbroker1	
nbaspauldixp.wsdynamics1	

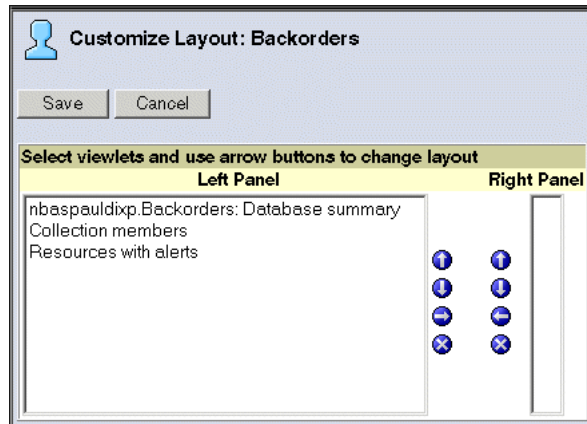
Customizing the view layout

You have the option of overriding the default view column layout and the order in which the viewlets appear in a column.



To customize the view layout:

1. From the detail menu, choose **View**→**Customize View** <name of view>→**View Layout**. The **Customize Layout** page appears for the view you chose:








The **Left Panel** box lists the viewlets that appear in the left panel of the layout, and the **Right Panel** box lists the viewlets that appear in the right panel of the layout. The order of the viewlets as listed in a panel corresponds to the order in which the viewlets appear in the collection view.

Note that the width of the panel in the layout is determined by its contents.

- 2. Use the directional buttons to move viewlets within a panel or from one panel to the other, as described in [Table 3–1](#).

Table 3–1: Moving the viewlets

Click this button...	To move the viewlet...
	Up one position in the panel.
	Down one position in the panel.
	From the left panel to the right panel.
	From the right panel to the left panel.
	Out of the collection view (which deletes the viewlet).

- 3. Click **Save** when you finish organizing the viewlets. The collection view page reappears, with the viewlets organized as you specified.

Editing a collection view

You can change the content or layout of a collection view.



To edit a collection view:

- 1. Open a view, and choose **Customize View <name of view>→View Content** or **View Layout**.
- 2. Make the changes you want.
- 3. Click **Save**. The view page reappears with the newly chosen viewlets displayed.

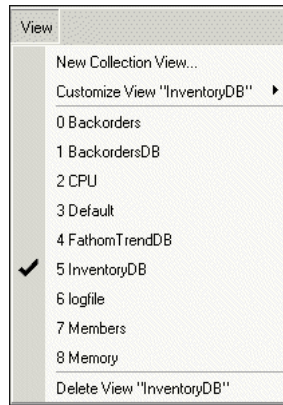
Deleting a collection view

You can delete a view you no longer need; however, use caution as you do so. Be sure that you are deleting the currently active view and not one that you were using previously.



To delete a collection view:

1. Open the view.
2. From the detail menu, choose **View**. A list of views appears, with the currently active view preceded by a checkmark, as shown:



3. If the active view is not the one you want to delete, click the view you do want to delete. The view you clicked becomes the active view.
4. Once you determine that the view identified as active is the one you want to delete, choose the **Delete View** command at the bottom of the menu. A message appears asking you to confirm that you want to remove the view.
5. Click **OK**. The view is deleted.


Customizing a viewlet

In addition to choosing the content and layout for a view, you can also customize many of the individual viewlets. A customizable viewlet has a customize icon in the upper right corner; the icon appears in [Figure 3–6](#).



Figure 3–6: Customize Viewlet icon

If you click the **Customize Viewlet** icon on a **Memory** viewlet, for example, the **Customize Viewlet** page shown in [Figure 3–7](#) appears.

 **Customize Viewlet: "nbaspauldixp.Memory: Memory (physical) used"**

SaveCancel

Select viewlet components to display

☒ Resource name in title

☒ Resource status in title

☒ Tabular data

☒ Graph

Layout: ☒ Horizontal ☐ Vertical

Select graph properties

Family:Type:

current:☐ pie ☐ bar ☐ column

meter:☐ full ☐ half left ☐ half right ☐ half bottom ☐ half top

historical:☒ line ☐ hi/low ☐ column ☐ area ☐ stacked column ☐ stacked area

Size:

☐ tiny ☒ small ☐ medium ☐ large ☐ very large

Max display time*: 2 hours

Legend:☒ on ☐ off

☒ on ☐ off

☐ on ☒ off

Average*:☒ on ☐ off

☒ 2D ☐ 3D

☐ on ☒ off

Pinup:☒ on ☐ off

☐ on ☒ off

☒ on ☐ off

Dimensionality*:☒ 2D ☐ 3D

☐ on ☒ off

☒ on ☐ off

Grid*:☐ on ☒ off

☒ on ☐ off

☐ on ☒ off

Threshold*:☒ on ☐ off

☐ on ☒ off

☐ on ☒ off

* a grayed background indicates the selection is ineffective for the graph type selected

Figure 3–7: Customizing a viewlet

3–24

**To customize the viewlet:**

1. Select only the viewlet components you want to appear (and clear any components you do not want to include). For the **Memory** viewlet shown in [Figure 3-7](#), you can choose the following options:

- **Resource name in title** — The name of the resource.
- **Resource status in title** — The status of the resource.
- **Tabular data** — Data displayed in a table.
- **Graph** — Whether to display a graph or not.
- **Layout** — The way the viewlet data appears.

A typical viewlet display shows the data in three different sections: tabular, graph, and legend. If you choose to see the data in a vertical format, the sections stack on top of one another instead of being positioned side by side. This results in a narrower but taller display of the viewlet contents. If column width is of concern to you, choose the **Vertical** option.

If you want the sections to display side by side, choose the **Horizontal** option.

2. Select the following graph properties:
 - **Family — Current, meter, or historical.** Current and meter graphs produce only the most current view of the polling sample, if the data being presented is sensible in that format. Typically, a current graph is used to display multiple values, whereas a meter graph displays only one datum.

If the data you want to display does not make sense in a particular family, the option does not appear.

Historical graphs always show multiple points in time.

- **Size** — Tiny, small, medium, large, or very large.

- **Max display time** — Available only for historical reports. Choose the display time from the dropdown list; the maximum time possible depends on the graph cache. Note that the higher you set the maximum display time, the more processing time will be required to produce the data; and the fewer details will be visually evident.

For details about the graph cache, see the *Installation and Configuration Guide*.

If the background for the **Max display time** field is gray, the option is not applicable for the graph type selected.

3. Set the following properties **on** or **off**:

- **Legend** — An explanation of what the colors in the graph represent.
- **Pinup** — Whether you can create a separate pinup version of the graph.
- **Anti aliasing** — Further processing on an image to make image's lines cleaner and smoother. If image quality is important, turn this option on. However, if image quality is not of concern, turn the option off, since the anti aliasing process takes both CPU time and disk space.
- **Average** — Whether Fathom does averaging of data values. Fathom takes the data and computes weighted averages to reduce the number of data points and create more meaningful data points for the graph image.
- **Grid** — A grid to help you examine data more closely.
- **Threshold** — Whether rule thresholds, if available and currently in use, are displayed on the graphs.

4. Select the **Dimensionality** by choosing **2D** or **3D**.

5. Click **Save** when you finish choosing the components and properties.

An example of a customized **Memory** viewlet appears in [Figure 3–8](#).

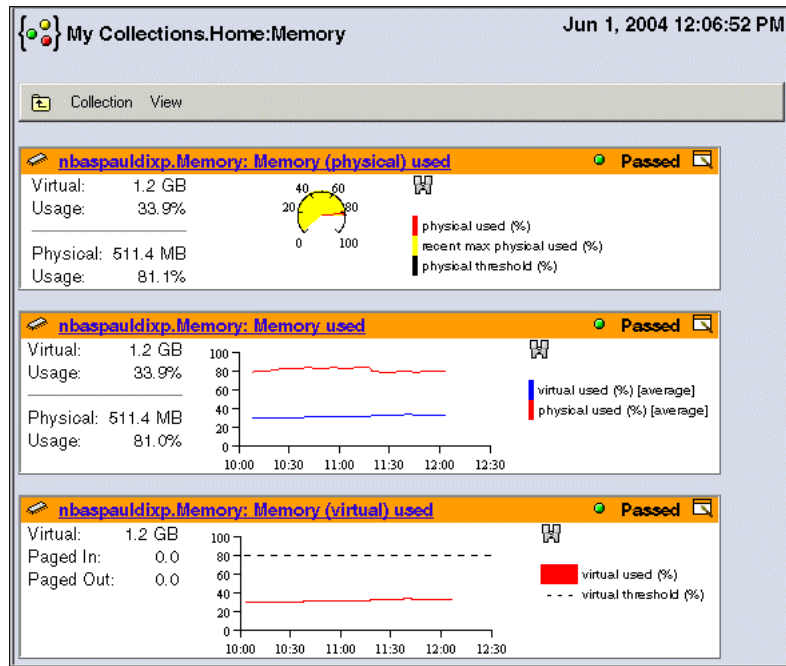


Figure 3–8: Customized viewlet

The customizing options that a viewlet provides depend on the particular viewlet and apply only to the selected viewlet in a single view. You can display different options in different views.

Setting up Resource Monitoring

This chapter describes how to create a resource you want to monitor and define its monitoring plan, including schedules and rules. The chapter also describes how to establish meaningful threshold values for rules and how to create actions that occur in response to Fathom alerts.

The chapter contains the following sections:

- [Before you begin](#)
- [Monitoring remote resources](#)
- [Monitoring a system, network, or file resource: an overview](#)
- [Working with CPU and memory resources](#)
- [Selecting a system, network, or file resource to monitor](#)
- [Creating a resource monitoring plan](#)
- [Calculating meaningful thresholds with the Configuration Advisor](#)
- [Understanding alerts](#)
- [Determining Fathom's action in response to an alert](#)
- [Using default actions](#)
- [Editing or copying a resource monitor](#)

- [Deleting a resource monitor](#)
- [Working with default values](#)
- [Using job and report templates](#)
- [Sharing monitoring components using the Fathom Library](#)

Before you begin

Examining current resource considerations and future operational needs will help you make some preliminary decisions about resource monitoring before you set up specific monitoring criteria in Fathom Management.

For example, consider these points as you think through your current resource-related operations and processes:

- Which employee at your company is typically notified that a resource is down, and what method do you typically use to contact that individual? Is it possible that there is too much downtime between a resource trouble report and the response from personnel assigned to handle a given problem? Do problems stack up because you do not currently have a system in which these problems are prioritized and queued for the right person's attention?
- What is your typical weekly resource load? Can you define the peak load times for your applications? If so, do you have procedures in place to address the higher-than-average strain these events place on your resources? Similarly, do you also experience idle time? Do you adequately plan this slower-than-normal time into your schedule so that you routinely run particular processes at this time?
- Do you have a scheduling process that helps you not only run your applications, but also automatically notify interested personnel when these jobs are done? Can these processes also alert you to a problem and take predefined, corrective action?

As these questions suggest, there are considerations you must address as you move from your present approach for determining your resource needs to systematically analyzing and fulfilling these needs using Fathom Management.

Monitoring remote resources

You can monitor remote disks, CPU, memory, file systems, databases, and OpenEdge server components, such as AppServer, NameServer, and WebSpeed resources, once you run the Fathom Remote Configuration Utility. See [Chapter 6, “Configuring Remote Monitoring for Fathom”](#) in the *Installation and Configuration Guide* for details about the utility.

Note: This guide does not describe monitoring databases remotely. See the *Database Management Guide* for details about remote databases.

Naming conventions

Observe the following naming conventions when you create a resource monitor:

- You cannot have two resources of the same type with the same name.
- When you name a resource, the name must be HTML-compliant. HTML-compliant means that the value you enter in the **Name** field follows the formatting rules and conventions that the Hyper Text Markup Language honors. For example, you cannot enter spaces between words or use special characters such as an asterisk (*), an ampersand (&), or a period.
- When you delete a resource, the name used for that resource becomes available for you to use again.

Monitoring a system, network, or file resource: an overview

Using Fathom Management, you can monitor the specific resources you want.



To monitor a resource:

1. Select the type of resource you want to monitor.
2. Define the resource monitor's properties. The properties you define depend upon whether you select a system, network, or file resource and can include name, description, file name, host, or port, for example.

3. Create a monitoring plan for the resource, which includes:
 - **A monitoring plan definition** — The monitoring plan definition identifies the schedule you want Fathom to follow when monitoring, how often you want Fathom to poll the resource, and whether you want to enable alerts for the resource. Alerts notify you of potential problems with the resource's performance.
 - **Rule definitions** — Rule definitions specify under what circumstances Fathom generates an alert for the resource and what action Fathom should take, if any, as a result of the alert. You can choose from several different actions, such as sending an e-mail to a specific recipient, or adding an entry to a particular log file.
 - **Rule sets** (for log files and OpenEdge server components) — Each rule set is a logical grouping of one or more rules.
 - **Schedules** — A schedule is a block of monitoring time.
4. Optionally use the Configuration Advisor to calculate more meaningful threshold values for resource rules.

Monitoring a database or an OpenEdge resource

The information presented in this guide pertains primarily to system, network, and file resource types, unless otherwise noted. Much of the information, however, also applies to database and OpenEdge server resource monitors. For details about creating database resource monitors, see the *Database Management Guide*. For details about creating resource monitors for OpenEdge server components, see the *OpenEdge Server Management Guide*.

Working with CPU and memory resources

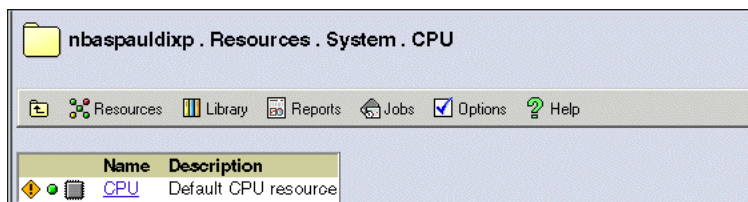
Monitoring a CPU resource or a memory resource is essentially the same as monitoring any other resource with Fathom. The one difference, however, is that Fathom automatically sets up one of each of these resources with default values when you initially start Fathom. You cannot delete either the CPU resource or the memory resource, nor can you create additional instances of either resource type.



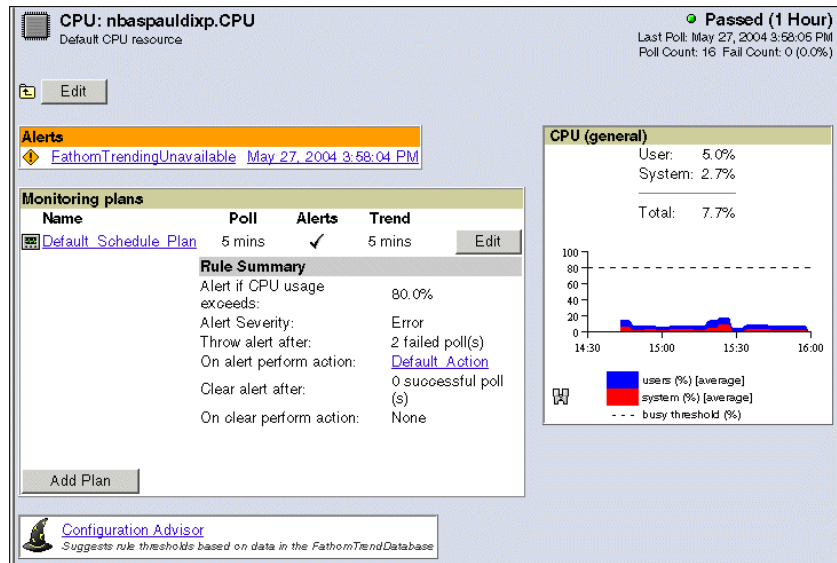
To access detailed information about each of these predefined resources:

1. Select **Resources** from the menu bar.
2. In the list frame, sort by **Type**.
3. Select **System→CPU** or **System→Memory** resource in the list frame.

The **Resources System** page appears. For example, if you select **CPU**, the following page appears:



- Click a resource in the **Name** column. The **CPU** page appears, showing the default values for the resource:



You can now accept the default values or replace them with values you prefer. See the “[Selecting a system, network, or file resource to monitor](#)” section on page 4–8 for more information about replacing the values.

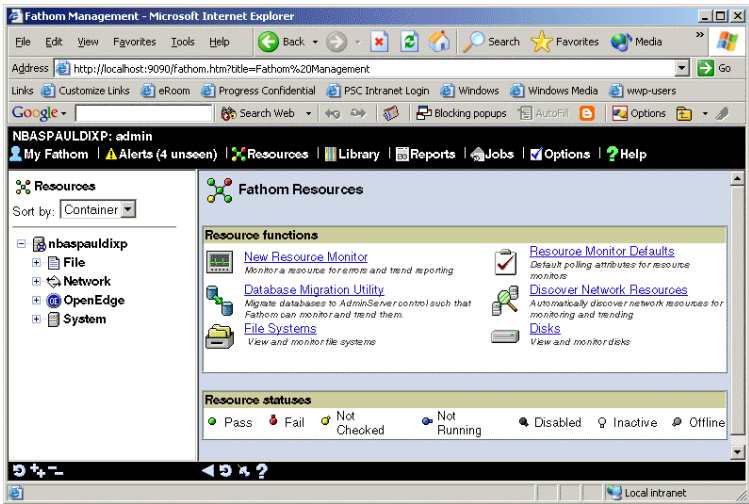
Selecting a system, network, or file resource to monitor

Fathom automatically creates one CPU resource and one memory resource for each container. You use the management console to create additional system, network, or file resources to monitor.

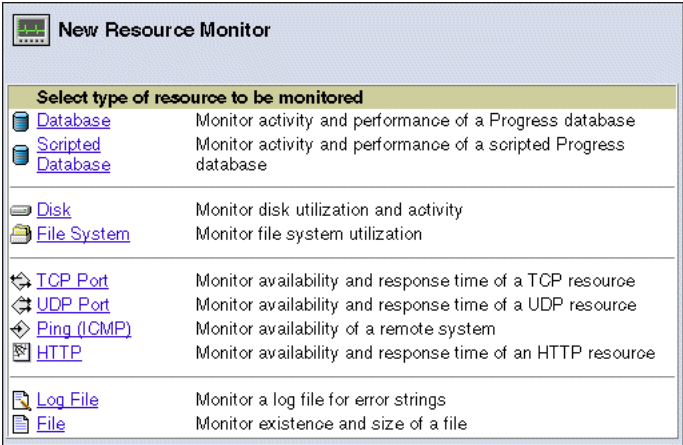


To create a resource monitor:

- 1. Select **Resources** from the menu bar. The **Fathom Resources** page appears:



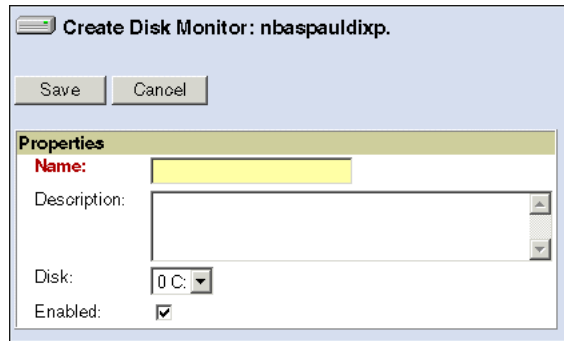
- 2. Click **New Resource Monitor**. The **New Resource Monitor** page appears:



3. From the list of resource types available, select the specific resource for which you want to add a resource monitor.

Note: For the purpose of illustration, the procedures in this section describe how to create a disk resource monitor and then define its properties and monitoring plan.

4. Click **Disk**. The **Create Disk Monitor** page appears:



The screenshot shows a dialog box titled "Create Disk Monitor: nbaspauldixp.". At the top, there are "Save" and "Cancel" buttons. Below them is a section titled "Properties". Inside the "Properties" section, there are four fields: "Name:" with a yellow-highlighted text input field; "Description:" with a large text area; "Disk:" with a dropdown menu currently showing "0 C:"; and "Enabled:" with a checked checkbox.

If there are remote containers online, a dropdown list of container names also appears.

You can now specify the resource's properties.

5. Enter the name of the resource in the **Name** field. For all resources, this value must be less than or equal to 32 characters with no spaces between words. Also, you cannot use periods or special characters.
6. Enter a description of the resource in the **Description** field. You can enter a maximum of 256 characters.
7. From the **Disk** drop-down list, select the disk for which you are creating this resource monitor. The drop-down list displays the reference that your operating system uses to recognize each disk drive available on your system.
8. Select the **Enabled** option to enable the resource monitor to begin monitoring. This option is usually checked by default. (If you want to create a monitor that does not immediately begin monitoring, clear the option. The monitor is then disabled until you enable it.)

9. Click **Save**. The **Create Monitoring Plan** page appears:

NBASPAULDIXP: admin
 My Fathom | Alerts (2 unseen) | Resources | Library | Reports | Jobs | Options

Resources
 Sort by: Type

- File
- Network
- OpenEdge
- System
 - CPU
 - Disk
 - FileSystem
 - Memory

Create Monitoring Plan for: nbaspauldixp.Disk1

Save Cancel

Monitoring plan definition

Available Schedules: Default_Schedule

Polling Interval: 900 seconds

Alerts Enabled: ☒

Trend Performance Data: ☐

Trend Performance Data every: 1 poll(s)

Rule definition

Alert if disk activity exceeds: 90.0 %

Alert severity: Error

Throw alert after: 1 failed poll(s)

On alert perform action: Default_Action

Clear alert after: 0 successful poll(s)

On clear perform action: Default_Clear_Action

You can now create the resource's monitoring plan.

Creating a resource monitoring plan

When you create a monitoring plan, you provide both a monitoring definition and one or more rule definitions.

The monitoring definition includes:

- The schedule selected from all the schedules that are available. The schedule specifies when the plan is active, and the available schedules include only those schedules that do not overlap with schedules already in use for a resource.
- A polling interval, which indicates the frequency with which this resource's rules are checked by Fathom.

- An option to enable alerts for this resource. Enabling alerts means that alerts will be generated while the plan is active.
- An option to store, or *trend*, the performance data collected by this resource to the FathomTrendDatabase while the plan is active. See the “[Trending considerations](#)” section on page 4–11 for details.
- The number of polls after which performance data will be trended to the FathomTrendDatabase.

The rule definition identifies:

- When to generate an alert for the resource.
- What level of alert severity will cause Fathom to generate an alert.
- The number of failed polls after which Fathom generates an alert.
- The action that Fathom performs when an alert is generated.
- The number of successful polls after which Fathom clears an alert.
- The action Fathom performs when an alert is cleared.

Trending considerations

You can choose to have Fathom trend performance data to the FathomTrendDatabase. Consider the following points when you are setting trending options:

- Different trend expectations exist for different resource types. Therefore, each trend interval has a different meaning depending on the data to be trended. Refer to the specific resource type in this guide for detailed information about data trending expectations for each resource type.
- If you set a trending value in the **Trend Performance Data every polls** field, Fathom will use the value you provide in combination with the value in the **Polling Interval** field to calculate the trending interval.

For example, if you initially set a **polling interval** of 30 seconds and also set the **Trend Performance Data every** field to trend data every 3 polls, Fathom will automatically calculate the trending interval as 90 seconds and display this result when you view the summary of the resource monitor’s performance.

Choosing a schedule for the monitoring plan

A schedule defines the block of time for which a set of monitoring rules is active for a resource. When you add a monitoring plan to a resource, you specify the schedule to indicate when the monitoring plan will be active.

Fathom provides several predefined schedules. You can use the schedules as they are, or you can modify them to suit your operating needs. You can also use an existing schedule as the basis for a new schedule, changing its name and characteristics.

Note: The schedules discussed in this section refer to schedules you associate with resource monitors. Schedules that define frequency of an activity are associated with jobs, job templates, reports, and report templates. For specific information about job schedules, see [Chapter 8, “Creating Jobs and Job Templates.”](#) For specific information about report schedules, see the relevant sections in the *Reporting Guide*.

Each schedule you create appears, along with the Fathom-provided schedules, in the list frame under the **Schedules** category, as shown in [Figure 4–1](#).

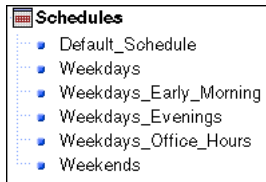


Figure 4–1: Schedules

General scheduling considerations

Keep the following points in mind regarding schedules:

- Before you create a new schedule, it is useful to review the existing schedules to determine if you can use or simply modify an existing schedule.
- You must create two separate schedules if you want to span an overnight period. For example, if you want to create a schedule that includes 8:00 PM through 8:00 AM, you must create two schedules:
 - 8:00 PM to 12 AM
 - 12:00 AM to 8:00 AM

You must also select the appropriate days for each schedule.

- You can schedule different rules to apply to a resource at different times and on different days. For example, you might want to monitor your OpenEdge databases more frequently during the week than on the weekends. To accomplish this, you can create and associate different schedules with each monitoring plan.
- You can associate more than one schedule with a resource, but you cannot associate overlapping schedules with a single resource.
- The selection list of available schedules for a monitoring plan does not include schedules that overlap their time or day criteria with other schedules or that are already in use by the resource.

Using predefined schedules

Fathom provides several predefined schedules that you can use in your monitoring plan. You can also use any predefined schedule as the basis for a new schedule, which you can then modify to suit your needs.

Table 4–1 describes the predefined schedules.

Table 4–1: Predefined schedules

Name	Block schedule defined for...
Default_Schedule	Sunday through Saturday, 24 hours per day. See the “Using the Default_Schedule” section on page 4–15 for more details.
Weekdays	Monday through Friday, 24 hours per day.
Weekdays_Early_Morning	Monday through Friday from 12 AM to 8 AM.
Weekdays_Evenings	Monday through Friday from 5 PM to 12 AM.
Weekdays_Office_Hours	Monday through Friday from 8 AM to 5 PM.
Weekends	Saturday through Sunday, 24 hours per day.

All predefined schedules appear in the management console list frame under the **Schedules** category when you select **Library** from the menu bar, as shown in Figure 4–2.

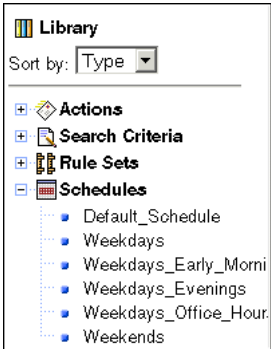


Figure 4–2: Predefined schedules

Once you have created a resource monitor, you can edit an existing schedule or create a new schedule to associate with it at any time.

Using the Default_Schedule

The **Default_Schedule** is a reusable 24/7 schedule that you can use or modify just as you can any other schedule, whether predefined by Fathom or created by you. However, the **Default_Schedule** is unique among all other schedules because:

- Fathom automatically associates it with new resources when you create them.
- You can edit it, but not delete or rename it.

Updating and deleting schedules

Once your resource monitor exists, you can update its schedule at any time. This task is accomplished by accessing the monitoring plans for the resource and selecting another schedule from the drop-down list of currently available schedules.

You cannot delete a schedule that is currently being used by a resource monitor.

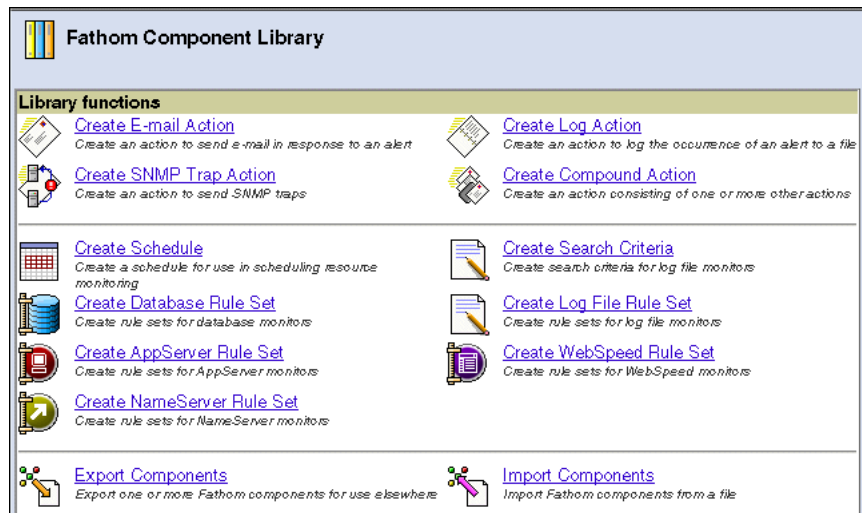
Creating a new schedule

You can create a new schedule from the **Fathom Component Library**.

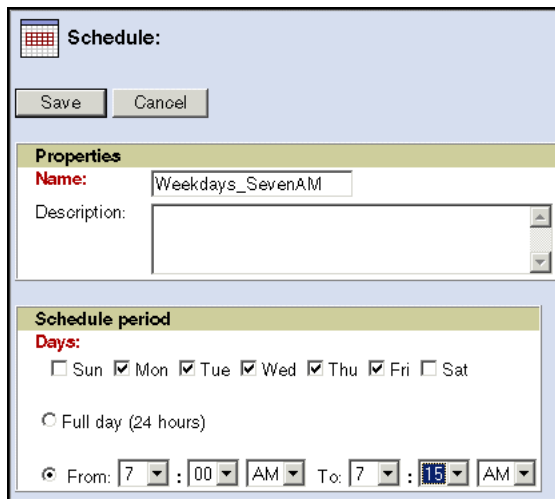


To create a new schedule:

1. Select **Library** from the menu bar. The **Fathom Component Library** page appears in the detail frame:



2. Click **Create Schedule**. The **Schedule** page appears.
3. Enter a name for the schedule in the **Name** field. You cannot enter spaces between words or use special characters such as an asterisk (*), ampersand (&), or period (.) in the **Name** field.
4. Enter a description of the schedule in the **Description** field. The **Description** field is for reference only. It appears in the schedule's title when you reaccess the schedule once you save it.
5. In the **Schedule period**, select the days and times you want the schedule to include (note that **Days** is a required field):



Schedule:

Save Cancel

Properties

Name: Weekdays_SevenAM

Description:

Schedule period

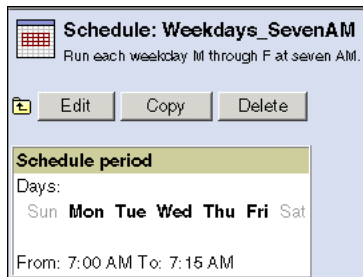
Days:

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

☐ Full day (24 hours)

☒ From: 7 : 00 AM To: 7 : 15 AM

6. Click **Save** to save the schedule or **Cancel** to discard the schedule. If you save the schedule, the detail frame displays the days and times of the new schedule:



Schedule: Weekdays_SevenAM

Run each weekday M through F at seven AM.

Edit Copy Delete

Schedule period

Days:

Sun Mon Tue Wed Thu Fri Sat

From: 7:00 AM To: 7:15 AM

You can edit the schedule you created, copy it to use as the basis for another new schedule, or delete it.

Adding rules to the monitoring plan

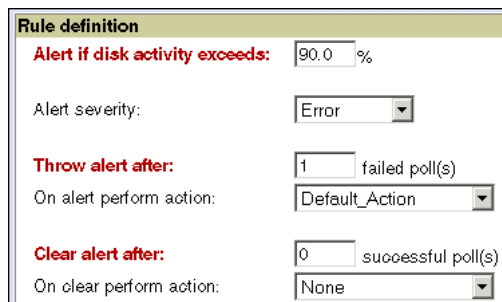
Rule definitions identify the specific attributes of a resource that you want to monitor, the severity of an alert Fathom generates in response to performance, and the action that occurs when an alert is generated. Rule definitions for system, network, and file resource types are composed of these elements:

- Specific rules you set for each resource type. For example, the rule definition for a disk resource includes the setting of an alert that triggers if disk activity exceeds a specified percentage.

Refer to the appropriate sections in [Chapter 5, “Monitoring System Resources,”](#) [Chapter 6, “Monitoring Network Resources,”](#) or [Chapter 7, “Monitoring File Resources”](#) for details about the specific rules for system, network, or file resources.

- **Alert severity**, which is one of four alert levels: **Information**, **Warning**, **Error**, or **Severe**.
- The **Throw alert after failed poll(s)** and **Clear alert after successful poll(s) fields**, which allow you to either monitor changing resource circumstances over any number of polling cycles rather than set an alert to occur immediately after a single failure of an active rule, or automatically clear the alert after a single successful cycle. Monitoring resource successes and failures over a number of polling intervals allows you to better reduce noise that would cause erroneous alerts due to normal fluctuation in resource behavior.
- The **On alert perform action** and **On clear perform action** fields, which indicate whether the alert initiates an action. Possible actions include the sending of an e-mail to a designated individual, the logging of the alert in a log file, or the combination of several different actions into one compound action.

[Figure 4–3](#) shows a sample rule definition for a disk resource type.



Rule definition	
Alert if disk activity exceeds:	90.0 %
Alert severity:	Error
Throw alert after:	1 failed poll(s)
On alert perform action:	Default_Action
Clear alert after:	0 successful poll(s)
On clear perform action:	None

Figure 4–3: Sample rule definition

Using default rules

Fathom provides default rule values for system, network, and file resources. A rule indicates a performance standard that you expect and about which you want notification when broken. Default values provided by Fathom suggest performance settings you can use when creating your resources.

Default rules help you to create your resources and associated values as quickly as possible. You can change default rule values to more specifically reflect your resource monitoring objectives at any time.

For more detailed information about the default rules and their default values, see the relevant sections in [Chapter 5, “Monitoring System Resources,”](#) [Chapter 6, “Monitoring Network Resources,”](#) and [Chapter 7, “Monitoring File Resources.”](#)

Using resource-specific rules

Each resource type has specific rules you can set to ensure that the resource monitoring data provides you with meaningful details about the resource. For example, you set a CPU resource monitor to monitor CPU-related performance characteristics, and you set a disk resource monitor to monitor disk-related performance characteristics. Resource-specific rules reflect how trend data intervals have different meaning to the various resource types.

Sharing rules and rule sets

You can logically group multiple rule definitions for certain (complex) rule types, such as log file monitors, AppServers, NameServers, WebSpeed Transaction Servers, and databases. These rule combinations, called *rule sets*, are established and stored in the Fathom Component Library. A rule set comprises one or more rule definitions.

One of the advantages of using rule sets is that they are late-binding: a change to the rule set (such as adding, deleting, or modifying a rule definition) will propagate to all monitoring plans that use the rule set.

By sharing groups of rule definitions, you can manage a large number of resource monitors consistently and efficiently. For example, once a rule set exists, you can associate it with a log file monitor’s monitoring plan. When the monitoring plan is active and the log file monitor is polled, Fathom can evaluate each rule in the set. See [Chapter 7, “Monitoring File Resources,”](#) for details about how log file monitors use rule sets; see the [Database Management Guide](#) for details about database resources and rule sets; and see the [OpenEdge Server Management Guide](#) for details about AppServer, NameServer, and WebSpeed rule sets.

Choosing a rule's values

You can accept the default resource rule values, or you can set your own values.



To review and change rule definitions or other default values for a sample disk resource:

1. Click the **Disk** category in the list frame. The list of disks appears in the detail frame.
2. Click the disk resource. The **Disk Monitor** page opens.
3. In the monitoring plan, click either a schedule or its **Edit** button. (The **Edit** button is located to the right of the plan's trending information.)

The **Monitoring Plan** page for the disk opens.

4. Review the rule definition:
 - Accept or change the default value that displays in the **Alert if disk activity exceeds** field. This is the only rule unique to setting up a disk resource monitor. For example, you might want to perform disk monitoring to determine if your disk usage is greater than 75 percent busy at certain peak times during the work week. In this field, override the default value of 90.0 with **75.0**.
 - Accept the default alert severity, or choose another severity option from the drop-down list associated with the **Alert severity** field.

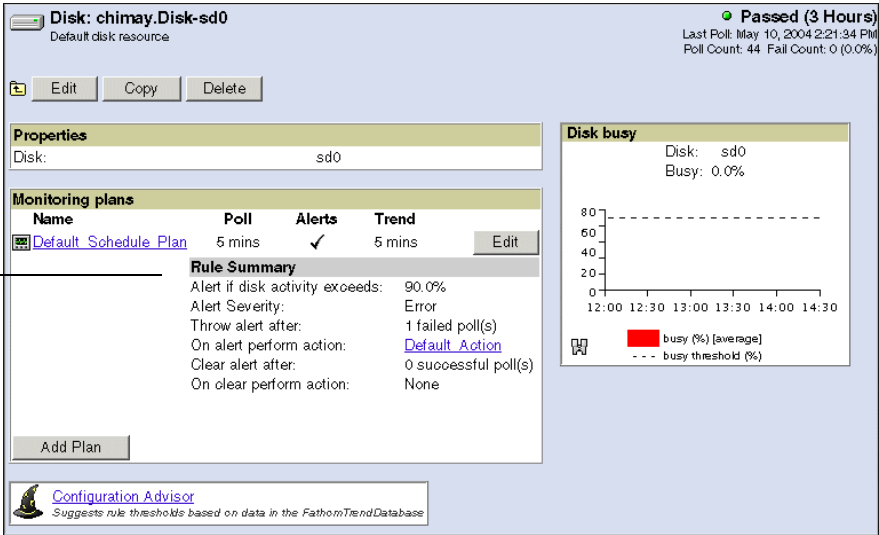
- Identify alert behavior by accepting or changing values in the following fields:

Field	Description
Throw alert after: failed poll(s)	Indicates how many times in a row the polling interval must fail before an alert is generated.
On alert perform action	Triggers the action you specify to occur when an alert is generated.
Clear alert after: successful poll(s)	Indicates the number of sequential successful polls that must occur before an alert is cleared.
On clear perform action	Triggers the action you specify when an alert is cleared.

Note that by default the **On alert perform action** displays with the **Default_Action** displayed. You can elect to use or change to another action. However, the **On clear performance action** displays a default value of **None**; this field is optional.

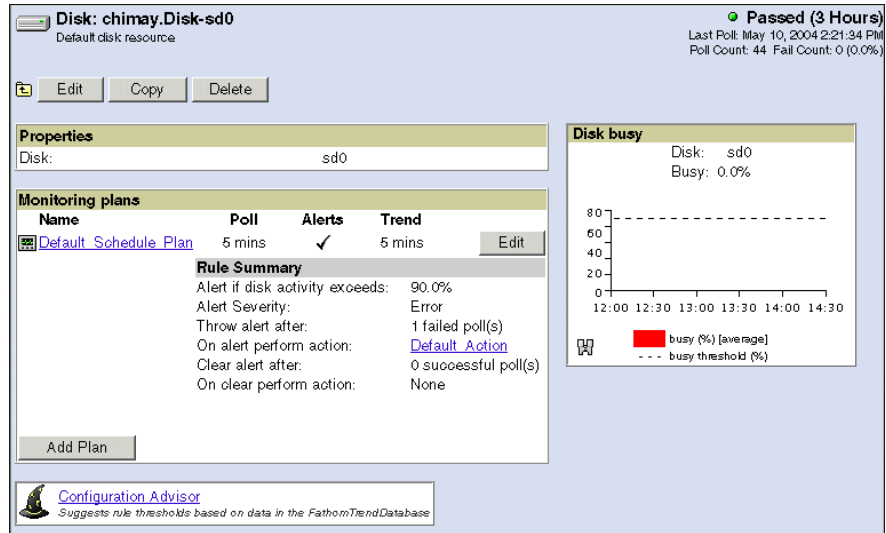
5. When you finish, click **Save**. The **Disk Monitor** page reappears, with the updated values in the **Rule Summary**:

Rule
Summary



All values you entered for the plan and rule definitions are immediately in effect. Any future alerts generated for this resource are based on the new criteria you set.

The following figure shows a sample **Disk Monitor** page for **Disk-sd0** on the container **chimay**. The page includes all the values accepted or updated to define the basic properties, the monitoring plan, and rules for this resource monitor:



The page also provides a graphical view of the disk's status, as well as a link to the Configuration Advisor. See the [“Calculating meaningful thresholds with the Configuration Advisor”](#) section on page 4–22 for details about using the Configuration Advisor with a disk resource.

Calculating meaningful thresholds with the Configuration Advisor

The Configuration Advisor calculates suggested threshold values for rules by analyzing trend data. When you apply a recommended rule threshold setting, the alerts triggered will provide a more meaningful indication of your resource's performance than if you were to arbitrarily set rule values.

The Configuration Advisor analyzes a rule's past performance for a specified period of time and, based on this data, calculates a baseline value. A *baseline value* is a threshold setting that is based on your system's past activity for the particular rule.

You must be an administrator user to use the Configuration Advisor.

Configuration Advisor baselining guidelines

In order to receive the most meaningful feedback, consider these guidelines when setting up baselining with the Configuration Advisor:

- Make sure you have set up Fathom to store trend data. If you did not set this option initially, you can set it by choosing **Options**→**Configuration**→**Trend database** in the management console.
- It is important that you collect data and trend data on a 1:1 basis; in other words, it is recommended that you trend on every poll. Whether you set the polling interval to five minutes or ten minutes, for example, is not significant for baselining; it is, however, important that you trend the performance data on every poll, regardless of the poll interval.
- Consider carefully the timeframe for which you request baselining recommendations. For example, if your resource typically sees little or no activity between the hours of 5 PM and 9 AM, you would not want to get a baseline for an entire 24-hour period. If you did, you would be mixing times of high activity with times of low or nonexistent activity, which would skew the baselining results. Instead, it would be sensible to choose a timeframe of 9 AM to 5 PM, for example.
- Typically, one week of data collection, using the Fathom-provided defaults, provides enough information for the Configuration Advisor to provide meaningful threshold recommendations. Note that if you choose longer time frames, more data will be analyzed; this means that the calculating done by the Configuration Advisor will be more time-consuming than if you had chosen a shorter time frame.

- Each rule you want to analyze must have at least 32 data samples stored in the FathomTrendDatabase. This sampling provides sufficient data from which the Configuration Advisor can determine a baseline value and subsequently perform a successful analysis of each rule's data.
- A polled rule must currently be associated with a defined monitoring plan for that resource in order for the Configuration Advisor to provide a recommendation.

Using the Configuration Advisor with a disk, CPU, or file system resource

You can use the Configuration Advisor with the following resources: database, disk, CPU, and file system, and OpenEdge server components. (For details about using the Configuration Advisor with the database or OpenEdge server components, see the [Database Management Guide](#) or the [OpenEdge Server Management Guide](#), respectively.)

The way in which you use the Configuration Advisor with a disk, CPU, or file system resource is similar because each resource has only one rule. For each rule, the Configuration Advisor calculates recommended values based on a particular formula, as listed in [Table 4-2](#).

Table 4-2: CPU, disk, and file system rules and formulas

Resource	Rule	Formula
CPU	CPU High	$\text{CPU_Usr} + \text{CPU_System} + \text{CPU_Wait}$
Disk	Disk busy	Dev_Pct_Busy
File system	Filesystem used	FileSys_UsedPct

In the case of the CPU rule CPU High, the Configuration Advisor looks at the sum of CPU_Usr, CPU_System, and CPU_Wait when calculating recommended values; for the disk resource, the Configuration Advisor looks just at the Dev_Pct_Busy value.

The following steps describe the process of creating meaningful threshold settings for a disk resource; however, the steps pertain also to the CPU and file system resources.



To use the Configuration Advisor with a disk resource:

1. Click the **Disk** category in the list frame.
2. Click the disk resource in the detail frame. The **Disk Monitor** page appears.
3. Click **Configuration Advisor** in the detail frame. The **Configuration Advisor** page for the disk appears:

Configuration Advisor
chimay.Disk-sd0

Submit Cancel

For rule threshold calculations to take place, data must be retrieved from the FathomTrendDatabase. Please select the start and end date range to use for calculating the thresholds.

Start Date: 2004 May 3
End Date: 2004 May 10

Choose time period to analyze :

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

☐ Full day (24 hours)

☒ From: 9 : 00 AM To: 5 : 00 PM

Select rules (for analysis) :

☒ Disk Busy

4. In the **Start Date** and **End Date** fields, define a date range that Fathom will use to collect data from the FathomTrendDatabase. (The default data range covers one week.)
5. In the **Choose time period to analyze** section, identify the time frame that defines a representative period of time in which the rules are generally active, or being used; this time frame is the period against which you want Fathom to calculate your baseline activity. (The default time period is Monday through Friday, 9:00 AM to 5 PM.)

In the **Select rules (for analysis)** section, the **Disk Busy** rule, which is the only rule available for analysis for a disk resource, is preselected.

6. Click **Submit**. The Configuration Advisor begins to calculate the threshold settings, and one of the following occurs:
 - If sufficient data exists for analysis, the Configuration Advisor displays the calculated result:

Configuration Advisor
chimay.Disk-sd0

Update Selected Rules Cancel

The following time period was used for analysis
 Start Date: 2004 / May / 3
 End Date: 2004 / May / 10
 Days:
 Sun Mon Tue Wed Thu Fri Sat
 Hours:
 From: 9:00 To: 17:00

Default Schedule
 Select:
 All
 None

Rule	Recommend Values	Update	Current Threshold
Disk Busy	0.4 [0] * percent busy	<input checked="" type="checkbox"/>	90.0

Detail

You can now review the Configuration Advisor's recommendation and choose whether or not to update your threshold values. See the [“Reviewing the recommended threshold settings”](#) section on page 4–26 for details.

- If insufficient data exists for analysis, a message appears (under **Recommend Values**) informing you that there is insufficient data for analysis. For example, you might have fewer than 32 data samples stored in the FathomTrendDatabase. In this case, consider expanding the time between start and end dates to capture more data; then rerun the Configuration Advisor.

Reviewing the recommended threshold settings

The recommendations that the Configuration Advisor presents include a range of possible values from which to select. The asterisked value that appears in the **Recommend Values** field indicates the primary recommended threshold setting, based on the data analysis. Click on the drop-down list to see the additional recommended values, as shown in [Figure 4-4](#).

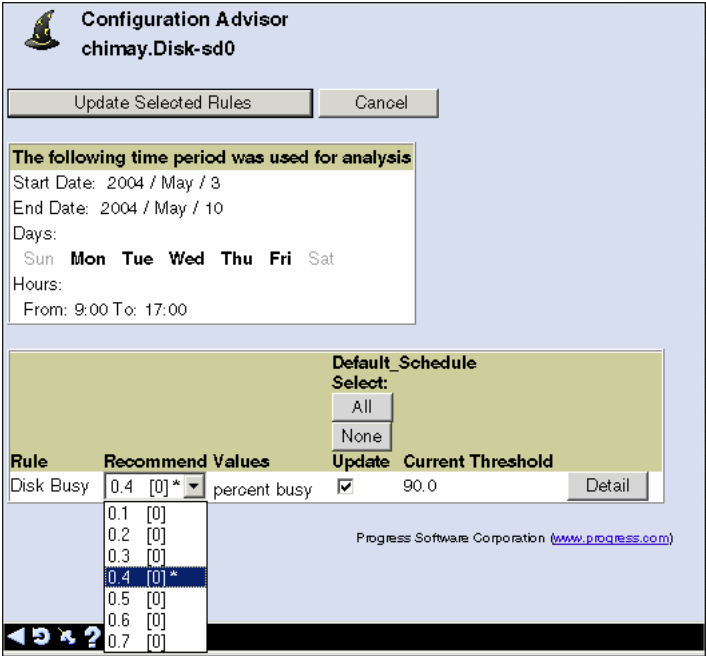


Figure 4-4: Recommended threshold values for disk resource

If there were more than one rule being evaluated by the Configuration Advisor for this resource, each rule would appear in its own row, with its own recommended values, update, current threshold, and **Detail** button.

Each recommended value is expressed as a pair of numbers. The first number specifies the recommended threshold setting; the second number, displayed in brackets, identifies the number of times this threshold value, if used with the collected data, would have broken the rule and triggered an alert. As you review the recommended threshold settings, keep in mind the rule behavior and alert notification frequency you want to establish for a resource.

Reviewing threshold calculation details

Each row has an associated **Detail** button that displays information about the rule's analysis, as shown in [Figure 4-5](#).



Figure 4-5: Threshold calculation details

The following details are provided:

- **Number of useable samples** — Number of data samples extracted from the FathomTrendDatabase.
- **Min Value** — The minimum value derived from the data set.
- **Max Value** — The maximum value derived from the data set.
- **Std Deviation** — The root mean squared deviation.
- **Average** — The average value derived from the data set.

When you finish looking at the details, click **OK** to close the window.

Comparing and selecting threshold settings

By default, the Configuration Advisor assumes that you are going to select and submit one of the recommended threshold settings. The **Update** field for each rule is selected by default; however, you have options concerning the selection process. As you compare the existing and recommended values, you can elect to change none, some, or all values for a rule and each individual monitoring plan.



To compare and select threshold settings:

1. For the one disk rule, note the value that displays in the **Current Threshold** field under a specific schedule.
2. Click the **Recommend Values** drop-down arrow to display all recommended values for the associated rule.
3. Compare the possible recommended values that display with the value in the **Current Threshold** field. As you determine the best threshold rule setting, keep your goals for this rule in mind. Also, consider any additional selection criteria as you compare values.

Additional selection criteria

Reasons for selecting one value and not another may include:

- How often you want alerts generated.
- Your knowledge of your system's operational needs and goals.
- Any other factors unique to your resource's performance that you want to consider in making your selection.

Submitting your threshold setting selections

When you click **Update Selected Rules**, Fathom applies your selection. There is no undo option associated with this submission; to reset any values back to a previously defined setting, you must access the resource's monitoring plan, display the individual rule, and set (manually) the displayed value.

Determining the effectiveness of your selections

The most effective way to determine if your threshold adjustment is serving your needs is to review your alert notifications. Strive for a threshold setting that is consistent with your resource and business needs. If you receive alerts too frequently or infrequently to suit your operational needs, you might want to further refine your threshold settings.

Understanding alerts

An *alert* is an indication that a resource is not performing in compliance with the rules you established in the resource's monitoring plan. When Fathom triggers an alert for a resource, the following events occur:

- The actions you assigned to the resource monitor are initiated. For example, you might define an action to send an e-mail or page an operator when an alert occurs.
- The alert is added to Fathom's open alert table. To see the current open alerts, select **Alerts** from the menu bar.

The level of severity you set for an individual resource in its rules definition determines the type of alert that Fathom generates: **Information**, **Error**, **Warning**, or **Severe**. For more information, see the [Alerts Guide and Reference](#).

All alerts (with the exception of information alerts) cause the resource status to change to **Failed** and its status icon to become the color red.

Note: You can also set up actions and alerts to respond to job status details and job execution time expectations. For more information about job execution, actions, and alerts, see [Chapter 8, "Creating Jobs and Job Templates."](#)

Determining Fathom's action in response to an alert

An *action* is an automatic, user-defined process that occurs in response to a rule violation on a monitored resource. You create actions and associate them with rules to ensure that certain activities occur when the rule triggers.

As you do with schedules, you create and store actions in the Fathom Component Library. You can use actions to send e-mails, record the occurrence of an alert in a log file, send an SNMP trap, or perform a combination of these activities.

All actions, with the exception of jobs, appear in the management console list frame, under the **Actions** category, when you select **Library** from the menu bar. [Figure 4–6](#) shows the expanded **Actions** category.

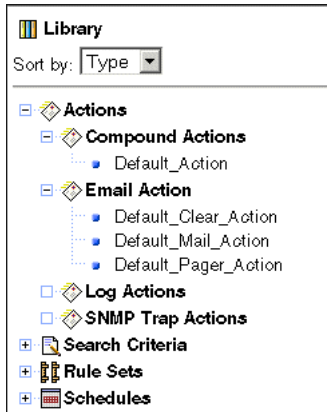


Figure 4–6: Expanded Actions category

Using default actions

Fathom provides four default action definitions: **Default_Action**, **Default_Mail_Action**, **Default_Clear_Action**, and **Default_Pager_Action**. The **Default_Action** is a compound action that contains a single action: the **Default_Mail_Action**, which is configured to send email to the user you specified when you initially configured Fathom. Like the **Default_Mail_Action**, the **Default_Clear_Action** is initially configured to send mail to the default email recipient. The **Default_Pager_Action** sends a message to a pager.

The **Default_Action** is set on the **On alert perform action** field when you initially configure a monitor. If you prefer, you can choose a different action for Fathom to perform when an alert is generated.

Each default serves as a reusable, initial action definition that you can use or modify just as you can any action that you create. These default actions are meant to help you to get your Fathom resources created and running quickly.

You can edit these default actions, but you cannot delete or rename them.

Creating an e-mail action

You can associate an e-mail action with a rule violation. The e-mail action defines the name, description, e-mail addresses of the sender and recipient, and a user-defined subject and message that is initiated in response to an alert.



To create an e-mail action:

1. Select **Library** from the menu bar. The **Fathom Component Library** page appears in the detail frame.
2. Click **Create E-mail Action**. The **E-mail Action** page appears:

The screenshot shows the 'E-mail Action' configuration window. It has a title bar with a document icon and the text 'E-mail Action:'. Below the title bar are 'Save' and 'Cancel' buttons. The main area is divided into two sections: 'Properties' and 'Message'. The 'Properties' section contains fields for 'Name' (a yellow text box), 'Description' (a large text area), 'Send to:' (a text box containing 'aspauldi@progress.com'), 'Send from:' (a text box containing 'Fathom'), 'Subject:' (a text box containing 'Fathom Alert %CONTAINERNAME%.%RE'), and 'Send As:' (a dropdown menu set to 'Text'). The 'Message' section contains a large text area with the following text: 'Fathom Alert [%ALERTID%]', 'Alert Name: %ALERTNAME%', 'Severity: %ALERTSEVERITY%', 'Host: %HOST%', 'Container: %CONTAINERNAME%', 'Resource: %RESOURCENAME%', 'Occurred: %ALERTLASTOCCURRENCE%', 'Reason: %ALERTREASON%', 'Count: %ALERTCOUNT%', and 'Trigger value: %ALERTTRIGVALUE%'. The text area has scrollbars on the right and bottom.

3. In the **Name** field, enter the name of your action. You cannot enter spaces between words or use special characters such as an asterisk (*), ampersand (&), or period in this field.
4. Enter a description of the action in the **Description** field.
5. Enter the e-mail address of the intended alert recipient in the **Send to** field. (This is a required field.) Consider the following points when entering these values:
 - You should explicitly enter e-mail addresses (for example, `smith@company.com`). However, depending on your mail server implementation, Fathom might be able to determine the mail server domain name and automatically provide the `@company.com` portion of the address.
 - You can also enter names using quotation marks. The quotation marks will display when the recipient receives the e-mail. Also, you can enter a comma-delimited list of recipients. For example: `"Some User" <someuser@somedomain.com>`, `"Some Other User" <someotheruser@somedomain.com>`.
6. Enter the e-mail address of the sender in the **Send from** field.

Fathom Management supports either of the following formats to enter a value for the **Send from** field:

- `someuser@somedomain.com`

When this format is received in the recipient's inbox and appears in the **FROM:** header text of the message, the entire entry name and e-mail address, as entered in this format, display.

- `"Some User" <someuser@somedomain.com>`

When the recipient receives an e-mail that is sent using this format, the recipient's inbox displays only `"Some User"` with quotation marks, as the sender of the e-mail; the address does not appear. Similarly, when you open the message, the **FROM:** header appears as: **From: "Some User."** Only when you display a received e-mail will you display both the user name and domain name as entered using this format.

7. Enter a description of the e-mail's topic in the **Subject** field.

In the **Subject** field, the phrase **Fathom Alert** automatically appears, followed by the e-mail variable **%CONTAINERNAME%** to immediately identify the specific container to which the alert applies. However, you can override any of this information. Also, you can use any of the e-mail variables identified in [Table 4–3](#) in the **Subject** field to clarify the content of the e-mail.

Table 4–3: Variables for an e-mail action

Variable	Description
%ALERTID%	The ID of the current alert.
%ALERTNAME%	The name of the current alert.
%ALERTSEVERITY%	The severity of the current alert.
%HOST%	The host on which Fathom is running.
%CONTAINERNAME%	The container whose resource caused the alert to generate.
%RESOURCENAME%	The name of the resource that caused the alert to generate.
%ALERTLASTOCCURRENCE%	The date and time of the last occurrence.
%ALERTREASON%	The reason that the alert occurred.
%ALERTCOUNT%	The number of times that this alert has occurred.
%ALERTTRIGVALUE%	The value that triggered the alert.
%HOSTLINK%	The link to the host on which Fathom is running.
%RESOURCELINK%	The link to the resource that generated the alert that caused the e-mail to be sent.
%ALERTLINK%	The link to the description of the alert that caused the e-mail to be sent.

Note: The percent symbol (%) is used before and after each variable. If you need to include the percent symbol in the text of a message, you must enter two percent symbols (%%) in the message body.

8. Select either **Text** (the default option) or **HTML** as the format option for your message in the **Send As** field. If you select **Text**, no additional work to your message is required. However, if you select **HTML**, you must use proper HTML-formatting techniques to ensure that your message will be readable by the recipient.
9. Use the default message variables that appear in the **Message** area, or edit these variables with the values that will appear in the specific e-mail action that you create.

Refer to [Table 4-3](#) for a listing of the variables you can define for an e-mail message.

10. Click **Save** to save the action or **Cancel** to discard the action. When you save the e-mail action, the detail frame displays the properties of the new action:

E-mail Action: Special_Action
Special action

Edit Copy Delete Test

Properties

Send to: aspauldi@progress.com
Send from: Fathom
Subject: Fathom Alert %CONTAINERNAME%.%RESOURCENAME% %ALERTNAME%
Send As: Text

Message:

Fathom Alert [%ALERTID%]
Alert Name: %ALERTNAME%
Severity: %ALERTSEVERITY%
Host: %HOST%
Container: %CONTAINERNAME%
Resource: %RESOURCENAME%
Occurred: %ALERTLASTOCCURRENCE%
Reason: %ALERTREASON%
Count: %ALERTCOUNT%
Trigger value: %ALERTTRIGVALUE%
Link to Fathom: %HOSTLINK%
Link to resource: %RESOURCELINK%
Link to alert: %ALERTLINK%

You can now edit, copy, delete, or test the e-mail action.

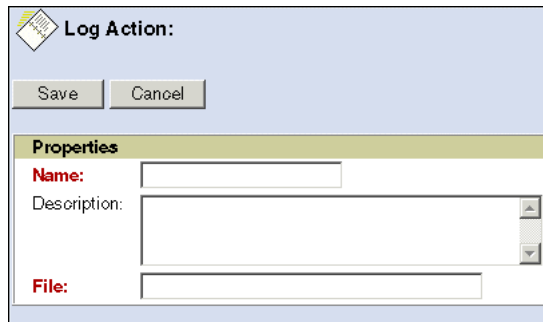
Creating a log action

A log action allows you to record a predefined message in a log file when an alert is generated.

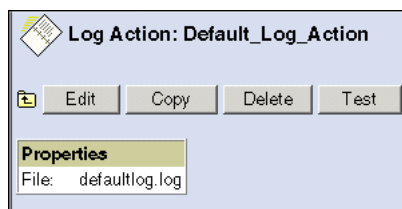


To create a log action:

1. Select **Library** from the menu bar. The **Fathom Component Library** page appears in the detail frame.
2. Click **Create Log Action**. The **Log Action** page appears:



3. Enter the name in the **Name** field.
4. Enter the description in the **Description** field.
5. Enter the name of the log file in the **File** field.
6. Select **Save**. The **Log Action** page appears:



You can now edit, copy, delete, or test the log action.

Creating a compound action

When you create a compound action, you define one single action based on a number of individual actions that you frequently perform as a series of notification and operational steps in response to an alert. Fathom provides a default compound action you can use called `Default_Action`.



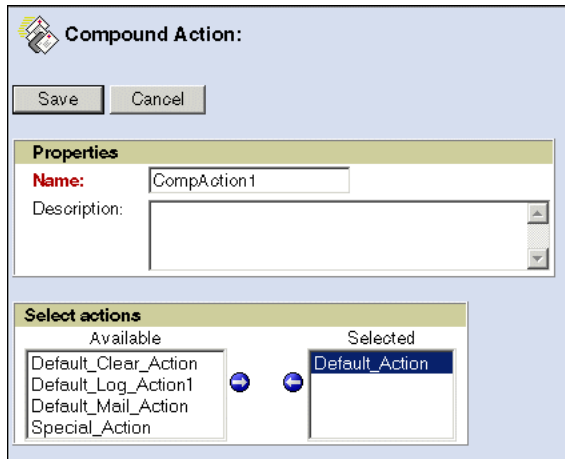
To create a compound action:

1. Select **Library** from the menu bar. The **Fathom Component Library** page appears in the detail frame.
2. Click **Create Compound Action**. The **Compound Action** page appears:

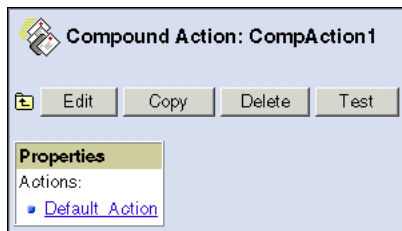
3. Enter the name in the **Name** field. (This is a required field.)
4. Enter the description in the **Description** field.

5. In the **Select actions** section, select an action in the **Available** list and click the right arrow. The action you selected moves to the **Selected** list to be added to the compound action. Also, you can select an action in the **Selected** list and click the left arrow. The action you selected is removed from the compound action.

Repeat these additions and/or removals until you have only those actions you want in the compound action in the **Selected** list:



6. Click **Save**. A summary of the actions that compose the compound action you created appears:



The compound action you created is added to the list of compound actions you see in the list frame.

You can now edit, copy, delete, or test the compound action.

Creating a Simple Network Management Protocol (SNMP) trap action

You use the SNMP trap action if you want Fathom resource-related event notifications to be sent to your SNMP management console. You define name, description, host, port, and read community details to send event notifications, referred to as *traps*, to SNMP management consoles such as BMC's PATROL Enterprise Manager Connect SNMP and Tivoli Enterprise Console.

The SNMP trap action generates an asynchronous message to an SNMP management console.

Note the following information about SNMP trap actions:

- To define SNMP trap actions, you must have previously installed the Fathom SNMP Adapter product. Also, you must define the Fathom SNMP Adapter option on the **Fathom Management Configuration** page.
- To send SNMP trap actions and make SNMP requests, the SNMP agent must be running. To review or change the current status of the SNMP agent, select **Options** from the menu bar and select **SNMP** to display the **SNMP Adapter** page. Note that this page also displays a summary of the SNMP information set up on the **Fathom Management Configuration** page. You can elect to edit this information.
- All Fathom-specific SNMP variables and tables are located in the Fathom Management Information Base (MIB). The MIB file, `PSC-FM-MIB.txt`, is located in the `<Fathom-install-dir>\config` directory. Review the contents of this file and focus specifically on the `fmalertTable`, which contains information specific to each alert. The alert ID information in this file allows you to understand the contents of this table.

Table 4–4 presents two examples that identify how you can obtain alert details from the `fmalertTable`.

Table 4–4: Alert details obtained from the `fmalertTable`

To obtain an alert reason associated with Alert ID...	Issue an SNMP GET request using this Object Identifier (OID)...
3	1.3.6.1.4.1.1730.1.2.1.1.6.1.6.3
4	1.3.6.1.4.1.1730.1.2.1.1.6.1.6.4

For more information about the SNMP Adapter and its configuration, see the [Installation and Configuration Guide](#). For information about initiating SNMP GET requests from an SNMP agent, see the SNMP management console documentation for your particular SNMP management console product.



To create an SNMP Trap Action:

1. Select **Library** from the menu bar. The **Fathom Component Library** page appears in the detail frame.
2. Click **Create SNMP Trap Action**. The **SNMP Trap Action** page appears:

3. Enter the name in the **Name** field.
4. Enter a description in the **Description** field.

5. Enter the name of the host machine on which the SNMP management agent resides in the **Host** field. Traps will be sent to this host machine. (If you set a default value for the **Host** field on the **Fathom Management Configuration** page, that value appears in this field.)
6. Enter the port number of the host machine on which the SNMP management agent resides in the **Port** field. Traps will be sent to this port number on the host machine. (If you set a default value for the **Port** field on the **Fathom Management Configuration** page, that value appears in this field.)
7. Enter the community who will have read access to the trap information in the **Read Community** field. Your choices are public, private, or any other community you have set up for access. (If you set a default value for the **Read Community** field on the **Fathom Management Configuration** page, the value appears in this field.)
8. Click **Save** to submit your selections.

Once you have set up SNMP trap actions, you can associate them with resources just as you would any Fathom action. When the resource generates an alert, the SNMP trap action is thrown.

You can review the content of the trap (known as variable bindings) as they are defined in the MIB. You can query these variables any time the Fathom SNMP Adapter agent is running.

Updating and deleting actions

Once your resource monitor exists, you can update actions assigned to it at any time. However, you cannot delete an action that is in use by a resource. If you try to delete an action that is currently in use, Fathom displays a message box to notify you that the action is being used. Fathom also provides a list of resources that are using the action.

Editing or copying a resource monitor

You can edit and copy the properties, monitoring plans, or rule definitions for most resources. There are some limits to the types of editing you can perform for the Fathom-provided default resources such as CPU, Memory, and databases. For example, you cannot rename, copy, or delete any default resource monitors. You can, however, change monitoring plan and rule definitions associated with each of them.

Note that if two or more people simultaneously edit a resource, the last changes submitted overwrite all previous changes.



To edit or copy a resource:

1. Select **Resources** in the menu bar.
2. Select the system, network, or file resource you want to edit or copy from the list frame. The resource's summary data, which includes properties, monitoring plans, and rule definitions, appear in the detail frame.
3. Choose one:
 - Click **Edit**. The property summary data reappear, allowing you to change editable fields.
 - Click **Copy**. You can change the properties, monitoring plans, or rule definitions as necessary. Note that when you copy a resource, the copy displays the same name as the original resource. You must change this name before saving the copy.
4. Click **Save** when you finish.

Deleting a resource monitor

Once you delete a resource, you cannot undelete it. You might consider disabling an **Enabled** option rather than deleting it if you seek a less-permanent way to disengage a monitor.

You cannot delete the Fathom-provided CPU default resource or Memory default resource. Similarly, you cannot delete or rename Default_Action, Default_Clear_Action, or Default_Mail_Action. For details about deleting database resource monitors, see the [Database Management Guide](#). For details about deleting WebSpeed broker, AppServer broker, or NameServer resource monitors, see the [OpenEdge Server Management Guide](#).



To delete other resource monitors:

1. Select **Resources** from the menu bar.
2. In the list frame, select the specific resource that you want to delete.
3. Click **Delete**. Fathom displays a message asking you to confirm that you want to delete the resource.
4. Click **OK**. A message appears informing you that the resource has been deleted.

Working with default values

Fathom Management provides different opportunities for you to set up and use default values to:

- Quickly and easily update default information at global and general resource levels. As necessary, you can override these values on individual instances of each resource.
- Minimize duplication of error in creating resource monitors.

Using default values can also help you to become operational with Fathom quickly and standardize your resource performance criteria.

You can establish default values:

- At the Fathom global settings level.
- From specific default pages associated with the different Fathom resource monitoring types.

Reviewing and changing global settings

During the Fathom Management installation process, you have the option of choosing global settings for various resource options. At any time after the initial installation, you can review and update these settings. Specifically, you can enable and disable global settings for the following Fathom elements:

- Polling activities for all resources.
- Trending activities data for all resources.
- Alert generation.



To update the global settings:

1. Click **Options** on the menu bar.
2. In the list frame, click **Configuration→Resource monitoring**. The **Fathom Resource Monitoring Configuration** page appears:

Fathom Resource Monitoring Configuration

Submit Cancel

Current resource monitoring settings

☒ Poll resources? Help

☒ Generate alerts?

Trending

☒ Collect trend data?

☒ Include status changes?

3. To enable or disable global resource monitoring settings, select or clear the appropriate options.

The resource monitoring settings are independent of each other and are useful for diagnostic purposes because they allow you to disable specific Fathom functionality. For example, if you know that your FathomTrendDatabase is going to be taken down for maintenance, you can elect to turn off trending, but leave the rest of Fathom Management running.

If you disable polling, trending, or alerts, an associated icon appears in the upper-right corner of the menu bar to indicate that the option is currently disabled. Also, when polling is disabled at this configuration level, a message indicating that the polling has been disabled appears on each individual resource monitor-related page.

For further information about updating global resource monitoring settings, see the *Installation and Configuration Guide*. For details about setting actions for Fathom internal alerts, see the *Alerts Guide and Reference*.

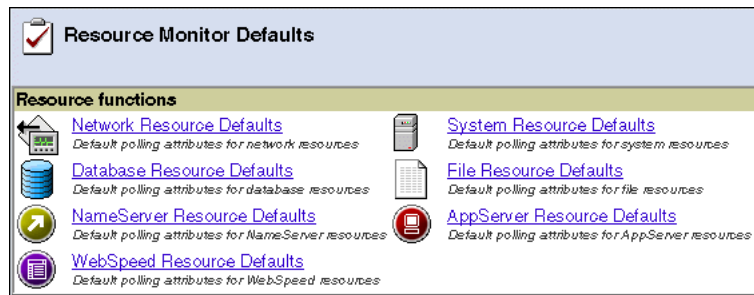
Reviewing and changing resource type defaults

Each of the general Fathom resource types — file, system, network, database, and OpenEdge server— has predefined default values. You can accept or change these defaults.



To see current default values:

1. Click **Resources** from the menu bar.
2. On the **Fathom Resources** page, click **Resource Monitor Defaults**. The **Resource Monitor Defaults** page appears:



3. To view the current defaults for a resource type, click the appropriate link.

For more information about system, network, or file resource defaults, see [Chapter 5](#), “Monitoring System Resources,” [Chapter 6](#), “Monitoring Network Resources,” or [Chapter 7](#), “Monitoring File Resources.” For information about database resource default values, see the *Database Management Guide*, and see the *OpenEdge Server Management Guide* for details about OpenEdge server component default values.

Using job and report templates

Fathom provides a template feature to help you create and maintain jobs and report data:

- A Fathom job template helps you standardize and quickly create numerous individual job instances using predefined, common values.

For details about working with job templates, see [Chapter 8, “Creating Jobs and Job Templates.”](#) For details about the Fathom-supplied database maintenance job templates, see the [Database Management Guide](#).

- A Fathom report template helps you standardize and quickly create numerous individual reports using predefined, common values. For information about working with report templates, see the [Reporting Guide](#).

Sharing monitoring components using the Fathom Library

The Fathom Library contains resource monitoring components that you define, share, and, in many instances, transfer among your company’s various work sites. Two of the primary benefits of employing library components are:

- Minimizing duplication of effort when creating numerous and similar resources.
- Standardizing implementation of your company’s business policies through the definition and distribution of these components.

You can define schedules, actions, search criteria, and rule sets at the library level. The import and export activities that are also available in the library allow you to distribute all library components (except schedules) that you have created on one machine to other machines located throughout your company.

To access the Fathom Library, click **Library** from the menu bar. The **Fathom Component Library** appears, as shown in Figure 4–7.

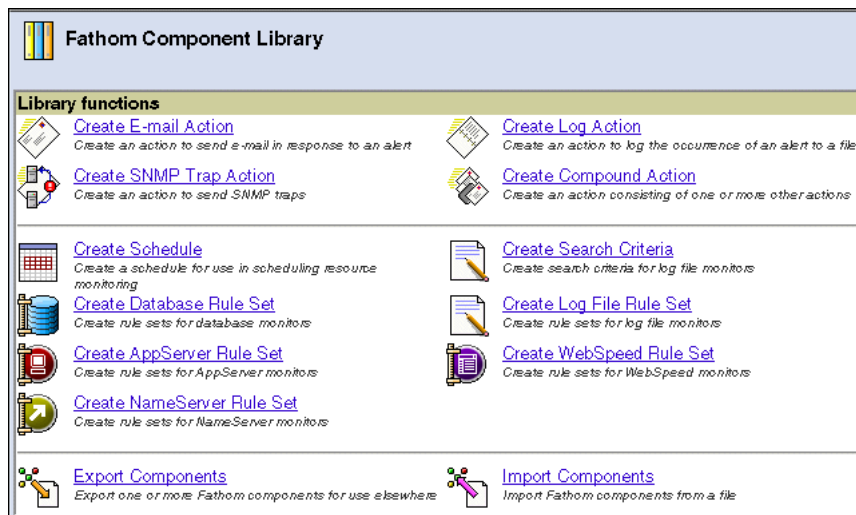


Figure 4–7: Fathom Component Library page

The components you build, maintain, and access through the **Fathom Component Library** page are independent of each other. This independence allows you flexibility to combine and reuse these components, minimize redundant resource setup work for numerous items that are very similar, and help standardize work flow processes across an enterprise.

[Table 4–5](#) briefly highlights the remaining library function options, according to the type of resource with which they are associated.

Table 4–5: Additional Fathom Library features

To help...	Use these library components...
Create log file monitors	<p>Search Criteria and Log File Rule Set. These components allow you to define rules-related data to be shared among log file monitors:</p> <ul style="list-style-type: none">• Create Search Criteria defines rule properties from which you can select and associate with other rule properties to create individual rules to run within your log file monitors.• Create Log File Rule Set defines a set of log file monitor rules that you can associate with one or more log file monitor resources. <p>For details, see Chapter 7, “Monitoring File Resources.”</p>
Create database monitors	<p>The database rule set, which allows you to define a set of database rules that you can use with one or more database resources.</p> <p>For details, see the Database Management Guide.</p>
Create OpenEdge monitors	<p>The NameServer, AppServer, or WebSpeed rule set, which allows you to define a set of rules that you can use with each type of resource.</p> <p>For details, see the OpenEdge Server Management Guide.</p>
Identify existing Fathom components to export to other computers	<p>The Export Components option. This option allows you to identify various components that you create and share by importing from and/or exporting to another machine.</p> <p>For details, see Chapter 9, “Exporting and Importing in Fathom.”</p>
Identify existing Fathom components to import to computers	<p>The Import Components option. This option allows you to identify various components that you create and share by importing from and/or exporting to another machine.</p> <p>For details, see Chapter 9, “Exporting and Importing in Fathom.”</p>

Monitoring System Resources

This chapter describes system resource monitoring and contains the following sections:

- [System resource monitoring overview](#)
- [Reviewing system resource default values](#)
- [Reviewing system resource monitoring plans](#)

System resource monitoring overview

You can monitor the following system resources in Fathom: CPU, disk, file system, and memory. Fathom automatically creates a CPU resource monitor and a memory resource monitor and assigns default values. You can accept the default values, or you can change them. You cannot, however, delete or rename either the CPU or the memory resource.

You can choose to monitor all file systems and disks on your machine. If you make this choice during the initial configuration of Fathom, Fathom automatically creates a default resource monitor for each disk and file system. For details about selecting this configuration option, see the section about initial configuration settings in the *Installation and Configuration Guide*.

Reviewing system resource default values

Fathom provides various default values for system, network, file, database, and OpenEdge server resources. You see these default values when you create a resource monitor and define its monitoring plan.

If the default values are acceptable to you, you can maintain them for use with the resource monitors you create. If, however, you want to change the default values, you can do so as follows:

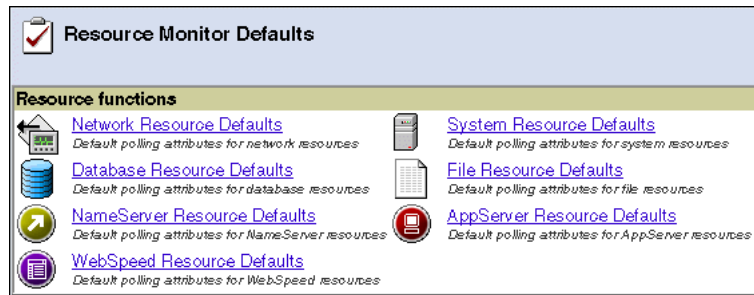
- For each resource monitor you create, adjust the values, on a per-resource basis, so that you get the feedback data you want on the resource. In this case, each new resource monitor is still initially created with the Fathom default.
- Change the actual defaults provided by Fathom so that each new resource monitor you create already has the default values you find most useful.

Changing default values does not affect any resource monitor already created.

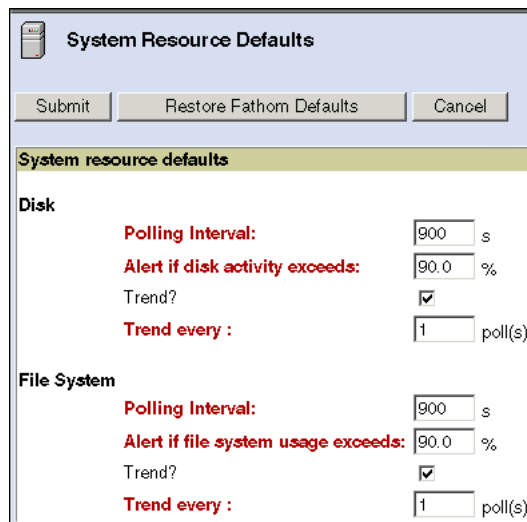


To display default values for system resources:

1. Select **Resources** from the menu bar.
2. Click **Resource Monitor Defaults**. The **Resource Monitor Defaults** page appears:



3. Click **System Resource Defaults**. The **System Resource Defaults** page appears:



4. Review the default values defined for **Disk** and **File System**:

Polling Interval — The frequency with which this resource's rules are checked by Fathom; for example, every 5 minutes.

Alert if disk activity/file system usage exceeds — The percentage of disk activity or file system usage that if exceeded causes Fathom to generate an alert.

Trend — Whether you want performance data about this resource stored in the FathomTrendDatabase.

Trend every — How often you want the performance data stored in the FathomTrendDatabase.

5. Change the default values, as necessary, and click **Submit**.

The new defaults will be in place when you create a new disk or file system resource. If when you create the new resource the default values are still not what you want, you can change the values of the individual disk or file system resource at that time to suit your own needs.

Note that you can revert back to the original Fathom-supplied default values at any time by selecting **Restore Fathom Defaults**.

Reviewing system resource monitoring plans

The CPU resource and the memory resource are automatically created when you initially start up Fathom Management. However, you can change the default monitoring plan and rules associated with each of these system resources.

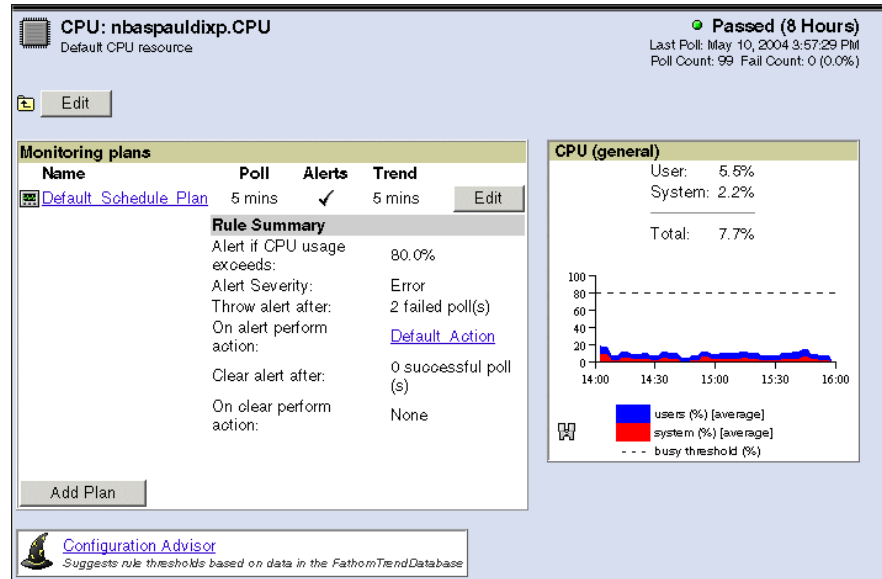
Reviewing the CPU resource monitoring plan

You do not have to set up monitoring plans and rules for your CPU resource. Fathom automatically provides a default resource named CPU when you initially start up Fathom Management. You cannot delete this Fathom-provided default resource, nor can you change its name. However, you can change the values in the CPU resource's monitoring plan definition and rule definition.

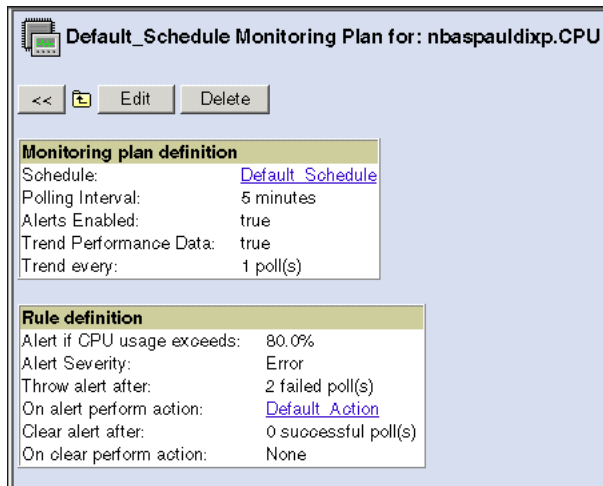


To review the default CPU resource monitoring plan:

1. Click **Resources** from the menu bar.
2. In the list frame, expand the **System** category.
3. Expand the **CPU** category, and click the **CPU** resource. The **CPU** page opens in the detail frame:



4. To review the values set in the CPU's monitoring plan definition and rule definition, click the monitoring plan in the **Name** column. The monitoring plan appears, as shown in the following example:



Default_Schedule Monitoring Plan for: nbaspauldixp.CPU

<< [icon] Edit Delete

Monitoring plan definition

Schedule:	Default_Schedule
Polling Interval:	5 minutes
Alerts Enabled:	true
Trend Performance Data:	true
Trend every:	1 poll(s)

Rule definition

Alert if CPU usage exceeds:	80.0%
Alert Severity:	Error
Throw alert after:	2 failed poll(s)
On alert perform action:	Default Action
Clear alert after:	0 successful poll(s)
On clear perform action:	None

The default monitoring plan consists of the following monitoring plan definition values:

- **Schedule** — Identifies the system-defined 24/7 default schedule used when the plan is active. The default is **Default_Schedule**.
- **Polling Interval** — Identifies the polling cycle, which is the frequency at which the resource's rules are checked. The default is five minutes.
- **Alerts Enabled** — Indicates whether alerts are active and will be generated when the plan is active. The default is true.
- **Trend Performance Data** — Indicates whether you want to store performance data in the FathomTrendDatabase. The default is true.
- **Trend Every** — Indicates how often performance data is trended. The default is 1 poll.

The default monitoring plan consists of the following rule definition values:

- **Alert if CPU usage exceeds** — Identifies when Fathom issues an alert on CPU usage. The default is 80%.

Fathom monitors the percentage of CPU usage according to the value you enter in the **Alert if CPU usage exceeds** field within the rule definition. Fathom polls the CPU according to the **Polling Interval** value. This percentage reflects the percentage of time that a processor is busy executing a nonidle thread. You can view this percentage as the time spent doing useful work. You can also extrapolate the idle time based on this statistic.

This statistic is presented as an average percentage based on snapshots taken at the beginning and end times of the defined sample period. Expressing the value as an average reduces the possibility of false alerts for random spikes in usage. For example, if your CPU monitor has a polling interval of 15 minutes, the average CPU time is calculated over this period of time.

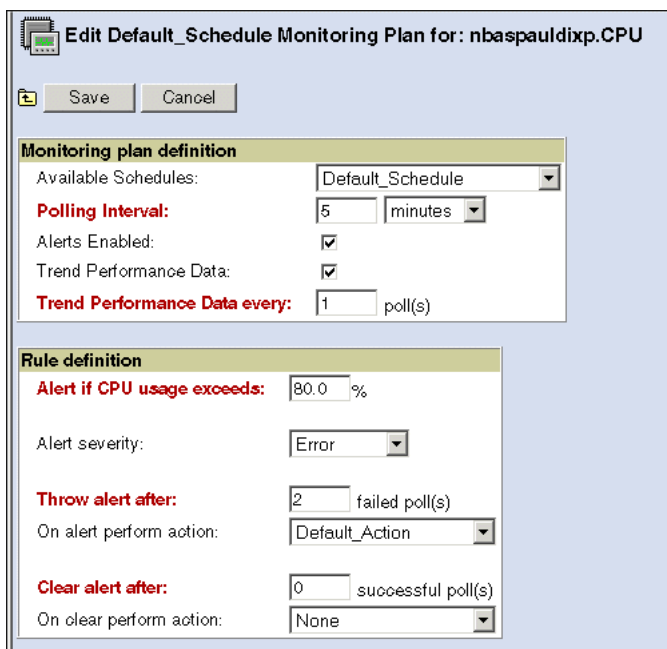
- **Alert Severity** — Identifies the severity level at which Fathom triggers an alert. The default is Error.
- **Throw alert after** — Identifies at which point Fathom triggers an alert. The default is 2 failed polls.
- **On alert perform action** — Identifies the action Fathom takes when an alert is generated. The default is Default Action.
- **Clear alert after** — Identifies the number of successful polls after which Fathom clears the alert. The default is zero.
- **On clear perform action** — Identifies a user-defined action or a compound action. For example, Fathom might run a job that was defined as an action. The default is None.

Trending performance data for CPU resources

Once you enable trending by selecting the **Trend Performance Data** field, you can also override the default value of 1 in the **Trend Performance Data every poll(s)** field. Any value that you enter in this field that is greater than the default value of 1 causes a CPU resource monitor to trend an average of the data that it gathers between trends. This average is calculated as the sum of the values divided by the number of polls.

Editing the CPU resource defaults

If you want to change any of the default CPU resource monitor values, click **Edit** from the **Monitoring Plan** page. The **Edit Monitoring Plan** page appears, as shown in [Figure 5–1](#).



Edit Default_Schedule Monitoring Plan for: nbaspauldixp.CPU

Save Cancel

Monitoring plan definition

Available Schedules: Default_Schedule

Polling Interval: 5 minutes

Alerts Enabled: ☒

Trend Performance Data: ☒

Trend Performance Data every: 1 poll(s)

Rule definition

Alert if CPU usage exceeds: 80.0 %

Alert severity: Error

Throw alert after: 2 failed poll(s)

On alert perform action: Default_Action

Clear alert after: 0 successful poll(s)

On clear perform action: None

Figure 5–1: Editing the CPU monitoring plan defaults

Make any modifications you want, and click **Save**. The **CPU** page opens and reflects any changes you have made.

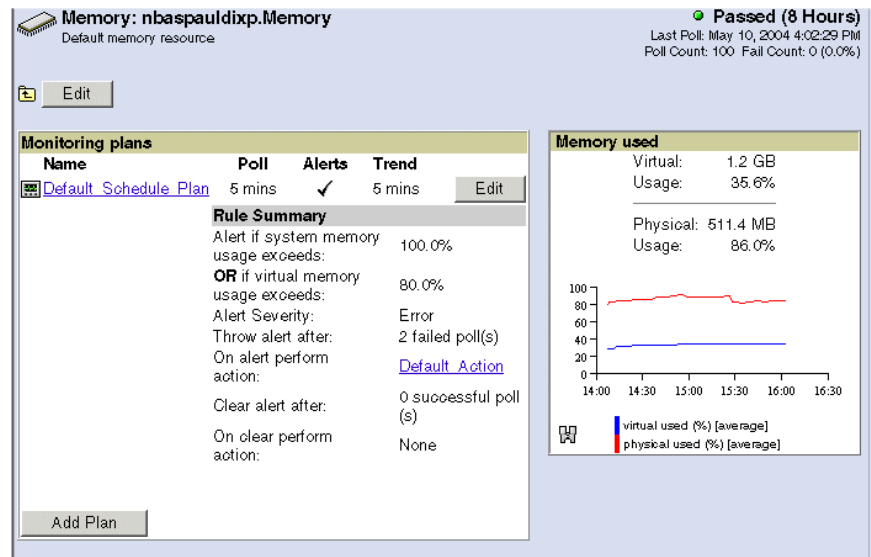
Reviewing the memory resource monitoring plan

You do not have to set up monitoring plans and rules for your memory resource. Fathom automatically provides a default resource named Memory when you initially start up Fathom Management. You cannot delete this Fathom-provided default resource, nor can you change its name. However, you can change the values in the memory resource's monitoring plans definition and rules definition.

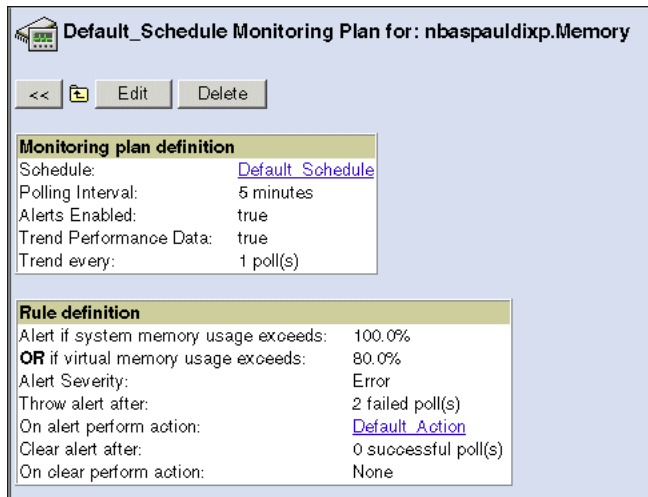


To review the default memory resource monitoring plan:

1. Click **Resources** from the menu bar.
2. In the list frame, expand the **System** category.
3. Expand the **Memory** category, and click the **Memory** resource. The monitoring plan and a tabular and graphical representation of the memory status appear, as shown in the following example:



- To review the values set in the memory resource's monitoring plan definition and rule definition, click the monitoring plan in the **Name** column. The monitoring plan for the memory resource appears:



Default_Schedule Monitoring Plan for: nbaspauldixp.Memory

<< Edit Delete

Monitoring plan definition

Schedule: [Default_Schedule](#)

Polling Interval: 5 minutes

Alerts Enabled: true

Trend Performance Data: true

Trend every: 1 poll(s)

Rule definition

Alert if system memory usage exceeds: 100.0%

OR if virtual memory usage exceeds: 80.0%

Alert Severity: Error

Throw alert after: 2 failed poll(s)

On alert perform action: [Default_Action](#)

Clear alert after: 0 successful poll(s)

On clear perform action: None

The default monitoring plan consists of the following monitoring plan definition values:

- Schedule** — Identifies the system-defined 24/7 default schedule used when the plan is active. The default is `Default_Schedule`.
- Polling Interval** — Identifies the polling cycle, which is the frequency at which the resource's rules are checked. The default is five minutes.
- Alerts Enabled** — Indicates whether alerts are active and will be generated when the plan is active. The default is true.
- Trend Performance Data** — Indicates whether you want to store performance data in the FathomTrendDatabase. The default is true.
- Trend every** — Indicates how often performance data is trended. The default is 1 poll.

The default monitoring plan consists of the following rule definition values:

- The **Alert if system memory usage exceeds** field indicates the threshold percent value that generates an alert. This alert indicates that the percentage of physical memory in use by the system has been exceeded.
- The **Alert if virtual memory usage exceeds** field indicates the threshold value that generates an alert. This alert indicates that the percentage of virtual memory in use by the system has been exceeded.

These memory-related statistics are displayed as single snapshots when Fathom polls the system to determine the amount of free virtual memory. For example, Fathom displays the amount of free virtual memory at a single instant. Therefore, these statistics are more likely to reflect random spikes in performance that might not accurately reflect overall performance. You should consider configuring these monitors so that an alert is not generated the first time the threshold is crossed, but only after it has been crossed enough times to validate concern about performance.

- **Alert severity** — Identifies the severity level at which Fathom triggers an alert. The default is Error.
- **Throw alert after** — Identifies at which point Fathom triggers an alert. The default is 2 failed polls.
- **On alert perform action** — Identifies the action Fathom takes when an alert is generated. The default is Default Action.
- **Clear alert after** — Identifies the number of successful polls after which Fathom clears the alert. The default is zero.
- **On clear perform action** — Identifies a user-defined action or a compound action. For example, Fathom might run a job that was defined as an action. The default is None.

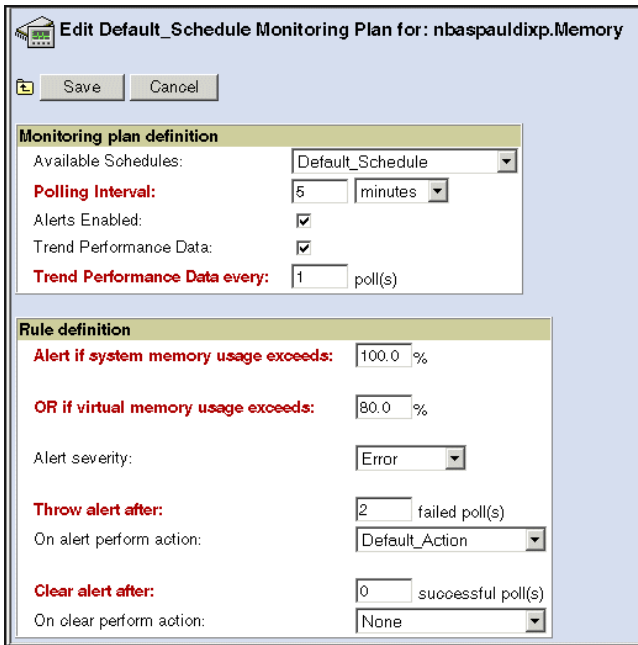
Trending performance data for memory resources

Once you enable trending by selecting the **Trend Performance Data** field, you can also override the default value of 1 in the **Trend Performance Data every poll(s)** field. Any value that you enter in this field that is greater than the default value 1 causes a memory resource monitor to trend data that it gathered from the last poll, with the exception of page in and page out fields. Page in and page out data can only be queried through the FathomTrendDatabase.

Note: The page in and page out values represent the delta values from the previous trend.

Editing the Memory resource defaults

If you want to change any of the default memory resource monitor values, click **Edit** from the **Monitoring Plan** page. The **Edit Memory Resource** page shown in [Figure 5–2](#) appears.



Edit Default_Schedule Monitoring Plan for: nbaspauldixp.Memory

Save Cancel

Monitoring plan definition

Available Schedules: Default_Schedule

Polling Interval: 5 minutes

Alerts Enabled: ☒

Trend Performance Data: ☒

Trend Performance Data every: 1 poll(s)

Rule definition

Alert if system memory usage exceeds: 100.0 %

OR if virtual memory usage exceeds: 80.0 %

Alert severity: Error

Throw alert after: 2 failed poll(s)

On alert perform action: Default_Action

Clear alert after: 0 successful poll(s)

On clear perform action: None

Figure 5–2: Editing the Memory monitoring plan defaults

Make any modifications you want and click **Save**. The **Memory** page opens and reflects any changes you have made.

Reviewing a disk resource monitoring plan

Fathom provides a default disk resource monitor, the name of which depends on the operating system and what drives are found on the machine.

You can also add more disk resource monitors. Depending on the initial configuration options you selected, it is possible that all disks found on your system will have default monitors created for them. For more information about disk options available during the Fathom Management setup and installation process, see the appropriate section of the *Installation and Configuration Guide*.

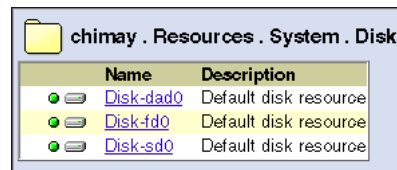
Reviewing disk monitoring data




Fathom Management provides a complete list of available system disk devices for which you can also set up and maintain individual disk resource monitors.



To access a list of available disk devices:

1. Select **Resources** from the menu frame. The **Fathom Resources** page appears.
2. Select **Disk**. The **Disk** page appears:



Name	Description
 Disk-dad0	Default disk resource
 Disk-fd0	Default disk resource
 Disk-sd0	Default disk resource

This page lists the available disk drives on your system.

3. From the **Disk** page, you can:
 - Define monitors for each of the disks.

If, when you were initially configuring Fathom, you chose the option for Fathom to define monitors for all disks, resource monitors will already be in place for each disk. For more information about this configuration setting, see the section about initial configuration in the *Installation and Configuration Guide*.

 - Access detailed monitoring plans and rules for available disks you want to set up or whose values you want to edit.

Disk device statistics

Fathom monitors the value in the **Disk activity exceeds** field, which indicates the percentage of elapsed time that the selected disk drive is busy servicing read or write requests. You can set an alert to trigger when this percentage is exceeded.

Trending performance data for disk resources

Once you enable trending by selecting the **Trend Performance Data** field, you can also override the default value of 1 in the **Trend Performance Data every poll(s)** field. Any value that you enter in this field that is greater than the default value 1 causes a disk resource monitor to trend data that it gathered primarily from the last poll.

Reviewing the file system resource monitoring plan

Fathom provides a default file system resource monitor, the name of which depends on the operating system and what file systems are found on the machine.

You can also add more file system monitors. Depending on the initial configuration options you selected, it is possible that all file systems found on your machine will have default monitors created for them. For more information about file system options available during the Fathom Management setup and installation process, see the appropriate section of the [Installation and Configuration Guide](#).

Note: Keep in mind that some of the file systems that are available to be monitored might not, in fact, be suitable for monitoring. UNIX-related examples that are considered unsuitable for monitoring include pseudo file systems used by the Kernel such as `/proc`, file systems that are actually mount points for remote or unmounted file systems. File system resource monitors set up for these types of file systems would be ineffective.

File system statistics

By establishing values for statistics, you define the rules for a file system resource monitor. Fathom collects the following statistics related to the utilization of file systems:

- **File System Name** — The name of the file system as it is known to the operating system.
- **File system usage** — The percentage of file system capacity used.

The **File system usage exceeds** statistic is gathered primarily for trend analysis. You can review these statistics and trend details to predict, to some extent, when it is time to extend or redesign your file system. Provided nothing other than the database is located on the file system, this detail indicates the database growth over time. You can set an alert to trigger when the percentage of file system capacity is exceeded.

The file system information can also help with mapping device-busy metrics to a file system. You can see which files are involved with performance issues.


Reviewing file system monitoring data

Fathom Management provides a complete list of available file systems for which you can set up and maintain individual file system resource monitors. Fathom also provides detailed data for all available file systems, whether monitored or not.

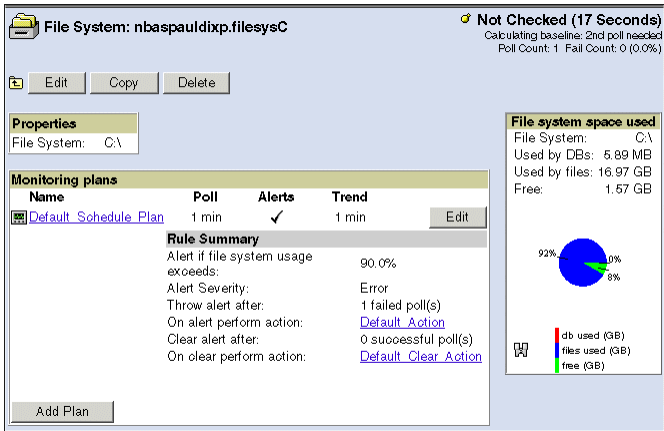


To access a list of available file systems:

1. Select **Resources** from the menu frame. The **Fathom Resources** page appears.
2. Click **FileSystem**. The **FileSystem** page appears and lists the available file systems on your machine:

nbaspauldixp . Resources . System . FileSystem	
Name	Description
 filesysC	

3. Click a file system. Details similar to the following appear:



Trending performance data for file systems

Once you enable trending by selecting the **Trend Performance Data** field, you can also override the default value of 1 in the **Trend Performance Data every poll(s)** field. Any value that you enter in this field that is greater than the default value 1 causes a file system resource monitor to trend data that is taken from the last poll. No calculations are performed on this data.

Monitoring Network Resources

This chapter provides detailed information about network resource monitoring and contains the following sections:

- [Network resource monitoring overview](#)
- [Reviewing network resource default values](#)
- [Discovering and monitoring TCP and UDP ports](#)
- [Creating a TCP or UDP resource monitor](#)
- [Creating a PING \(ICMP\) resource monitor](#)
- [Using the HTTP resource monitor to determine Web site status](#)

Network resource monitoring overview

You can use Fathom to set up resource monitors for non-OpenEdge resources. To determine the availability of some non-OpenEdge network resources, you follow network discovery procedures that allow you to search for ports that are present on your network.

This chapter describes network discovery procedures and explains how to create specific port connections for network resources. These network resources are:

- TCP port

You can set up resource monitors for ports that use Transmission Control Protocol (TCP) to monitor machine availability to enable a data connection between two machines.

- UDP port

You can set up resource monitors for ports that use User Datagram Protocol (UDP) to determine the availability of these ports so that a given machine can broadcast messages over a network.

- PING (ICMP)

Packet Internet Groper (PING) is a utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. ICMP supports packets that can contain error, control, and informational messages. Fathom allows you to set up resource monitors on a PING to monitor the availability of specific machines and IP addresses.

- HTTP Monitor

Hypertext Transfer Protocol (HTTP) is a Fathom-supported resource monitoring feature that allows you to monitor various aspects of a Universal Resource Locator (URL). Businesses that rely heavily on the Internet need to ensure that their company's Web site is reliable, accurate, and accessible. The HTTP Monitor supports an authentication feature.

You cannot use the discovery process with the HTTP Monitor resource process.

Caution: Give serious consideration to the types of devices for which you are creating network resources. Fathom does not allow you to PING broadcast or multi-cast addresses. However, it is possible to PING other devices, such as hubs, switches, and routers. Polling devices such as these can lead to network problems.

Trending considerations for network resources

Trend information for network resources is limited to the response times received by the resource and status details generated up to and including that time frame. With regard to network resources, information trended to the FathomTrendDatabase refers to the worst-case poll information received between trends.

Reviewing network resource default values

Fathom provides various default values for system, network, file, database, and OpenEdge server resources. You see these default values when you create a resource monitor and define its monitoring plan.

If the default values are acceptable to you, you can maintain them for use with the resource monitors you create. If, however, you want to change the default values, you can do so as follows:

- For each resource monitor you create, adjust the values, on a per-resource basis, so that you get the feedback data you want on the resource. In this case, each new resource monitor is still initially created with the Fathom defaults.
- Change the actual defaults provided by Fathom so that each new resource monitor you create already has the default values you find most useful.

Changing default values does not affect any resource monitor already created.

**To display default values for network resources:**

1. Click **Resources** from the menu bar.
2. Click **Resource Monitor Defaults**. The **Resource Monitor Defaults** page appears.
3. Click **Network Resource Defaults**. The **Network Resource Defaults** page appears:

Network Resource Defaults

Submit Restore Fathom Defaults Cancel

Network resource defaults

TCP

Polling Interval: 300 s

Alert if response time greater than: 500 ms

OR if no response within: 2000 ms

Trend? ☒

Trend every 1 poll(s)

UDP

Polling Interval: 300 s

Alert if response time greater than: 500 ms

OR if no response within: 2000 ms

Trend? ☒

Trend every 1 poll(s)

ICMP

Polling Interval: 300 s

Alert if response time greater than: 1000 ms

OR if no response within: 5000 ms

Trend? ☒

Trend every 1 poll(s)

HTTP

Polling Interval: 300 s

Alert if response time greater than: 15000 ms

OR if no response within: 30000 ms

Trend? ☒

Trend every 1 poll(s)

Review the default values defined for TCP ports, UDP ports, ICMP, and HTTP monitors. Values set at this resource level display as default values when you create an individual resource's monitoring plan and rule definitions.

4. Change the default values, as necessary, and click **Submit**.

The new defaults will be in place when you create a new network resource. If, when you create the new resource, the default values are still not what you want, you can change the values of the individual resource at that time to suit your own needs.

Note that you can revert back to the original Fathom-supplied default values at any time by selecting **Restore Fathom Defaults**.

Discovering and monitoring TCP and UDP ports

Fathom supports network discovery procedures, which allow you to search for ports that are present on your network. The resource discovery process can save you time in identifying ports for which you want to set up resource monitors. Once you obtain search results, you can then quickly add resource monitors for active ports that you discover, populating the resource-monitoring plans with default values that you can later change, as necessary.

Network discovery includes:

- Reviewing the list of well-known ports.
- Discovering network resources.
- Adding resource monitors for discovered machines and ports.

Reviewing the list of well-known ports

Fathom can provide you with a list of well-known ports.



To review the list of available ports:

1. Click **Resources** from the menu bar.
2. Click **Discover Network Resources**. The **Discover Network Resources** page appears:

The screenshot shows the 'Discover Network Resources' page. It has a title bar with a magnifying glass icon and the text 'Discover Network Resources'. Below the title bar are four buttons: 'Discover...', 'Reset', 'Cancel', and 'Previous Results'. Under these buttons is a section titled 'IP address range' with two input fields: 'Starting Address:' and 'Ending Address:', both containing '172.16.'. Below the input fields is a link labeled 'Well-known ports'.

3. Click **Well-known Ports**. The **Well-known Ports** page appears:

The screenshot shows the 'Well-known Ports' page. It has a title bar with a document icon and the text 'Well-known Ports'. Below the title bar are three buttons: 'Submit', 'Discover Network Resources', and 'Fathom Resource Page'. Below the buttons is a table with four columns: 'Port', 'Type', 'Description', and 'Add/Delete'. The table contains 11 rows of data, each representing a well-known port. The 'Port' column contains the port number, the 'Type' column contains the protocol (TCP or UDP), the 'Description' column contains the service name, and the 'Add/Delete' column contains an 'Add' button for the first row and 'Delete' buttons for the others.

Port	Type	Description	Add/Delete
	TCP		Add
161	UDP	SNMP	Delete
53	UDP	DNS	Delete
547	TCP	DHCPv6	Delete
389	TCP	LDAP	Delete
23	TCP	Telnet	Delete
143	TCP	IMAP	Delete
119	TCP	NNTP	Delete
25	TCP	SMTP	Delete
110	TCP	POP3	Delete
80	TCP	HTTP	Delete
21	TCP	FTP	Delete

This page displays a list of predefined ports that are available to be discovered. Each port is identified by the port number, the port type, and an editable default description.

You can delete any port from the list by selecting the port and clicking **Delete**. You can also add ports to this list. Type a description in the available field, and then click **Add**; repeat this step for each port you want to add.

Besides adding and deleting ports, you can also perform the following actions related to port discovery:

- Update a port description in the space provided, and click **Submit** to save the update.
- Click **Discover Network Resources** to discover which machines are available.
- Click **Fathom Resource Page** to return to that page.

Naming conventions in port descriptions

If a port number is one of the registered well-known numbers, a short description of the port appears as the port's name. (Once you create a resource monitor for a port, Fathom displays this descriptive information on the resource monitoring page, under the page title.)

Table 6–1 identifies names associated with several well-known TCP and UDP port numbers.

Table 6–1: Well-known ports and their associated names *(1 of 2)*

Well-known port	Description field acronym
TCP Port 21	FTP
TCP Port 23	Telnet
TCP Port 25	SMTP
TCP Port 80	HTTP
TCP Port 110	POP3
TCP Port 119	NNTP
TCP Port 143	IMAP
TCP Port 389	LDAP
TCP Port 547	DHCPv6

Table 6–1: Well-known ports and their associated names (2 of 2)

Well-known port	Description field acronym
UDP Port 53	DNS
UDP 161	SNMP

If a port is not considered well known, Fathom displays a port name in the **Description** field that is based on combination of the port number and the protocol type you specify. For example, if you specify the port type as **TCP** and the port number as **3510**, Fathom displays the port name as **tcp3510**.


Discovering network resources

You can use Fathom to determine whether a particular machine is available.



To discover network resources:

1. Select **Resources** from the menu bar. The **Fathom Resources** page appears.
2. Click **Discover Network Resources**. The **Discover Network Resources** page appears:

 **Discover Network Resources**

Discover... Reset Cancel Previous Results

IP address range

Starting Address: 172.16.

Ending Address: 172.16.

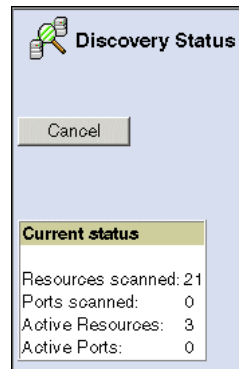
[Well-known ports](#)

3. Enter values in the **Starting Address** and **Ending Address** fields to identify a range of Internet Protocol (IP) addresses you want Fathom to PING. This activity enables Fathom to discover machine and port information.

To simplify your entries in the **Starting Address** and **Ending Address** fields, Fathom provides the first two fields of your local host in each of these entries. In the example shown in [Step 2](#), the value 172.16. appears in each of these fields. To enter a valid starting address, you must append these partially provided values with the remaining two fields.

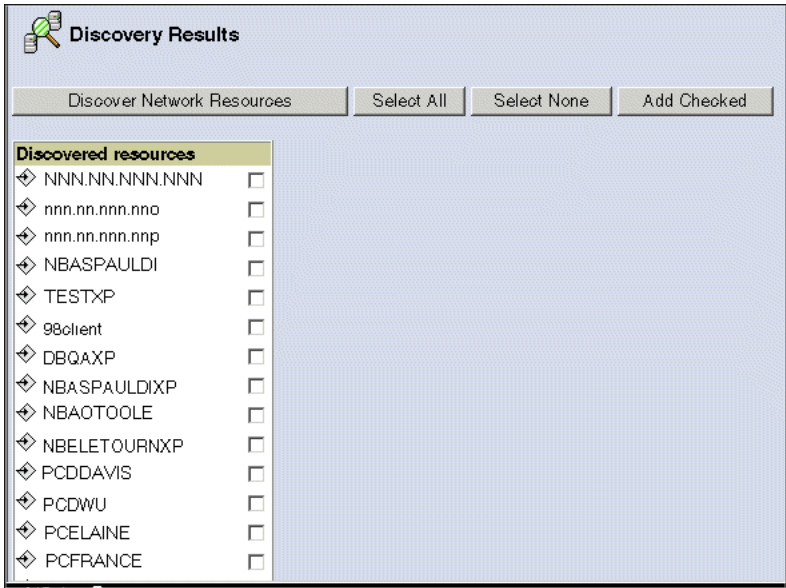
Both the **Starting Address** and the **Ending Address** must begin with the same values.

4. Click **Discover**. Depending on the number of resources Fathom must PING (and the corresponding time it takes to perform this activity), the **Discovery Status** page appears:



The **Discovery Status** page displays and updates the status of the discovery process as resources and ports associated with the IP addresses are scanned. PING information obtained for active resources, and UDP and TCP ports that are discovered to be active, are reported and updated on this page approximately every three seconds.

Once the discovery process ends, the **Discovery Results** page appears:



The following details about discovered resources are returned and displayed if a machine is available:

- TCP and/or UDP port data.
- Machine name.

The icon that displays next to a discovered resource indicates whether the resource is a TCP port, a UDP port, or an ICMP resource.

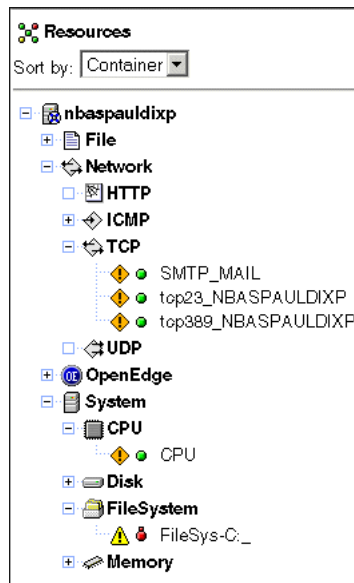
Adding resource monitors for discovered machines and ports

Once you have discovered machines and ports, you can quickly set up resource monitors for them.



To set up the resource monitors:

1. Select the individual check box associated with each resource you want to add, or click **Select All** to select all resources.
2. Click **Add Checked**. An informational message appears in the detail frame, stating that the network resources you selected have been successfully added to Fathom.
3. Click **OK** to close the informational message. The network resources you identified appear in the list frame:



Discovered network resources also follow a naming convention. These resource names are derived from the hostname associated with the discovered resource and a character string derived from the resource's type and port number. Each of these elements is separated by a colon, using the following format:

`resource typeresource port number:discovered resource`

For example, if an activity on port 80 on a machine with a host name of DELL1 is discovered, the resource name that Fathom generates is HTTP:DELL1. In contrast, if an activity on port 1234 on a machine with a host name of DELL2 is discovered, the resource name that Fathom generates is tcp1234:DELL2.

When you add the discovered network resource to Fathom, the colon is replaced by an underscore; for example, tcp23:nbaspauldixp becomes tcp23_nbaspauldixp.

4. Select a newly added network resource to display its default monitoring plans and rules. You can now work with the monitor for the newly discovered resource just as you would any other monitor.

Accessing a previously discovered resource

You can later reaccess any discovered resource that you do not add to Fathom at the time of discovery. The results are retained from one previous discovery process only and are replaced once a subsequent session concludes.



To reaccess a previously discovered resource:

1. Click **Resources** on the Fathom menu bar.
2. Click **Discover Network Resources**. The **Discover Network Resources** page opens.
3. Click **Previous Results**.

Creating a TCP or UDP resource monitor

Fathom supports setting up individual TCP and/or UDP monitors.

The TCP monitor attempts to connect to a TCP port and reports status and response time. The TCP monitor can be useful in determining the status and response times for servers that listen on a TCP port. This includes servers such as mail, FTP, and Web servers.

Note: Fathom supports a default operator e-mail TCP monitor identified as a Simple Mail Transfer Protocol (SMTP) SMTP_Mail. You can set host, port, and default e-mail recipient values in the **Default alert recipient** section of the **Fathom Management Configuration** page. However, you can edit values as you would any user-defined TCP resource monitor.

The UDP monitor attempts to communicate with a UDP port and reports status and response time.

Note: Monitoring a NameServer using UDP resource monitors is not recommended. If you set up a UDP monitor to monitor a NameServer UDP listener port, the NameServer will detect the UDP messages. However, the NameServer will inspect the UDP messages and reject them because they do not follow the convention expected by the NameServer. Consequently, the NameServer will log error messages to indicate that invalid message requests are being received.

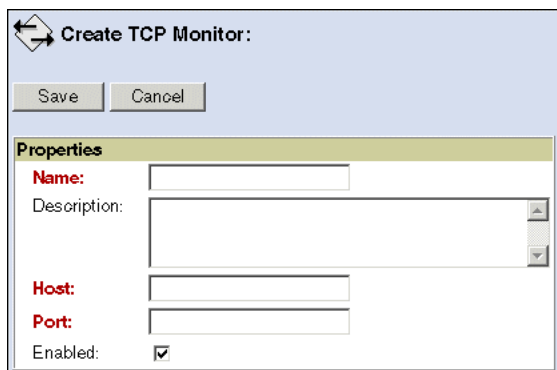


To define a TCP or UDP resource monitor:

1. Click **Resources** from the menu bar. The **Fathom Resources** page appears.
2. Click **New Resource Monitor**.
3. Click either **TCP Port** to create a TCP port resource monitor or **UDP Port** to create a UDP port resource monitor.

Once you make this initial selection, the fields you need to complete to create either a TCP port or UDP port are identical. (For the purpose of this procedure, the steps to create a TCP port are shown.)

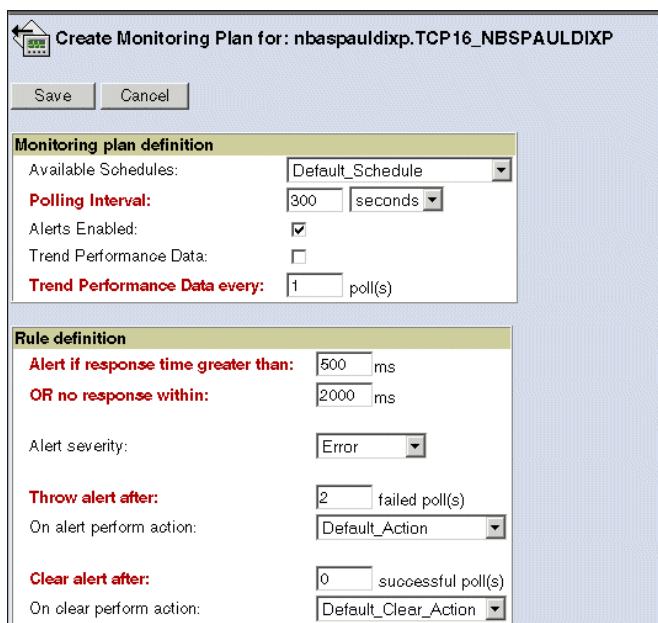
The **Create TCP Monitor** page appears:



The **Create TCP Monitor** dialog box features a title bar with a back arrow icon and the text "Create TCP Monitor:". Below the title bar are "Save" and "Cancel" buttons. The main area is titled "Properties" and contains the following fields:

- Name:** A text input field.
- Description:** A multi-line text area.
- Host:** A text input field.
- Port:** A text input field.
- Enabled:** A checkbox that is currently checked.

4. Enter values in the **Name** and **Description** fields.
5. In the **Host** field, enter the name of the host or IP address where the port is located.
6. In the **Port** field, enter the number of the port.
7. Ensure that the **Enabled** field is checked to begin monitoring.
8. Click **Save**. The **Create Monitoring Plan** page appears:



The **Create Monitoring Plan** dialog box has a title bar with a back arrow icon and the text "Create Monitoring Plan for: nbaspauldixp.TCP16_NBSPAULDIXP". It includes "Save" and "Cancel" buttons. The dialog is divided into two sections:

Monitoring plan definition

- Available Schedules:** A dropdown menu showing "Default_Schedule".
- Polling Interval:** A text input field with "300" and a dropdown menu with "seconds".
- Alerts Enabled:** A checked checkbox.
- Trend Performance Data:** An unchecked checkbox.
- Trend Performance Data every:** A text input field with "1" and a dropdown menu with "poll(s)".

Rule definition

- Alert if response time greater than:** A text input field with "500" and a dropdown menu with "ms".
- OR no response within:** A text input field with "2000" and a dropdown menu with "ms".
- Alert severity:** A dropdown menu showing "Error".
- Throw alert after:** A text input field with "2" and a dropdown menu with "failed poll(s)".
- On alert perform action:** A dropdown menu showing "Default_Action".
- Clear alert after:** A text input field with "0" and a dropdown menu with "successful poll(s)".
- On clear perform action:** A dropdown menu showing "Default_Clear_Action".

9. Update the default values, as necessary, which provide for monitoring plan and rule definition fields. See the [“Reviewing network resource default values”](#) section on page 6–3 for details about the **Alert if response time greater than** and **OR if no response within** fields.
10. Click **Save**. The **TCP Monitor** resource summary page appears.

Creating a PING (ICMP) resource monitor

Fathom supports setting up a large number of network resources simultaneously for which you can define PING activities individually. Fathom can PING a network resource to determine its availability. Fathom sends an ICMP echo request to an IP host and returns a response time and status.

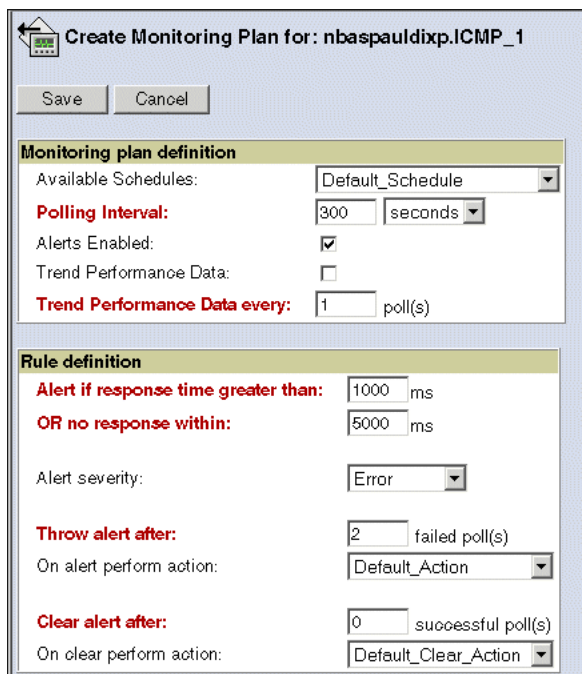


To define an ICMP resource monitor:

1. Click **Resources** from the menu bar. The **Fathom Resources** page appears.
2. Click **New Resource Monitor**.
3. Click **PING (ICMP)**. The **Create ICMP Monitor** page appears:

4. Enter values in the **Name** and **Description** fields.
5. In the **Host** field, enter the name of the host or IP address where the port is located.
6. Ensure that the **Enabled** field is checked to begin monitoring.

- Click **Save**. The **Create Monitoring Plan** page appears:



Create Monitoring Plan for: nbaspauldixp.ICMP_1

Save Cancel

Monitoring plan definition

Available Schedules: Default_Schedule

Polling Interval: 300 seconds

Alerts Enabled: ☒

Trend Performance Data: ☐

Trend Performance Data every: 1 poll(s)

Rule definition

Alert if response time greater than: 1000 ms

OR no response within: 5000 ms

Alert severity: Error

Throw alert after: 2 failed poll(s)

On alert perform action: Default_Action

Clear alert after: 0 successful poll(s)

On clear perform action: Default_Clear_Action

- Update the default values, as necessary, provided for monitoring plan and rule definition fields. See the [“Reviewing network resource default values”](#) section on page 6–3 for details about the **Alert if response time greater than** and **OR if no response within** fields.
- Click **Save**. The **ICMP Monitor** resource summary page appears.

Using the HTTP resource monitor to determine Web site status

Fathom supports a Hypertext Transfer Protocol (HTTP) resource monitoring feature that allows you to monitor various aspects of a Web page. Businesses that rely heavily upon the Internet to convey information to customers and conduct business transactions need to ensure that their company's Web site is reliable, accurate, and accessible. Establishing HTTP resource monitors for these Web sites can help fulfill this need.

Like other resources you can set up in Fathom Management, characteristics of an HTTP resource monitor are defined in properties that you establish. You can also establish optional authentication properties for an HTTP resource monitor. The purpose of this process is to provide basic authentication capabilities; however, this authentication scheme is not considered to be a secure method of authentication unless it is used with another external security system because username and password data are passed over the network as clear text.

General considerations

Review the following information about HTTP rules and Web page redirection before you set up HTTP resource monitors.

HTTP rules

HTTP monitors use a unique set of resource rules to monitor the status and content details of a Universal Resource Locator (URL). When enabled, the *status rule* can indicate whether:

- The URL you are monitoring was redirected.
- The GET method was successful and was accomplished within the time range you specified.

Similarly, the *content rule* can also be enabled to indicate content details such as whether:

- A hash value comparison should be performed.
- A search should be performed on a given page for the search string you specify.

For each schedule you define for a URL that you intend to monitor, you also define status and content rules to suit your specific URL monitoring needs. See the [“Editing rules for the HTTP resource monitor”](#) section on page 6–23 for details about editing status rules and content rules.

Web page redirection

When attempting to retrieve a web page, your client may be directed to a page other than the one initially requested.

This situation can occur for the following reasons:

- Redirection

Redirection occurs when the server informs the client that it is being redirected, and sends the client to the new page. When redirection occurs within the context of using an HTTP Monitor, a redirection alert occurs if you have selected the **Alert if URL was redirected** option on the **Edit status rule** page.

- Aliasing

Aliasing occurs when the server sends the client to a different page without informing the client. The client believes that it has retrieved the Web page that was originally requested. Because the server does not inform the client that it has been sent to a different page, the HTTP Monitor cannot trigger redirection alerts, even if the **Alert if URL was redirected** option is selected on the **Edit status rule** page.

Creating an HTTP resource monitor

You can create an HTTP resource monitor to determine a Web site's availability.



To define an HTTP monitor:

1. Select **Resources** from the menu bar. The **Fathom Resources** page appears.
2. Click **New Resource Monitor**.

3. Click **HTTP**. The **Create HTTP Monitor** page appears:

Create HTTP Monitor:

Save Cancel

General properties

Name:

Description:

URL:

Proxy server:

Form data:

HTTP headers:

Accept cookies: ☒

Polling Enabled: ☒

Authentication properties

URL realm:

URL user name:

URL password:

Proxy server realm:

Proxy server user name:

Proxy server password:

You can now set up the resource monitor's properties.

Setting up an HTTP resource's properties

You must set properties for an HTTP resource you create.



To set the HTTP resource monitor's properties:

1. Enter the name of the HTTP monitor in the **Name** field.

A maximum of 32 alphanumeric characters and underscores are allowed.

2. Enter the HTTP monitor description in the **Description** field.

3. Enter the name of the URL to monitor in the **URL** field.

HTTP is the only supported protocol. If the URL does not begin with `http://`, Fathom prepends it.

4. Enter the name and port number of the proxy server in the **Proxy server** field that identifies this URL (optional). The correct format to enter this information is `<proxy>: <port>`.

5. Enter a set of name-value pairs to be appended to the URL in the **Form Data** field.

6. Enter HTTP headers, one per line, in the **HTTP headers** field.

The acceptable header format is `<header name>: <header value>`. Field names are case insensitive.

The following example shows HTTP headers using this format:

```
Accept:img/*;q=0.0,img/gif;q=0.0,text/*;q=0.0
```

7. Decide whether you want Fathom to allow the server to set cookies. The **Accept cookies** option is selected by default; clear the option if you do not want the server to set cookies.

Cookies are not retained as persistent to the disk.

8. Decide whether you want to enable the HTTP monitor. The **Polling Enabled** option is selected by default; clear the option if you want to turn polling off for the monitor.

You can now set the HTTP monitor's authentication properties.

Setting an HTTP monitor's Authentication properties

Setting HTTP resource authentication properties is optional. However, depending on the Web site you are accessing, values might be required in these fields. For example, if you intend to link to a site that is typically secured, such as a bank's Web site, you might need to supply values in all the authentication fields. In contrast, public Web sites that are interested in providing information to all users who want access to information generally do not require an authenticated connection.



To set the HTTP resource monitor's authentication properties:

1. Enter the name of the URL realm that you want to access in the **URL realm** field.
2. Enter the name of the authenticated user in the **URL user name** field. The value you provide in this field is not authenticated when you enter this information.
3. Enter the password associated with the user name in the **URL password** field.
4. If accessing your URL involves a proxy server, also enter the following values:
 - a. Enter the name of the realm associated with the proxy server in the **Proxy Server realm** field.
 - b. Enter the name of the user in the **Proxy server user name** field.
 - c. Enter the password associated with the user name in the **Proxy server password** field.
 - d. Click **Save**. The **Create Monitoring Plan** page for the HTTP Monitor appears:

You can now set up the HTTP resource monitor's monitoring plans.

Setting up the HTTP resource monitoring plans

You determine the monitoring plan and rules for an HTTP resource monitor you create.



To establish HTTP resource monitoring plans and rules:

1. Click on the **Available Schedules** drop-down list to select a schedule.
2. As necessary, change the default number that appears in the **Polling Interval** field.
3. To disable the alerts option, clear the **Alerts Enabled** option.

If you leave this option selected, you should review and possibly change the additional alert-related fields presented in the **Rule definition** section. See the [“Editing rules for the HTTP resource monitor”](#) section on page 6–23 for more information.

4. Select the **Trend Performance Data** option to turn on the option to store data to the FathomTrendDatabase.
5. As necessary, change the default number that appears in the **Trend Performance Data every** field. See the [“Trending considerations for network resources”](#) section on page 6–3 for more information about the **Trend Performance Data** option and the **Trend Performance Data every** field.
6. Click **Save**. The **Edit status rule** page appears:

Edit status rule for Default_Schedule for HTTP monitor:

Save Cancel

Status rule definition

Enable status rule: ☒

Alert if URL was redirected: ☐

Alert if response time greater than: 15000 ms

OR no response within: 30000 ms

Alert severity: Error

Throw alert after: 2 failed poll(s)

On alert perform action: None

Clear alert after: 0 successful poll(s)

On clear perform action: None

You can now edit the HTTP resource monitor's rules.

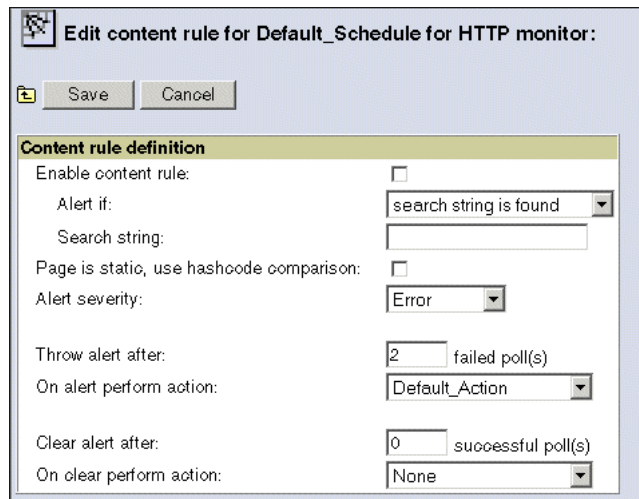
Editing rules for the HTTP resource monitor

You can edit all of the rules-related definitions for an HTTP resource monitor.

The following status rule definition fields are unique to the HTTP resource monitor:

- The **Enable status rule** option allows you to either enable or disable all of the criteria specified in the rule definition.
- The **Alert if URL was redirected** option triggers an alert to inform you that the URL was redirected to a page other than the one you expected to access. This alert is generated even if the response time and status code results are acceptable. You can also set the boolean expression **Alert if response time greater than or no response within xx milliseconds** for each of these phrases.

Figure 6–1 shows the **Edit content rule** page.



Edit content rule for Default_Schedule for HTTP monitor:

Save Cancel

Content rule definition

Enable content rule: ☐

Alert if: search string is found ▼

Search string:

Page is statio, use hashoode comparison: ☐

Alert severity: Error ▼

Throw alert after: 2 failed poll(s)

On alert perform action: Default_Action ▼

Clear alert after: 0 sucoessful poll(s)

On clear perform action: None ▼

Figure 6–1: Editing the content rule definition for an HTTP monitor

You can edit all of the rules-related definitions on this page.

The **Enable content rule** option is unique to the HTTP resource monitor. The option allows you to either enable or disable all of the criteria specified in the rule definition. This page defines two means to determine the validity of the page returned, based on your URL definition. You can set one or both of the following fields:

- **Page is static, use hashcode comparison**

Select this option if the page associated with the URL you have defined is static. If the data displayed on the page does not change, Fathom performs a compare based on hashcode details.

- **Alert if search string found in page**

Select this option when you know a particular string should appear on the page you want to access.

Reviewing the HTTP resource monitor settings

When you finish setting up an HTTP monitor and you click **Save**, you view a summary of the various values you entered or accepted, as shown in [Figure 6–2](#).

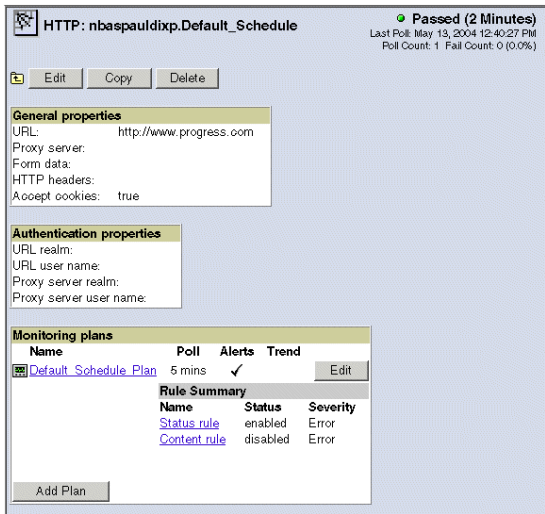


Figure 6–2: HTTP Monitor resource summary

Click **Status rule** to display status rule definition data; click **Content rule** to display content rule definition data. On each of the pages that appears, you can choose to edit values.

Monitoring File Resources

You can monitor a log file or other file by creating a resource monitor. This chapter describes how to create log file monitors, which monitor file contents, and file monitors, which monitor file characteristics, and contains the following sections:

- [File resource monitoring overview](#)
- [Verifying mapped network drives](#)
- [Reviewing log file and file resource default values](#)
- [Creating a log file monitor](#)
- [Enabling the log file monitor](#)
- [Editing, copying, or deleting a log file monitor](#)
- [Creating a file resource monitor](#)
- [Creating a file monitor](#)

File resource monitoring overview

When you create a *log file monitor*, you choose the specific file content you want to monitor. Your ability to focus on the content you are interested in is valuable because log files typically contain considerable data. For example, you might be especially concerned about tracking system errors or monitoring any warnings that are recorded in the log.

You create a *file monitor* to check on the characteristics, rather than the content, of a file. You can create a monitor that will gather specific information about a file, such as its size or age, for example.

Because the log file monitor and the file monitor are concerned with different aspects of a file, you can create one of each for the same file. For example, you might create a log file monitor for the AdminServer log (`admserv.log`) to keep you informed of particular areas of concern in the file's contents. You can also create a file monitor for the AdminServer log that will check on one or more of the file's characteristics, such as its size or growth rate. Then if you find that the AdminServer log is growing too quickly, you can lower the logging level so that less data is written to the log.

Log file monitor features

Log file resource monitors have characteristics similar to other Fathom resource monitors. You define monitoring plans and rules for log file monitors just as you can for all resource monitors. You can also elect to use Fathom-supplied default values to create log file monitoring resources.

Unlike other Fathom resource monitors, however, log file resource monitors have several unique qualities that you can use to define their monitoring capabilities, such as:

- **A bookmark feature** — The bookmark feature helps ensure that log files are monitored unobtrusively and according to search criteria you define.

See the [“Using a bookmark”](#) section on page 7–9 for information about setting and working with bookmarks.

- **A search criteria feature** — You specify search criteria in the log file monitor's rule properties and identify expressions that you can use to obtain specific information about log file contents.

See the [“Specifying search criteria”](#) section on page 7–25 for information about search criteria.

- **A library feature** — The library feature allows you to define a collection of independently stored search criteria and rule sets that you can share (including by importing and exporting across different machines) among the log file monitors you create and maintain.

See the [“Associating rule sets with log file monitors”](#) section on page 7–20 for information about library features.

For details about importing and exporting search criteria and log file rule sets, see [Chapter 9, “Exporting and Importing in Fathom.”](#)

File monitor features

You can monitor the following file attributes by creating a file monitor:

- The file's existence.
- The file's size.
- The file's age.
- The file's growth rate.
- If the file has been modified.

The file monitor does not support rule sets.

Verifying mapped network drives

If you want to monitor a log file or other file, and Fathom is installed on a Windows NT, Windows 2000, or a Windows XP system, you must ensure that Fathom Management can see your mapped network drives.



To verify the mapped network drives:

1. Do one of the following:
 - On Windows NT, choose **Start**→**Settings**→**Control Panel**. Click **Services**.
 - On Windows 2000, choose **Start**→**Settings**→**Control Panel**→**Administrative Tools**→**Services**.
 - On Windows XP, choose **Start**→**Control Panel**. Choose **Administrative Tools**, then choose **Services**.
2. Select the **AdminService for OpenEdge**, and then do one of the following:
 - On Windows NT, click **Startup**.
 - On Windows 2000, right-click, then choose **Properties**. Choose the **Log On** tab.
 - On Windows XP, click the link to **Start** the service. Choose the **Log On** tab.
3. Select the **This Account** option and specify a user with administrative privileges for the account you specify. (You must override the default value LocalSystem with this user information.)
4. Enter the password, and confirm the password entry.
5. Click **OK**.
6. As necessary, restart the AdminServer.

Now you can define file-specific details to create and edit log file and file monitors.

Reviewing log file and file resource default values

Fathom supplies default values for the log file monitor and the file monitor. You can keep the default values established by Fathom, or you can change the values. Whatever default values exist are automatically used when you create a log file monitor or file monitor.

If you choose not to change the default values, you still have the option of altering the values when you create a new monitor. You simply remove the default values and replace them with values you choose.

Before you begin to create log file or file monitors, review the default settings. Performing this review can:

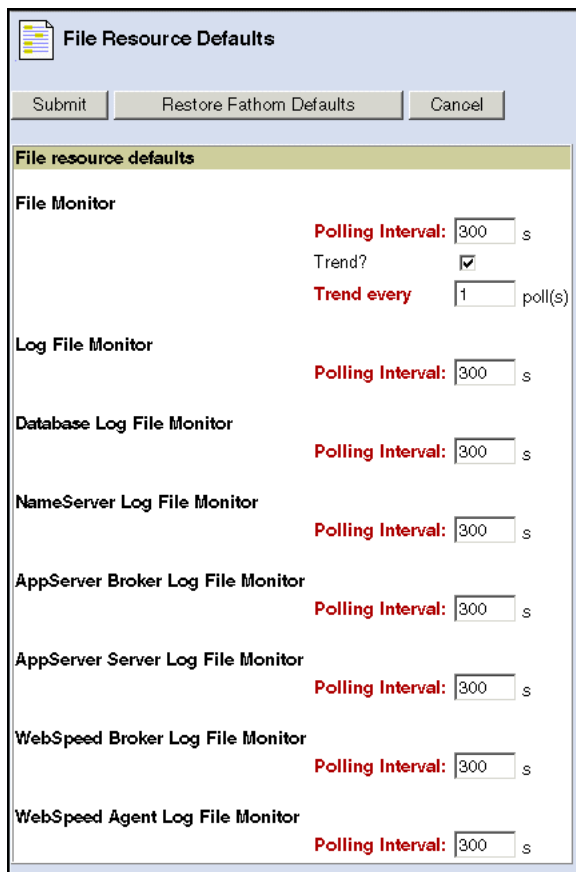
- Help standardize resource rule definitions according to your company's needs.
- Minimize the duplication of effort involved in unnecessarily creating new or editing existing file resource monitors.
- Produce useful resource monitoring data as quickly as possible.



To display the log file monitor and file monitor default values:

1. Select **Resources** from the menu bar. The **Fathom Resources** page appears.
2. Click **Resource Monitor Defaults**. The **Resource Monitor Defaults** page appears.

- Click **File Resource Defaults**. The **File Resource Defaults** page appears as shown:



The screenshot shows a web-based configuration window titled "File Resource Defaults". At the top, there are three buttons: "Submit", "Restore Fathom Defaults", and "Cancel". Below the buttons is a section header "File resource defaults" in a yellow bar. The main area contains several configuration items, each with a "Polling Interval" set to 300 seconds. The "File Monitor" section also includes a "Trend?" checkbox (checked) and a "Trend every" field set to 1 poll(s). The other monitors listed are Log File Monitor, Database Log File Monitor, NameServer Log File Monitor, AppServer Broker Log File Monitor, AppServer Server Log File Monitor, WebSpeed Broker Log File Monitor, and WebSpeed Agent Log File Monitor.

Monitor Name	Polling Interval	Trend?	Trend every
File Monitor	300 s	<input checked="" type="checkbox"/>	1 poll(s)
Log File Monitor	300 s		
Database Log File Monitor	300 s		
NameServer Log File Monitor	300 s		
AppServer Broker Log File Monitor	300 s		
AppServer Server Log File Monitor	300 s		
WebSpeed Broker Log File Monitor	300 s		
WebSpeed Agent Log File Monitor	300 s		

If, when you create a new resource monitor, the default values are still not what you want, you can change the values of the individual log file or file monitor at that time to suit your own needs.

Changing default values does not affect any resource monitor already created.

Note that you can revert back to the original Fathom-supplied default values at any time by selecting **Restore Fathom Defaults**.

- Change the default values as necessary, and click **Submit**.

Creating a log file monitor

Creating a log file monitor involves:

1. Defining properties.
2. Using a bookmark.
3. Creating a monitoring plan.
4. Adding log file rules.
5. Adding log file rule sets.
6. Associating rule sets with log file monitors.
7. Specifying search criteria.
8. Creating search criteria.
9. Enabling the log file monitor.

Typically, you set up one log file resource monitor at a time on a given log file. However, you can set up a variety of monitoring plans, consisting of a number of different schedules that are all defined and enabled to run at different times, for a specific log file resource. It is most beneficial to have only one *active* log file monitor enabled at a time for any given log file.

Once you create a log file monitor, you can edit it, copy it as the basis for a new log file monitor, or delete it.

Defining properties

The log file monitor properties you define are the log file monitor name and description and the name of the file you are monitoring.



To define the properties:

1. Select **Resources** from the menu bar. The **Fathom Resources** page appears.
2. Click **New Resource Monitor**. The **New Resource Monitor** page appears.

- Click **Log File**. The **Create Log File Monitor** page appears:

Create Log File Monitor:

Save Cancel

Properties

Name:

Description:

Filename:

On First Poll:

Please Note: This resource will be automatically disabled on creation to enable you to add rules. Not having all rules defined before the resource is enabled may adversely affect the "On First Poll" property above. Please enable the resource when done adding rules by either editing the log file properties or pressing the "Done" button on the Monitoring Plan page.

Bookmark

☒ Use bookmark

☒ Use custom bookmark (Specify bookmark)

☒ Prepend Time Stamp

☐ Use last line as bookmark

☒ Each line unique? (If unchecked, specify Truncate Action)

☐ Do not use bookmark (Specify Truncate Action)

Truncate Action:

- Enter the log file monitor name in the **Name** field.
- Enter the log file description in the **Description** field.
- Enter the file name of the log file you are monitoring in the **Filename** field. You can enter the path to the log file and the log file's file name using either UNIX or Windows notation conventions.
- If Fathom is installed on a Windows NT or a Windows 2000 system, you must follow additional steps to allow you to see your mapped network drives. This task also enables the log file monitor you create to recognize mapped network drives. See the ["Verifying mapped network drives"](#) section on page 7-4 for general instructions about how to perform this task.

8. Set the value for the **On First Poll** field.

On the first poll of a log file, you must identify how you want the log file monitor to interact with preexisting log file data. You select one of two options:

- **Search entire file selection** tells the log file monitor to search all preexisting log file data. If your log file is a relatively small file, consider this option.
- **Search only new data** tells the log file monitor to *ignore* any preexisting log file data and perform the setup needed for subsequent polls based on the bookmark properties set at the current end of file.

Note: As indicated by the note associated with the **On First Poll** field in the management console, there are two ways to enable a log file resource monitor. You can either edit the log file properties for the log file monitor, or you can click **Done** on the **Monitoring Plan** page. See the “[Creating a file resource monitor](#)” section on page 7–37 for details.

Using a bookmark

You create a *bookmark* and insert it into your log file to indicate the exact point from which the log file monitor is reading data. To accurately monitor and manage a log file, the log file monitor needs to know its exact position within the file and have a dependable means to reset its file position if it loses its place within the file due to *truncation*. If you opt not to set a bookmark, you choose which truncation action Fathom follows: searching only new data, or searching the entire file.

You are strongly encouraged to use bookmarks with monitors you create for OpenEdge log files. However, using the bookmark feature in non-OpenEdge log files might cause problems using the log. If you have an application that parses out its own log file, it could get tripped up on information it considers foreign.

You might detect a small performance gain in running the log file resource monitor when the log file is truncated; however, you will sacrifice accuracy within your log file data, exposing the data and monitoring operations to an unnecessary high level of risk and unpredictable accuracy in your log file reads.

Bookmark and truncation considerations

Due to the volume of data stored, some log files have a potential to grow very large. A database administrator (DBA) will typically truncate these files periodically to minimize the amount of space they occupy on a system. The existence of bookmarks within a log file ensures that regardless of what happens to your file when it is truncated, your log file monitor always has a way to reposition itself accurately within the file.

Data can be truncated at any point within a file. Consequently, when bookmarks are not used and a file has been truncated, the log file monitor has only a limited number of options to determine its new position. Bookmarks represent your most reliable means to reposition your log file monitor accurately so that the data you use is accurate.

For example, if a DBA truncated 500 lines of data at the beginning of a log and, in the meantime, 1000 more data lines were added at the end of the file, the log file will reposition the new reference mark somewhere within the last 500 data lines; having “lost” 500 lines, the log file monitor only “knows” it has to read ahead 500 lines into the new data and reposition itself. Under this situation, the fact that 500 lines of data have been truncated has been obscured by the existence of the new data. Not having a bookmark to reference as a point of origin, the log file monitor can, and does, reposition itself 500 lines into the “newer” data lines that have been written. Unfortunately, this approach incorrectly allows the data to be misread, since the balance of the 500 newer data lines are left unread. Had bookmarks been used in this circumstance, this error would have been avoided.

Note: Under certain circumstances, you might not be concerned with unread data. For example, if you are performing software testing activities, log files might be deleted frequently. Therefore, you might not need to set bookmarks to ensure accurate repositioning occurs after a file has been truncated.

If the monitored log file has changed since the last poll and the bookmark feature is enabled, a new bookmark is inserted.

Setting a bookmark

You can set a custom bookmark or use the last line as the bookmark.



To set a bookmark from the Create Log File Monitor page:

1. In the **Bookmark** section, select **Use bookmark**.
2. Select one of the following two ways to set bookmark attributes:

- **Use custom bookmark (Specify bookmark)**

You can choose either to use the default bookmark named `Fathom_Bookmark` or define a new bookmark. If you define a bookmark, the value you enter is not restricted to a certain length. However, for practical purposes, you might want to consider keeping it a reasonable length.

Additionally, you can choose to prepend a time stamp to your bookmark name selection. You should *always* select this option. The date and time value uniquely qualifies each bookmark that has this data prepended to its bookmark name. In situations where the log file monitor must reposition itself within the log file, this type of bookmark will always be found.

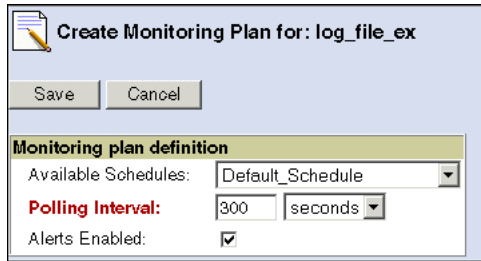
- **Use last line as bookmark**

This option records the last line of a given poll as a bookmark internally (Unlike the custom bookmark, this information is not written in the log file being monitored.)

Choosing this option indicates that you want to use the last line as the bookmark. The last line is referenced as it is randomly defined in the file; it is likely that the line will not be unique. If your log file has a date and time stamp on each line, or other data that makes each line unique, select the **Each line unique** option. This refinement will increase the log file monitor's accuracy.

If you do not use the **Each Line Unique** option, you must specify one of the possible two **Truncate Action** selections from the drop-down list.

3. Click **Save**. The **Create Monitoring Plan** definition page appears:



Create Monitoring Plan for: log_file_ex

Save Cancel

Monitoring plan definition

Available Schedules: Default_Schedule

Polling Interval: 300 seconds

Alerts Enabled: ☒

Truncating a log file

If you choose to truncate a log file, the file will not use a defined bookmark to reference its position within the log file. Therefore, you must indicate how you want the log file monitor to interact with the log file when the file has been truncated.

You might detect a small performance gain in running the log file resource monitor when the log file is truncated. However, you will sacrifice accuracy within your log file data, exposing the data and monitoring operations to an unnecessary high level of risk and unpredictable accuracy in your log file reads.

You can choose either of the following truncation actions:

- **Search only new data**

Fathom resets the log file monitor's internal place marker to the end of the file on its first poll after the file has been truncated.

- **Search entire file**

Fathom searches the log file from beginning to end on its first poll after the file has been truncated. Remember that this technique will ensure that no data is missed when a file is truncated, but much of the file could be searched a second time. If the file is very large, this can be a slow operation.

Creating a monitoring plan

Once you make your decisions about the bookmark, you create the log file monitor's monitoring plan. You begin by viewing the monitoring plan's default values, as shown in [Figure 7–1](#).

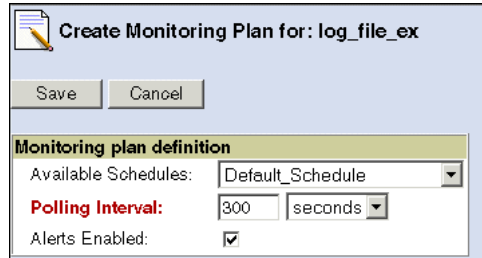


Figure 7–1: Log file monitoring plan

The following default values are identified:

- **Available Schedules** — A list of all schedules available for this monitoring plan.
- **Polling Interval** — The interval at which the resource is polled.
- **Alerts Enabled** — An indication of whether alerts defined for this resource are enabled.

You can elect to accept or change any of the default values.



To continue creating the monitoring plan from the Create Monitoring Plan page:

1. Click **Save** to save the monitoring plan definition. The **Monitoring Plan** page appears, showing the monitoring plan definition and the rules and rule sets selected for the plan:

Default_Schedule Monitoring Plan for: log_file_ex

Edit Delete

Monitoring plan definition

Schedule: [Default Schedule](#)

Polling Interval: 5 minutes

Alerts Enabled: true

Rules selected for this plan

None

Add Rule Select Rule Sets

Done

You can now add rules or rule sets to this monitoring plan.

2. Click either **Add Rule** or **Select Rule Sets** from the **Rules selected for this plan** section.

You can now continue with the “[Adding log file rules](#)” section on page 7–15 for details about including rules or the “[Adding log file rule sets](#)” section on page 7–16 for details about including rule sets in the plan.

Adding log file rules

You can include one or more rules and/or rule sets in a log file monitor. When you add a rule, you must also select search criteria and then associate it with severity and alert information to fully define the rule.

Log file monitor rule components

A log file monitor rule consists of the following components:

- **Search criteria** — The core element of log file rules. A search criterion allows you to create and store exactly what data a log file resource monitor will look for when it searches a log file. Fathom- and user-defined search criteria are stored in the library so they can be shared and reused in various log file monitor rules.

See the [“Specifying search criteria”](#) section on page 7–25 for details about the search criteria.

- **Severity** — One of the four standard, user-selected severity levels: **Information**, **Warning**, **Error**, or **Severe**. This information is stored in the **Severity** field.
- **Alert** — Identifies which action Fathom performs when an alert occurs. This user-selected information is stored in the **On Alert Perform Action** field.

You can include a rule in the log file resource monitor in three ways:

- By adding it to a single log file resource under the resource’s monitoring plan, in which case the rule definition *cannot* be shared by other log file resource monitors.
- By adding it to one or more rule sets, in which case the rule *can* be shared among several log file resource monitors.

Note: Edits to any user-defined search criteria immediately affect all current instances in which the search criteria is used in individual rules or rule sets, and will also be used in instances to be created in the future. You can edit or delete Fathom-supplied search criteria.

- Associating it with a log file resource monitor. An identical rule definition, defined in a rule set, can also be applied to this same log file resource monitor. In this situation, the individual, or locally defined rule, takes precedence. The rule definition associated with the rule set will be listed as part of the rule set, but the status icon for this duplicate rule will be gray and the status listed as **Inactive**.

Adding log file rule sets

A log file rule set is composed of one or more rule definitions. The purpose of a rule set is to help you manage a large number of log file monitors consistently and efficiently by sharing rule definitions. By creating and selecting appropriate log file rule sets to be added to log file resource monitors, you eliminate the requirement to add log file rules on an individual basis to each log file monitor.

Once a rule set exists, you can access it from the list frame and then associate it with the monitoring plan of a log file monitor. Then, when the monitoring plan is active and the log file monitor is polled, Fathom can evaluate each rule in the set. Keep in mind that a log file monitor's monitoring plan can have one or more rule sets associated with the plan.

Accessing existing log file rule sets

The Fathom Library provides access to existing log file rule sets.



To access existing log file rule sets:

1. Select **Library** from the menu bar. The existing Library objects display in the list frame.
2. As necessary, select **Type** as the **Sort by** option, and expand the **Rule Sets** category. These predefined categories display: AppServer, Database, LogFile, NameServer, and WebSpeed. Click **LogFile** to display a list of all available log file rule sets.
3. To display details about a specific rule set in the detail frame, click an individual rule set name in the list frame. Within the detail frame, you can edit the rule set.

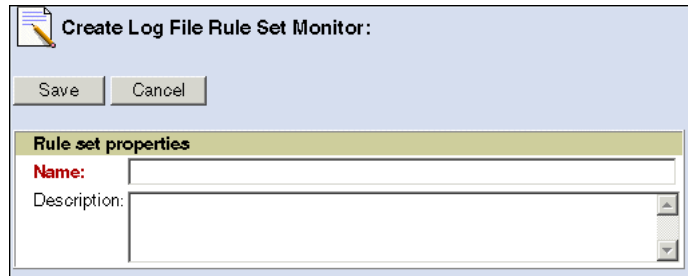
Creating a new log file rule set

A log file rule set allows you to centrally define rules at the library level and associate rule sets with one or more log file resource monitors.

Rules within rule sets are composed of three rules-required components: search criterion, severity level, and alert details. Library-based log file rule sets are comprised of rules that have search criteria you define for local search criteria, or select from the search criteria stored in the library.

**To set up library-based log file rule sets:**

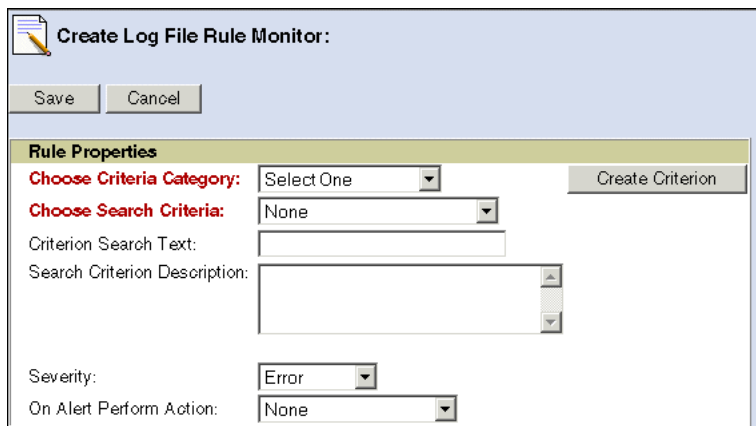
1. Select **Library** from the menu bar. The **Fathom Component Library** page displays in the detail frame.
2. Click **Create Log File Rule Set Monitor**. The **Create Log File Rule Set Monitor** page appears:



3. Enter the name of the rule set in the **Name** field.
4. Enter a description of the rule set in the **Description** field.
5. Click **Save**. The **Log File Rule Set Monitor** page appears:

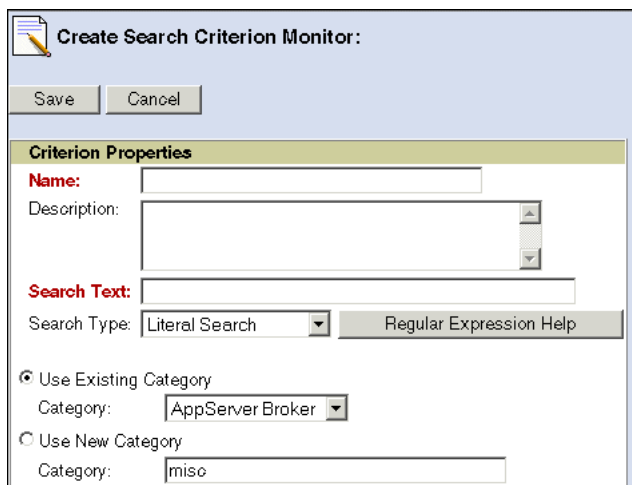


6. To add a rule to this rule set, click **Add Rule**. The **Create Log File Rule Monitor** page appears:



The screenshot shows the 'Create Log File Rule Monitor' dialog box. It has a title bar with a document icon and the text 'Create Log File Rule Monitor:'. Below the title bar are 'Save' and 'Cancel' buttons. The main area is titled 'Rule Properties' and contains the following fields: 'Choose Criteria Category:' with a dropdown menu showing 'Select One' and a 'Create Criterion' button; 'Choose Search Criteria:' with a dropdown menu showing 'None'; 'Criterion Search Text:' with a text input field; 'Search Criterion Description:' with a text area; 'Severity:' with a dropdown menu showing 'Error'; and 'On Alert Perform Action:' with a dropdown menu showing 'None'.

7. Choose one of the following options:
 - Use existing search criteria. Select values available from the drop-down list fields on the **Create Log File Rule Monitor** page. See the [“Selecting search criteria to define a local rule”](#) section on page 7–33 for the specific steps, complete the steps as defined, and then return to [Step 8](#) in this procedure.
 - Use new search criteria. Continue with [Step 8](#) in this procedure.
8. Click **Create Criterion**. The **Create Search Criterion Monitor** page, from which you will create a new rule to add to the rule set, appears:



The screenshot shows the 'Create Search Criterion Monitor' dialog box. It has a title bar with a document icon and the text 'Create Search Criterion Monitor:'. Below the title bar are 'Save' and 'Cancel' buttons. The main area is titled 'Criterion Properties' and contains the following fields: 'Name:' with a text input field; 'Description:' with a text area; 'Search Text:' with a text input field; 'Search Type:' with a dropdown menu showing 'Literal Search' and a 'Regular Expression Help' button; and two radio button options: 'Use Existing Category' (selected) with a 'Category:' dropdown menu showing 'AppServer Broker', and 'Use New Category' with a 'Category:' text input field showing 'miso'.

9. Enter a value in the **Name** field. The search name can be a maximum of 32 characters, and it must not contain spaces between words or use special characters such as an asterisk (*), an ampersand (&), or a period (.).
10. Enter a description in the **Description** field.
11. In the **Search Text** field, enter the search string you want this rule to look for in the log file. The entry must be consistent with the type of search you are performing.
12. In the **Search Type** field, select either **Literal Search** or **Regular Expression**. See the [“Specifying search criteria”](#) section on page 7–25 for a detailed description of these search types.
13. Store this search criterion in a Search Criteria category:
 - **Use Existing Category** (default value) — From **Category**, scroll through the list of Fathom predefined categories and select one. The list includes these categories: AppServer Broker, AppServer Server, Database, Miscellaneous, NameServer, WebSpeed Broker, and WebSpeed Server.
 - **Use New Category** — In the **Category** field, use the predefined **misc** category, or enter the name of a new category.
14. Click **Save**. The **Create Log File Rule Monitor** page reappears, displaying the newly identified search criterion values in the **Criteria Category** and **Search Criteria** fields.
15. Identify the remaining properties for this rule:
 - In the **Severity** field, select the level of severity you want to set for this rule.
 - In the **On Alert Perform Action** field, select the action you want Fathom to perform when an alert triggers.
16. Click **Save**. The **Log File Rule Set Monitor** page redisplay with this newly created rule displayed in the **Rules selected for this Rule Set** section.
17. As necessary, repeat [Step 6](#) through [Step 16](#) to add additional rules to this rule set.

Your rule set appears in the list frame under the **LogFile** category. See the [“Associating rule sets with log file monitors”](#) section on page 7–20 for details about associating the rule set with a log file monitor.

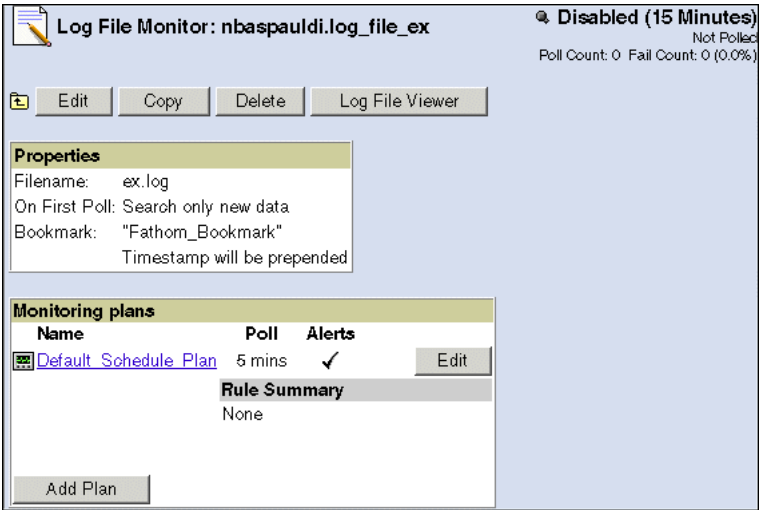
Associating rule sets with log file monitors

Once you have created at least one rule set, you can associate it with a log file monitor.



To associate a rule set with an existing log file monitor:

1. Select **Resources** from the menu bar. In the list frame, expand the **File** category. Expand the **LogFile** subcategory and click the log file resource monitor to which you want to add a rule set. In the detail frame, the summary information about the log file monitor appears:



2. Choose one:
 - Click the link associated with the monitoring plan name you want to display.
 - Click the **Edit** button associated with the monitoring plan for which you want to add a rule set.

The current monitoring plan and rules display in edit mode:

Edit Default_Schedule Monitoring Plan for: log_file_ex

Save Cancel

Monitoring plan definition

Available Schedules: Default_Schedule

Polling Interval: 5 minutes

Alerts Enabled: ☒

Rules selected for this plan

None

Add Rule Select Rule Sets

3. Click **Select Rule Sets**. The rule sets that currently exist appear:

Select Rule Sets for: Default_Schedule

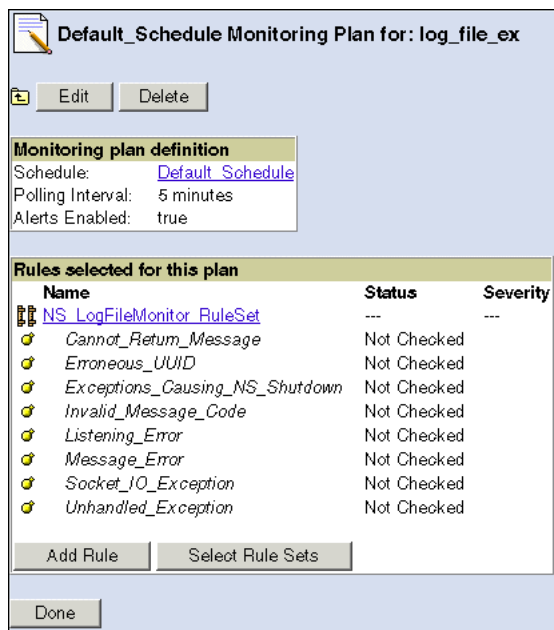
Save Cancel

Select rule sets for this plan

Name	Description
<input type="checkbox"/> AS_Broker_LogFileMonitor_RuleSet	This Rule Set can be used for an AppServer broker log file. This may be modified but cannot be deleted or renamed.
<input type="checkbox"/> AS_Server_LogFileMonitor_RuleSet	This Rule Set can be used for an AppServer server log file. This may be modified but cannot be deleted or renamed.
<input type="checkbox"/> DB_AI_LogFileMonitor_RuleSet	This Rule Set is for the Database Log File Monitor. It keeps track of after-image activity. When a new database is added to Fathom, this Rule Set will be added to its Log File Monitor. This may be modified but cannot be deleted or renamed.
<input type="checkbox"/> DB_LogFileMonitor_RuleSet	This Rule Set is for the Database Log File Monitor. When a new database is added to Fathom, this Rule Set will be added to its Log File Monitor. This may be modified but cannot be deleted or renamed.
<input type="checkbox"/> NS_LogFileMonitor_RuleSet	This Rule Set can be used for a NameServer log file. This may be modified but cannot be deleted or renamed.
<input type="checkbox"/> WS_Broker_LogFileMonitor_RuleSet	This Rule Set can be used for a WebSpeed broker log file. This may be modified but cannot be deleted or renamed.
<input type="checkbox"/> WS_Server_LogFileMonitor_RuleSet	This Rule Set can be used for a WebSpeed server log file. This may be modified but cannot be deleted or renamed.

4. Select the check box or check boxes associated with each rule set you want to add to the log file monitor.

5. Click **Save**. The **Monitoring Plan** page reappears and includes the new rule sets:












Default_Schedule Monitoring Plan for: log_file_ex

Edit Delete

Monitoring plan definition

Schedule: [Default_Schedule](#)
Polling Interval: 5 minutes
Alerts Enabled: true

Rules selected for this plan

Name	Status	Severity
 NS_LogFileMonitor_RuleSet	---	---
 <i>Cannot_Return_Message</i>	Not Checked	
 <i>Erroneous_UUID</i>	Not Checked	
 <i>Exceptions_Causing_NS_Shutdown</i>	Not Checked	
 <i>Invalid_Message_Code</i>	Not Checked	
 <i>Listening_Error</i>	Not Checked	
 <i>Message_Error</i>	Not Checked	
 <i>Socket_IO_Exception</i>	Not Checked	
 <i>Unhandled_Exception</i>	Not Checked	

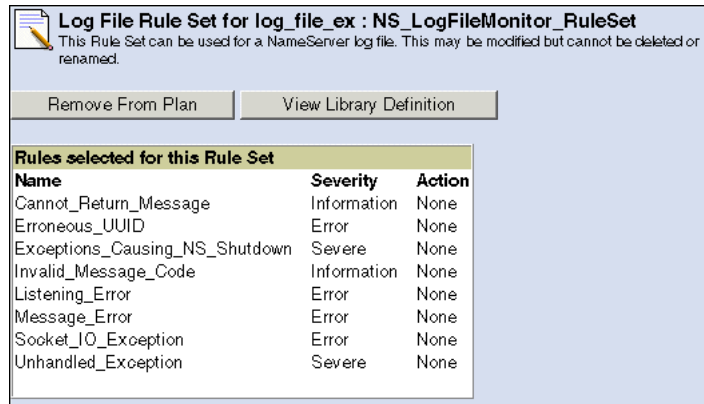
Add Rule Select Rule Sets

Done

Note the following points relative to the rule set addition:

- All rule sets are identified by a rule set icon. The icon appears to the left of each rule set name in the rules list.
- Rule sets appear after individual rules in the list.
- Any edits you make to individual rules within a rule set, or to the rule set itself, immediately affect all instances of the rule sets—current and future.
- Individual rule definitions take precedence over the same rule that is defined within a rule set.

6. To review the specific rules contained in any rule set, click the rule set link in the **Rules selected for this plan** section of the **Monitoring Plan** page. The **Log File Rule Set** page associated with the specific rule set appears, displaying each rule that it contains:



Log File Rule Set for log_file_ex : NS_LogFileMonitor_RuleSet
 This Rule Set can be used for a NameServer log file. This may be modified but cannot be deleted or renamed.

Remove From Plan View Library Definition

Rules selected for this Rule Set

Name	Severity	Action
Cannot_Return_Message	Information	None
Erroneous_UUID	Error	None
Exceptions_Causing_NS_Shutdown	Severe	None
Invalid_Message_Code	Information	None
Listening_Error	Error	None
Message_Error	Error	None
Socket_IO_Exception	Error	None
Unhandled_Exception	Severe	None

7. As necessary, you can perform the following actions:
- Click **Remove From Plan**. The **Monitoring Plan** page appears. You can elect to remove any of the rule sets defined for the current plan. Any changes you make to rule sets affect only this plan's use of the rule set.
 - Click **View Library Definition**. A new page appears, allowing you to link to and display the detail properties that compose each rule. You can edit, copy, or delete individual rules from the library-stored definition at this time. Any changes you make will also affect the current and future uses of this rule.

8. When you are done adding rules and rule sets, click **Done**. The **Log File Monitor** page appears:

Log File Monitor: nbaspauldi.log_file_ex

Failed (0 Seconds)
 Last Poll: Aug. 14, 4:16 PM
 Last Failure: Aug. 14, 4:16 PM
 Poll Count: 1 Fail Count: 1 (100.0%)

Edit Copy Delete Log File Viewer

Alerts
 ⚠ LogFileNotFound Aug 14, 2003 4:16:26 PM

Properties
 Filename: ex.log
 On First Poll: Search only new data
 Bookmark: "Fathom_Bookmark"
 Timestamp will be prepended

Monitoring plans

Name	Poll	Alerts
Default Schedule Plan	5 mins	✓

Rule Summary

Name	Status	Severity
NS_LogFileMonitor_RuleSet	---	---
Cannot_Return_Message	Not Checked	
Erroneous_UUID	Not Checked	
Exceptions_Causing_NS_Shutdown	Not Checked	
Invalid_Message_Code	Not Checked	
Listening_Error	Not Checked	
Message_Error	Not Checked	
Socket_IO_Exception	Not Checked	
Unhandled_Exception	Not Checked	

Add Plan

9. Repeat these steps to associate rule sets with additional monitoring plans for this log file monitor.

Specifying search criteria

Search criteria identify expressions that Fathom can use to obtain specific information about the contents of log files. You can use either a text literal or a Perl 5 regular expression, which you select or create as one of the rule properties, as an individual search criterion. When you specify search criteria, Fathom searches the log file for strings and tries to match the search criteria you specify.

Fathom provides some default search criteria; you can also create your own search criteria. This section presents each type of search criteria in detail.

Accessing search criteria

You access existing search criteria from the Fathom Component Library.

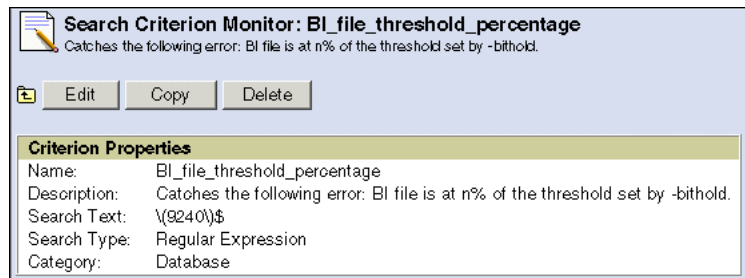


To access either Fathom- or user-defined search criteria:

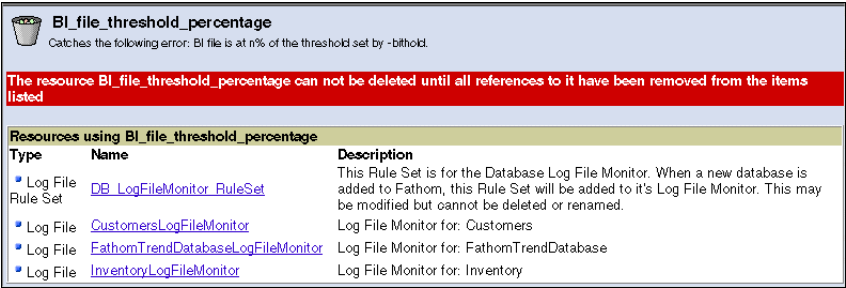
1. Select **Library** from the menu bar. The existing Library objects display in the list frame.
2. As necessary, click **Type** as the **Sort by** option, and expand the **Search Criteria** category. These predefined categories appear: AppServerBroker, AppServerServer, Database, Miscellaneous, NameServer, WebSpeedBroker, and WebSpeedServer.

Note: If you upgraded Fathom Management and you had defined search criteria or log file rule sets in a previous version, these rules will now be redefined in the **Upgraded** category in the list frame.

3. Click the category from which you want to select a predefined search. From the expanded sublist, select the specific search you want to access. The **Search Criterion Monitor** properties summary page displays in the detail frame:



4. Review, edit, copy, or delete the search, as needed. Keep the following points in mind if you elect to change or delete any existing search criteria:
- If you change any values associated with a search criterion that is currently associated with log file monitors, those changes will propagate through all existing instances of the log file monitors that use that specific search criteria.
 - If you attempt to delete a search criterion that is the last one currently defined in a given category, a message displays asking if you would like to delete the category at the same time.
 - If you attempt to delete a search criterion that is associated with any log file monitor, Fathom displays a warning message. This message appears regardless of the log file monitor being enabled or disabled:



Using Fathom-supplied search criteria

You define, store, and access all search criteria from the Fathom library, which is a collection of sharable components.

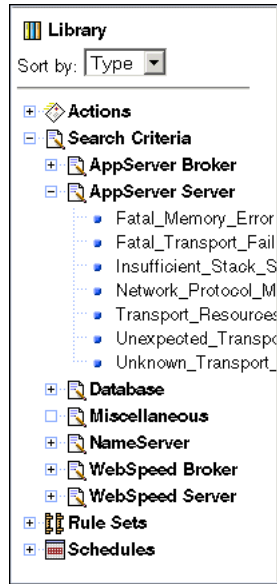


To see the Fathom-provided search criteria:

1. Click **Library** on the menu bar. The following categories appear in the list frame: Actions, Search Criteria, Rule Sets, and Schedules.
2. Expand the **Search Criteria** category. The following criteria categories appear: AppServer Broker, AppServer Server, Database, Miscellaneous, NameServer, WebSpeed Broker, and WebSpeed Server.

Each of these categories has predefined search criteria specifically designed to build rules for each of these products. These predefined elements are intended to address some of the more common search criteria you might use to examine log file data.

3. To see the predefined search criteria in a category, expand it. For example, if you expand the **AppServer Server** category, the criteria appear in a list:



Note: Keep in mind that you can add to, modify, or remove search criteria categories, so the list of categories you see in your own management console might not match the list shown in [Step 3](#).

You can store any search criteria that you define in these categories according to the type of log file with which the criteria is associated. You can also use the **Miscellaneous** category to store other search criteria.

Creating search criteria

You create the search criteria phrases to be accessed by and shared among several log file monitors from the Fathom library. These search criteria phrases, along with the severity level and alert detail you define, are the rule properties you use to create log file resource monitor rules and rule sets.

You can use the search criteria that you create and store at the library level in multiple log file monitors simultaneously. You can also share search criteria by exporting it from or importing it to other machines. For details about importing and exporting search criteria, see [Chapter 9, “Exporting and Importing in Fathom.”](#)

Within your work environment, it is likely important for you to know when a database is unexpectedly down. Perhaps the effectiveness of your company’s operations have suffered lately due to unplanned database down time. Obtaining information from the log file about these events could help you better research the issue.

To help you assess what might be happening, you can set up a literal search for the words *database down*. Once you enable the search against the log file, Fathom checks the file for an occurrence of the phrase, based on your polling cycle, and reports on its findings.

You must provide values for the **Search Type** and the **Search Text** fields on the **Create Search Criterion** page. The **Search Type** is a drop-down list. Depending on the type of expression you enter in the **Search Type** field, select either the literal search string or Perl 5 regular expression option. In the **Search Text** field, you enter the specific value for the type of expression you selected.

Another example of a literal text string you might search for in a log file is *abnormal shutdown*. A search based on this value yields a match only if the exact expression *abnormal shutdown* is found in the file. In contrast, a Perl 5 regular expression search supports a variety of notations that you can use for pattern matching, potentially yielding broader search results.

Note: The **Search Text** field does not impose any length limits on your entry. However, for practical reasons, you might want to limit the length. Also, keep in mind that the **Search Text** field is case sensitive.



To create a search criterion:

1. Select **Library** from the menu bar and click **Create Search Criteria**. The **Create Search Criterion Monitor** page appears:

2. In the **Criterion Properties** section, enter a value in the **Name** field. The search name can be a maximum of 32 characters, and it must not contain spaces between words, or use special characters such as an asterisk (*), an ampersand (&), or a period.
3. Enter a description in the **Description** field.
4. In the **Search Text** field, enter the search string you want the log file resource monitor to look for in the log file. The entry must be consistent with the type of search you are performing.
5. In the **Search Type** field, select either **Literal Search** or **Regular Expression**. See the [“Specifying search criteria”](#) section on page 7–25 for a detailed description of these search types.

6. Store this search criterion in a **Search Criteria** category by choosing either:
- **Use Existing Category** — From **Category**, scroll through the list of Fathom predefined categories and select one. The list includes these categories: AppServer Broker, AppServer Server, Database, Miscellaneous, NameServer, WebSpeed Broker, and WebSpeed Server.
 - **Use New Category** — In the **Category** field, use the predefined **misc** category, or enter the name of a new category.
7. Click **Save** to save this search criterion.
- The search criterion is now available from the list frame. You can display it from the category to which you assigned it.
8. Repeat these steps for each additional criterion you want to create.

Using Perl 5 expressions to create search criteria

Table 7–1 identifies some Perl 5 regular expressions you can use. Similarly, Table 7–2 suggests specific examples based on this notation.

Table 7–1: Perl 5 regular expressions (1 of 2)

Perl 5 expression	Description
.	Matches exactly one character, regardless of what the character is.
?	The preceding item is optional and matched at most once (error if no preceding item).
*	The preceding item will be matched zero or more times (error if no preceding item).
+	The preceding item will be matched one or more times (error if no preceding item).
^	Match at beginning of line.
\$	Match at end of line.
{n}	The preceding item is matched exactly <i>n</i> times (error if no preceding item).

Table 7–1: Perl 5 regular expressions*(2 of 2)*

Perl 5 expression	Description
<code>{n, }</code>	The preceding item is matched <i>n</i> or more times (error if no preceding item).
<code>{,m}</code>	The preceding item is optional and is matched at most <i>m</i> times (error if no preceding item).
<code>{n,m}</code>	The preceding item is matched at least <i>n</i> times, but not more than <i>m</i> times (error if no preceding item).
<code>[abc]</code>	Matches the characters <i>a</i> OR <i>b</i> OR <i>c</i> .
<code>[a-z]</code>	Matches any character from <i>a</i> to <i>z</i> .
<code>[^abc]</code>	Matches any character EXCEPT <i>a</i> , <i>b</i> , or <i>c</i> .
<code>\d</code>	Matches exactly one digit.
<code>\D</code>	Matches any character EXCEPT a digit.
<code>\w</code>	Matches exactly one letter, number, or the underscore character(<code>_</code>).
<code>\W</code>	Matches any one character EXCEPT a letter, number, or the underscore character.
<code>\s</code>	Matches exactly one character of white space (for example, spaces, tabs, newlines, or any character that would not use ink if printed on a printer).
<code>\S</code>	Matches any character that is NOT a white space.
<code>\</code>	Dereferences metacharacters (called “quoting”).
<code> </code>	Separates two or more choices such as either or behavior.

Table 7–2 provides some examples based on the Perl 5 regular expressions identified in Table 7–1.

Table 7–2: Examples using the Perl 5 regular expressions (1 of 2)

Example	Description
<code>^error</code>	Matches the exact word error only when it appears at the beginning of a line.
<code>\(9239\)</code>	Matches the exact entry (9239) only when it appears at the end of a line.
<code>da.*e</code>	Matches the exact words date , daze , database , and dat tape . This Perl 5 regular expression, <code>.*</code> , is similar to the wild card <code>*</code> on UNIX.
<code>abc abd abe</code>	Matches abc , abd , and abe .
<code>b.d</code>	Matches bad , bud , and bid , but not bald .
<code>da.....e</code>	Matches database and dat tape , but not date and daze .
<code>3.14</code>	Matches 3.14 , 3f14 , and 3814 .
<code>3\.14</code>	Matches 3.14 , but not 3f14 and 3814 .
<code>ab?c</code>	Matches ac and abc .
<code>ab*c</code>	Matches ac , abc , abbc , abbbc , and so forth.
<code>ab+c</code>	Matches abc , abbc , and so forth, but not ac .
<code>d\.*z</code>	Matches dz , d.z , d..z , d...z , and so forth.
<code>d\. *z</code>	Matches da*z , db*z , dc*z , and so forth.
<code>l\.\d\d</code>	Matches any three-digit floating point number from 1.00 to 1.99*****.
<code>a\Dc</code>	Matches abc , a&c , and aFc , but not a2c or a8c .
<code>a\wc</code>	Matches abc , aGc , and a_c , but not a%c .
<code>a\Wc</code>	Matches a%c , a?c , and a c , but not abc , aGc , or a_c .
<code>a\sc</code>	Matches any three-character string starting with a and ending with c whose second character is a space, tab, or newline.

Table 7–2: Examples using the Perl 5 regular expressions (2 of 2)

Example	Description
a\Sc	Matches any three-character string starting with a and ending with c whose second character is not a space, tab, or newline.
ab{3,5}c	Matches abbbc , abbbbc , abbbbcc , only.
.{3,5} pentane	Matches cyclopentane , neopentane , and isopentane , but not n-pentane .
a[bc]d	Matches abd and acd , only.
a[a-z]c	Matches any three-character string starting with a and ending with c , and whose second character is any letter from a to z , inclusive.

Selecting search criteria to define a local rule

Adding and defining a rule requires you to select search criteria and to associate severity and alert information with it.



To add a rule to a log file monitor:

1. On the **Edit Monitoring Plan** page, click **Add Rule**. The **Create Log File Rule Monitor** page appears:

2. From **Choose Criteria Category**, select the category in which the search criteria you want to use is defined.

3. From **Choose Search Criteria**, display all currently defined search criteria for the category previously selected and select a search criteria.

The search text automatically appears in the **Criterion Search Text** field, and a description automatically appears in the **Search Criterion Description** field.

4. From **Severity**, select the level of severity you want to set.
5. From **On Alert Perform Action**, select the action you want Fathom to perform when an alert is triggered.
6. Click **Save**. The **Monitoring Plan** page reappears and includes the new rule:

Default_Schedule Monitoring Plan for: log_file_ex

Edit Delete

Monitoring plan definition

Schedule: [Default_Schedule](#)
Polling Interval: 5 minutes
Alerts Enabled: true

Rules selected for this plan

Name	Status	Severity
BI_processing_stalled	Not Checked	
NS_LogFileMonitor_RuleSet	---	---
<i>Cannot_Return_Message</i>	Not Checked	
<i>Erroneous_UUID</i>	Not Checked	
<i>Exceptions_Causing_NS_Shutdown</i>	Not Checked	
<i>Invalid_Message_Code</i>	Not Checked	
<i>Listening_Error</i>	Not Checked	
<i>Message_Error</i>	Not Checked	
<i>Socket_IO_Exception</i>	Not Checked	
<i>Unhandled_Exception</i>	Not Checked	

Add Rule Select Rule Sets

7. As necessary, repeat [Step 1](#) through [Step 6](#) to add more individual rules.

Note the following points concerning individual rules that you add to a log file monitor resource:

- Individual rules display in alphabetical order and appear in the list before rule sets.
- Each rule appears with an associated resource status indicator.
- You can click any rule to display summarized details about it.
- You must explicitly create an individual rule to add it to the rule set; an individual rule is not directly available for use in any rule set.

8. Choose one:

- If you want to add rule sets, see the “[Associating rule sets with log file monitors](#)” section on page 7–20 for details.
- If you are done adding rules, click **Done**. The **Log File Monitor** summary page appears, displaying any rules and rule sets selected for a log file monitor.

Enabling the log file monitor

A log file monitor cannot begin polling until you do one of the following tasks:

- Click **Done** on the **Log File Monitor** summary page.
- Edit the log file properties, select the **Enabled** option, and click **Save**.

Polling will begin based on the polling criteria you have set, and polling data will begin to display in the upper right-hand corner of the **Log File Resource** page.

Editing, copying, or deleting a log file monitor

All log file monitors have a summary page. The **Log File Monitor** summary page displays all the values entered to define the bookmark feature, the monitoring plans, and the rules and rule sets for this log file monitor. From the summary page you can:

- Click **Edit**, **Copy**, or **Delete** at the top of this page to access the basic properties to update, copy the values for the entire log file monitor to create a new one, or delete the log file resource monitor.
- Click **Default Schedule Plan** (or any plan you have established) to display the monitoring plans and rules for this log file resource monitor for review.
- Click **Edit** in the monitoring plans section to display the monitoring plans and rules so you can edit them.
- Select **Add Plan** in the monitoring plans section to create additional, unique monitoring plans and rules for this log file resource monitor. Once you create a new plan, the details of the new plan are appended to those plans that already exist.

Note: Fathom provides a database log file monitor designed to be used specifically with OpenEdge databases. Its functionality is similar to that of the log file monitor. For detailed information about the database log file monitor and the procedure to use it, see the appropriate section in the *Database Management Guide*.

Creating a file resource monitor

You can set up Fathom to monitor a file resource in the following ways:

- **File size** — Examine the file size and trigger an alert if the file size is less than, greater than, equal to, or not equal to a size you specify. You can specify the size in bytes, kilobytes, megabytes, gigabytes, or terabytes.
- **File existence** — Check to see if the file exists or not. You can choose the condition under which an alert will be generated — for example, if the file does not exist after two polls. You also choose the specific action you want performed in response to the alert.
- **File age** — Examine the file date and determine if the file is older than the number of seconds, minutes, hours, or days you specify.
- **File growth rate** — Examine the file size and generate an alert based on a size change for a particular period of time; for example, you might specify that Fathom generate an alert if the file growth exceeds 100 megabytes per day.
- **File modification** — Examine the file data and determine if the file has been modified. You can specify that Fathom generate an alert if there is evidence that the file has been modified, either because the timestamp has changed or the timestamp and size of the file have both changed.

Before you can set up a file resource monitor, you must ensure that Fathom Management can see your mapped network drives.

Trending performance data for file monitor resources

From the monitoring plan, you can trend performance data for file monitors.

Once you enable trending by selecting the **Trend Performance Data** field, you can also override the default value of 1 in the **Trend Performance Data** every poll(s) field. Any value that you enter in this field that is greater than the default value 1 causes a file system resource to trend data that is taken from the last poll. No calculations are performed on this data.

Creating a file monitor

To monitor a file, you must create a monitoring plan definition, select rules for the plan, and set the rules' properties.



To define a file monitor:

1. From the console list frame, click **File→File**.
2. From the detail frame, click the **New instance** icon. The **Create File Monitor** page appears:

Create File Monitor:

Save Cancel

Properties

Name:

Description:

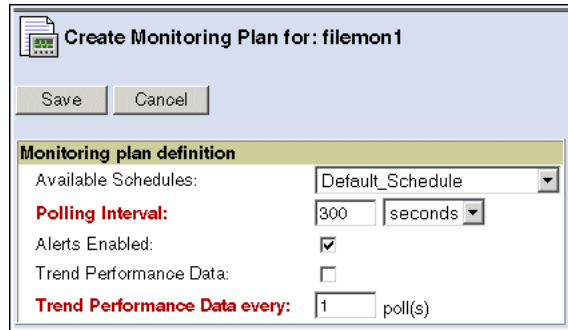
File Name:

Enabled: ☒

3. Provide the following information:
 - **Name** — Enter the name of the file monitor.
 - **Description** — Provide an optional description of the monitor.
 - **File Name** — Provide the name of the file you want to monitor.

The **Enabled** option is selected by default. To disable the monitor, clear the option.

4. Click **Save**. The **Create Monitoring Plan** for the file monitor appears:



The dialog box titled "Create Monitoring Plan for: filemon1" has a "Save" button and a "Cancel" button. Below the buttons is a section titled "Monitoring plan definition" with the following fields:

- Available Schedules: Default_Schedule (dropdown)
- Polling Interval: 300 (text box) seconds (dropdown)
- Alerts Enabled: ☒
- Trend Performance Data: ☐
- Trend Performance Data every: 1 (text box) poll(s)

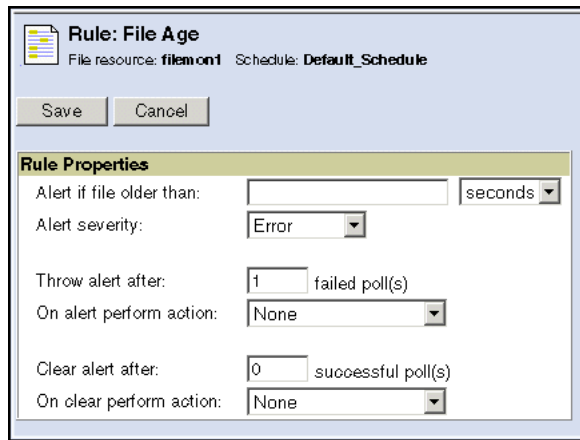
5. Choose the monitoring plan specifics. When you finish, click **Save** on this page; the file monitor's monitoring plan definition and a list of rules selected for this plan appear.
6. To add one or more rules to the plan, click **Add Rule**. The **Available File Monitor Rules** page appears:



The dialog box titled "Available File Monitor Rules" has a "Done Adding Rules" button. Below the button is a section titled "Select rule to add" with a list of rules:

- [File Age](#)
- [File Exists](#)
- [File Growth Rate](#)
- [File Modified](#)
- [File Size](#)

- Click the first rule you want to add. The rule properties page appears, as in the following example for the **File Age** rule:



The screenshot shows a dialog box titled "Rule: File Age". Below the title, it says "File resource: filemon1" and "Schedule: Default_Schedule". There are "Save" and "Cancel" buttons. Below these is a section titled "Rule Properties" with the following fields:

- "Alert if file older than:" with a text input field and a "seconds" dropdown menu.
- "Alert severity:" with a dropdown menu showing "Error".
- "Throw alert after:" with a text input field containing "1" and the text "failed poll(s)".
- "On alert perform action:" with a dropdown menu showing "None".
- "Clear alert after:" with a text input field containing "0" and the text "successful poll(s)".
- "On clear perform action:" with a dropdown menu showing "None".

- Provide values for the following rule properties (which might differ depending on the rule you are adding):
 - Alert if file older than OR Alert severity**
 - Throw alert after**
 - On alert perform action**
 - Clear alert after**
 - On clear perform action**
- Click **Save**.
- Repeat [Step 7](#), [Step 8](#), and [Step 9](#) for each rule you want to add.
- When you finish adding rules, click **Done Adding Rules**. The file monitor's monitoring definition and rules appear.

You can now edit or delete the plan.

Creating Jobs and Job Templates

As you work with Fathom, you will find that you want to perform certain monitoring-related tasks on a regular basis. To help you accomplish this, Fathom enables you to create custom jobs that you run only once or on a recurring basis, as well as job templates that you can reuse when you want to perform the same job over again but possibly on a different set of data.

Fathom also provides several predefined database-maintenance job templates that you can use to keep your OpenEdge database performing efficiently. For details about these maintenance templates, see the *Database Management Guide*.

This chapter describes how to work with jobs and job templates. Specifically, the chapter contains the following sections:

- [Jobs overview](#)
- [Creating a job instance](#)
- [Editing a job](#)
- [Copying a job](#)
- [Deleting a job](#)
- [Running a job immediately](#)
- [Scheduling a job](#)
- [Viewing scheduled jobs](#)

- [Viewing running jobs](#)
- [Viewing job history](#)
- [Viewing database maintenance job instances associated with an individual database](#)
- [Working with job templates](#)
- [Viewing debug details about jobs](#)

Jobs overview

Fathom provides several different ways for you to work with jobs:

- You can create a custom job to run once or on a recurring basis.
- You can create a job template and run job instances based on the template's properties.
- You can use one of the predefined database maintenance job templates.

Creating a custom job

A *custom job*, also known as a *job instance*, is an individual job that Fathom executes once or at a regularly scheduled interval. A custom job is generally a batch (noninteractive) task that runs as a background process.

Examples of custom jobs include:

- Hourly database after-image roll over.
- Weekly disk defragmentation.
- Monthly database index rebuild.
- Monthly scan disk.

Once you create a job instance, you can schedule it to execute at a regular interval, such as hourly, daily, and weekly, and also at a specific time, such as at startup. Job schedules differ from resource monitor schedules in that job schedules define a frequency of occurrence (every fifteen minutes, for example) while monitor schedules define a block of time (9:00 AM – 5:00 PM, for example). You can create schedules through either the repeat interval or a cron expression.

You can view a list of scheduled jobs as well as check on the status of currently running jobs. Once jobs have completed, you can also query job history data.

See the [“Creating a job instance”](#) section on page 8–5 and the [“Scheduling a job”](#) section on page 8–21 for details about creating and scheduling a custom job.

Creating a job template

Fathom allows you to create and maintain job templates. The advantage of using a job template is that you can use it more than once, saving time in recreating the job's specifics and also making sure that any job based on the job template runs with the same specifications each time.

You do not run the job template itself; instead, you create a unique job instance from the common values in a job template and then run the job instance.

See the [“Creating a job template”](#) section on page 8–36 for details about creating a job template.

Using a predefined database maintenance job template

Fathom supplies predefined database maintenance job templates to help get you started right away in performing some routine database maintenance activities. Fathom supplies the following predefined templates:

- Database Analysis
- Database Restore
- Grow BI
- Index Compaction
- Offline Backup
- Online Backup
- Truncate BI
- Backup Configuration

Fathom also provides a Data Compaction job template that you can use to obtain details about the FathomTrendDatabase. For details, see the [FathomTrendDatabase Guide and Reference](#).

The information in this guide focuses primarily on creating custom jobs and job templates. For definitions and detailed information about using the predefined database maintenance templates, see the [Database Management Guide](#).

Creating a job instance

When you want to create and run a Fathom job, you have several options. You can create a job that runs once or on a recurring basis. You can also create a template for a job and then run separate job instances based on the specifics you provide only once in the template.

When you want to create a job for one-time or recurring use, or if you want to create a job based on an existing template, you create a job instance.



To create a job instance:

1. Click **Jobs** from the menu bar. The **Fathom Jobs** page appears.
2. Choose one of the following options, depending on how you want to create the job:
 - To create a unique job not based on any template, click **Create Job**. The **Job** page appears.
 - To create a job from an existing job template, click **Create Job from a Template**. The **Create Custom Job** page appears. Choose one of the existing templates. The **Job** page for that template appears.
3. Complete the following fields:
 - **Name** — Define the job's name. You use the job name when you want to edit the job's properties or check on the job's status. Names cannot contain spaces or special characters.
 - **Description** — Provide a sentence or phrase that describes the job's purpose. (Optional, but recommended.)

- **Resources** — Identify database resources to associate with a job or job action. When you create a job instance, you can associate with it zero or more databases.

If you are creating a unique job, highlight the database you want to add from the list of available database resources, and click **Add**. The selected database displays in the **Selected** list. To remove a database that you do not want selected, highlight the database name in the **Selected** list and click **Remove**.

If you are creating a job from a template and want to include a database, select the database from the list of **Available Resources**.

Note: If you are using one of the predefined database maintenance job templates, you can choose only one database. If you are using a job template that you have defined, you can choose multiple databases.

- **User name** — Provide the operating system user account. It is not necessarily the same as your Fathom user account name. If specified, the name must be a valid account on the server machine (or server domain) where the AdminServer and Fathom are running. On Windows 2000 and Windows NT platforms, the name can also include a domain.
- **Group** — On supported UNIX platforms, identify the name of the group. A *group* is a collection of users who share the same privileges.
- **Password** — Provide your password. If the value you entered in the **User name** field does not have an associated password, you must leave this field blank; otherwise, an error message is generated.
- **Command** — Identify the command you want the job to perform.

If you are creating a job instance from a template, it is possible that the command will be predefined for you. If you are creating a unique job, you can define any command that would typically execute from an OS shell, and you can include a full or relative place-name. You can also use environment variables such as %DLC% or \$DLC.

- **Command parameters** — Define the input parameter to the command. The list of parameters take the same format as from an OS shell. Additionally, you can use environment variables (\$SHELL or %WINDIR%, for example) and Windows registry values (@SOFTWARE\PSC\FATHOM\3.0A\10.0B\FATHOMINIT, for example).

- **Working directory** — Identify the command’s current working directory. If you specify a directory, the directory must exist. This property defaults to the working directory defined at installation.
- **Input file** — Identify the file used for read redirection with a job’s command. This is typically used for any keyboard input the command might require.
- **Output file (stdout)** — Identify the file to which any output written to stdout is routed. Fathom creates a default stdout filename based on the name of the job instance. However, you can change it. If you select the **Append** option, any new information will be added to the existing stdout file.
- **Output file (stderr)** — Identify the file to which any output written to stderr is routed. Fathom creates a default stderr filename based on the name of the job instance. However, you can change it. If you select the **Append** option, any new information will be added to the existing stderr file.

Note: When you create or edit a job, Fathom will prefill the stdout and stderr filenames for you if any of these fields are left blank. The filenames will be the same as the job name, with a different suffix. You can change the filename or remove it if you do not want to create the output files. Also, if you edit the job name, Fathom will not change the filenames to reflect the new job name. You should review these filenames *before* saving the page to ensure the job creates the expected output files.

- **Environment: name=value pairs** — Define application-specific variables to be set in the process context of the task that runs to execute the specified job.

If you are creating a job instance from a template, a **name=value pair** will be predefined for you.

- **Debug log file** — Select this option to obtain diagnostic details that can help debug a job.

For example, if you set this option and use the **Run Now** feature to run the job, a debug log file will be generated in the default working directory. The debug log file will be named based on the job name with a .log extension.

Once you have submitted the job, Fathom makes debug trace file data available. See the “[Viewing job history](#)” section on page 8–31 for details.

- **Indicate if the job can be used as an action** — Select this option if you want the job to be available as a job action. As with other Fathom actions, such as an e-mail or log file action, you can set up job actions to automatically trigger in response to alerts.

You can execute a job in response to these events:

- An alert trigger.
- An alert that has been cleared.
- A schedule that is set up so that the job action occurs on a predetermined basis.

- **Completion Actions and Alerts** — If you intend to set up actions and alerts for this job, click **Edit**. For more information about this page, see [Step 4](#) in this procedure.

4. After you specify the job instance's properties (or accept the predefined properties, if you are using a template), you can do either of the following:

- Define action and alert occurrences for the job as described in the [“Setting up job completion actions and alerts”](#) section on page 8–8.
- Save the job. You can then run the job immediately, as described in the [“Running a job immediately”](#) section on page 8–21, or hold off until another time.

Setting up job completion actions and alerts

You can optionally monitor and manage information about jobs that have executed. In so doing, you can:

- Associate job status details with actions to automatically notify appropriate personnel about the status of the job's execution.
- Set up alerts to trigger if a job execution exceeds the time frame in which the job was scheduled to run.
- Initiate a series of job activities based on exit code values. This activity, known as *job chaining*, allows you to plan job actions to occur for more than one exit code condition. See the [“Job chaining”](#) section on page 8–11 for more information.

Job completion actions

You can associate exit codes with existing actions to define which actions occur based on the status of a job's execution. Once a job execution completes, an *exit code* is generated. The exit code indicates whether or not the process succeeded. Based on the exit code and the action you associate with the code, Fathom can ensure that the specified action occurs.

Typically, an exit code of zero indicates success, while a nonzero code indicates an error. For more information on nonzero exit codes, search the log file. If a job running on Windows returns a positive, nonzero code, use the `net helpmsg` command for information.

For example, consider a job that returns an exit code of 1326. Entering **net helpmsg 1326** at the command line returns the following message:

Logon failure: unknown user name or bad password

You can also use exit codes to chain jobs together using flow control. See the [“Job chaining”](#) section on page 8–11 for more information.

Job completion alerts

A job alert definition instructs Fathom to trigger a warning alert if the job execution time frame exceeds the time frame during which the process is scheduled to run. You can also associate an action with the alert.



To specify job completion actions and alerts:

1. Click the **Edit** button at the bottom of the **Job** page:

Debug log file? ☐

Indicate if the job can be used as an action

Action: ☐

Completion Actions and Alerts:

The **Job Completion Action and Alerts** page opens:

Job Completion Actions and Alerts: Weekendingrun

Save Cancel

Action Definition

Exit Code	Action	Operation
<input type="text"/>	None	
default	None	None

Add/Update
Delete

Alert Definition

Alert if execution time exceeds: Hours

On alert perform action: None

2. Enter an exit code number in the **Exit Code** field. The number must be between 0 and 255; you can also type the word **default**. From the **Action** drop-down list, select a predefined action to associate with the exit code. Click **Add/Update**. The exit code and action pair created display in parallel columns under their respective fields.
3. Repeat [Step 2](#) in this section to define additional exit code and action pairs. For example, you might have several exit code and action pairs:

Action Definition

Exit Code	Action	Operation
<input type="text"/>	None	
default	None	
3	Default_Mail_Action	
0	None	
2	Default_Clear_Action	

Add/Update
Delete

4. In the **Alert if execution time exceeds** field, enter the threshold of time after which you want a warning alert to trigger. You can specify the time in minutes or hours, and you must use whole numbers.

For example, if you want to be notified at the 30-minute mark that the job execution has not occurred, enter the value **30** in the first field and click **Minutes** from the drop-down list.

5. From the **On alert perform action** drop-down list, select an action from the list of available, predefined actions that you want to associate with this alert.
6. Click **Save** to submit your selections. The **Job** summary page appears.

Updating job completion actions and alerts

You can update or delete exit code and action pairs.



To update exit code and action pairs:

1. Enter the exit code you want to update in the **Exit Code** field. From the **Action** drop-down list, select a different action to associate with the exit code. Click **Add/Update**. The exit code and its new action are display in parallel columns under their respective fields.
2. Repeat [Step 1](#) in this section to update additional exit code and action pairs.
3. Once you have completed all tasks on this page, click **Save** to make the updated pairs available for use the next time the job is executed. The **Job** summary page appears.



To delete exit code and action pairs:

1. Enter the exit code you want to delete in the **Exit Code** field. Click **Delete**. The exit code and its action will be deleted from their respective columns.
2. Repeat [Step 1](#) in this section to delete additional exit code and action pairs.
3. Once you have completed all tasks on this page, click **Save**. The **Job** summary page appears.

Job chaining

When you link individual job instances together in a sequence based on the presence of a specific exit code, you are performing job chaining. Using the value of an exit code that occurs in response to a job having been run, you can determine the processes, or control the flow of processes, that occur once one job ends and the next one begins.

Figure 8–1 shows a simple job chaining scenario involving four job instances: Job Instance A, Job Instance B, Job Instance C, and Job Instance D. Each job instance has an exit code of 0 already defined. The job chaining in this scenario occurs only if the exit code of 0 is recognized at the end of job instances A, B, and C. If any of these jobs concludes with an exit code other than 0, the job chain ends at that point in the process.

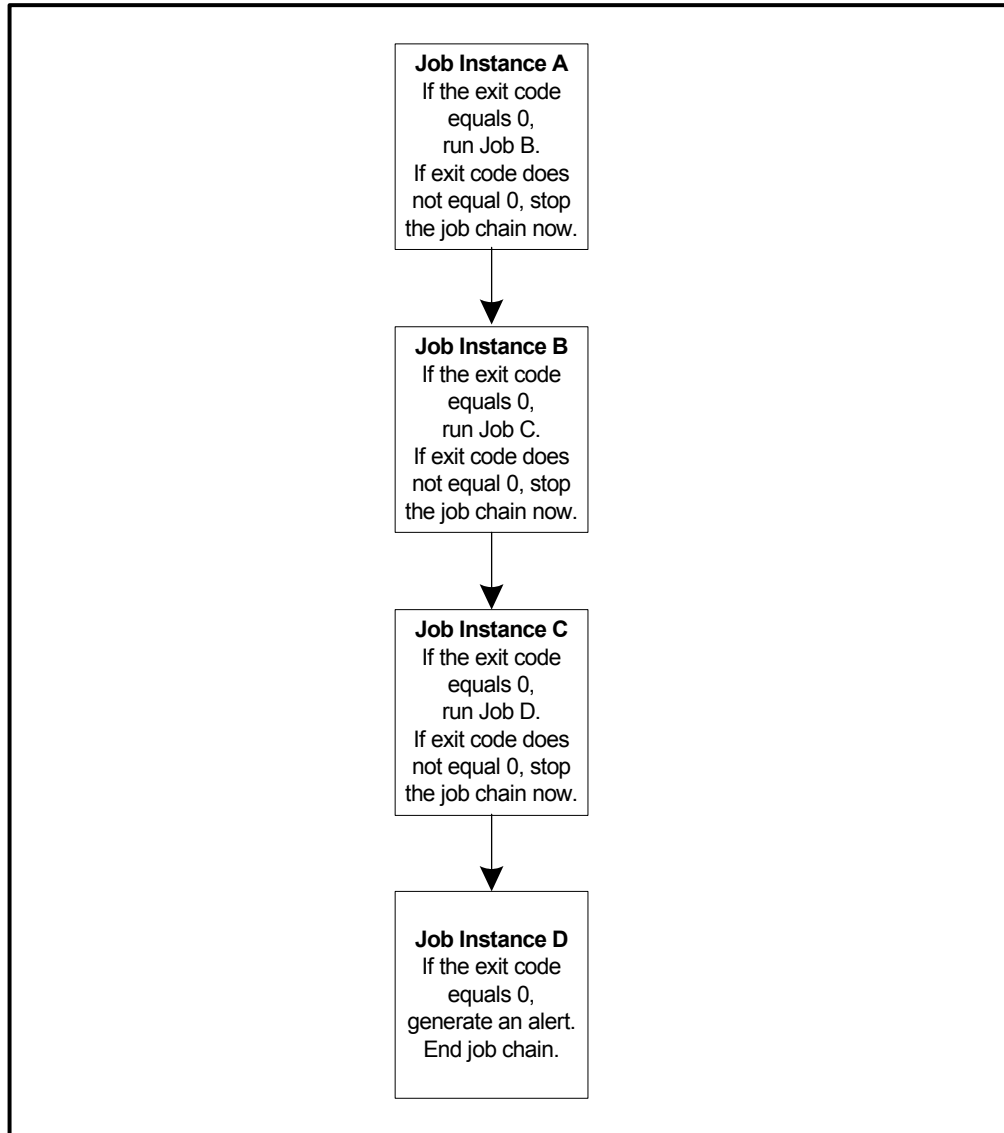


Figure 8–1: Sample job chaining scenario

If you want to account for more than one exit code condition, you can use a more sophisticated implementation of job chaining known as *job chaining with flow control*. You can set up one job chain to implement different job chains, depending on the exit code generated by a given job in the chain.

Figure 8–2 illustrates a sample job chaining with flow control scenario. One of two possible flows is determined based on the value of the exit codes.

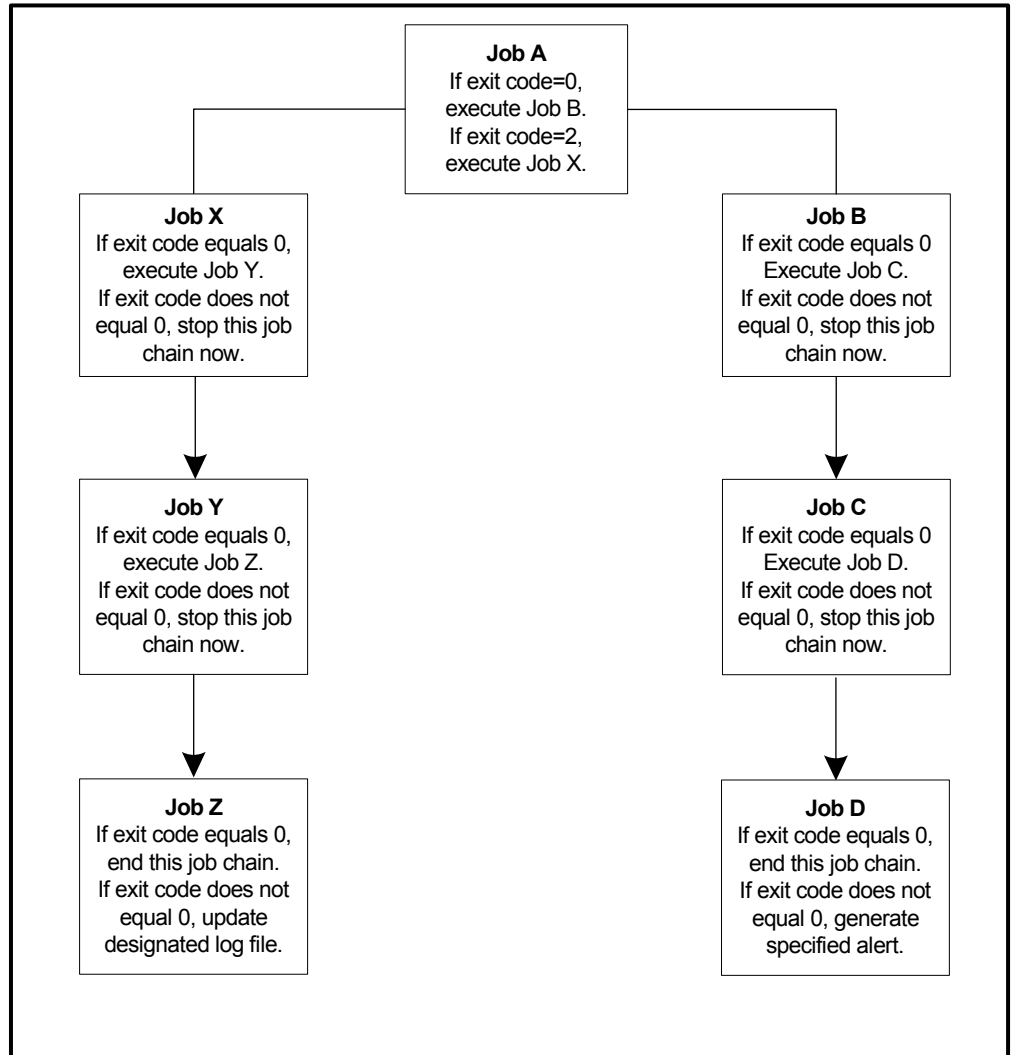


Figure 8–2: Sample job chaining with flow control scenario

A word about recursion

You cannot create a job exit action that is self-referencing. Fathom prevents you from creating this type of situation in a job chain. However, Fathom will not detect the situation in which you create a self-reference further down a job chain.

It is possible for recursion to occur in any other instance in a job chain when the job called is any other number of steps removed from the original job in the chain. For example, Fathom will not be able to detect a self-referencing job in a situation in which Job A references Job B and concludes with a reference back to Job A.

Recursion is not a potential issue in the example described in [Figure 8–1](#). Each of the job instances in the job chain is uniquely defined. Similarly, recursion is not an issue in [Figure 8–2](#) because only one of the two possible chains in the job flow will be followed.

Using environment variables

Environment variables define the context in which a job or job action runs. Fathom sets up an environment variable context to associate jobs with resources and alerts and provides a set of predefined environment variables that are common to all jobs you can run.

There are additional, specific environment variables that will vary from one job to another, depending on the job to be executed. For example, jobs run in response to an alert have an alert context. Jobs for which associated database resources have been defined have a resource context. Fathom provides a unique context definition for a job run against the FathomTrendDatabase.

[Table 8–1](#) identifies environment variables that are common to all jobs.

Table 8–1: Environment variables common to all jobs (1 of 2)

Environment variable	Description
FM_HTTPPORT	Fathom’s Web server port.
ADMSRVSPORT	The AdminServer’s listening port.
JOBNAME	The name of the job as defined in Fathom.
FATHOMINSTALLDIR	Fathom’s installation directory as defined in <code>fathom.init.params</code> .

Table 8–1: Environment variables common to all jobs*(2 of 2)*

Environment variable	Description
FM_CONTAINERNAME	The resources's container name and the resource name (for example, Dev01.sports2004).
FATHOMCONFIGDIF	Fathom's directory for configuration data as defined in <code>fathom.init.params</code> .
FATHOMLOGSDIR	Fathom's log directory as defined in <code>fathom.init.params</code> .
FATHOMWORKDIR	Fathom's work directory as defined in <code>fathom.init.params</code> .
FATHOMREPORTDIR	Fathom's directory for report data as defined in <code>fathom.init.params</code> .
PROGRESSINSTALLDIR	Directory of Progress' version that Fathom is associated with as defined in <code>fathom.init.params</code> .
PERL5BIN	Perl v5 interpreter bin directory as defined in <code>fathom.init.params</code> .
PERL5LIB	Perl v5 library directory as defined in <code>fathom.init.params</code> .

Table 8–2 identifies environment variables for jobs associated with database resources. If a job is associated with more than one database, the value of each of the variables will be identified in a comma-separated list. For example, if there are three databases associated with a job, and the databases are named db1, db2, and db3, the database names will be defined as follows:

RESRC_DBNAME=db1, db2, db3

Table 8–2: Environment variables for jobs with associated database resources

Environment variable	Description
RESRC_NAME	The name of the associated resource. This will be a database name because only databases can be associated with a job.
RESRC_DBNAME	The name of the database as defined in the Progress Explorer.
RESRC_DBPATH	The full pathname of the database. For example, /usr1/myapp/sports.db.
RESRC_DBCONFIG	The database configuration name as defined in the Progress Explorer.
RESRC_DBDISPLAY	The database display name as defined in the Progress Explorer.
RESRC_DBPORT	The TCP port number of the database broker.
RESRC_DBHOST	The TCP host name of the database DataServer.
RESRC_DBADMSRVRPORT	The AdminServer TCP port number on the database server host.

Figure 8–3 shows the **Job Action** field that appears on the bottom of the **Job** page. Select this option to enable these environment variables to be available to the job’s alert context.

Indicate if the job can be used as an action

Action: ☐

Figure 8–3: Using a job as an action

Table 8–3 identifies the environment variables that can also be run in response to an alert. These environment variables are available when you identify a job as a job action.

Table 8–3: Alert environment variables for job actions

Environment variable	Description
ALERT_ID	The ID of the generated alert.
ALERT_NAME	The name of the alert (for example, “FathomTrendingUnavailable, NetworkResourceFailure”).
ALERT_SEVERITY	The alert severity: Severe, Error, Warning, or Informational.
ALERT_MESSAGE	A text description of the alert.
ALERT_COUNT	The number of times the alert has been thrown.
ALERT_RESOURCE	The name of the resource that threw the alert.
ALERT_DBNAME	If the resource was a database, this variable will be set to the full name of the database.
ALERT_DBPATH	If the offending resource was a database, this variable will be set to the full name of the database.
ALERT_DBCONFIG	If the offending resource was a database, this variable will be set to the database configuration as defined in the Progress Explorer.
ALERT_DBDISPLAY	If the offending resource was a database, this variable will be set to the database display name as defined in the Progress Explorer.
ALERT_DBPORT	If the offending resource was a database, this variable will be set to the database TCP port number.
ALERT_DBHOST	If the offending resource was a database, this variable will be set to the database TCP host name.
ALERT_DBADMSRVREPORT	If the offending resource was a database, this variable will be set to the AdminServer TCP port number on the database server host.

Table 8–4 describes the environment variables that you can identify for jobs with database resource associations.

Table 8–4: Environment variables for jobs associated with the FathomTrendDatabase

Variable	Description
FM_DBNAME	The full name of the database. In this situation, it is FathomTrendDatabase.
FM_DBPATH	The absolute pathname of the FathomTrendDatabase.
FM_DBCONFIG	This variable will be set to the FathomTrendDatabase configuration as it is defined in the Progress Explorer.
FM_DBDISPLAY	This variable will be set to the FathomTrendDatabase display name as it is defined in the Progress Explorer.
FM_DBPORT	This variable will be set to the FathomTrendDatabase TCP port number.

Editing a job

You can edit a created job. If you edit the job name, be sure to change the output filenames (stdout and stderr), and any other fields that retained the name of the original job. Review these file names *before* saving the edits to ensure that the job creates the expected output files.



To edit a created job:

1. Click **Jobs** in the console menu bar.
2. Under **Defined Jobs** in the list frame, click the job you want to edit. The job instance opens in the detail frame:

GrowBI Job: GrowBIMay1104
GrowBI AJS 5/11/04

Edit Copy Delete Run Now Schedule

Job history
[View Job History](#)
View the status of jobs that have finished running

Properties

Resource:	nbaspauldixp.Backorders
User name:	
Command:	\$(PERL5BIN)/perl
Command parameters:	\$(fathomInstallDir)/perl/scripts/growBI.pl
Working directory:	C:\Fathomwork
Input file (stdin):	None
Output file (stdout):	C:\Fathomwork\GrowBIMay1104.out
Output file (stderr):	C:\Fathomwork\GrowBIMay1104.err
Debug log file:	None
Next scheduled run:	Disabled

3. Click **Edit**.
4. Make the changes you want, and click **Save**. The summary of the job reappears, reflecting the changes you made.

Copying a job

You can copy a created job and use it as the basis for another job. When you make a copy of an existing job, you must change the name of the newly created job. Also, you should change the updated `stdout` and `stderr` filenames, and any other fields that retained the value of the original job from which you created this copy. Review these file names *before* saving the page to ensure that the job creates the expected output files.



To copy a job:

1. Click **Jobs** on the console menu bar.
2. Under **Defined Jobs** in the list frame, click the job you want to copy. The job opens in the detail frame.
3. Click **Copy**.
4. Rename the job, and click **Save**. The summary of the job reappears.

Deleting a job

You can delete a job you no longer need.



To delete a job:

1. Click **Jobs** on the console menu bar.
2. Under **Defined Jobs** in the list frame, click the job you want to delete. The job opens in the detail frame.
3. Click **Delete**. You are asked if you want to delete the job.
4. Click **OK**. A message appears confirming the deletion.

Running a job immediately

You can run a created job immediately or schedule it to run in the future.



To run a created job immediately:

1. Click **Jobs** on the console menu bar.
2. Under **Defined Jobs** in the list frame, click the job you want to run. The job opens in the detail frame.
3. Click **Run Now**. A message appears showing that the request has been submitted.

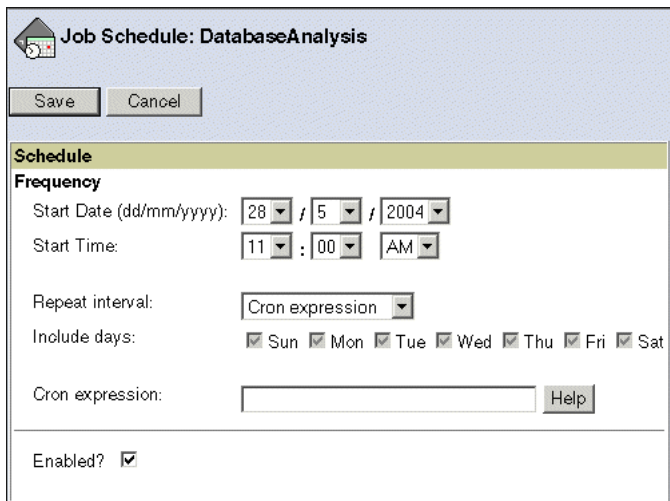
Scheduling a job

When you create a job instance, you also determine how often it will run. Jobs adhere to a number of execution policies: Short Duration, Long Duration, and Single Time. Full understanding of these policies allows you to schedule jobs more effectively.

Using cron-based scheduling

You can now set up more complex scheduling by incorporating cron expressions in your job schedules. You can still specify that a job execute at a repeating calendar interval, such as every sixty minutes or once each day, for example. With cron-based scheduling, you can be even more specific about when you want a job to run, according to a business period interval: on the last Friday of the month, or every ten minutes from 4 PM to 6 PM daily, for example.

If you choose to use a cron expression in scheduling a job, you select it as the **Repeat interval**, as shown in [Figure 8-4](#).



The screenshot shows a dialog box titled "Job Schedule: DatabaseAnalysis". It has "Save" and "Cancel" buttons at the top. Below them is a "Schedule" section with a "Frequency" label. The "Start Date (dd/mm/yyyy)" is set to 28/5/2004. The "Start Time" is 11:00 AM. The "Repeat interval" is set to "Cron expression". The "Include days" section has checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. The "Cron expression" field is empty, and there is a "Help" button next to it. At the bottom, the "Enabled?" checkbox is checked.

Figure 8-4: Selecting Cron expression as the Repeat interval

You can include from one to five cron expressions (separated by semi-colons) in the **Cron expression** field in a job schedule. Each cron expression consists of five fields; each field describes a different part of the scheduling definition:

- Minutes.
- Hours.
- Day of the month.
- Month.
- Day of the week.

For example, you might use a cron expression as shown in [Figure 8–5](#).

Job Schedule: DatabaseAnalysis

Save Cancel

Schedule

Frequency

Start Date (dd/mm/yyyy): 28 / 5 / 2004

Start Time: 11 : 00 AM

Repeat interval: Cron expression

Include days: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Cron expression: 15 8 ? * MON-FRI Help

Enabled? ☒

Figure 8–5: Sample cron expression

In this example, you specify that a job should be run at 8:15 AM every weekday of every month.

If you also want the job to run once every Saturday and Sunday, but at a different time from when it runs each weekday, you can use two cron expressions, as shown in [Figure 8–6](#).

Job Schedule: DatabaseAnalysis

Save Cancel

Schedule

Frequency

Start Date (dd/mm/yyyy): 28 / 5 / 2004

Start Time: 11 : 00 AM

Repeat interval: Cron expression

Include days: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Cron expression: 15 8 ? * MON-FRI; 30 19 ? * SAT,SU Help

Enabled? ☒

Figure 8–6: Sample of two cron expressions

In this case, the job will still run at 8:15 AM each weekday of every month; the job will also run at 7:30 PM every Saturday and Sunday of every month.

For more details about using cron expressions, click the **Cron expression** field **Help** button.

Scheduling a job instance or a job template

You schedule a job according to whether you are scheduling a job instance or a job template, as follows:

- To associate a schedule with a job instance, complete all steps in the following procedure.
- To associate a schedule with a job template, complete only [Step 1](#) through [Step 7](#) in the following procedure.



To schedule a job:

1. Click **Jobs** on the console menu bar.
2. In the list frame under **Defined Jobs**, click the job you want to schedule.
3. Click **Schedule**. The **Job Schedule** page appears.

For example, the schedule might look as follows:

Job Schedule: GrowBIMay1104
GrowBI AJS 5/11/04

Save Cancel

Schedule

Frequency

Start Date (dd/mm/yyyy): 11 / 5 / 2004

Start Time: 4 : 30 PM

Repeat interval: Every 60 minutes

Include days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Cron expression: Help

Enabled? ☒

4. Indicate the date on which you want your job to start, using the drop-down list. Note that the **Start Date** is entered in a dd/mm/yyyy format.
5. Indicate the time you want your job to start, using the drop-down list.
6. Choose the job's repeat interval from the drop-down list. The repeat interval options are:
 - **One time** — The job runs once on the specified start date and time.
 - **At startup** — The job runs once when the AdminServer and Fathom start. After running, the job is disabled until the next time the AdminServer restarts.
 - **Weekly from date** — The job runs once a week, beginning on the specified date.
 - **Monthly from date** — The job runs once a month, beginning on the specified date.
 - **Every 5, 15, 30, 60 Minutes** — The job runs every *n* minutes, beginning at the specified start date and time on the days chosen in the **Include days** list.

Keep in mind that these increments of 5, 15, 30, and 60 offer a relatively short run time for a job. Since the length of time it takes a job to run can vary, a set time in your schedule might be missed.

Daily — The job runs once a day, beginning on the specified date.

Cron expression — The job runs as indicated by the cron expression. (See [Step 8.](#))

7. Determine which days to select from the **Include days** list. The choices in the **Include days** list are valid and enabled only for repeat intervals of every 5, 15, 30, and 60 minutes and Daily. For all other repeat intervals, all days are active.
8. If you want, enter a cron expression in the **Cron expression** field. For help specific to cron expressions, click **Help**.
9. Select the **Enabled** option to enable the job's schedule.
10. Click **Save**.

If you were to enable the schedule for the job shown here, the job would run:

- Starting on 5/11/04 at 4:30 PM.
- Every 60 minutes from Monday through Friday.

Duration Execution Policy

When you define a job to run at intervals of Daily, Weekly, or Monthly, the Duration Execution Policy determines the time between runs. With the Duration Execution Policy, the Start Time is used to set the next run Date and Time. The Duration Execution Policy allows the time between runs to vary.

Example: Daily interval

Job execution begins at its scheduled time, 3:00 AM.

Job execution ends at 8:00 AM.

The next scheduled job execution begins at 3:00 AM on the next day on which this job is scheduled to run.

Single Execution Policy

When you define a job to run **At Startup** or **One Time**, the Single Execution Policy determines the time between runs. If a job runs at startup, it executes when the AdminServer starts (through the `proadsv -start` command on UNIX or NT Services on Windows 2000 and Windows NT). With the Single Execution Policy, the job does not run again until the next time the AdminServer starts. If the job is defined as **One Time**, the Single Execution Policy ensures that the job, after completion, is permanently disabled. **One Time** jobs are reenabled only if you define new start times and **Repeat Intervals** for them on the **Schedule** page.

At startup

Job execution begins with the starting of the AdminServer at 7:30 AM.

Job execution ends at 7:45 AM.

The job does not begin again until the AdminServer is restarted.

One time

Job execution begins at its scheduled time, 6:15 PM.

Job execution ends at 6:53 PM.

The job is disabled. It will not run again unless its starting date and time are redefined on the **Schedule** page.

Job Execution Policy over time

Under typical conditions a job's **Start Date** and **Time** will reflect a point in the past. If the AdminServer and Fathom are shut down and restarted, Fathom determines the next execution date of any enabled jobs from the original **Start Date** and the time the AdminServer restarted (which would be the present time). Fathom then uses the **Repeat Interval** and the original **Start Time** to calculate the job's next occurrence.

Job execution with a restarted AdminServer

Original Job's Start Date and Start Time: July 21, 2004, at 10:00 AM.

Original Job's Repeat Interval: Every 60 Minutes as determined from the original Start Time indicated as 10:00 AM.

Date of AdminServer shutdown and restart: July 28, 2004.

Time of AdminServer restart: 8:25 PM.

The next scheduled execution of this job begins at 9:00 PM on July 28, 2004.

If the job in the above example had a Repeat Interval of Every 15 Minutes, it would next execute at 8:30 PM on July 28, 2004.

Monthly By Date Execution Policy

Tasks scheduled to run monthly on the thirtieth or thirty-first of the month run on the last day of the month, regardless of the month.

Tasks in April

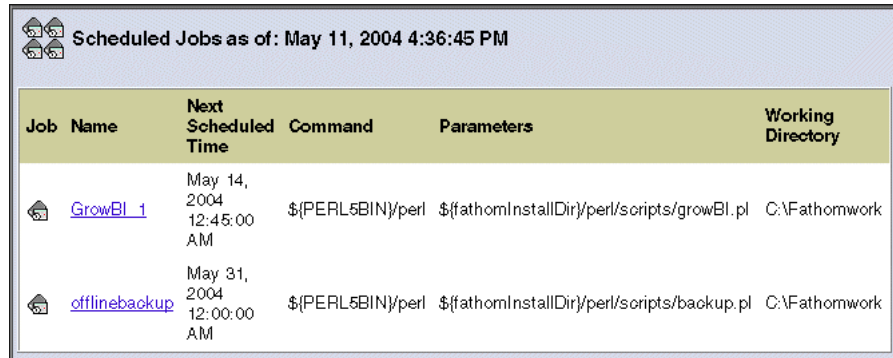
A report of the Inventory database is scheduled to run on the thirty-first of the month. Since there are only thirty days in April, Fathom executes the report on April 30.

Tasks in February

The same report used in the above example would execute on February 28 in nonleap years and on February 29 in leap years.

Viewing scheduled jobs

To view jobs scheduled to run, click **View Scheduled Jobs** in the **Fathom Jobs** page. The **Scheduled Jobs** page appears.



Scheduled Jobs as of: May 11, 2004 4:36:45 PM



Job	Name	Next Scheduled Time	Command	Parameters	Working Directory
	GrowBI_1	May 14, 2004 12:45:00 AM	\$(PERL5BIN)/perl	\$(fathomInstallDir)/perl/scripts/growBI.pl	C:\Fathomwork
	offlinebackup	May 31, 2004 12:00:00 AM	\$(PERL5BIN)/perl	\$(fathomInstallDir)/perl/scripts/backup.pl	C:\Fathomwork

Figure 8–7: Scheduled Jobs page

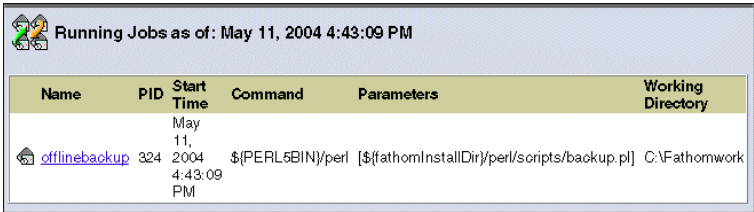
As shown in [Figure 8–7](#), the following information is given for each scheduled job:

- The name of the job.
- The next time the job is scheduled to run.
- The command to be executed when the job runs.
- Any parameters defined for the command.
- The working directory.

To see a job's summary page, click the specific job name.

Viewing running jobs

To view a list of jobs currently running in Fathom, click **View Running Jobs** in the **Fathom Jobs** page. The **Running Jobs** page appears.




Name	PID	Start Time	Command	Parameters	Working Directory
 offlinebackup	324	May 11, 2004 4:43:09 PM	\$(PERL5BIN)/perl	[\$(fathomInstallDir)/perl/scripts/backup.pl]	C:\Fathomwork

Figure 8–8: Running Jobs page

As shown in [Figure 8–8](#), Fathom displays the following information about each running job:

- The name of the currently running job.
- The time the job began to run.
- The command executed when the job runs.
- Any parameters defined for the command.
- The working directory.

To see a job’s summary, click the specific job name.

Viewing job history

The **Job History** section of the **Job** summary page allows you to:

- Display historical details about individual jobs that are run for the specific job within a date range that you define.
- Display output, error, and debug trace details for the specific job instance.



To view data for all jobs that have completed running in a specified time frame:

1. Click the **View Job History** option in the **Jobs** home page. The **Job History** page appears:

Job History:

Submit Cancel

Job History query

Select a *Start Date* range for the query (dd/mm/yyyy)


From: 4 / 5 / 2004

To: 11 / 5 / 2004

2. Specify the date range for the job history query you intend to submit, using the drop-down lists. Note that the **From** and **To** values of the date range are entered in a dd/mm/yyyy format.

The date range default value displays the past seven days. The seven days are determined as inclusive of the current date through the seventh day as you count forward in a given week.

3. Click **Submit** to submit your query. If no job history exists for the time frame you submitted, a **No history records available** statement displays. However, if a job history does exist, the following information appears:

 **Job History: as of: May 11, 2004 4:52:29 PM**

Submit

Cancel

Purge Selection

Job History query

Select a *Start Date* range for the query (dd/mm/yyyy)

From:

4

/

5

/

2004

To:










11

/

5

/

2004

Job	Name	Start Time	End Time	Command	Exit Code
	<u>job</u>	May 11, 2004 3:46:56 PM	May 11, 2004 3:46:59 PM	ls	0
	<u>job1</u>	May 11, 2004 3:47:10 PM	May 11, 2004 3:47:12 PM	ls	0
	<u>joba</u>	May 11, 2004 3:49:15 PM	May 11, 2004 3:49:17 PM	ls	0
	<u>jobb</u>	May 11, 2004 3:49:26 PM	May 11, 2004 3:49:30 PM	ls	0
	<u>joba</u>	May 11, 2004 3:50:24 PM	May 11, 2004 3:50:27 PM	ls	0
	<u>jobb</u>	May 11, 2004 3:50:33 PM	May 11, 2004 3:50:35 PM	ls	0
	<u>jobc</u>	May 11, 2004 3:51:05 PM	May 11, 2004 3:51:08 PM	ls	0
	<u>job3</u>	May 11, 2004 3:51:50 PM	May 11, 2004 3:51:52 PM	ls	0
	<u>job4</u>	May 11, 2004 3:51:59 PM	May 11, 2004 3:52:01 PM	ls	0

4. Click on an underlined name in the **Name** column to see a job status that includes:
- Name of the completed job.
 - Start date and time.
 - End date and time.
 - Command executed when the job ran.
 - Exit code.

When a job completes, Fathom stores its data in the FathomTrendDatabase. Fathom pulls the information about a completed job from the database table Cf_Task_Detail. For more information about FathomTrendDatabase tables, see the appropriate section of the *FathomTrendDatabase Guide and Reference*.

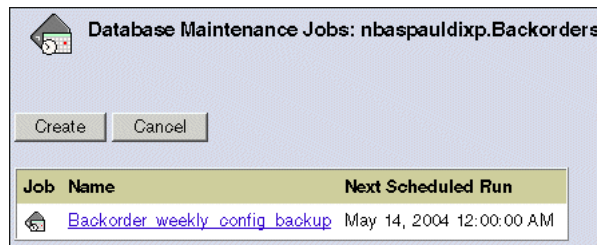
Viewing database maintenance job instances associated with an individual database

Fathom supports functionality to view job instances currently associated with a specific database.



To view instances associated with databases:

1. Select **Resources** from the menu bar. The list frame displays all resources.
2. Select **OpenEdge→Databases**.
3. Select the database for which you want to display this job information. The **Database Control** page for the database you selected appears.
4. Click the **Maintenance Jobs** link in the **Command and control** section of the **Database Control** page. The **Database Maintenance Jobs** page appears:



This page displays the list of jobs that are associated with the particular database and each job's next scheduled run time. Jobs that do not display information in the **Next Scheduled Run** column do not have schedules that are enabled.

5. From this page you can perform the following tasks:
 - Click a job's name to display its **Job** summary page.
 - Click **Create** to go directly to the **Jobs** home page.

Note: Complete functionality associated with the **Database Control** page is discussed in the *Database Management Guide*.

Working with job templates

Fathom makes it possible to create and continuously reuse job templates. A *template* is a sample outline for a resource category that you create. It usually includes some instance data. Values you define in a job template can be reused to help create individual job instances. Job templates are also a time-saving tool to help you standardize the creation of job instances and ensure that they are exportable.

In those situations where job instances require just a few unique values, you can define a job template from which you can create these individual jobs. To create a job template, you define common values for the template. Then, when you create a job instance from the template, you supply the unique values for the job, accepting appropriate default values from the template. This approach minimizes your data entry tasks and data entry errors.

These common values typically include:

- Commands such as executables or scripts.
- Command arguments.
- Job properties.
- A default schedule.

When you are ready to create instances from the template, you can access and reuse these values in job instances derived from the template.

For example, in analyzing your current OpenEdge database maintenance practices, your company determines that productivity in your IT department could be greatly improved if database restructuring activities were performed on a regularly scheduled basis for all the databases. To help standardize these processes, and ensure that they are performed routinely for all databases, you can create a user-defined job template and associated schedule for each of these unique database activities.

Using Fathom-supplied generic tools such as environment variables, you can tailor your job template to your specific needs. When you are ready to use this template, you associate the appropriate database resources with a job instance derived from the specific template.

Note: When reviewing your current database maintenance practices, keep in mind the Fathom-supplied, specialized Database maintenance job templates from which you can create job instances to address fundamental OpenEdge database maintenance activities. Designing user-defined job templates can be extremely effective, but they can also require additional analysis and design time to effectively produce. In contrast, the Database maintenance job templates are already tailored to address specific database tasks. Consider all your template options as you analyze your database needs. It is possible that a combination of user-defined and Fathom-supplied Database maintenance job templates might be optimum for your company.

For more information about these database maintenance jobs, see the appropriate section in the *Database Management Guide*.

Keep in mind that templates can be imported or exported; for example, users at your company's satellite offices can use the identical templates that are employed at your corporate office, ensuring that your practices are standardized throughout your company. For details about import and export activities, see [Chapter 9, “Exporting and Importing in Fathom.”](#)

Additional characteristics of job templates

Note these points as you create and work with any custom job templates:

- You do not run a job template. You run a job instance derived from a job template.
- To access user-defined templates and the Fathom-supplied database maintenance templates, select **Jobs** from the menu bar and review the contents of the **Defined Jobs** and **Job Templates** categories that display in the list frame.
- When you create a job template, you can define schedule information, but you cannot enable the schedule to run with the template. This schedule definition can be enabled once you create an instance from the template.

You can associate one or more command actions with job templates.

- You cannot define specific database resources for a job template. The job template is an outline of common values that you can copy and apply to various instances derived from the template. You associate specific database resources when you create a job instance.
- Once you have created a job instance from a job template, these items are completely separate from each other. Edits to the job instance do not affect the job template; edits to the job template do not affect any instances previously derived from the template.
- Unlike job instances, which can only be used local to the machine on which they are created, job templates can be exported and imported. However, the definition of job templates that you export or import does not include resource- or device-specific properties.
- You can also access existing job templates from the **Jobs** home page. See the [“Accessing existing job templates”](#) section on page 8–42 for more details.

Creating a job template

When you create a job template, you can choose the job’s characteristics. You need not recreate the job template criteria each time you want to create another job instance based on the template.

Once you create a job instance from a job template, the two are no longer tied together. You can modify the characteristics of a job instance without affecting the template on which the job is based, and you can update the template without affecting the characteristics of a job instance you have already created.

You choose the following characteristics for the job template: **Menu group**, **Menu entry**, and **Menu description**. Once you create the template, these characteristics enable you to identify it from among all other existing templates. For example, consider a scenario in which a user creates a Database Restore template for use on company databases related to inventory. The user makes the following choices regarding menus:

Menu group	Database Maintenance
Menu entry	DB Restore Inventory
Menu description	DBrestore for all inventory dbs

Once the job template is created, the template appears, as shown in [Figure 8–9](#).

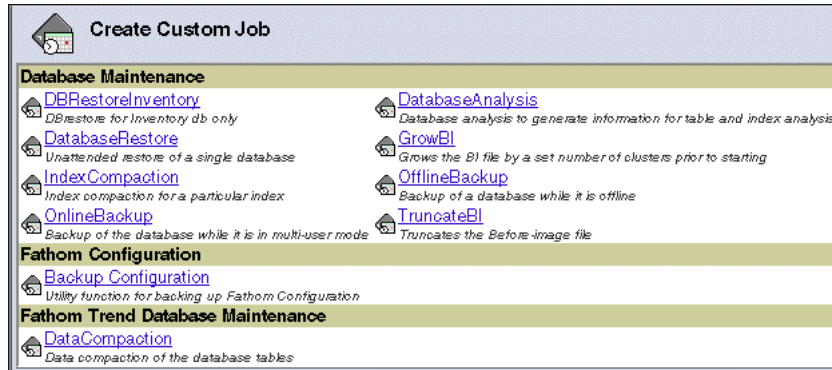


Figure 8–9: New job template in Create Custom Job page

The new job template **DBRestoreInventory** menu entry appears in the **Database Maintenance** menu group with the **DBrestore Inventory db only** menu description.

You specify each Fathom job template's properties and characteristics on two pages. The first template page defines the properties of the job. On the second page, you provide default values for the job instance; however, you can change these values, such as the schedule, for each instance.



To create a job template:

1. From the **Fathom Jobs** page, click **Create Job Template**. The first of two **Job Template** pages appears:

The screenshot shows a web form titled "Job Template:" with a "Save" and "Cancel" button at the top. Below the buttons is the text "Page 1 of 2". The form is divided into sections. The first section, "Template properties", contains a "Name:" label followed by a text input field. The second section, "Information for the Create Custom Job screen", contains three labels: "Menu group:", "Menu entry:", and "Menu description:". The "Menu group:" label is followed by a text input field and an "Existing:" label followed by a dropdown menu. The "Menu entry:" label is followed by a text input field. The "Menu description:" label is followed by a text input field with a small "v" icon at the end. The third section, "Limit how many databases can be associated with the job", contains a "Databases:" label followed by a dropdown menu with "no limit" selected.

2. In the **Name** field, enter the job template name. Note that the name must be unique among the job templates. Note also that spaces are not allowed in the name fields on this page.
3. In the **Menu group** field, enter the name of the new menu group; or choose an existing menu group in the **Existing** field. (When you choose an existing group, the name automatically appears in the **Menu group** field.)

The menu group is the heading under which the new template will appear (for example, **Database Maintenance**).

4. In the **Menu entry** field, enter the template name you want to appear on the **Custom Job** page.
5. In the **Menu description** field, enter a brief description of the job template. This description appears on the list of available job templates on the **Create Custom Job** page, under the template name you provide in [Step 4](#).
6. Under the **Limit how many databases can be associated with the job** field, select one, two, or no limit of databases. **No limit** is the default value.

7. Click **Save**. The second of two **Job Template** pages appears, as shown below, with the **Name** field prefilled:

DBRestoreInventory Job Template: DBRestoreInventory

Save Cancel

Page 2 of 2

Properties

Name: DBRestoreInventory

Description:

Account information

User name:

Password:

Job specification

Command:

Command parameters:

Environment
name=value pairs

Debug log file? ☐

Indicate if the job can be used as an action
Action: ☐

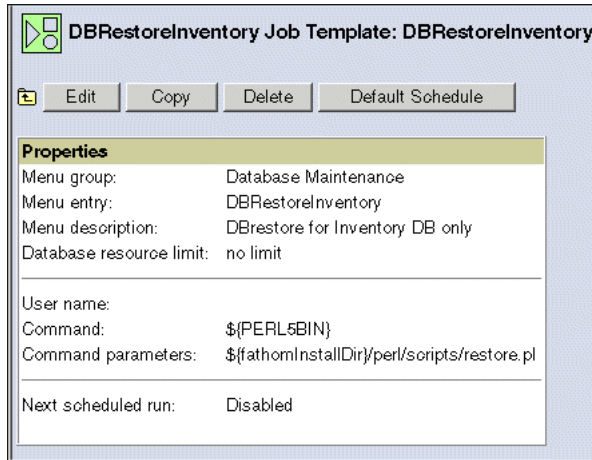
Completion Actions and Alerts:

8. Provide the properties.

Entering the **User name** is optional; if you do not supply a user name, any job instance created based on this template is run under the account Fathom is running under. Entering a password is required only if you also enter a user name; otherwise, it is optional.

For details about any other field, see the [“Creating a job instance”](#) section on page 8–5.

9. Click **Save**. The job template summary appears:



The screenshot shows a web interface for a job template. At the top, there is a green play button icon and the title "DBRestoreInventory Job Template: DBRestoreInventory". Below the title are four buttons: "Edit", "Copy", "Delete", and "Default Schedule". The main content area is titled "Properties" and contains a table of configuration details.

Menu group:	Database Maintenance
Menu entry:	DBRestoreInventory
Menu description:	DBrestore for Inventory DB only
Database resource limit:	no limit
<hr/>	
User name:	
Command:	\$(PERL5BIN)
Command parameters:	\$(fathomInstallDir)/perl/scripts/restore.pl
<hr/>	
Next scheduled run:	Disabled

You can now edit or copy the template's characteristics, delete the template, or schedule a job instance to run based on the template.

10. After you specify the properties that you want to default to each instance created from this template, you can then:
- Click **Edit** at the bottom of the page directly to the right of the **Completion Actions and Alerts** field to continue entering values. The **Job Completion Actions and Alerts** page appears. This page allows you to define default action and alert occurrences for each job instance created from this template. See the "[Setting up job completion actions and alerts](#)" section on page 8–8 for details.
 - Click **Save** at the top of the page to conclude entering values for the job template. The **Job** summary page appears.

If you want to set additional values for job actions and/or alerts, you can access the **Job Completion Actions and Alerts** page and perform these tasks at a later time by editing the **Job** page.

You can also initiate the job immediately by clicking **Run Now** on the **Job** summary page.

Choosing the job template schedule

When you create a job template, you also determine the schedule you want job instances created from the template to use.

Setting up a schedule for a template is very similar to setting up a schedule for a job instance. However, you cannot enable a schedule at the template level. To create schedule data, complete the **Job Schedule** page, as shown in [Figure 8–10](#). Then see the “[Scheduling a job](#)” section on page 8–21 for more information.

Job Schedule: BackupAJS

Save Cancel

Schedule

Frequency

Start Date (dd/mm/yyyy): 11 / 5 / 2004

Start Time: 5 : 30 PM

Repeat interval: One time

Include days: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Cron expression: Help

Enabled? ☒

Figure 8–10: Job template schedule

Accessing existing job templates

From the **Jobs** home page, click **Create Job from a Template**. The **Create Custom Job** page appears, as shown in [Figure 8–11](#).



Figure 8–11: Create Custom Job page

The example page shown in [Figure 8–11](#) displays the Fathom-supplied menu groups **Database Maintenance**, **Fathom Configuration**, and **FathomTrendDatabase Maintenance** and their respective job templates. Any templates that you create are also listed here, according to the menu groups, descriptions, and entities that you define for these templates.

Viewing debug details about jobs

Fathom provides a diagnostic report that includes debug information about jobs and reports. For details about the **Task Detail** report, see the [Reporting Guide](#).

Exporting and Importing in Fathom

When you create a resource monitoring plan, you can use Fathom to export and import selected plan components from one machine running Fathom to another.

This chapter describes exporting and importing and contains the following sections:

- [Exporting and importing overview](#)
- [Exporting Fathom Library components](#)
- [Importing Fathom Library components](#)

Exporting and importing overview

As you work with Fathom, you may find that you want to share certain Fathom-related components that you created on one machine with one or more other machines as well. You can export or import any of the sharable Fathom components, as follows:

- Actions.
- Report templates.
- Job templates.
- Rule sets for databases, log files, or OpenEdge server components.
- Search criteria for log files.

General export and import considerations

Keep the following points in mind before you perform either an import or export activity:

- It is advisable to back up the Fathom configuration database *before* you proceed with the import process.
- You will be informed of any potential conflicts through error messages in the Fathom Management console and in the log file. For example, if a component you are exporting from Machine A to Machine B has a schedule that conflicts with the schedule of an existing component on Machine B, you will be notified of this conflict.

Exporting Fathom Library components

When you *export* a sharable Fathom component from one machine, you place a copy of the Fathom component's definition into a file that you can then import onto another machine and use. When you export sharable Library components, the export process automatically determines any related resource dependencies and exports these components, too. For example, if you select a job template to export and the job template references an action to be performed when the job completes, Fathom will automatically include the action in the exported file.

Note: You can perform only one export or import operation during a given HTTP session at any one time.

The Fathom components you can export are contained in the Fathom Library.



To perform the export process:

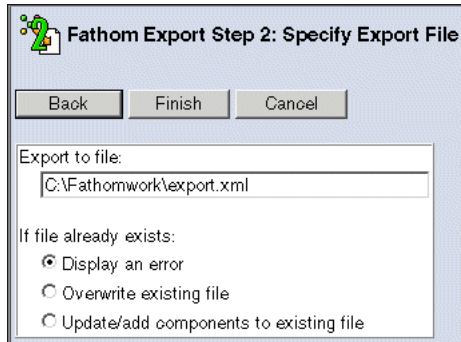
1. Click **Library** from the menu bar. The **Fathom Component Library** page appears.
2. Click **Export Components**. The **Fathom Export Step 1: Select Resources for Export** page appears.
3. Select the components you intend to export. You can select from any of the links to add to the same export file.
4. To add other components, select the appropriate link. When all the components of that type appear, you can click **Select All** to choose every one listed:



(To deselect all search criteria, click **Unselect All**.)

5. Click **OK** to return to the **Fathom Export Step 1: Select Resources for Export** page. The list of components selected for export appears.

- Click **Export** when you have selected all components you want to export at this time. The **Fathom Export Step 2: Specify Export File** page appears:

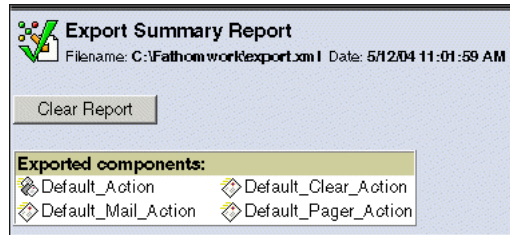


In the **Export to file** field, Fathom provides a default path and filename for the export file to be created; you can change either default value in the field.

You can also indicate what action you want taken if the file already exists. The options available are:

- **Display an error** (default option).
 - **Overwrite existing file**, which removes any data currently in the file.
 - **Update/add components to existing file**, which allows you to add the components you just selected to the list of components already in the file. If you have selected a component to export that already exists in the .xml file, the old definition will be removed and the selected component added.
- Choose one of the following:
 - **Back** — Returns you to the **Fathom Export Step 1: Select Resources for Export** page.
 - **Cancel** — Ends the export setup process.
 - **Finish** — Initiates the export operation. The **Exporting File** page appears, noting the path and filename of the exported file. The **Exporting File** page is updated every three seconds. In general, the larger the number of components you are exporting in the export.xml file, the longer the operation can take.

Once the export operation is completed, the **Export Summary Report** page appears:



The header information on this page identifies the path and filename to which the exported components were sent. The date and time information identifies when the export operation occurred. Also, the report details on the **Export Summary Report** page display the list of components that were exported, updated, or determined to be dependent because they are referenced by an exported resource.

This process also determines if any errors occur that prevent the export from succeeding. If an error occurs, the error will display in a separate page, and the report page, as shown, provides detailed information about the error.

8. Click **Clear Report** once you have reviewed and/or printed your exported resources list. You must select **Clear Report** before you can initiate another export operation.

Exporting referenced items

Components that you export might be dependent on other components to function as intended. For example, if you want to export a job resource and the job resource references an action to be performed when the job completes, Fathom automatically includes the action in the exported file.

Figure 9–1 and Figure 9–2 show implicit and explicit components.

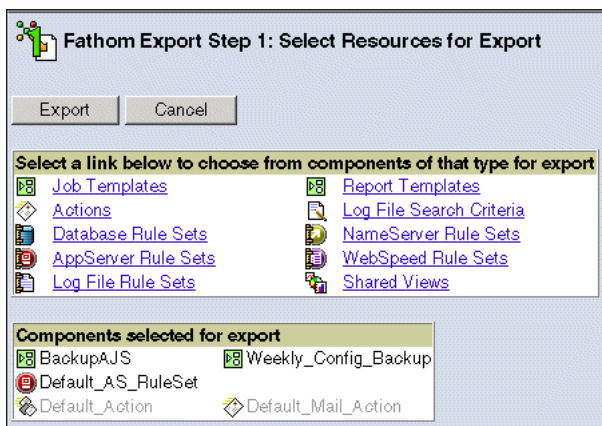


Figure 9–1: Implicit and explicit components selected for export

An explicit component is one that you select; an implicit component is one that is also exported because a selected component has a dependency on it.

In the **Components selected for export** list shown in Figure 9–1, the default AppServer rule set and the two job templates BackupAJS and Weekly_Config_Backup are explicitly exported; Default_Action and Default_Mail_Action are implicitly exported because the rule set or one of the job templates is dependent upon its availability.

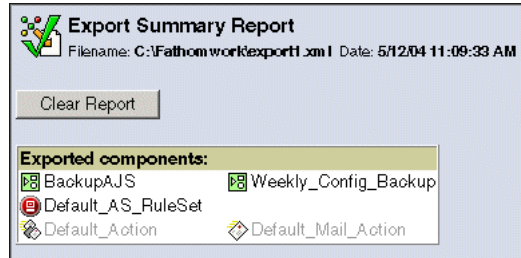


Figure 9–2: Implicit and explicit components export confirmation

The **Exported components** list that appears in Figure 9–2 confirms that the explicitly selected components and their two component dependents have in fact been successfully exported. The implicit components are dimmed to identify their dependency.

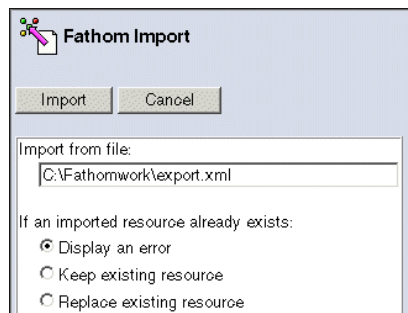
Importing Fathom Library components

When you import a component, you add the component definition from an import file to your project.



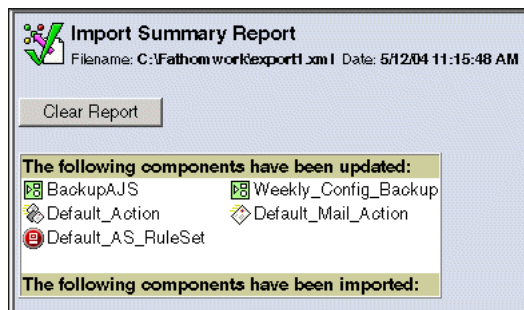
To perform the import process:

1. Click **Library** from the menu bar. The **Fathom Component Library** page appears.
2. Click **Import Components**. The **Fathom Import** page appears:



3. If you want, you can change the default value in the **Import from file** field. (The default path and filename are the same as the default values used for the most recent export operation.)
4. Indicate which action you want taken if any of the components that you are importing already exist. You can choose to:
 - **Display an error** — Indicates that none of the components will be imported if any component in the import file conflicts with an existing component. (This is the default.)
 - **Keep existing resources** — Indicates that the existing definition of a given component be maintained and the imported definition discarded.
 - **Replace existing resource** — Indicates that the existing definition will be deleted and the imported definition will be added.
5. Choose one:
 - **Import** — Initiates the import operation. The **Importing File** page displays and is updated every three seconds. In general, the larger the of number of components you are importing from the export.xml file, the longer the operation can take.
 - **Cancel** — Terminates the current import selections.

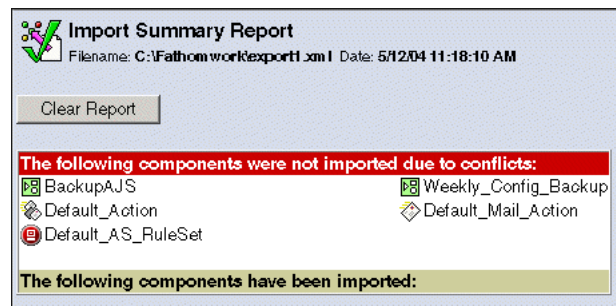
Once the import operation is completed, the **Import Summary Report** page appears:



The report data on the **Import Summary Report** page indicates which components have been updated. Such an update occurs if you select the **Replace existing resource** option on the **Fathom Import** page.

Note: Unlike the export operation, there are no explicit and implicit components associated with the import operation. No components appear dimmed in the import operation's report page.

If you select the **Display an error** option on the **Fathom Import** page and then a conflict is encountered, you are notified that the import failed:



Index

A

Accessing help in the management console
2–16

Actions

- creating
 - compound 4–37
 - e-mail 4–32
 - log 4–36
 - SNMP Trap 4–39 to 4–41
- default mail 4–31
- default pager 4–31
- definition 1–5, 4–30
- updating and deleting 4–41

Alerts

- definition 1–5, 4–29
- option in the Fathom menu bar 2–7

C

Collapsing resource categories 2–15

- Collapse all icon 2–14, 2–15

Collection views

- creating 3–19
- customizing layout for 3–21, 3–22
- definition 3–14
- deleting 3–23
- differences from collections 3–4

- editing 3–22
- working with 3–15 to 3–27

Collections

- and administrators or operators 3–8
- creating 3–8 to 3–12
- definition 1–4, 3–4
- deleting 3–14
- differences from collection views 3–4
- editing 3–13
- My Collections 3–5
- Referenceable collections 3–5
- sample scenario 3–6, 3–7
- Shared Collections 3–5
- terminology and hierarchy 3–5
- working with 3–8 to 3–14

Configuration Advisor 4–22 to 4–29

- comparing and selecting threshold settings 4–28
- determining effectiveness of selections 4–29
- guidelines 4–22
- overview 4–22
- reviewing calculation details 4–26
- reviewing threshold settings
 - recommended by 4–26
- submitting threshold setting selections 4–28
- using with a disk, CPU, or file system resource 4–23 to 4–25

- Container
 - definition 1–4
 - viewing the contents of 2–6, 2–7
- Control bar
 - icons 2–14
- Copying resource monitors 4–42
- Creating resource monitors
 - Monitoring Plan and Rule Definition page 4–10
 - resource naming conventions 4–4
- Cron-based scheduling
 - for jobs 8–22 to 8–24
- Custom views
 - creating 3–19 to 3–20
 - customizing the layout of 3–22
 - displaying custom viewlets in 3–15
 - My Fathom Home page 3–2
 - standard viewlets 3–16

D

- Database maintenance job templates 8–4
- Debug file
 - reviewing for job details 8–42
- Default action (Default_Action) 4–31
- Default mail action (Default_Mail_Action) 4–31
- Default pager action (Default_Pager_Action) 4–31
- Default values
 - changing at the individual resource level 4–46
 - CPU and memory resources 4–6
 - definition 4–43
 - file monitor resources 7–5
 - global settings 4–44
 - resource type 4–45

- Default_Action 4–31
- Deleting resource monitors 4–43
- Detail control bar 2–3, 2–4
- Detail frame 2–4
- Detail menu 2–3, 2–4
- Detail menu bar 2–11
- Disabled status 2–13
- Discovery
 - of machine availability 6–5
 - TCP ports 6–5
 - UDP ports 6–5
- Displaying a page in a new window in the console
 - icon 2–14
- Displaying a page in a new window of the console
 - icon 2–16
- Displaying custom viewlets
 - in custom views 3–15

E

- Editing resource monitors 4–42
- Environment variables
 - job 8–14 to 8–18
- Exit code
 - for jobs 8–9
- Expanding resource categories
 - Expand all icon 2–14, 2–15
- Exporting sharable Fathom components 9–2
 - considerations before 9–2
 - details 9–3
 - explicit 9–7
 - implicit 9–6
 - that include referenced items 9–6, 9–7

F

Fail status 2–13

FathomTrendDatabase
definition 1–6

File monitors
defining 7–37
rules 7–37

G

Global settings
reviewing and changing 4–44, 4–45

H

Help
option in the Fathom menu bar 2–7

Help icon 2–14

HTTP resource monitor
considerations 6–17
creating 6–18 to 6–24
using to determine Web site status 6–17

I

Importing sharable Fathom components
9–2, 9–7
considerations before 9–2

Inactive status 2–13

J

Job Action field 8–16

Job chaining 8–11
recursion 8–14

Job instances

alert environment variables for job
actions in 8–17
associated with an individual database
8–33
common environment variables in 8–14
definition 8–3
environment variables associated with
database resources 8–16
environment variables associated with
FathomTrendDatabase 8–18
Job Action field in 8–16
job chaining in 8–11
viewing when associated with an
individual database 8–33

Job templates

accessing existing 8–42
creating 8–36 to 8–41
definition 4–46
for database maintenance 8–4
job chaining 8–11
menu group, menu entry, menu
description 8–36
setting up 8–34
job completion actions and alerts for
8–8
schedules for 8–41

Jobs

and job chaining 8–11
creating
as an instance 8–5
templates for 8–36
custom 8–3
database maintenance templates for 8–4
definition 1–10
environment variables in 8–14 to 8–18
execution policies
duration 8–26
monthly by date 8–28
over time 8–27
single 8–27
Job Action field and 8–16
job completion actions and alerts for 8–8
option in the Fathom menu bar 2–7

- overview 8–5
- recursion 8–14
- reviewing debug file for details about 8–42
- scheduling 8–21
 - using cron expressions 8–22 to 8–24
- templates 8–4
 - accessing existing 8–42
 - additional characteristics 8–35
 - schedule data in 8–41
 - setting up 8–34
- viewing
 - history 8–31
 - running 8–30

L

- Library
 - option in the Fathom menu bar 2–7
- Library functions
 - defining search criteria 4–46
 - definition 4–46
 - schedules and actions 4–46
- List control bar 2–3, 2–4
- List frame 2–3, 2–4
 - expanding and collapsing contents 2–9, 2–10
 - sorting 2–11, 2–12
- Log file monitors
 - accessing library-defined search criteria for 7–25
 - creating library-based search criteria for 7–28
 - definition 7–2
 - enabling 7–35
 - library features
 - accessing rule sets 7–16
 - associating rule sets with log file monitors 7–20
 - overview 7–2
 - rule components 7–15

- setting up 7–7
 - library-based log file rule sets for 7–16
 - monitoring plans 7–13
 - properties 7–7
 - rules 7–15
- Truncate Action 7–12
- viewing summary details 7–36

M

- Management console
 - accessing 2–2
 - accessing help in 2–16
 - and logging on to Fathom 2–2, 2–3
 - changing the display of 2–14
 - default user name and password 1–6
 - definition 2–2
 - detail control bar 2–3, 2–4
 - detail frame 2–3, 2–4
 - detail menu 2–3, 2–4
 - displaying a page in a new window in 2–16
 - expanding or collapsing list frame
 - categories in 2–15
 - list control bar 2–3, 2–4
 - list frame 2–3, 2–4
 - menu bar 2–3, 2–4
 - navigating 2–9 to 2–14
 - refreshing 2–15
 - resource statuses in 2–12
 - returning to the previous page in 2–15
 - using 1–6, 2–1 to 2–17
 - using to start Fathom 2–2, 2–3
 - viewing host machine name in 2–8

- Menu bar 2–3, 2–4

- Menu description
 - job template 8–36

- Menu entry
 - job template 8–36

- Menu group
 - job template 8–36

- Monitor
 - definition 1–5
- Monitoring remote resources 4–3
- My Collections 3–5
- My Fathom Home page 3–2, 3–3
- My Fathom page 2–3
 - option in the Fathom menu bar 2–7

N

- Naming conventions for resources 4–4
- Network resources
 - adding 6–11
 - determining machine and port availability for 6–8
 - discovery 6–5
 - monitoring 6–2
- Not Checked status 2–13
- Not Running status 2–13

O

- Offline status 2–13
- Options
 - option in the Fathom menu bar 2–7

P

- Parent folder 2–11
- Pass status 2–13
- Perl 5 regular expressions
 - as search criteria 7–30 to 7–33

- PING/ICMP monitors
 - creating 6–15 to 6–16
 - defining 6–15

R

- Realtime reports 1–10
- Redirection
 - Web page 6–18
- Referenceable collections 3–5
- Refreshing the console 2–15
 - Refresh icon 2–14
- Remote Configuration Utility 4–3
- Report templates
 - definition 4–46
- Reports
 - option in the Fathom menu bar 2–7
- Resource monitoring
 - overview 4–4, 4–5
- Resource monitoring plans
 - definition 1–5
- Resource monitors
 - deleting 4–43
 - editing and copying 4–42
- Resource statuses 2–12
- Resource viewlets, in custom views 3–15
- Resources
 - definition 1–3
 - naming conventions 4–4
 - option in the Fathom menu bar 2–7
- Returning to the previous page in the console 2–15

Rules

- definition 1–5

Rules definitions

- default 4–18
- for CPU usage 5–4
- for file systems 5–14
- for files 7–37
- for memory usage 5–9
- for system disk devices 5–13
- resource-specific 4–18

S

Schedules

- considerations 4–13
- default 4–14
- definition 1–5, 4–12
- predefined by Fathom 4–14
- updating and deleting 4–15

Search criteria

- definition 7–25
- Fathom-supplied 7–26
- for log file monitors 7–25
- literal strings as 7–25
- Perl 5 regular expressions in 7–25, 7–30 to 7–33

Shared Collections 3–5

SNMP Trap Action

- creating 4–39 to 4–41

Sort by

- option in the list frame 2–11, 2–12

Sort by option in the list frame 2–11

Standard viewlets 3–16

- in custom views 3–16

Status indicators 2–12, 2–13

- and alerts 2–14

System Activity report 2–7

System disk devices

- monitoring 5–13

System information report 2–7

T

TCP monitors

- creating 6–13 to 6–15

Terminology

- common 1–3 to 1–6

Terminology, Fathom

- actions 4–30
- alerts 4–29
- alerts and actions 1–5
- collections 3–5
- container 1–4
- FathomTrendDatabase 1–6
- monitor 1–5
- resource-monitoring plan 1–5
- rule set 1–5
- rules 1–5
- rules or rules definitions 4–17
- schedule 1–5
- schedules for jobs 8–21

Trending considerations for

- CPU resources 5–7
- disk resources 5–14
- file systems 5–16
- memory resources 5–12
- network resources 6–3

Truncate Action 7–12

U

UDP monitors

- creating 6–13 to 6–15

V

View previous page icon 2–14

Viewing

- job history 8–31
- running jobs 8–30
- scheduled jobs 8–29

Viewing the previous page 2–15
icon 2–14, 2–15

Viewlet

definition 3–14

Viewlets

- characteristics 3–18
- characteristics and functionality 3–18
- customizing 3–24, 3–24 to 3–27
- resource 3–15
- standard 3–16
- view panel 3–17

