Informatica

Informatica® Proactive Monitoring for PowerCenter

3.0.2

Governance User Guide

Informatica Proactive Monitoring for PowerCenter Governance User Guide
3.0.2
March 2024

© Copyright Informatica LLC 1993, 2024

This software and documentation contain proprietary information of Informatica LLC and are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering of the software is prohibited. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC. This Software may be protected by U.S. and/or international Patents and other Patents Pending.

Use, duplication, or disclosure of the Software by the U.S. Government is subject to the restrictions set forth in the applicable software license agreement and as provided in DFARS 227.7202-1(a) and 227.7702-3(a) (1995), DFARS 252.227-7013©(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

The information in this product or documentation is subject to change without notice. If you find any problems in this product or documentation, please report them to us in writing.

Informatica, Informatica Platform, Informatica Data Services, PowerCenter, PowerCenterRT, PowerCenter Connect, PowerCenter Data Analyzer, PowerExchange, PowerMart, Metadata Manager, Informatica Data Quality, Informatica Data Explorer, Informatica B2B Data Transformation, Informatica B2B Data Exchange Informatica On Demand, Informatica Identity Resolution, Informatica Application Information Lifecycle Management, Informatica Complex Event Processing, Ultra Messaging, Informatica Master Data Management, and Live Data Map are trademarks or registered trademarks of Informatica LLC in the United States and in jurisdictions throughout the world. All other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties, including without limitation: Copyright DataDirect Technologies. All rights reserved. Copyright © Sun Microsystems. All rights reserved. Copyright © RSA Security Inc. All Rights Reserved. Copyright © Ordinal Technology Corp. All rights reserved. Copyright © Aandacht c.v. All rights reserved. Copyright Genivia, Inc. All rights reserved. Copyright Isomorphic Software. All rights reserved. Copyright © Meta Integration Technology, Inc. All rights reserved. Copyright © Intalio. All rights reserved. Copyright © Oracle. All rights reserved. Copyright © Adobe Systems Incorporated. All rights reserved. Copyright © DataArt, Inc. All rights reserved. Copyright © ComponentSource. All rights reserved. Copyright © Microsoft Corporation. All rights reserved. Copyright © Rogue Wave Software, Inc. All rights reserved. Copyright © Teradata Corporation. All rights reserved. Copyright © Yahoo! Inc. All rights reserved. Copyright © Glyph & Cog, LLC. All rights reserved. Copyright © Thinkmap, Inc. All rights reserved. Copyright © Clearpace Software Limited. All rights reserved. Copyright © Information Builders, Inc. All rights reserved. Copyright © OSS Nokalva, Inc. All rights reserved. Copyright Edifecs, Inc. All rights reserved. Copyright Cleo Communications, Inc. All rights reserved. Copyright © International Organization for Standardization 1986. All rights reserved. Copyright © ej-technologies GmbH. All rights reserved. Copyright © Jaspersoft Corporation. All rights reserved. Copyright © International Business Machines Corporation. All rights reserved. Copyright © yWorks GmbH. All rights reserved. Copyright © Lucent Technologies. All rights reserved. Copyright © University of Toronto. All rights reserved. Copyright © Daniel Veillard. All rights reserved. Copyright © Unicode, Inc. Copyright IBM Corp. All rights reserved. Copyright © MicroQuill Software Publishing, Inc. All rights reserved. Copyright © PassMark Software Pty Ltd. All rights reserved. Copyright © LogiXML, Inc. All rights reserved. Copyright © 2003-2010 Lorenzi Davide, All rights reserved. Copyright © Red Hat, Inc. All rights reserved. Copyright © The Board of Trustees of the Leland Stanford Junior University. All rights reserved. Copyright © EMC Corporation. All rights reserved. Copyright © Flexera Software. All rights reserved. Copyright © Jinfonet Software. All rights reserved. Copyright © Apple Inc. All rights reserved. Copyright © Telerik Inc. All rights reserved. Copyright © BEA Systems. All rights reserved. Copyright © PDFlib GmbH. All rights reserved. Copyright © Orientation in Objects GmbH. All rights reserved. Copyright © Tanuki Software, Ltd. All rights reserved. Copyright © Ricebridge. All rights reserved. Copyright © Sencha, Inc. All rights reserved. Copyright © Scalable Systems, Inc. All rights reserved. Copyright © jQWidgets. All rights reserved. Copyright © Tableau Software, Inc. All rights reserved. Copyright© MaxMind, Inc. All Rights Reserved. Copyright © TMate Software s.r.o. All rights reserved. Copyright © MapR Technologies Inc. All rights reserved. Copyright © Amazon Corporate LLC. All rights reserved. Copyright © Highsoft. All rights reserved. Copyright © Python Software Foundation. All rights reserved. Copyright © BeOpen.com. All rights reserved. Copyright © CNRI. All rights reserved.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/), and/or other software which is licensed under various versions of the Apache License (the "License"). You may obtain a copy of these Licenses at http://www.apache.org/licenses/. Unless required by applicable law or agreed to in writing, software distributed under these Licenses is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the Licenses for the specific language governing permissions and limitations under the Licenses.

This product includes software which was developed by Mozilla (http://www.mozilla.org/), software copyright The JBoss Group, LLC, all rights reserved; software copyright © 1999-2006 by Bruno Lowagie and Paulo Soares and other software which is licensed under various versions of the GNU Lesser General Public License Agreement, which may be found at http:// www.gnu.org/licenses/lgpl.html. The materials are provided free of charge by Informatica, "as-is", without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

The product includes ACE(TM) and TAO(TM) software copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (©) 1993-2006, all rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (copyright The OpenSSL Project. All Rights Reserved) and redistribution of this software is subject to terms available at http://www.openssl.org and http://www.openssl.org/source/license.html.

This product includes Curl software which is Copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at http://curl.haxx.se/docs/copyright.html. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

The product includes software copyright 2001-2005 (©) MetaStuff, Ltd. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at http://www.dom4j.org/ license.html.

The product includes software copyright © 2004-2007, The Dojo Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at http://dojotoolkit.org/license.

This product includes ICU software which is copyright International Business Machines Corporation and others. All rights reserved. Permissions and limitations regarding this software are subject to terms available at http://source.icu-project.org/repos/icu/icu/trunk/license.html.

This product includes software copyright © 1996-2006 Per Bothner. All rights reserved. Your right to use such materials is set forth in the license which may be found at http:// www.gnu.org/software/ kawa/Software-License.html.

This product includes OSSP UUID software which is Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Permissions and limitations regarding this software are subject to terms available at http://www.opensource.org/licenses/mit-license.php.

This product includes software developed by Boost (http://www.boost.org/) or under the Boost software license. Permissions and limitations regarding this software are subject to terms available at http:/ /www.boost.org/LICENSE_1_0.txt.

This product includes software copyright © 1997-2007 University of Cambridge. Permissions and limitations regarding this software are subject to terms available at http:// www.pcre.org/license.txt.

This product includes software copyright © 2007 The Eclipse Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at http:// www.eclipse.org/org/documents/epl-v10.php and at http://www.eclipse.org/org/documents/edl-v10.php.

This product includes software licensed under the terms at http://www.tcl.tk/software/tcltk/license.html, http://www.bosrup.com/web/overlib/?License, http://www.stlport.org/doc/ license.html, http://asm.ow2.org/license.html, http://www.cryptix.org/LICENSE.TXT, http://hsqldb.org/web/hsqlLicense.html, http://httpunit.sourceforge.net/doc/ license.html, http://jung.sourceforge.net/license.txt , http://www.gzip.org/zlib/zlib_license.html, http://www.openldap.org/software/release/license.html, http://www.libssh2.org, http://slf4j.org/license.html, http://www.sente.ch/software/OpenSourceLicense.html, http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3- license-agreement; http://antlr.org/license.html; http://aopalliance.sourceforge.net/; http://www.bouncycastle.org/licence.html; http://www.jgraph.com/jgraphdownload.html; http://www.jcraft.com/jsch/LICENSE.txt; http://jotm.objectweb.org/bsd_license.html; . http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231; http://www.slf4j.org/license.html; http://nanoxml.sourceforge.net/orig/copyright.html; http://www.json.org/license.html; http://forge.ow2.org/projects/javaservice/, http://www.postgresql.org/about/licence.html, http://www.sqlite.org/copyright.html, http://www.tcl.tk/software/tcltk/license.html, http://www.jaxen.org/faq.html, http://www.jdom.org/docs/faq.html, http://www.slf4j.org/license.html; http://www.iodbc.org/dataspace/iodbc/wiki/iODBC/License; http://www.keplerproject.org/md5/license.html; http://www.toedter.com/en/jcalendar/license.html; http://www.edankert.com/bounce/index.html; http://www.net-snmp.org/about/license.html; http://www.openmdx.org/#FAQ; http://www.php.net/license/3_01.txt; http://srp.stanford.edu/license.txt; http://www.schneier.com/blowfish.html; http://www.jmock.org/license.html; http://xsom.java.net; http://benalman.com/about/license/; https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js; http://www.h2database.com/html/license.html#summary; http://jsoncpp.sourceforge.net/LICENSE; http://jdbc.postgresql.org/license.html; http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto; https://github.com/rantav/hector/blob/master/LICENSE; http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html; http://jibx.sourceforge.net/jibx-license.html; https://github.com/lyokato/libgeohash/blob/master/LICENSE; https://github.com/hjiang/jsonxx/blob/master/LICENSE; https://code.google.com/p/lz4/; https://github.com/jedisct1/libsodium/blob/master/LICENSE; http://one-jar.sourceforge.net/index.php?page=documents&file=license; https://github.com/EsotericSoftware/kryo/blob/master/license.txt; http://www.scala-lang.org/license.html; https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt; http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html; https://aws.amazon.com/asl/; https://github.com/twbs/bootstrap/blob/master/LICENSE; https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt; https://github.com/documentcloud/underscore-contrib/blob/master/LICENSE, and https://github.com/apache/hbase/blob/master/LICENSE.txt.

This product includes software licensed under the Academic Free License (http://www.opensource.org/licenses/afl-3.0.php), the Common Development and Distribution License (http://www.opensource.org/licenses/cddl1.php) the Common Public License (http://www.opensource.org/licenses/cpl1.0.php), the Sun Binary Code License Agreement Supplemental License Terms, the BSD License (http:// www.opensource.org/licenses/bsd-license.php), the new BSD License (http://opensource.org/licenses/BSD-3-Clause), the MIT License (http://www.opensource.org/licenses/mit-license.php), the Artistic License (http://www.opensource.org/licenses/artistic-license-1.0) and the Initial Developer's Public License Version 1.0 (http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/).

This product includes software copyright © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. All rights reserved. Permissions and limitations regarding this software are subject to terms available at http://xstream.codehaus.org/license.html. This product includes software developed by the Indiana University Extreme! Lab. For further information please visit http://www.extreme.indiana.edu/.

This product includes software Copyright (c) 2013 Frank Balluffi and Markus Moeller. All rights reserved. Permissions and limitations regarding this software are subject to terms of the MIT license.

See patents at https://www.informatica.com/legal/patents.html.

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

Publication Date: 2024-04-01

Table of Contents

Preface 7

Informatica Resources 7

- Informatica Network 7
- Informatica Knowledge Base 7
- Informatica Documentation 7
- Informatica Product Availability Matrixes 8
- Informatica Velocity 8
- Informatica Marketplace 8
- Informatica Global Customer Support 8

Chapter 1: Proactive Monitoring for PowerCenter Governance Overview 9

Introduction 9

Solution Components 10

- Informatica RulePoint 11
- Informatica Real-Time Alert Manager 12
- Proactive Monitoring Repository 12
- Proactive Monitoring for PowerCenter Management Console 13

Solution Usage 13

Chapter 2: Monitoring PowerCenter Governance 15

Overview 15

Proactive Monitoring Objects 15

- Sources 16
- Analytics 16
- Responders 17

Proactive Monitoring Rules 17

- Types of Rules 17
- Templates 18
- Advanced Rules 18

Chapter 3: Manage Objects 19

Manage Objects Overview 19

- Manage Objects View 19

Managing PMPC SQL Source Services 21

- Deploying, Undeploying, or Redeploying SQL Source Services 21

Monitored Event Management 22

- Viewing Topics 22

Monitored Objects Management 22

- Viewing and Editing Watchlists 23
- Monitored Folder Management 23

Monitor Files and Directories on a Node. . . . 24
Managing Templates Rules. . . . 27
Creating a Template Rule . . . 27
Editing a Template Rule. . . . 28
Copying a Template Rule. . . . 28
Deleting a Template Rule. . . . 28
Deploying, Undeploying, and Redeploying Rules . . . 28
Viewing the Statistics of a Rule Activation. . . . 29

Chapter 4: Proactive Monitoring Reports. . . . 30

Proactive Monitoring Reports Overview. . . . 30
Reports Tab - Filter and Display Options. . . . 31
Monitoring Application Services and Hosts in the Domain. . . . 31
Monitoring Alerts for Application Services and Host Statistics for the Current Day. . . . 32
Monitoring the Alert History for Application Services and Hosts. . . . 33
Monitoring PowerCenter Operation Alerts. . . . 33
Monitoring the PowerCenter Operation Alerts for the Current Day. . . . 34
Monitoring the Alert History for PowerCenter Operations. . . . 34
Export Alerts for PowerCenter Operations. . . . 34
Monitoring PowerCenter Governance Alerts. . . . 35
Monitoring the PowerCenter Governance Alerts for the Current Day. . . . 35
Monitoring the PowerCenter Governance Best Practice Violations. . . . 36
Export Alerts for PowerCenter Governance. . . . 36
Monitoring the PowerCenter Governance Alerts Using On Demand Reports. . . . 37

Chapter 5: Proactive Monitoring SNMP Alerts. . . . 42

Proactive Monitoring SNMP Alerts. . . . 42

Chapter 6: Proactive Monitoring Watchlists. . . . 44

Proactive Monitoring Watchlists. . . . 44

Chapter 7: Proactive Monitoring Topics. . . . 46

Proactive Monitoring Topics. . . . 46

Chapter 8: Proactive Monitoring Services. . . . 48

Sources. . . . 48
Analytics. . . . 50
Responders. . . . 52

Chapter 9: Proactive Monitoring Templates and Rules. . . . 53

Proactive Monitoring Templates. . . . 53
Template Rules. . . . 61
Advanced Rules. . . . 69

Chapter 10: Proactive Monitoring Responses. 81

Proactive Monitoring Responses. 81

Appendix A: Troubleshooting. 83

Troubleshooting Real-Time Alerts 83

Appendix B: Topic Properties Reference. 84

Topic Properties. 84

Appendix C: Frequently Asked Questions. 91

Appendix D: Glossary. 93

Index. 96

Preface

The *Proactive Monitoring for PowerCenter Governance User Guide* provides information about the Proactive Monitoring components.

It describes the environment and the monitoring components. It also contains reference material that describes components such as rules, watchlists, and topics. This guide is written for users who configure monitoring for the PowerCenter environment.

Informatica Resources

Informatica Network

Informatica Network hosts Informatica Global Customer Support, the Informatica Knowledge Base, and other product resources. To access Informatica Network, visit https://network.informatica.com.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- Review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com.

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions.

If you are an Informatica Network member, you can access Informatica Velocity resources at http://velocity.informatica.com.

If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that augment, extend, or enhance your Informatica implementations. By leveraging any of the hundreds of solutions from Informatica developers and partners, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through Online Support on Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

If you are an Informatica Network member, you can use Online Support at http://network.informatica.com.

CHAPTER 1

Proactive Monitoring for PowerCenter Governance Overview

This chapter includes the following topics:

- Introduction, 9
- Solution Components, 10
- Solution Usage, 13

Introduction

Proactive Monitoring for PowerCenter Governance provides advanced monitoring capabilities for PowerCenter development environments.

PowerCenter development environments can have hundreds of developers who create and change objects such as workflows, sessions, mappings, and transformations stored in the PowerCenter repository. The solution collects data from the PowerCenter repository databases at regular intervals, checks for anomalies in the metadata of PowerCenter objects, and alerts appropriate users. The alert messages contain the required contextual information, such as the object name, name of the user who modified the object, and cause of the alert. The PowerCenter developers or architects can refer the alert messages to take corrective action effectively.

The solution contains rules that perform a wide range of checks against the PowerCenter objects metadata and generates alerts whenever there is a deviation. A simple example is to alert users when a developer does not follow prescribed naming convention for objects or saves an object without comments. A complex example is to perform detailed checks on object metadata, such as to see whether the developer uses the session name to derive the session log file name.

Proactive Monitoring for PowerCenter contains built-in rules that detect deviations. You can also create and change rules. You can customize and extend the solution based on the business needs.

A single installation of the solution monitors a single domain and its numerous repository databases.

Proactive monitoring solution provides targeted alerting capabilities. The solution contains predefined personas who receive alerts specific to their function.

The Proactive Monitoring solution contains the following predefined personas:

- pcadmin. Any user who ensures proper functioning of PowerCenter domains, integration, repository, and other services.
- apparchitect. Any user who is responsible for the logic of PowerCenter mappings, mapplets, transforms, sources, and targets.
- dataarchitect. Any user who oversees the data movement with in PowerCenter.
- itsecurity. Any user responsible for dealing with IT security issues, such as sensitive data and malware.
- pcmonitor. Any user who tracks PowerCenter performance. By default, the pcmonitor persona receives all alerts.

In a continuous monitoring system, the solution can detect the same anomaly multiple times and send the same alert multiple times. To avoid such a situation, the solution provides the snooze feature. You can use the snooze feature to set a time period before which the solution does not generate any alert on the same anomaly.

For example, a developer updates a PowerCenter object that results in a session processing failure. This could be a planned development activity where the architects would want to stop receiving alerts for a specified period of time.

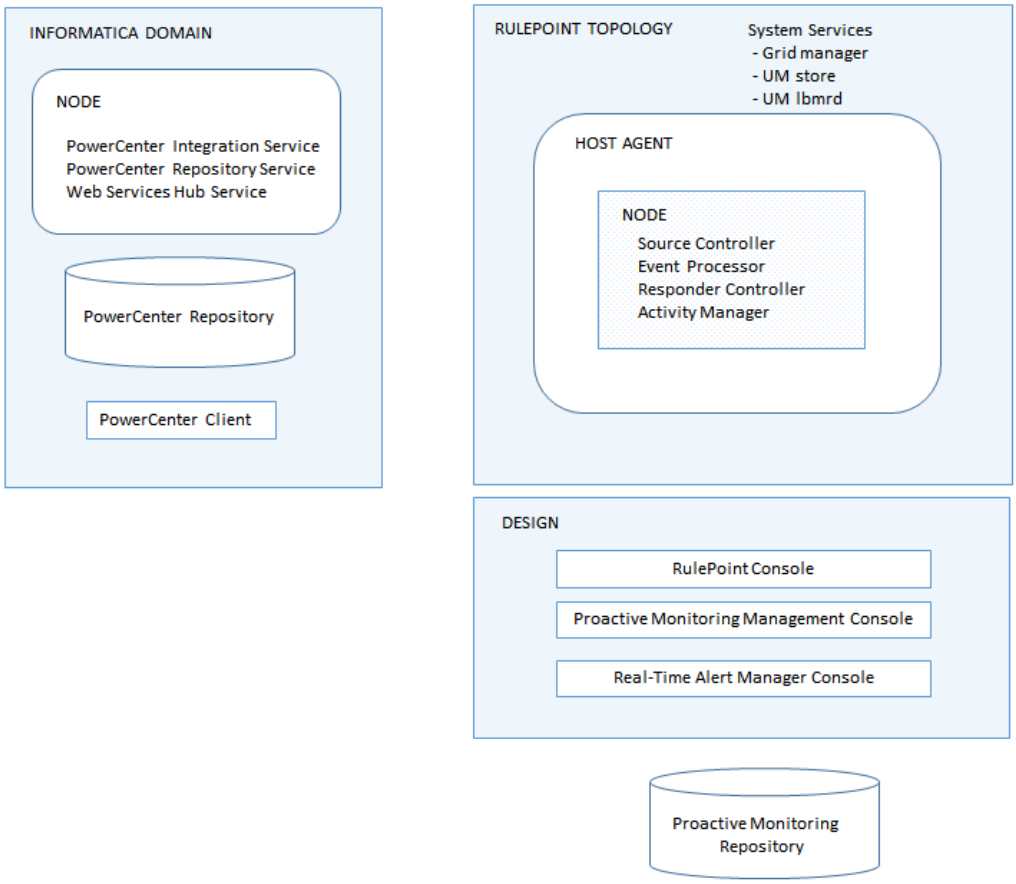
You can use the Reports dashboard in the Proactive Monitoring solution to get information about the health of the monitored services and a summary of deviations that occur over a period of time. Use the Manage Objects tab to manage objects configured for monitoring PowerCenter. You can manage rules, sources, folders, watchlists, and topics. You can also view the monitored events and activations.

Solution Components

The Proactive Monitoring solution monitors both large and small PowerCenter domain configurations.

The Proactive Monitoring solution requires the infrastructure for continuous data collection, continuous processing, analysis, and continuous alerting. Informatica RulePoint provides such an infrastructure and programming model.

The following image shows the Proactive Monitoring for PowerCenter Governance components:



Informatica RulePoint

Informatica RulePoint is a general purpose Complex Event Processing server. You can build an application on RulePoint to process large amounts of data in real time, detect anomalies, and take action. Informatica RulePoint provides a programming model to build such applications.

The RulePoint programming model consists of the following primary objects:

- Sources. Sources connect to external systems to fetch data. The sources convert the fetched data into events. The events are published on topics.
- Rules. Rules process events on topics. You can use the rule processing language, DRQL to create rules. The rule definition includes information about the topics and the number of events you want RulePoint to process, the conditions to check, and the response to generate when there is a deviation. As part of overall rule processing, the rule might call out functions called analytics. Rules also rely on watchlists that act as reference data sets during rule processing.
  RulePoint also provides an easy way to create rules using templates. Templates are abstract rules that could become a rule when you provide all its parameters.
- Responders. Responders dispatch alerts to external systems. When a rule condition is matched, the rule processing engine creates a response that is sent to the specified external system using a conduit called responder.

RulePoint consists of the following supporting objects that you reference in the primary objects:

- Topics. Logically group events into a group. A topic describes the types and properties of events coming into the system.
- Connections. Connect RulePoint objects, such as sources, analytics, and responders to the target database.
- Response. Define how you want RulePoint to respond if the event matches the conditions defined in the rule.
- Analytics. Analyze data within a system and implements a data processing function.
- Watchlists. Contain the items that you store as a single object with a unique name that you define. The rule uses this name so that it can use the data stored in the object.
- Templates. Enable users to easily create new rules. A template includes a rule statement that contains substitution parameters and instructional text to define those parameters.

For more information about the objects, see the *RulePoint User Guide*.

Proactive Monitoring for PowerCenter ships with a set of sources, topics, rules, templates, analytics, watchlists, and responders that are specific for the governance monitoring of PowerCenter.

Object States

Objects are in Draft state when you create the objects, you never deploy the objects, or when you undeploy objects. You need to deploy the objects to the application services for rule processing to begin. In the default topology, when you deploy the objects, the grid manager deploys the sources along with the supporting objects to the source controller, responders and supporting objects to the responder controller, and rules and supporting objects to the event processor. When you successfully deploy the primary objects and their supporting objects, the objects are in Deployed state. After you deploy the objects, the source controller begins to fetch events, the rule processor processes events, and the responder controller dispatches alerts.

If you need to change the object properties, undeploy the objects. When you undeploy primary objects, all secondary objects associated with the primary objects are also undeployed. After a successful undeploy, the state of the objects changes to Draft. After you complete the changes, you can deploy the objects again. When you edit and save the objects, the state of the objects changes to Needs_Deployment state. You need to deploy the objects again. For more information about deployment and the state of RulePoint objects, see the "Managing Deployment" chapter in the *RulePoint Administrator Guide* .

You can configure the application and system services in RulePoint for high availability, and reassign objects across the configured application services for processing. For more information, see the "High Availability" chapter in the *RulePoint Administrator Guide*.

Informatica Real-Time Alert Manager

Informatica Real-Time Alert Manager (RTAM) is a web-based dashboard to receive alerts from RulePoint.

You can group the RTAM alerts as channels. Each alert has a priority, subject, and body. RulePoint includes a standard RTAM responder to send alerts to RTAM.

The Proactive Monitoring solution provides two standard modes of alert delivery, through email and RTAM. You can configure the solution to get alerts through email, RTAM, or both. In case of RTAM, you can log in to the RTAM web application and see the alerts on-demand.

Proactive Monitoring Repository

The Proactive Monitoring repository stores all the solution metadata, solution configuration data, and the data collected from PowerCenter repository databases. The repository is also used to store the history of alerts generated by the solution.

The solution includes a set of analytics that use the Proactive Monitoring repository as part of rule processing.

Proactive Monitoring for PowerCenter Management Console

Proactive Monitoring for PowerCenter Management Console is a web-based application for configuring the Proactive Monitoring solution.

The Management Console allows users to add details of hosts, nodes, grids, files, folders, and PowerCenter Repository Service for monitoring purposes. The Management Console allows user to change the monitoring solution settings and the mode of alert delivery, whether to use email or RTAM.

You can use the Management Console to manage the monitored folder lists, topics, sources, watchlists, and rules. You can deploy, undeploy, or redeploy PMPC SQL source services and rules, edit topics, and view the statistics of a rule activation. Use the Reports dashboard to view the health of the services and to get information on the alerts that occur over a period of time.

Solution Usage

Proactive Monitoring for PowerCenter connects to the PowerCenter environment with minimum configuration requirements.

The following steps provide an overview of the solution usage:

Installation

Install Proactive Monitoring for PowerCenter on a machine that is separate from the host machines in the PowerCenter domain.

The solution objects connect to the PowerCenter repository to gather metadata of all the objects that the developers modifies. To fetch data from the tables and views in the PowerCenter repository, the solution requires creation of a read-only user with specific privileges.

See the Installation chapters for pre-requisites and detailed installation instructions.

Configuration and customization

The solution needs to connect to specific services in the PowerCenter domain to start monitoring the domain. This involves configuring the solution through Proactive Monitoring for PowerCenter Management Console.

When the solution is online, you can customize and extend built-in rules to enhance the monitoring capabilities based on the business needs.

See the installation and configuration chapters for detailed instructions on the post-installation configuration steps.

Receiving alerts

The solution can be configured to send email alerts and RTAM alerts to the personas defined in the solution, namely pcadmin, pcmonitor, dataarchitect, apparchitect, itsecurity. Each of these personas can have an associated RTAM login or email ID. In case of email, the user will start receiving email alerts as and when anomalies are detected by the solution. In case of RTAM, the user needs to login to the RTAM web application to check the alerts on demand. You can also configure the PMPC solution to send alerts as SNMP traps. The Proactive Monitoring solution supports SNMP v2.

Viewing Reports

You can use the Reports dashboard to get information about the health of the monitored services, hosts, and nodes in a PowerCenter domain. View the best practice violations that occur over a period of time and drill down into the alert details from the Reports dashboard. Use the on demand reports to generate reports for workflow, session, or transformation attributes.

Managing Objects

You can use the Manage Objects tab to manage watchlists, SQL sources, rules, and topics. You can view the events generated for a source and the activations for a rule.

CHAPTER 2

Monitoring PowerCenter Governance

This chapter includes the following topics:

- Overview, 15
- Proactive Monitoring Objects, 15
- Proactive Monitoring Rules, 17

Overview

The Proactive Monitoring solution retrieves modified objects information from the PowerCenter repository database at regular intervals to provide the benefit of continuous governance monitoring.

The Proactive Monitoring solution includes various sources, analytics, and responders that connect to PowerCenter services and nodes to collect and process the above data.

Proactive Monitoring Objects

Proactive monitoring includes a set of pre-defined objects that connect to PowerCenter services in order to drive rule processing and alerting. In the RulePoint programming model, the objects that connect to external systems are broadly classified as sources, analytics, responders, and responses. These objects are configurable and can link to other systems, such as email, Real-Time Alert Manager, or a database.

These predefined objects have the following function:

- Sources gather information from a system.
- Analytics analyze data within a system.
- Responders execute a response through a system.
- Responses are where you define how you want RulePoint to respond if your event matches the rule condition.

Sources

The Proactive Monitoring sources connect to PowerCenter services, collect data, and turn this data into events for rule processing.

The sources run against the respective PowerCenter services at a predefined interval and collect incremental data changes. For example, a query to retrieve modified workflows information from the PowerCenter repository runs every six hours. The query selects the modified workflows in the six hours by using the timestamp from the previous run.

The Proactive Monitoring solution contains the following predefined sources:

PMPC SQL Source

The PMPC SQL Source is a custom built SQL source for the Proactive Monitoring solution. The source can connect to multiple repository databases and run SQL queries in parallel. In addition, the PMPC SQL source includes queries relevant for the database types, Oracle, IBM DB2, and Microsoft SQL Server.

All PMPC SQL related services use the repository configuration provided through the Proactive Monitoring for PowerCenter Management Console to connect to the PowerCenter repository databases.

The solution includes multiple instances of PMPC SQL Source that run predefined SQL queries against the configured PowerCenter repository databases at regular intervals. The PMPC SQL Sources run the SQL queries to create events and publish these events on the following predefined topics:

- pc_command_tasks
- pc_mappings
- pc_mapplets
- pc_sessions
- pc_transforms
- pc_workflows
- pc_worklets

For example, *PowerCenter Workflows Modified Incremental* is the PMPC SQL Source that connects to the PowerCenter repository, retrieves information about workflows changed in the last six hours, and publishes them as events on the pc_workflows topic.

The solution also includes instances of other predefined RulePoint source types to manage solution specific internal data, such as cache and purge management.

Analytics

The solution contains predefined SQL analytics that are used in rules.

As part of rule processing, the analytics run predefined queries against the Proactive Monitoring repository database or the configured PowerCenter repositories on demand.

For example, the SQL Analytic, pc_get_session_attribute, gets value of a specific attribute name for a session. The SQL Analytic, pc_get_email, gets the email address for a specified alert recipient from the Proactive monitoring repository.

Responders

The solution contains predefined responders that dispatch alerts to external systems.

The Proactive Monitoring solution includes the following responders:

- The email responder sends email alerts to the various personas.
- The RTAM responder sends RTAM alerts to the various personas.
- The SNMPv2 responder sends SNMP traps to the network manager that you configure to receive traps.

Proactive Monitoring Rules

The Proactive Monitoring solution contains a set of predefined rules and rule templates that detect anomalies within the PowerCenter environment.

Types of Rules

The predefined rules are categorized based on the types of checks that they perform.

You can use the following types of predefined rules to monitor PowerCenter governance:

Best practice violations

Best practices are methodical guidelines to get better run-time performance from PowerCenter in addition to better maintainable objects. Proactive enforcement of best practices helps in improving overall efficiency of development, testing, and production phases of a PowerCenter deployment. Proactive monitoring solutions continuously monitor PowerCenter object changes to look for deviations from the best practices. For example, the solution has a rule to verify whether you have set the truncate table option in a session or whether all objects have descriptions.

Duplicate objects

You might copy the objects across folders for modifications and possibly leave them with same names. Duplicate objects across folders may cause erroneous usage and impact the production runs. The solution continuously monitors for duplicate objects across repository and alerts application architects when it finds a duplicate objects.

Objects that are not valid

The Proactive Monitoring solution checks for workflows, sessions, and mappings that are not valid, and alerts the users. Proactive alerts enables the application architects to know about the objects that are not valid and to take corrective action.

Naming convention violations

An organization can define naming conventions for PowerCenter objects. You can customize the Proactive Monitoring solution to detect violations in naming conventions and alert the application architects. This enables organizations to audit compliancy of the guidelines and take appropriate action.

Disabled objects

The Proactive Monitoring solution checks for disabled sessions and alerts users. Proactive alerts on disabled objects enable application architects to take appropriate action.

Hardcoded values in objects

Hardcoded values may cause run-time errors as objects move from one environment to another, such as between development to staging and from staging to production. Early detection of hardcoded value

prevents errors and saves time in migrating objects between environments. The Proactive Monitoring solution looks for hardcoded source parameters, paths in sessions and workflows, and alerts users when it detects an anomaly.

Illegal values in objects

A special case of hardcoded values check is the check for illegal values. The Proactive Monitoring solution looks for specified commands that you cannot use in the objects and alerts application architects when it detects any deviation.

Frequent changes to objects

Frequent changes to objects may not be allowed in certain PowerCenter deployments because of the impact they may cause to other objects in the repository. The solution allows the users to check whether a session has been modified too frequently in a specific period of time and alert.

Attribute checks for objects

You can specify multiple attribute to each PowerCenter object. The Proactive Monitoring solution allows you to check for specific attributes on workflows, sessions, and transformations. When it detects a deviation from the defined norm, the Proactive Monitoring solution sends you an alert.

Templates

The Proactive Monitoring solution provides predefined rule templates that include built-in checks and customizable parameters.

Templates enable users to leverage the base logic and customize it for many use cases. For example, a template that checks whether a mapping is modified too often in a specific duration includes all the predefined conditions to detect the violation. The template also allows the user to specify the number of times that object changed and the duration to trigger an alert.

You can create template rules from templates. The solution includes a set of template rules to illustrate their usage and behavior.

The template, *PC_GMT2 Mapping modified often within a specified duration*, has built-in checks to detect if a mapping is modified often. You can customize the number of changes and the duration of the check.

Advanced Rules

Advanced rules do not provide any parameterization.

For example, a rule that checks for duplicate mappings may not require any parameterization. The Proactive Monitoring solution provides many advanced rules.

CHAPTER 3

Manage Objects

This chapter includes the following topics:

- Manage Objects Overview, 19
- Managing PMPC SQL Source Services, 21
- Monitored Event Management, 22
- Monitored Objects Management, 22
- Managing Templates Rules, 27

Manage Objects Overview

You can manage the monitored topics, watchlists, sources, and rules from the **Manage Objects** tab.

Perform the following tasks from the **Manage Objects** tab:

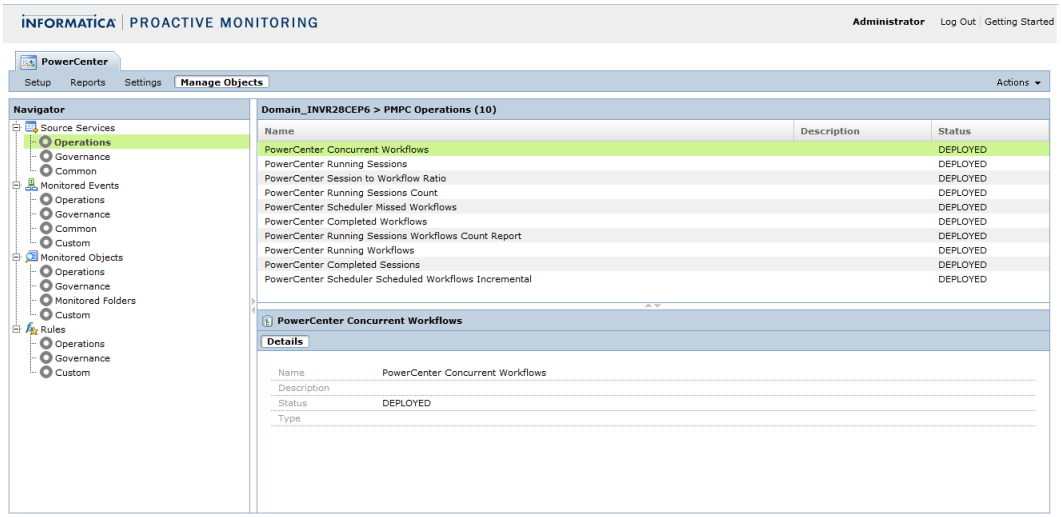
- Manage the PowerCenter folders that you monitor from the PowerCenter Monitored Folders watchlist. You can add a folder that you want to monitor to the PowerCenter Monitored Folders watchlist or remove a folder that you do not want to monitor from the PowerCenter Monitored Folders watchlist.
- Deploy, undeploy, or redeploy the PMPC SQL source services.
- View the statistics of events generated for a topic, including the event count and the deployment details.
- View and edit watchlists
- View the activation count, status, and details of a rule. You can also view the statistics along with the number of activations for a selected timeline.
- Create, edit, copy, deploy, undeploy, redeploy, edit, or delete template rules.

For more information on the state of objects and deployment related actions, see the "Deployment Overview" chapter in the *RulePoint Administrator Guide*.

Manage Objects View

In the **Manage Objects** tab, you can manage the source services, topics, watchlists, and rules.

The following figure shows the **Manage Objects** tab:



The **Manage Objects** tab has the following components:

Navigator

Appears in the left pane of the **Manage Objects** tab. The Navigator displays the following entities that you can monitor from the Proactive Monitoring for PowerCenter Management Console:

- PMPC source services. Deploy or undeploy source services from the Proactive Monitoring for PowerCenter Management Console.
- Monitored events. View the statistics of generated events.
- Monitored objects. View the monitored folders where you can manage the list of PowerCenter folders to monitor. You can also manage watchlists.
- PMPC rules. Manage template rules.

Contents panel

Appears in the right pane of the **Manage Objects** tab and displays information about monitored events, objects, rules, folders, and source service that you select in the Navigator.

Actions menu

When you select a source service in the contents panel, you can deploy, undeploy, or redeploy a source service.

When you select monitored events in the contents panel, you can view the event count and status of the topic. You can also view the events arrived for a the associated source for a selected timeline.

When you select monitored objects in the contents panel, you can edit that object. You can also deploy, undeploy, or redeploy the object. When you select monitored folders, you can add or remove the monitored folders.

When you select a template rule, you can create, edit, copy, delete, deploy, undeploy, or redeploy template rules. You can also view the statistics of a rule activation, including the status of the rule and the rule details.

Managing PMPC SQL Source Services

You can use the PMPC SQL source service to connect to a database and run SQL queries or commands to create RulePoint events. You can deploy, undeploy, or redeploy PMPC SQL source services from the Proactive Monitoring for PowerCenter Management Console.

The PMPC SQL source is a custom built SQL source for the proactive monitoring solution. You can manage PMPC SQL source services from the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console.

Note: To manage other SQL source services, use RulePoint.

Deploying, Undeploying, or Redeploying SQL Source Services

Use the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console to deploy, undeploy, or redeploy Proactive Monitoring for PowerCenter source services.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select the **Operations**, **Governance**, or **Common** source service.

   The **Operations** source service lists the predefined source services that are available by default after you install Proactive Monitoring for PowerCenter Operations. The **Governance** source service lists the predefined source services that are available by default after you install Proactive Monitoring for PowerCenter Governance. The **Common** source service lists the predefined source services that are common to both Operations and Governance.

   Based on the source service that you select in the Navigator, the list of predefined source services along with the description and status information appear in the contents panel. You can view the details of the source service from the **Details** view in the contents panel.
3. To deploy a source service, perform the following tasks:
   a. Select the source service, and click **Deploy** on the **Actions** menu.

      You can deploy an object that is in the Drafts state.

      A message appears that indicates that the source is deployed successfully.
   b. Click **OK**.

      The status of the source service changes from Draft to Deployed.
4. To undeploy a source service, perform the following tasks:
   a. Select the source service, and click **Undeploy** on the **Actions** menu.

      You can undeploy a source that is in the Deployed or Needs_Deployment state.

      A message appears that indicates that the source is undeployed successfully.
   b. Click **OK**.

      The status of the source service changes from Deployed to Draft.
5. To redeploy a source service, perform the following tasks:
   a. Select the source service, and click **Redeploy** on the **Actions** menu.

      You can redeploy a source when you edit a deployed source. The state of the source changes from Deployed to Needs_Deployment.

      A message appears that indicates that the source is redeployed successfully.
   b. Click **OK**.

      The status of the source service changes from Needs_Deployed to Deployed.

For more information about object states and deployment, see *RulePoint Administrator Guide*.

Monitored Event Management

The Monitored Events view contains the list of monitored topics for PowerCenter and the events generated for a source. You can view the monitored Proactive Monitoring for PowerCenter topics from the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console.

You can view the statistics only when the topics and the associated objects are deployed. You might not be able to view the event statistics for a source if you have deployed only the topic and not the source associated with the topic. You also cannot view statistics for topics that do not have an associated source and are system generated.

Viewing Topics

View all the monitored topics, the events generated for each of the objects, and the status of the topics in the Management Console.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select the **Operations**, **Governance**, **Common**, or **Custom** topics.

Option	Description
Operations	Lists the predefined topics that are available by default after you install Proactive Monitoring for PowerCenter Operations.
Common	Lists the predefined topics that are common to both Operations and Governance.
Custom	Lists the topics that you create in RulePoint.

   Based on the topic that you select in the Navigator, the list of topics along with the description and status information display in the contents panel. Proactive Monitoring for PowerCenter takes some time to fetch the data and display the list of monitored events. You can view the details of the topic you select from the **Details** view in the contents panel.
3. To view the statistics of the events generated for a source associated with the selected topic, perform the following steps:
   a. Select the topic, and then select **Stats** from the **Actions** menu.
   b. Select a timeline to view the events generated for that period.

   The graph lists the statistics of the events, including the number of events generated for the source. Hover the mouse over the graph to view the activation for a particular period.
4. Click **Cancel** to exit from the view.

Monitored Objects Management

You can view and manage the watchlists and the monitored folders from the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console.

Viewing and Editing Watchlists

Use the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console to view or edit the watchlists. When you edit a watchlist and save it, that watchlist along with the referenced primary objects is also deployed.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select the **Operations**, **Governance**, **Common**, or **Custom** watchlist.

   The **Operations** watchlist lists the predefined watchlists that are available by default after you install Proactive Monitoring for PowerCenter Operations. The **Governance** watchlist lists the predefined topics that are available by default after you install Proactive Monitoring for PowerCenter Governance. The **Common** watchlist lists the predefined watchlists that are common to both Operations and Governance. The **Custom** watchlist lists the watchlists that you create.

   Based on the watchlist that you select in the Navigator, the list of predefined watchlists along with the name and status information appear in the contents panel. The details panel displays the details of the selected watchlist.
3. To edit a watchlist, select the watchlist, and then select **Edit** from the **Actions** menu.
4. In the **Content** field, edit the existing values or add additional values in a new line for the list **Type**.
5. Click **Save**.

   The watchlist along with the supporting objects is also deployed. The state of the object changes to Deployed.

Monitored Folder Management

PowerCenter Monitored Folders is a predefined watchlist that contains the list of PowerCenter folders to monitor. You can manage the monitored folders from the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console.

You manage the list of PowerCenter folders that you monitor by adding or removing folders from the list.

To receive notifications add your folder names to this watchlist. If the folder is same for multiple PowerCenter repositories, you receive notification for all configured repositories.

Adding or Removing Folders from Monitored Folders

You can add or remove folders to the predefined list of PowerCenter folders that you monitor.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Monitored Objects** and then click **Monitored Folders**.

   The list of folders that you monitor appears in the contents panel.
3. On the **Actions** menu, click **Add/Remove**.

   The **Add/Remove Monitored Folders** screen appears.
4. To add a folder or folders to the list of monitored folders, select and move the folder from the **All Folders** section to the **Monitored Folders** section.
   a. Select a Repository Service to display the folders in the repository. You can enter a folder name and use the **Filter** button to filter the folders based on the folder name.
   b. Select the folder that you want to add to the list of monitored folders. You can select multiple folders at the same time. To select all the folders of a repository service, double-click on the repository service.

c. To add the folder that you select to the list of monitored folders, click the **>>** button.

The folder name appears in the **Monitored Folders** section.

5. To remove a folder or folders from the list of monitored folders, select and move the folder from the **Monitored Folders** section to the **All Folders** section.
   a. Select a Repository Service to display the folders in the repository that you monitor. You can enter a folder name and use the **Filter** button to filter the folders based on the folder name.
   b. Select the folder that you want to remove from the list of monitored folders. You can select multiple folders at the same time. To select all the folders of a repository service, double-click on the repository service.
   c. To remove the folder from the list of monitored folders, click the **<<** button.

      The folder name appears in the All Folders section.
6. Click **Save** to save the changes that you made to the monitored folders list.

   A message appears that the Monitored Folders are updated successfully. You need to update the runtime with the changes.
7. To update the runtime with the changes, select **Update Runtime** from the **Actions** menu.

   A message appears that indicates that the runtime update will take a few minutes.
8. Click **OK**.

   A message appears that the runtime is successfully updated.

Monitor Files and Directories on a Node

The following scenarios explain how you can set the criteria in Proactive Monitoring for PowerCenter to monitor a file or folder in PowerCenter and alert you appropriately.

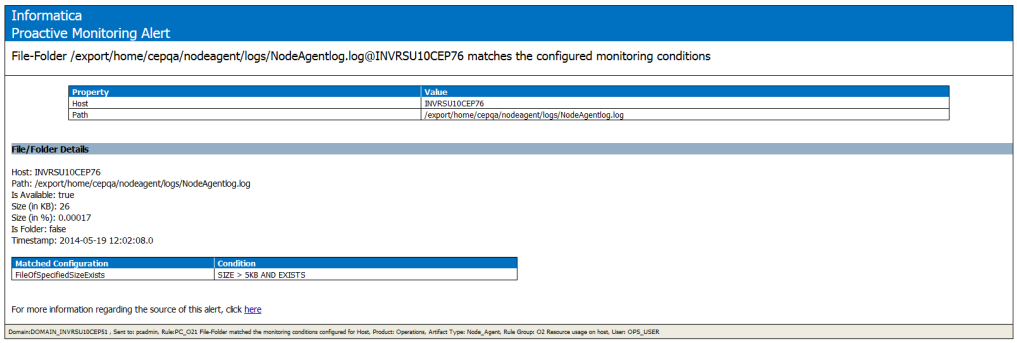
Example - Monitor File Size

You want to monitor if a file of a specified size exists on the PowerCenter host. For example, you want to monitor the workflow logs folder, `INFA_HOME/server/infa_shared/WorkflowLogs`. You need to monitor if a specific file, `wf_pmpc_reports.log.RUNINSTANCE3.5230.20140514121201.bin`, exists within this folder. You also want to check if the log file exceeds the specified threshold limit.

1. Select the host whose file you want to monitor, and provide the criteria in the **Add Monitored Path** page.
2. Provide a valid configuration name for the monitoring criteria.
3. Enter the path of the file that you want to monitor.
4. Select the **Path Type** as **File**, and choose the criteria based on which you want to monitor the file:
   a. Select **size > than 5 KB**.
   b. Select **Path Exits**.

5. Click **Save**.

   The following image shows the alert in RTAM when the rule activates:


Informatica
Proactive Monitoring Alert

File-Folder /export/home/cepqa/nodeagent/logs/NodeAgentlog.log@INVRSU10CEP76 matches the configured monitoring conditions

Property	Value
Host	INVRSU10CEP76
Path	/export/home/cepqa/nodeagent/logs/NodeAgentlog.log

File/Folder Details

Host: INVRSU10CEP76
Path: /export/home/cepqa/nodeagent/logs/NodeAgentlog.log
Is Available: true
Size (in KB): 26
Size (in %): 0.00017
Is Folder: false
Timestamp: 2014-05-19 12:02:08.0

Matched Configuration	Condition
FileOfSpecified5izeExists	SIZE > 5KB AND EXISTS

For more information regarding the source of this alert, click here

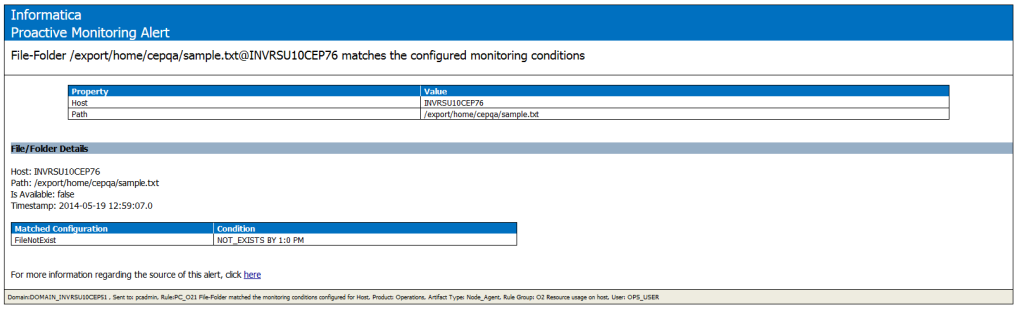
Domain:DOMAIN_INVRSU10CEPS1 , Sent to: pcadmin, Rule:PC_O21 File-Folder matched the monitoring conditions configured for Host. Product: Operations. Artifact Type: Node_Agent. Rule Group: O2 Resource usage on host. User: OPS_USER

Example - Monitor Removal of a File

You run a workflow that involves a command task to delete a specific file. You want an alert when the file is removed in the host by a specified time.

1. Select the host whose file you want to monitor, and provide the criteria in the **Add Monitored Path** page.
2. Provide a valid configuration name for the monitoring criteria.
3. Enter the path of the file that you want to monitor.
4. Select the **Path Type** as **File**, and choose the criteria **Path does not exist**.
5. Select **Time Filter**, and then select the condition **BY 1:00 PM**.
6. Click **Save**.

   The following image shows the alert in RTAM when the rule activates:


Informatica
Proactive Monitoring Alert

File-Folder /export/home/cepqa/sample.txt@INVRSU10CEP76 matches the configured monitoring conditions

Property	Value
Host	INVRSU10CEP76
Path	/export/home/cepqa/sample.txt

File/Folder Details

Host: INVRSU10CEP76
Path: /export/home/cepqa/sample.txt
Is Available: false
Timestamp: 2014-05-19 12:59:07.0

Matched Configuration	Condition
FileNotExist	NOT_EXISTS BY 1:0 PM

For more information regarding the source of this alert, click here

Domain:DOMAIN_INVRSU10CEPS1 , Sent to: pcadmin, Rule:PC_O21 File-Folder matched the monitoring conditions configured for Host. Product: Operations. Artifact Type: Node_Agent. Rule Group: O2 Resource usage on host. User: OPS_USER

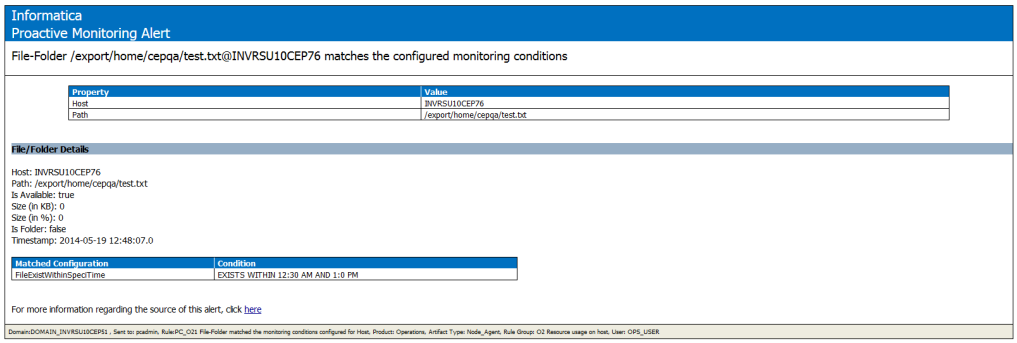
Example - Monitor Creation of a File

You want to monitor if a file exists at a specified time on the PowerCenter host. When you expect to run a workflow at a specified time interval, you want an alert after the log file for that workflow execution is created.

1. Select the host whose file you want to monitor, and provide the criteria in the **Add Monitored Path** page.
2. Provide a valid configuration name for the monitoring criteria.
3. Enter the path of the file that you want to monitor.
4. Select the **Path Type** as **File**, and select the criteria **Path exists**.
5. Select **Time Filter**, and then select the condition **WITHIN 12:30 PM AND 1:00 PM**.

6. Click **Save**.

   The following image shows the alert in RTAM when the rule activates:


Informatica
Proactive Monitoring Alert

File-Folder /export/home/cepqa/test.txt@INVRSU10CEP76 matches the configured monitoring conditions

Property	Value
Host	INVRSU10CEP76
Path	/export/home/cepqa/test.txt

File/Folder Details

Host: INVRSU10CEP76
Path: /export/home/cepqa/test.txt
Is Available: true
Size (in KB): 0
Size (in %): 0
Is Folder: false
Timestamp: 2014-05-19 12:48:07.0

Matched Configuration	Condition
FileExistWithinSpecTime	EXISTS WITHIN 12:30 AM AND 1:0 PM

For more information regarding the source of this alert, click here

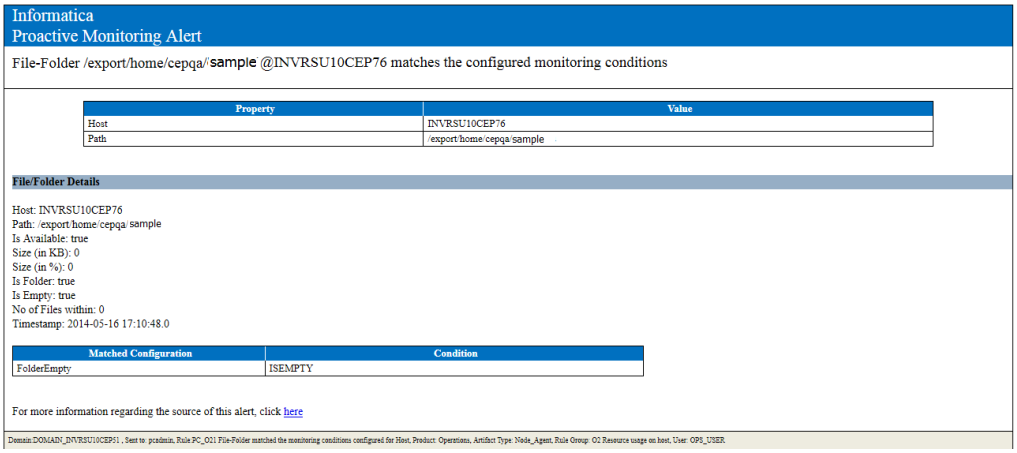
Domain:DOMAIN_INVRSU10CEP51 , Sent to: pcadmin, Rule:PC_O21 File-Folder matched the monitoring conditions configured for Host, Product: Operations, Artifact Type: Node_Agent, Rule Group: O2 Resource usage on host, User: OPS_USER

Example - Monitor Empty Paths

You want to verify that the workflow logs directory does not have content.

1. Select the host whose file you want to monitor, and provide the criteria in the **Add Monitored Path** page.
2. Provide a valid configuration name for the monitoring criteria.
3. Enter the path of the folder that you want to monitor.
4. Select the **Path Type** as **Folder**, and choose the criteria **Is Path Empty**.
5. Click **Save**.

   The following image shows the alert in RTAM when the rule activates:


Informatica
Proactive Monitoring Alert

File-Folder /export/home/cepqa/sample @INVRSU10CEP76 matches the configured monitoring conditions

Property	Value
Host	INVRSU10CEP76
Path	/export/home/cepqa/sample

File/Folder Details

Host: INVRSU10CEP76
Path: /export/home/cepqa/sample
Is Available: true
Size (in KB): 0
Size (in %): 0
Is Folder: true
Is Empty: true
No of Files within: 0
Timestamp: 2014-05-16 17:10:48.0

Matched Configuration	Condition
FolderEmpty	ISEMPTY

For more information regarding the source of this alert, click here

Domain:DOMAIN_INVRSU10CEP51 , Sent to: pcadmin, Rule:PC_O21 File-Folder matched the monitoring conditions configured for Host, Product: Operations, Artifact Type: Node_Agent, Rule Group: O2 Resource usage on host, User: OPS_USER

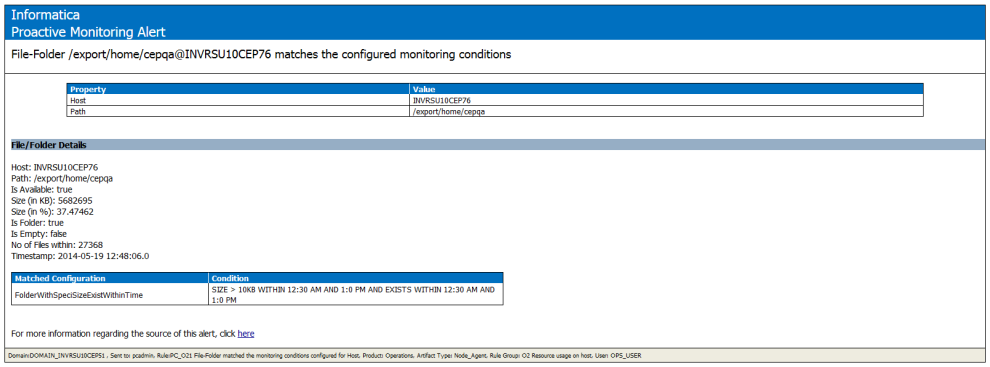
Example - Monitor Directory Size Within Time Period

You want to monitor the size of the workflow logs folder and receive an alert when the folder size exceeds a specified threshold within a specific time interval. You might want to do this because you want to trigger a script to archive the logs.

1. Select the host whose file you want to monitor, and provide the criteria in the **Add Monitored Path** page.
2. Provide a valid configuration name for the monitoring criteria.
3. Enter the path of the file that you want to monitor.

4. Select the **Path Type** as **Folder**, and select the following criteria:
   a. Select **Size > than 10 KB**.
   b. Select **Path exists**.
5. Select **Time Filter**, and then select the condition **WITHIN 12:30 AM AND 1:00 PM**.
6. Click **Save**.

   The following image shows the alert in RTAM when the rule activates:



Managing Templates Rules

You can view and manage the Proactive Monitoring for PowerCenter template rules from the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console.

The predefined template rules are available by default after you install Proactive Monitoring for PowerCenter Operations or Governance. You can also view the rules that you create other than the available predefined rules under **Custom Monitored Objects**. The contents panel lists the template rules, the activation count, and the status of the monitored rule. You can view the details of the template rule from the **Details** view in the contents panel.

Creating a Template Rule

Use the **Manage Objects** tab in the Proactive Monitoring for PowerCenter Management Console to create a template rule.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Operations**, **Governance**, or **Custom**.
3. To create a template, select **New** from the **Actions** menu.

   The Template Rule dialog box appears listing the name of the template, the description, and the rule count.
4. Select the template, and then click **Next**.
5. Enter a name for the template rule.
6. Optionally, enter a description for the template rule.
7. In the **Template Parameters** section, provide the properties.
8. Click **Save**.

Editing a Template Rule

When you edit and save a template rule, the template rule is deployed along with the supporting objects that are referenced in the template rule.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Operations**, **Governance**, or **Custom**.
3. To edit a template, select **Edit** from the **Actions** menu.
4. Edit the template parameters.
5. Click **Save**.

Copying a Template Rule

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Operations**, **Governance**, or **Custom**.
3. To copy a template rule, select the rule, and then select **Copy** from the **Actions** menu.
4. Enter the name of the template you want to create as a copy.
5. Click **Save**.

Deleting a Template Rule

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Operations**, **Governance**, or **Custom**.
3. To delete a template, select the template, and then select **Delete** from the **Actions** menu.

   Note: You cannot delete a template rule that is in Deployed state.
4. Click **OK**.

Deploying, Undeploying, and Redeploying Rules

You can deploy, undeploy, or redeploy rules.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Operations**, **Governance**, or **Custom**.
3. To deploy a template, perform the following tasks:
   a. Select the draft rule that you want to deploy, and then select **Deploy** from the **Actions** menu.

      A message appears that indicates successful deployment. To view the details of the message, click **Details**.
   b. Click **OK**.

      The status of the rule changes from Draft to Deployed.
4. To undeploy a template, perform the following tasks:
   a. Select the deployed rule that you want to undeploy, and then select **Undeploy** from the **Actions** menu.

      A message appears that indicates successful undeployment. To view the details of the message, click **Details**.

b. Click **OK**.

The status of the rule changes from Deployed to Draft.

5. To redeploy a template, perform the following tasks:

a. Select the rule that you want to undeploy, and then select **Redeploy** from the **Actions** menu.

Note: The rule must be in the Needs_Deployment state if you want to redeploy the rule. The rule is in Needs_Deployment when you edit a rule that is in Deployed status.

A message appears that indicates successful redeployment. To view the details of the message, click **Details**.

b. Click **OK**.

The status of the rule changes from Needs_Deployment to Deployed.

For more information on object states and deployment, see *RulePoint Administrator Guide*.

Viewing the Statistics of a Rule Activation

You can view the statistics for a deployed rule. Set a timeline to view the rule activations for that period.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Manage Objects** tab.
2. In the Navigator, select **Operations**, **Governance**, or **Custom**.
3. Select the template rule, and then select **Stats** from the **Actions** menu.
4. Select the timeline to view the statistics of a rule activation for the set timeline.

You can select a timeline between 5 minutes and 24 hours.

The graph lists the statistics of the rule activation, including the number of activations generated for the rule. Hover the mouse over the graph to view the activation for a particular period.

CHAPTER 4

Proactive Monitoring Reports

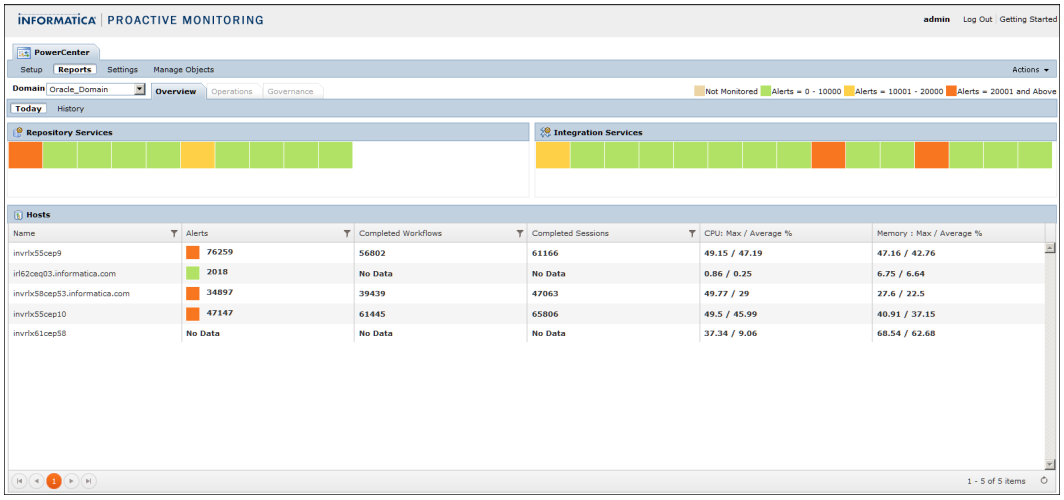
This chapter includes the following topics:

- Proactive Monitoring Reports Overview, 30
- Monitoring Application Services and Hosts in the Domain, 31
- Monitoring PowerCenter Operation Alerts, 33
- Monitoring PowerCenter Governance Alerts, 35

Proactive Monitoring Reports Overview

Use the Proactive Monitoring reports to monitor the Repository Services, Integration Services, and hosts within a single Informatica domain. You can use the Proactive Monitoring reports to analyze and view the current as well as past alerts. You can correlate resource usage on hosts and troubleshoot.

The following image shows the Reports tab in the Proactive Monitoring for PowerCenter Management Console:



You can configure the Reports dashboard to monitor the status of the application services and hosts in a domain. View the best practice violations, execution failures, and node agent alerts that occur over a period of time from the Reports dashboard. Use the on-demand reports to generate reports for workflow, session, or transformation attributes.

You can use the following tabs available in the **Reports** tab to monitor the PowerCenter alerts .

Overview

Monitor the alerts for Repository Services, Integration Services, and hosts in a domain from the **Overview** tab.

Operations

Monitor the PowerCenter execution failures and node agent alerts from the **Operations** tab. You can view the total number of alerts, alerts for a time period, and details of the execution failures and node agent alerts from the **Operations** tab. You can also export the alerts for the current day or for a specified period to a .csv file or an .xlsx file.

Governance

Monitor the violations in the PowerCenter development environment from the **Governance** tab. Generate on-demand reports for workflows, sessions, or transformations. You can view the total number of alerts and alerts for a time period from the **Governance** tab. ou can also export the alerts for the current day or for a specified period to a .csv file or an .xlsx file.

Reports Tab - Filter and Display Options

You can use the filter option to filter the details of the host statistics, execution failures, and best practice violations.

You can filter the values that appear in the contents panel of the **Reports** tab. To filter the details that appear for a column in the **Today** view or **History** view:

1. Click on the filter icon next to the column. The filter conditions appear based on the alert type, application service, or host.
2. Select the filter condition and enter the filter value.
3. Click the **Filter** button to filter the values based on the filter condition and value for that column. The filter icon on the column on which filter condition has been applied appears in orange color.
4. To clear the filter condition for a column, select the filter icon for that column and click the **Clear** button. You can also select "All Alerts" in the alerts table that appears in the **Total Alerts** section to display all the alerts and clear the filter condition.

You can use the **Maximize** icon to scroll to the alert details. To scroll to the alert details and hide the **Total Alerts** section in the **History** view, click the **Maximize** icon. To toggle back to the **Total Alerts** section, click the **Maximize** icon again.

You can also resize the width of the columns that appear in the contents panel to view the complete descriptions.

Monitoring Application Services and Hosts in the Domain

Monitor the status of the Repository Services, Integration Services, and hosts within a single Informatica domain from the **Overview** tab on the **Reports** tab. You can view the CPU, memory usage, running workflows, and running sessions statistics for all the hosts in the domain.

The contents that appear on the **Reports** tab vary based on the view that you select.

You can select the following views:

- **Today**. View the application services alerts and host statistics for the current day.
- **History**. View the application services alerts and host statistics for a particular time period.

In the Reports dashboard, the Repository Services and Integration Services appear in colors that indicate the number of alerts for each service. For example, if the number of alerts for a repository service is less that 50, then the repository service appears in green color. You can customize the alerts range for the colors in which the services appear.

Note: If application services run on multiple hosts for high availability or grid configurations, the alerts appear for the services on all the hosts and not just for the active hosts. In such cases, alert data appears even if application services are not running on the active hosts.

Monitoring Alerts for Application Services and Host Statistics for the Current Day

You can monitor the alerts for the application services and host statistics in the domain for the current day in the **Today** view on the **Overview** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Overview** tab and then click the **Today** view. The following sections appear in the Today view:
   Repository Services

   The Repository Services running in the domain appear in brown, green, yellow, or amber color in the **Repository Services** section based on the number of alerts for the Repository Services.

   Integration Services

   The Integration Services running in the domain appear in brown, green, yellow, or amber color in the **Integration Services** section based on the number of alerts for the Integration Services.

   Hosts

   The host name, alerts, number of running workflows and sessions, CPU and memory statistics appear in the **Hosts** section.

   Note: The CPU usage value is the total CPU usage divided by the number of cores. Memory usage is a percentage of the memory used by the process divided by the total memory available.
3. To view the past alerts for a application service, click the **History** link that appears in the tooltip for the application service.

Configuring Display Settings

In the Reports dashboard, the Repository Services and Integration Services appear in colors that indicate the health of the services. The health of the services is based on the number of alerts. You can configure the display settings for alerts in the **Today** view on the **Overview** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Overview** tab and then click the **Today** view.
3. In the **Actions** menu on the **Reports** tab, click **Display Settings**.

   The display color of the application services indicate the number of alerts for these services. Application services that you do not monitor appear in brown color.

   The **Settings** screen appears.

4. Specify the upper range of alerts for application services to appear in green and yellow color. For example, if you specify 200 as the upper range of alerts for green color, the application services appear in green color in the **Today** view till the number of alerts for that service exceed 200.
5. Click **Save**.

Monitoring the Alert History for Application Services and Hosts

You can monitor the alert history for a particular time period for PowerCenter application services and hosts in a domain.

You can select multiple Repository Services and Integration Services to monitor, but you can select only one host at a time to monitor.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Overview** tab and then click the **History** view.

   The **Total Alerts** and **Alerts for Period** sections appear in the contents panel. A graph that represents the alert history appears in the **Total Alerts** section.
3. Select the time period for which you want display the number of alerts.
   - To select the time period with the slider control, resize the width of slider control to indicate the time period or move the slider control over the time period.
   - To use predefined views to select the time period, click the **1 Day** view, **5 Day** view, **1 Month** view, **3 Months** view, **6 Months** view, or **Custom** view to display the number of alerts for the corresponding period.

   A graph that represents the number of alerts for the application service appears in the **Alerts for Period** section.
4. Select the application service or host for which you want to monitor the alerts.
   - To monitor the alerts for the Repository Service, click the **Repository Services** view and select the Repository Service from the list and then click **Ok**.
     You can select multiple Repository Services to monitor.
   - To monitor the alerts for the Integration Service, click the **Integration Services** view and select the Integration Service from the list and then click **Ok**.
     You can select multiple Integration Services to monitor.
   - To monitor the running sessions, running workflows, CPU statistics, and memory statistics of the host, click the **Host** view and then select the host from the list.

     Note: The CPU usage value is the total CPU usage divided by the number of cores. Memory usage is a percentage of the memory used by the process divided by the total memory available.

Monitoring PowerCenter Operation Alerts

You can monitor the execution failures in PowerCenter and view the alerts for the current day or for a time period.

The contents that appear on the **Operations** tab vary based on the view that you select.

You can select the following views:

- **Today**. View and export the PowerCenter operation alerts for the current day.
- **History**. View and export the PowerCenter operation alerts for a particular time period.

Monitoring the PowerCenter Operation Alerts for the Current Day

You can monitor the PowerCenter operation alerts for the current day in the **Today** view on the **Operations** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Operations** tab and then click the **Today** view. The following sections appear in the contents panel:

   Total Alerts

   The alert type, alert count, and percentage of the alert types appear in a graph and table format in the **Total Alerts** section.

   Execution Failures

   The alert details appear in the **Execution Failures** section.
3. To view the execution failures of a particular alert type, click on the corresponding alert type from the donut chart or table. The execution failures for the alert type that you select appear in the **Execution Failures** section.
4. To view detailed information of an alert that appears in the **Execution Failures** section, click the **View Details** button in **Details** column for that alert.

Monitoring the Alert History for PowerCenter Operations

You can monitor the total alerts for PowerCenter operations for a particular time period in the **History** view on the **Operations** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Operations** tab and then click the **History** view.

   The **Total Alerts**, **Alerts for Period**, and **Execution Failures** sections appear in the contents panel. A graph that represents the number of alerts over a period of time appears in the **Total Alerts** section.
3. Select the time period for which you want display the number of alerts.
   - To select the time period with the slider control, resize the width of slider control to indicate the time period or move the slider control over the time period.
   - To use pre-defined views to select the time period, click the **1 Day** view, **5 Day** view, **1 Month** view, **3 Months** view, **6 Months** view, or **Custom** view to display the number of alerts for the corresponding period.

   In addition to the pre-defined views, you can use the **Custom** view to create your own time period view.

   For the time period that you select in the **Total Alerts** section, a donut chart and a table that represent the alert count, alert type, and alert percentage appear in the **Alerts for Period** section.
4. Select an alert type that appears in the donut chart or table from the **Alerts for Period** section.

   For the alert type that you select in the **Alerts for Period** section, a graph that represents the number of alerts for a time period appears in the **Execution Failures** section.
5. To view detailed information of an alert that appears in the **Execution Failures** section, click the **View Details** button in **Details** column for that alert.

   The alert details appear in the **Alert Details** pane.

Export Alerts for PowerCenter Operations

You can export alerts for the current day or for a specified period to a standard comma-separated value (CSV) file or an excel (.xlsx) file. The exported file includes a snapshot of the alerts generated for the current

day or the alert history for a specified period. The report depicts the rule categories and the alert records. You can also choose to export the alert body.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Operations** tab, and choose if you want to export the alerts for the current day or the alert history.
   - To export alerts from the current day, click **Today** and then click the **Export** icon.
   - To export the alert history, click **History**, use the predefined views or the slider control to select a timeline to display the alerts, and then click the **Export** icon.
     By default, the timeline is set to 1 month.

   The **Export Alerts** dialog box appears.
3. From the menu, choose the format in which you want to export the alerts.
   - Select **Excel** to export the alerts to an .xlsx format.
     The file includes a summary sheet, along with a donut chart that represents the rule group and the alert count for each group. Each rule category sheet displays the object type, rule name, alert time, and other alert details. You can view the report only in Microsoft Office version 2007 and later versions.
   - Select **Csv** to export the alerts to a .csv file.
     The file contains all the alert records aggregated in one sheet.
4. To export the details of the alert, select **Include Alert Details**.
5. Click **Save**.

Monitoring PowerCenter Governance Alerts

Monitor the PowerCenter development environment alerts from the **Governance** tab on the **Reports** tab. You can view a comprehensive report or drill down into specific alert details of the current and historical alerts for PowerCenter governance.

The contents that appear on the **Governance** tab vary based on the view that you select.

You can select the following views:

- **Today**. View and export the PowerCenter development environment alerts for the current day.
- **History**. View and export the PowerCenter development environment alerts for a particular time period.
- **On Demand Reports**. Create and view on demand reports for workflows, sessions, or transformations in PowerCenter development environment.

Monitoring the PowerCenter Governance Alerts for the Current Day

You can monitor the PowerCenter governance alerts for the current day in the **Today** view on the **Governance** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab and then click the **Today** view. The following sections appear in the contents panel:

Total Alerts

The alert type, alert count, and percentage of the alert types appear in a graph and table format in the **Total Alerts** section.

Best Practice Violations

The alert details appear in the **Best Practice Violations** section.

3. To view the best practice violations of a particular alert type, click on the corresponding alert type from the donut chart or table. The violations for the alert type that you select appear in the **Best Practice Violations** section.
4. To view detailed information of an alert that appears in the **Best Practice Violations** section, click the **View Details** button in **Details** column for that alert.

Monitoring the PowerCenter Governance Best Practice Violations

You can monitor the PowerCenter governance best practice violations for a particular time period in the **History** view on the **Governance** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab and then click the **History** view.

   The **Total Alerts**, **Alerts for Period**, and **Best Practice Violations** sections appear in the contents panel. A graph that represents the number of alerts over a period of time appears in the **Total Alerts** section.
3. Select the time period or alert type for which you want display the best practice violations.
   - To monitor best practice violations for a time period, select the time period with the slider or views in the **Total Alerts** section.
   - To monitor best practice violations based on the alert type, select an alert type that appears in the donut chart or table from the **Alerts for Period** section.

   A graph that represents the number of best practice violations and the list of best practice violations for the time period appears in the **Best Practice Violations** section.
4. To view detailed information of an alert that appears in the **Best Practice Violations** section, click the **View Details** button in **Details** column for that alert.

   The alert details appear in the **Alert Details** pane.

Export Alerts for PowerCenter Governance

You can export alerts for the current day or for a specified period to a standard comma-separated value (CSV) file or an excel (.xlsx) file. The exported file includes a snapshot of the alerts generated for the current day or the alert history for a specified period. The report depicts the rule categories and the alert records. You can also choose to export the alert body.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab, and choose if you want to export the alerts for the current day or the alert history.
   - To export alerts from the current day, click **Today** and then click the **Export** icon.
   - To export the alert history, click **History**, use the predefined views or the slider control to select a timeline to display the alerts, and then click the **Export** icon.
     By default, the timeline is set to 1 month.

   The **Export Alerts** dialog box appears.

3. From the menu, choose the format in which you want to export the alerts.
   - Select **Excel** to export the alerts to an .xlsx format.
     The file includes a summary sheet, along with a donut chart that represents the rule group and the alert count for each group. Each rule category sheet displays the object type, rule name, alert time, and other alert details. You can view the report only in Microsoft Office version 2007 and later versions.
   - Select **Csv** to export the alerts to a .csv file.
     The file contains all the alert records aggregated in one sheet.
4. To export the details of the alert, select **Include Alert Details**.
5. Click **Save**.

Monitoring the PowerCenter Governance Alerts Using On Demand Reports

Use the on demand reports to retrieve information on instances of sessions, transformations, or workflows for an attribute value. You can create and view on demand reports in the **On Demand Reports** view on the **Governance** tab.

Use the **On Demand Reports** view to create and save on demand reports, edit the saved reports, and run on demand reports. For example, you can create an on demand report to retrieve all sessions for an attribute with a specified attribute value.

Creating On Demand Reports

You can create on demand reports from the **On Demand Reports** view on the **Governance** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab and then click the **On Demand Reports** view.
3. In the **Actions** menu on the **Reports** tab, click **New**.

   The **Profiles** screen appears.
4. Enter a name for the on demand report profile.
5. Optionally, enter a description for the on demand profile.
6. Select the Repository Service that manages the PowerCenter development environment.

   The folders associated with that Repository Service appear in the **Folder** list.
7. Select the folder in which the session, workflow, or transformation objects exist.
8. Select the workflow, session, or transformation object type that you want to monitor.

   The attributes specific to the selected object types appears in the **Attribute Check** list.
9. Select the attribute that you want to check from the **Attribute Check** list, and then specify the condition and value that you want to check.

   For example, if the attribute name is Commit Type, and the decoded attribute value is Source, then use the attribute value as 0.
10. Click **Save**.

Editing On Demand Reports

You can edit on demand reports that you create from the **On Demand Reports** view on the **Governance** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab and then click the **On Demand Reports** view.
3. Select the report profile that you want to edit from the **Profiles** section.
4. In the **Actions** menu on the **Reports** tab, click **Edit**.

   The **Profiles** screen appears.
5. Edit the on demand report properties.

   The following table displays the on demand report properties:

Property	Description
Name	Name of the on demand report profile.
Description	Description of the on demand report profile.
Repository Service	Repository Service that manages the PowerCenter development environment.
Folder	Folder in which the session, workflow, or transformation objects exist.
Artifact Type	Type of the object that you want to monitor.
Attribute Check	Attribute that you want to check for the selected object.

6. Click **Save**.

Deleting On Demand Reports

You can delete on demand reports from the **On Demand Reports** view on the **Governance** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab and then click the **On Demand Reports** view.
3. Select the report profile that you want to delete from the **Profiles** section.
4. In the **Actions** menu on the **Reports** tab, click **Delete**.

Running On Demand Reports

You can run on demand reports from the **On Demand Reports** view on the **Governance** tab.

1. In the Proactive Monitoring for PowerCenter Management Console, click the **Reports** tab.
2. Click the **Governance** tab and then click the **On Demand Reports** view.
3. Select the report profile that you want to run from the **Profiles** section.
4. In the **Actions** menu on the **Reports** tab, click **Run**.

   The **Run Profile** screen appears.
5. Enter the user name of the PowerCenter user.
6. Select the start date for the period for which you want to run the report. The format for the date is in yyyy-mm-dd hh:mm:ss format.

7. Click the **Run** button.

   The **Report** screen appears with a report for the selected workflow, session, or transformation object.

Attribute Values for On-Demand Reports

The following table provides attribute values and descriptions for each attribute name that you can configure:

Attribute Name	Attribute Value and Description
Commit Type	Use one of the following values: - 0. Source - 1. Target - 2. User-defined
Decimal Separator	Use one of the following values: - 1. comma (,) - 2. period (.)
Dynamic Partitioning	Use one of the following values: - 0. Disabled - 1. Based on the number of partitions - 2. Based on the number of nodes in a grid - 3. Based on source partitioning - 4. Based on the number of CPUs
Error Log Type	Use one of the following values: - 0. None - 1. Relational database - 2. Flat file
Is Partitionable	Use one of the following values: - 0. No - 1. Locally - 2. Across a grid
Join Type	Use one of the following values: - 1. Normal join - 2. Master outer join - 3. Detail outer join - 4. Full outer join
Lookup Policy on Multiple Match	Use one of the following values: - 1. Use first value - 2. Use last value - 3. Report error - 4. Use any value
Master Sort Order	Use one of the following values: - 0. Ascending - 1. Auto
Null Ordering	Use one of the following values: - 0. Null is highest value - 1. Null is lowest value
Null Ordering in detail	Use one of the following values: - 0. Null is highest value - 1. Null is lowest value

Attribute Name	Attribute Value and Description
Null Ordering in master	Use one of the following values: - 0. Null is highest value - 1. Null is lowest value
On Pre-Post SQL error	Use one of the following values: - 0. Stop - 1. Continue
On Pre-session command task error	Use one of the following values: - 0. Stop - 1. Continue
On Stored Procedure error	Use one of the following values: - 0. Stop - 1. Continue
Output Is Repeatable	Use one of the following values: - 0. Never - 1. Based on input order - 2. Always
Override Tracing	Use one of the following values: - 0. None - 1. Terse - 2. Normal - 3. Verbose initialization - 4. Verbose data
Pre-build Lookup Cache	Use one of the following values: - 0. Auto - 1. Always allow - 2. Never allow
Pushdown Optimization	Use one of the following values: - 0. None - 1. To source - 2. To target - 3. Full - 4. $PushdownConfig
Recovery Strategy	Use one of the following values: - 0. Fail task and continue workflow - 1. Resume from last checkpoint - 2. Restart task
Save Session log by	Use one of the following values: - 0. By runs - 1. By timestamp
Save Workflow log by	Use one of the following values: - 0. By runs - 1. By timestamp
Source Type	Use one of the following values: - 1. Database - 2. Flat file - 3. Source qualifier

Attribute Name	Attribute Value and Description
Stored Procedure Type	Use one of the following values: - 1. Target pre-load - 2. Target post-load - 3. Normal - 4. Source pre-load - 5. Source post-load
Thousand Separator	Use one of the following values: - 0. None - 1. Comma (,) - 2. Period (.)
Top/Bottom	Use one of the following values: - 0. Bottom - 1. Top
Tracing Level	Use one of the following values: - 1. Terse - 2. Normal - 3. Verbose initialization - 4. Verbose data
Transformation Scope	Use one of the following values: - 0. Row - 1. Transaction - 2. All input
Treat Source Rows As	Use one of the following values: - 0. Insert - 1. Delete - 2. Update - 3. Data driven
Type	Use one of the following values: - 0. Informatica - 1. COM

CHAPTER 5

Proactive Monitoring SNMP Alerts

This chapter includes the following topic:

- Proactive Monitoring SNMP Alerts, 42

Proactive Monitoring SNMP Alerts

You can configure the PMPC solution to send alerts as SNMP traps in addition to email and RTAM alerts. PMPC solution supports SNMP v2.

Configure the following PMPC components to send alerts as SNMP traps:

- SNMP Rule
- SNMP Responder
- SNMP Response

SNMP Rule

The SNMP rule generates SNMP traps for alerts. The rule activates whenever an event occurs on pc_notifications. The rule takes following variable values from the incoming activation and binds them to the trap Protocol Data Unit (PDU): body, priority, extended_properties, rs, rulename, artifact_type, domain, persona, product, rule_user, rule_group, and subject.

The PC_S7 SNMP Notification Response rule is available as part of RulePoint installation and is disabled by default. To reactivate the rule, edit the PC_S7 SNMP Notification Response rule from RulePoint and change the status of the rule to active.

To add bindings, check for the corresponding variable definition in the MIB. If the variable definition is present in the MIB then add the parameter name to OID mapping to the source code. Add the property to the response parameters.

SNMP Responder

The SNMP responder sends the trap PDU to the network manager that you configure to receive traps. The SNMPv2Responder is available as part of RulePoint installation and is disabled by default. To configure the SNMPv2Responder, edit the SNMPv2Responder from RulePoint and provide the network manger details.

The following table describes the responder properties that you need to configure:

Property	Description
Name	Name for the responder.
NMS Host	IP address of the host on which NMS is available.
NMS Port	Port number on which NMS will receive traps. The default value is 162.
Community String	Community string for SNMPv2. The default values is public.
Timeout	Timeout value for trap in milliseconds. The default values is 0.
Retry Count	Retry count for trap. The default value is 0.
Trap OID	OID of the trap.
Status	Status of the responder. Change the status of the responder to active to reactive the responder.

SNMP Response

The SNMPv2Response is available as part of RulePoint installation and is disabled by default. The SNMPv2Response is the default response for SNMPv2Responder.

Use the response parameters map values to construct the response variables. Edit the SNMPv2Response in Rulepoint. Change the status of the response to active to reactivate the response.

CHAPTER 6

Proactive Monitoring Watchlists

This chapter includes the following topic:

- Proactive Monitoring Watchlists, 44

Proactive Monitoring Watchlists

The following table lists the predefined watchlists that are available by default upon installing Proactive Monitoring for PowerCenter Governance:

Watchlists Name	Description	State
PowerCenter Workflow Attributes	The list of PowerCenter workflow attributes. This watchlist is referenced in the template, PC_GWT2 Compare workflow attributes.	Draft
PowerCenter Transformation Attributes	The list of PowerCenter transformation attributes. This watchlist is referenced in the template, PC_GTT1 Compare transformation attributes.	Draft
PowerCenter Monitored Folders	The list of PowerCenter folders that are monitored. To receive notifications add your folder names to this watchlist. If the folder is same for multiple PowerCenter repositories, you receive this notification for all configured repositories.	Deployed
PowerCenter Session Attributes	The list of PowerCenter session attributes. This watchlist is referenced in the template, PC_GST1 Compare session attributes.	Draft

Watchlists Name	Description	State
PowerCenter Default Transformation Names	The list of default names which should be renamed while creating PowerCenter transformations. Notifications will be sent if the transformation names specified in the list are used.	Deployed
PowerCenter CLI commands Watchlists	The list of CLI commands which should not be used in PowerCenter tasks of type Command.	Deployed

CHAPTER 7

Proactive Monitoring Topics

This chapter includes the following topic:

- Proactive Monitoring Topics, 46

Proactive Monitoring Topics

The following table lists the predefined topics that are available by default upon installing Proactive Monitoring for PowerCenter Governance:

Topic Name	Description	State
pc_notifications	This topic contains event properties associated with the proactive monitoring notification framework.	Deployed
pc_alert_history_purge_request	This topic contains event properties associated with the alert history purge request. Source: PowerCenter Daily Alert History Purge Requestor	Deployed
pc_pmpc_global_settings	This topic contains event properties associated with global settings framework. Source: PowerCenter Load PMPC Global Settings from Database	Deployed
pc_sessions	This topic contains event properties associated with PowerCenter sessions. Source: PowerCenter Sessions Modified Incremental	Deployed
pc_mapplets	This topic contains event properties associated with PowerCenter mapplets. Source: PowerCenter Mapplets Modified Incremental	Deployed

Topic Name	Description	State
pc_worklets	This topic contains event properties associated with the PowerCenter worklets. Source: PowerCenter Worklets Modified Incremental	Deployed
pc_transforms	This topic contains event properties associated with PowerCenter transformations. Source: PowerCenter Transforms Modified Incremental	Deployed
pc_mappings	This topic contains event properties associated with PowerCenter mappings. Source: PowerCenter Mappings Modified Incremental	Deployed
pc_workflows	This topic contains event properties associated with the PowerCenter workflows. Source: PowerCenter Workflows Modified Incremental	Deployed
pc_command_tasks	This topic contains event properties associated with Command task type used in PowerCenter workflows. Source: PowerCenter Command Tasks	Deployed

CHAPTER 8

Proactive Monitoring Services

This chapter includes the following topics:

- Sources, 48
- Analytics, 50
- Responders, 52

Sources

The sources fetch data from PowerCenter repositories and run-time instances which are used for rule evaluation.

The following table lists the predefined sources that are available by default after installing Proactive Monitoring for PowerCenter Governance:

Source Service Name	Description	Properties	State
PowerCenter Command Tasks	Retrieve the details of "Command" task type used in PowerCenter workflows.	- Type: PMPC SQL Source - Topic: pc_command_tasks - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed
PowerCenter Daily Alert History Purge Requestor	Retrieve alert history purge frequency from the global settings framework. The frequency is used for purging the alert history.	- Type: SQL - Topic: pc_alert_history_purge_request - Connected to: Rulepoint Repository (pc_rp) - Default interval: Daily	Deployed
PowerCenter Load PMPC Global Settings from Database	Retrieve Proactive Monitoring global settings from the RulePoint database.	- Type: SQL - Topic: pc_pmpc_global_settings - Connected to: Rulepoint Repository (pc_rp) - Default interval: 21600 seconds	Deployed

Source Service Name	Description	Properties	State
PowerCenter Mappings Modified Incremental	Retrieve the details of the PowerCenter mappings modified since the last run.	- Type: PMPC SQL Source - Topic: pc_mappings - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed
PowerCenter Mapplets Modified Incremental	Retrieve the details of the PowerCenter mapplets modified since the last run.	- Type: PMPC SQL Source - Topic: pc_mapplets - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed
PowerCenter Sessions Modified Incremental	Retrieve the details of non-reusable PowerCenter sessions inside a worklet, reusable sessions inside a folder, and non-reusable sessions inside a workflow.	- Type: PMPC SQL Source - Topic: pc_sessions - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed
PowerCenter Transforms Modified Incremental	Retrieve the details of PowerCenter transformations modified since the last run.	- Type: PMPC SQL Source - Topic: pc_transforms - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed
PowerCenter Workflows Modified Incremental	Retrieve the details of PowerCenter workflows modified since the last run.	- Type: PMPC SQL Source - Topic: pc_workflows - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed
PowerCenter Worklets Modified Incremental	Retrieve the details of PowerCenter worklets modified since the last run.	- Type: PMPC SQL Source - Topic: pc_worklets - Connected to: PowerCenter Repository (pcrs_readonly) - Default interval: 21600 seconds	Deployed

Analytics

RulePoint analytics implement a data processing function, and it can be referenced in rule activations.

The following table lists the predefined analytics that are available by default after installing Proactive Monitoring for PowerCenter Governance:

Name	Connects to...	Analytic Type	Description	State
pc_get_alert_history_csv	RulePoint Repository	SQL	Obtain alert history for the previous N days for reporting purposes.	Deployed
pc_get_alert_history_purge_count	RulePoint Repository	SQL	Obtain the count of alert history records to be purged.	Deployed
pc_get_email	RulePoint Repository	SQL	Obtain the email address for a specified recipient of an alert.	Deployed
pc_get_rtam	RulePoint Repository	SQL	Obtain the Real-Time Alert Manager target for a specified recipient of an alert.	Deployed
pc_get_global_setting	RulePoint Repository	SQL	Obtain value from the global settings framework for a specified attribute name.	Deployed
pc_get_purge_cutoff_date	RulePoint Repository	SQL	Obtain the text string for the cutoff date. The cutoff date will be specified in the alerts.	Deployed
pc_recent_alert	Rulepoint Repository	SQL	Check if a recent alert has been sent for a specific rule name, key-value combination, and a snooze interval. The snooze parameter determines the most recent alert.	Deployed
pc_is_mapping_duplicate	PowerCenter Repository	PMPC SQL Analytic	Obtain the duplicates of a specified mapping in all other folders.	Deployed
pc_is_session_duplicate	PowerCenter Repository	PMPC SQL Analytic	Obtain the duplicates of a specified session in all other folders.	Deployed
pc_is_workflow_duplicate	PowerCenter Repository	PMPC SQL Analytic	Obtain the duplicates of a specified workflow in all other folders.	Deployed
pc_get_session_details_for_mapping	PowerCenter Repository	PMPC SQL Analytic	Obtain PowerCenter session details corresponding to the specified mapping.	Draft
pc_get_session_attribute	PowerCenter Repository	PMPC SQL Analytic	Obtain the value for a specified session attribute name.	Deployed
pc_get_session_attribute_count	PowerCenter Repository	PMPC SQL Analytic	Obtain count for a specified session attribute name and value.	Draft
pc_get_workflow_attribute	PowerCenter Repository	PMPC SQL Analytic	Obtain the workflow attribute for a specified workflow.	Deployed

Name	Connects to...	Analytic Type	Description	State
pc_get_workflow_attribute_count	PowerCenter Repository	PMPC SQL Analytic	Obtain the number of workflows for a specified attribute value.	Draft
pc_get_transform_attribute	PowerCenter Repository	PMPC SQL Analytic	Obtain the value for a specified transformation attribute.	Deployed
pc_get_transform_attribute_count	PowerCenter Repository	PMPC SQL Analytic	Obtain the number of transformations for a specified attribute value.	Draft
pc_get_session_mapping_attribute	PowerCenter Repository	PMPC SQL Analytic	Obtain the mapping attributes for a specified session.	Deployed
pc_get_task_parent_failure_options	PowerCenter Repository	PMPC SQL Analytic	Obtain the value of failed parent task option for a specified session.	Deployed
pc_is_session_on_test_load	PowerCenter Repository	PMPC SQL Analytic	Check if a session has the Enable Test Load attribute set.	Draft
rs_formatter	RulePoint Repository	SQL	This formats the rs value in the notification response.	Deployed
get_mapping_ports	PowerCenter Repository	PMPC SQL Analytic	Return all the transformation ports that do not meet the port naming criteria within a mapping.	Draft
get_session_hardcoded_paths	PowerCenter Repository	PMPC SQL Analytic	Return all hardcoded paths configured for sources and targets within a session.	Draft

Responders

With a responder, you can define the interface parameters for a particular type of response, that is the action to be taken when a rule activates. From a single responder, you can create multiple specific responses.

The following table lists the predefined responders that are available by default after installing Proactive Monitoring for PowerCenter Governance:

Responder Service Name	Description	Properties	State
PowerCenter Alert History Purge Responder	Responds to events by purging alert history older than the specified number of days.	- Type: SQL Responder - Topic: - - Connected to: Rulepoint Repository (pc_rp)	Deployed
PowerCenter Alert Recorder	The alert recorder stores details of alerts in the RulePoint database.	- Type: SQL Responder - Topic: - - Connected to: Rulepoint Repository (pc_rp)	Deployed
PowerCenter Email Responder	Responds to events by sending email alerts.	- Type: Email - Topic: - - Connected to: Email server	Deployed
PowerCenter Notification Responder	Responds to events by transforming them as notification events.	- Type: Event Transformer - Topic: pc_notifications - Connected to: -	Deployed
RTAM	Sends notifications to the Real-Time Alert Manager.	- Type: RTAM Responder - Topic: - - Connected to: -	Deployed
SNMPv2Responder	Sends SNMP traps as an alert to SNMP Trap Receiver. To enable sending notifications as SNMP traps, deploy this responder along with the rule, PC_S7 SNMP Notification.	- Type: SNMP Responder - Topic: - - Connected to: -	Draft

CHAPTER 9

Proactive Monitoring Templates and Rules

This chapter includes the following topics:

- Proactive Monitoring Templates, 53
- Template Rules, 61
- Advanced Rules, 69

Proactive Monitoring Templates

Templates provide an easier way to create rules. You can create rules from predefined templates. You can restrict input from users by adding simple validations to the template. You can add specific user assistance wherever required to make the use of the template easier.

PC_GST1 Compare session attributes

Notify if the session attribute contains a specified value. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
session_attribute	Select the value of the session attribute.
operator	Enter comparison operator.
attr_value	Enter the Attribute Value.
alert_cause	Enter concise text to explain the cause of the alert.
priority	Select a priority level (0=Least critical to 5=Most Critical).

PC_GST2 Naming Convention Violation for Session Name prefix

Notify if the session name does not start with the specified prefix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
prefix	Check prefix for naming convention of session.

PC_GST3 Session modified often within a specified duration

Notify if the session is modified for a specified number of times within the stipulated duration. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
p_times	Number of times a session is modified.
p_minutes	Time range within which the session is modified the specified number of times.

PC_GMT1 Naming Convention Violation for Mapping Name prefix

Notify if the mapping name does not start with the specified prefix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
prefix	Check prefix for naming convention of mapping.

PC_GMT2 Mapping modified often within a specified duration

Notify if a mapping is modified for a specified number of times within the stipulated duration. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
p_times	Number of times the mapping is modified.
p_minutes	Time range within which the mapping is modified the specified number of times.

PC_GTT1 Compare transformation attributes

Notify if the transformation attribute contains a specified value. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_transforms
Analytics	pc_get_transform_attribute
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
transform_attribute	Select the transformation attribute from the drop down menu.
operator	Enter comparison operator.
attr_value	Enter the attribute value.
alert_cause	Enter text to explain the cause of the alert.
priority	Select a priority level (0=Least critical to 5=Most Critical).

PC_GWT1 Naming Convention Violation for Workflow Name prefix

Notify if the workflow name does not start with the specified prefix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Workflows Modified Incremental

Property	Value
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
prefix	Check prefix for naming convention of mapping.

PC_GWT2 Compare workflow attributes

Notify if the workflow attribute contains a specified value. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_workflows
Analytics	pc_get_workflow_attribute
Source	PowerCenter Workflows Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
workflow_attribute	Select the workflow attribute from the drop down menu.
operator	Enter comparison operator.
attr_value	Enter the attribute value.
alert_cause	Enter text to explain the cause of the alert.
priority	Select a priority level (0=Least critical to 5=Most Critical).

PC_GWT3 Windows pathname is hardcoded with a drive letter

Notify if the command tasks contains the specified drive letter, such as "C:\". The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_command_tasks
Source	PowerCenter Command Tasks
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
drive	Check for the drive letter in the command tasks.

PC_GWT5 Naming Convention Violation for Workflow Name suffix

Notify if the workflow name does not end with the specified suffix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Workflows Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
suffix	Check suffix for naming convention of workflow.

PC_GWKT2 Naming Convention Violation for Worklet Name suffix

Notify if the worklet name does not end with the specified suffix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_worklets
Source	PowerCenter Worklets Modified Incremental

Property	Value
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
suffix	Check suffix for naming convention of worklet.

PC_GST5 Naming Convention Violation for Session Name suffix

Notify if the session name does not end with the specified suffix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
suffix	Check suffix for naming convention of session.

PC_GMT4 Naming Convention Violation for Mapping Name suffix

Notify if the mapping name does not end with the specified suffix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
suffix	Check suffix for naming convention of mapping.

PC_GMPT2 Naming Convention Violation for Mapplet Name suffix

Notify if the mapplet name does not end with the specified suffix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_mapplets
Source	PowerCenter Mapplets Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
suffix	Check suffix for naming convention of mapplet.

PC_GMT5 Naming Convention Violation for Mapping Transformation Port prefix

Notify if transformation ports in a mapping do not start with the specified prefix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_mappings
Analytics	get_mapping_ports
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
prefix	Check prefix for naming convention of the mapping transformation port.

PC_GTT2 Naming Convention Violation for Transformation Name prefix

Notify if transformation name does not start with the specified prefix. The state is draft.

The following table lists the template properties:

Property	Value
Topic	pc_transforms
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

The following table describe the template parameters:

Parameter	Description
prefix	Check prefix for naming convention of transformation name.

Template Rules

You can create rules from the template rules by specifying values based on the requirement.

PC_GM5 Mapping name should begin with m_

Notify if the mapping name does not begin with m_. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GM6 Check if a mapping is modified 3 times within the last 60 minutes

Notify if a mapping is modified three times within the last 60 minutes. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS3 Session name should begin with s_

Notify if the session name does not begin with s_. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS8 Check whether rollback of transaction on error is not set

Notify if a *Rollback Transactions on Error* is not set for a session. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS9 Check if session is modified 3 times within the last 60 minutes

Notify if the session is modified three times within the last 60 minutes. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS12 Check whether save session log for these runs uses the global variable PMSessionLogCount

Notify if *Save session log for these runs* attribute does not use the global variable *$PMSessionLogCount*. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_attrib
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS13 Check whether stop on errors uses the global variable PMSessionErrorThreshold

Notify if *Stop on errors* attribute does not use the global variable *$PMSessionErrorThreshold*. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Analytics	pc_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS14 Check whether write backward compatible session log file is set

Notify whether a session does not have *Write Backward Compatible Session Log File* set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS16 Check for session where commit interval exceeds 1000 seconds

Notify if *Commit Interval* greater than equal to 1000 seconds for a session. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_task_parent_failure_options
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT3 Check for transformations with lookup SQL override

Notify if the *Lookup SQL Override* for a transformation is not NULL. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT4 Check for transformations with source SQL override

Notify if *SQL Query* for a transformation is not NULL. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT5 Check for transformations with tracing level higher than terse

Notify if a transformation has *Tracing Level* higher than terse.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Analytics	pc_get_transform_attribute
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT7 Check if sequence generator reset option is set

Notify if the sequence generator Reset option is set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Analytics	pc_get_transform_attribute
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW3 Workflow name should begin with wf_

Notify if a workflow name does not begin with wf_. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Workflows Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW6 Check whether save workflow log for these runs used the global variable PMWorkflowLogCount

Notify if *Save workflow log for these runs* attribute does not use the global variable *$PMWorkflowLogCount*.State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Analytics	pc_get_workflow_attribute
Source	PowerCenter Workflows Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW8 Check whether backward write compatible workflow log option is set

Notify whether a workflow does not have *Write Backward Compatible Workflow Log File* set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Analytics	pc_get_workflow_attribute
Source	PowerCenter Workflows Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW9 Check if Windows path name is hardcoded with drive letter C

Notify if the command task contains a hardcoded Microsoft Windows drive letter `C:\`. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_command_tasks
Source	PowerCenter Command Tasks
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW13 Workflow Name should end with _DEV

Notify if the workflow name does not end with _DEV. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Workflows Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GWK3 Worklet Name should end with _DEV

Notify if the worklet name does not end with _DEV. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_worklets
Source	PowerCenter Worklets Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS20 Session Name should end with _DEV

Notify if the session name does not end with _DEV. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GM8 Mapping Name should end with _DEV

Notify if the mapping name does not end with _DEV. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GMP3 Mapplet Name should end with _DEV

Notify if the mapplet name does not end with _DEV. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mapplets
Source	PowerCenter Mapplets Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GM9 Mapping Transformation Input Port must begin with in_

Notify if transformation ports in a mapping do not start with the specified prefix. You need to deploy this rule to receive the notifications. State is draft.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Analytics	get_mapping_ports
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT8 Aggregator Transformation Name should start with AGG_

Notify if the aggregator transformation name does not start with AGG_. You need to deploy this rule to receive the notifications. State is draft.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

Advanced Rules

Advanced rules do not have parameters. You can extend these rules after you are comfortable with the functioning of these rules.

PC_GM1 Check for mappings without description

Notify if the description for a mapping is NULL. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental

Property	Value
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GM2 Check for duplicate mappings

Notify if the name of the mapping is duplicated. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Analytics	pc_is_mapping_duplicate
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GM3 Check whether the mappings is not valid

Notify if a mapping is not valid. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GM4 Check for mapping names with spaces

Notify if the mapping name has spaces. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mappings
Source	PowerCenter Mappings Modified Incremental

Property	Value
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS1 Check whether the session is not valid

Notify if the session is not valid. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS2 Check for sessions without description

Notify if the description for a session is NULL. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Sessions Modified Incremental
Persona	apparchitect

PC_GS4 Check for duplicate sessions

Notify if a session name is repeated. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_is_session_duplicate
Source	PowerCenter Sessions Incremental

Property	Value
Response	PowerCenter Sessions Modified Incremental
Persona	apparchitect

PC_GS5 Check whether a sessions is not reusable

Notify if a session is not reusable. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS6 Check if session log file name is not derived from the session name

Notify if the session log file name does not contain the session name. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	c_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS7 Check whether the truncate table option is set

Notify if *truncate target table* is set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_mapping_attribute
Source	PowerCenter Sessions Modified Incremental

Property	Value
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS10 Check for disabled sessions

Notify if a session is disabled. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS11 Check for hardcoded source connection parameters in a session

Notify if the source connection value of a session does not begin with $. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS15 Check whether both the parent fail options are not set

Notify if a session has both Fail parent if the task fails and Fail parent if this task does not run options not set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	task_parent_failure_options

Property	Value
Source	Sessions Modified Incremental
Response	Notification Response
Persona	apparchitect

PC_GS17 Check whether the option fail parent if this task does not run is not set

Notify if a session has the option "*ail parent if this task does not run* not set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_task_parent_failure_options
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GS18 Check whether target connection value is empty

Notify if a *Target connection value* is empty for a session. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT1 Check for transformations without description

Notify if the description for a transformation is NULL. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT2 Check for transformations with default names

Notify if the transformation are saved with default names. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GT6 Check whether connection information option is set

Notify if the *Connection Information* option is not set. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_transforms
Analytics	pc_get_transform_attribute
Source	PowerCenter Transforms Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GMP2 Check whether the mapplet is not valid

Notify if a mapplet is not valid. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_mapplets
Source	PowerCenter Mapplets Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GWK2 Check whether the worklet is not valid

Notify if a worklet is not valid. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_worklets
Source	PowerCenter Worklets Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW1 Check for workflows without description

Notify if the description for a workflow is NULL. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Sessions Modified Incremental
Persona	apparchitect

PC_GW2 Check for duplicate workflows

Notify if a workflow name is repeated. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Analytics	pc_is_workflow_duplicate
Source	PowerCenter Workflows Incremental
Response	PowerCenter Sessions Modified Incremental
Persona	apparchitect

PC_GW4 Check for workflows that are not valid

Notify if the workflow is not valid. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Workflows Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW5 Check if the workflow is a web service

Notify if the workflow is a web service. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Source	PowerCenter Mappings Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW7 Check if workflow log file name is not derived from workflow name

Notify if the Workflow Log File name does not contain the workflow name. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_workflows
Analytics	pc_get_workflow_attribute
Source	PowerCenter Workflows Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW10 Check for hardcoded UNIX path

Notify if the command tasks contain hard coded UNIX path names. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_command_tasks
Source	PowerCenter Command Tasks
Response	PowerCenter Notification Response
Persona	apparchitect

PC_GW11 Check for illegal command tasks

Notify if the workflow contains illegal command tasks listed in the PowerCenter CLI command watchlist. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_command_tasks
Source	PowerCenter Command Tasks
Response	PowerCenter Notification Response
Persona	apparchitect

PC_S1 RTAM Notification

Generate aReal-Time Alert Manager notification. State is deployed.

Note: Do not edit. For internal use.

PC_S2 Email Notification

Generate email notification. State is deployed.

Note: Do not edit. For internal use.

PC_S3 Daily alert history report

Send a daily report of the alert history. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_alert_history_purge_request
Analytics	pc_get_alert_history_csv, pc_get_purge_cutoff_date
Source	PowerCenter Daily Alert History Purge Requestor
Response	PowerCenter Real-Time Alert Manager Alert
Persona	pcmonitor

PC_S4 Zero records purged from alert history

Send a daily report when zero records are purged.

The following table lists the rule properties:

Property	Value
Topic	pc_alert_history_purge_request
Analytics	pc_get_alert_history_purge_count, pc_get_purge_cutoff_date
Source	PowerCenter Daily Alert History Purge Requestor
Response	PowerCenter Real-Time Alert Manager Alert
Persona	pcmonitor

PC_S5 Purge alert history

Notify when alert history is purged. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_alert_history_purge_request
Analytics	pc_get_alert_history_purge_count, pc_get_purge_cutoff_date
Source	PowerCenter Daily Alert History Purge Requestor
Response	PowerCenter Real-Time Alert Manager Alert
Persona	pcmonitor

PC_S6 Load Global Settings from Database

Generate a Real-Time Alert Manager alert when global settings are loaded from the database. State is deployed.

The following table lists the rule properties:

Property	Value
Topic	pc_pmpc_global_settings
Analytics	pc_get_rtam
Source	PowerCenter Load PMPC Global Settings from Database
Response	PowerCenter Real-Time Alert Manager Alert
Persona	pcmonitor

PC_S7 SNMP Notification Response

Generate SNMP trap for alerts. To enable sending notifications as SNMP traps, deploy this rule. State is draft.

The following table lists the rule properties:

Property	Value
Topic	pc_notifications
Response	SNMP v2 Response

PC_S8 RTAM and Email Notification

Generate RTAM and Email Notification. State is deployed.

Note: Do not edit. For internal use.

The following table lists the rule properties:

PC_GS21 Check whether the session Target Load Type is Bulk

Notify if the session "Target Load Type" is set to "Bulk." State is draft.

The following table lists the rule properties:

Property	Value
Topic	pc_sessions
Analytics	pc_get_session_mapping_attribute
Source	PowerCenter Sessions Modified Incremental
Response	PowerCenter Notification Response
Persona	apparchitect

CHAPTER 10

Proactive Monitoring Responses

This chapter includes the following topic:

- Proactive Monitoring Responses, 81

Proactive Monitoring Responses

The response is where you define how you want responses if the rule's event matches the rule condition. In addition to simple notification response, such as send an email or text message, you can configure a response to function like an action.

You can configure to send responses to a single user or groups of users through email or Real-Time Alert Manager user interface.

The following table lists the predefined responses that are available by default upon installing Proactive Monitoring for PowerCenter Governance:

Name	Response Type	Description	State
PowerCenter Alert Recorder Response	SQL	Records alerts to the RulePoint database.	Deployed
PowerCenter Email Response	Email	Sends email to the specified users with content based on the response properties.	Deployed
PowerCenter Notification Response	Event Transformer	Transforms events to notification events.	Deployed
PowerCenter RTAM Alert	RTAM	Sends alerts to Real-Time Alert Manager.	Deployed

Name	Response Type	Description	State
PowerCenter Alert History Purge Response	SQL	Purges alert history older than the specified number of days.	Deployed
SNMP v2 Response	SNMP Response	Sends SNMP traps as an alert to SNMP Trap Receiver. Generate SNMP trap for alerts. To enable sending notifications as SNMP traps, deploy the rule, PC_S7 SNMP Notification.	Draft

APPENDIX A

Troubleshooting

This appendix includes the following topic:

- Troubleshooting Real-Time Alerts , 83

Troubleshooting Real-Time Alerts

Alerts do not appear in the Real-Time Alert Manager dashboard even though all services are running.

Perform the following tasks to troubleshoot alerts:

Verify that RTAM is configured to receive alerts.

1. Log in to Real-Time Alert Manager as the user that is not receiving alerts.
2. Click the **Settings** tab and select **Global Settings**.
3. In the navigator pane, verify that RTAM is available in the default notification.

Verify that the folders are being monitored.

1. Log in to the Proactive Monitoring Management Console.
2. Click **Manage Objects**.
3. In the navigator pane, click **Monitored Objects** and select **Monitored Folders**.
4. Click **Actions** and select **Add/Remove Monitored Folders**.
5. Add the PowerCenter repository folders that you want to monitor, and click **Save**.
6. You must update the run time option to update the monitored folders. Click **Actions**, select **Update run time**, and click **Save**.

Verify that the responder is deployed.

1. Log in to the RulePoint Console.
2. Click **Design** and select **Responders**. Verify that the status of the responders is in deployed state.

Review the log file.

Review the solutions.log file in the following location: `<Proactive Monitoring installation directory>/bin/logs`

APPENDIX B

Topic Properties Reference

This appendix includes the following topic:

- Topic Properties, 84

Topic Properties

The tables list the properties for the topics in Proactive Monitoring for PowerCenter Governance:

The following table lists the properties for the pc_sessions topic:

Property	Description
session_is_valid	Indicates whether the session status is valid.
session_is_impacted	Indicates whether there is an impact on a session status when a user makes a change in the session.
curr_tstamp	Indicates the current time of event generation.
version_number	Indicates the version number of the PowerCenter session that a user modifies within the incremental time window.
session_last_saved	Indicates the time stamp when the PowerCenter session was last saved within the incremental time window.
workflow_name	Indicates the workflow name of the associated PowerCenter session.
tstamp	Indicates the time stamp when the PowerCenter session was last saved within the incremental time window.
session_id	Indicates the internal ID generated within PowerCenter for the session.
mapping_last_saved	Indicates the last saved time for the mapping associated with the PowerCentre session.
is_reusable	Indicates whether you can reuse the session.
is_enabled	Indicates whether you can enable or disable the session.
session_name	Indicates the name of the PowerCenter session.

Property	Description
mapping_name	Indicates the mapping name associated with the PowerCenter session.
rs	Indicates the Repository Service name associated with the PowerCenter session.
session_comments	Provides the comments in the section content of the session.
folder	Indicates the folder name associated with the session.
domain	Indicates the domain name associated with the session.
user_name	Indicates the name of the user who enforced a change to the PowerCenter session within the incremental time window.

The following table lists the properties for the pc_mapplets topic:

Property	Description
comments	Provides the comments in the section content of the mapplet.
mapplet_name	Indicates the name of the PowerCenter mapplet.
last_saved	Indicates the time stamp when the PowerCenter mapplet was last saved within the incremental time window.
is_valid	Indicates whether the mapplet status is valid.
mapplet_id	Indicates the internal ID generated within PowerCenter for the mapplet.
rs	Indicates the Repository Service name associated with the PowerCenter mapplet.
folder	Indicates the folder name associated with the mapplet.
domain	Indicates the domain name associated with the mapplet.
user_name	Indicates the name of the user who enforced a change to the PowerCenter mapplet within the incremental time window.
version_number	Indicates the version number of the PowerCenter mapplet that a user modifies within the incremental time window.
tstamp	Indicates the time stamp when the PowerCenter mapplet was last saved within the incremental time window.

The following table lists the properties for the pc_worklets topic:

Property	Description
worklet_id	Indicates the internal ID generated within PowerCenter for the worklet.
comments	Provides comments of the PowerCenter worklet.

Property	Description
last_saved	Indicates the time stamp when the PowerCenter worklet was last saved within the incremental time window.
version_number	Indicates the version number of the modified PowerCenter worklet within the incremental time window.
worklet_name	Indicates the name of the PowerCenter worklet.
tstamp	Indicates the time stamp when the PowerCenter worklet was last saved within the incremental time window.
workflow_name	Indicates the workflow name associated with the PowerCenter worklet.
is_valid	Indicates whether the worklet status is valid.
rs	Indicates the Repository Service name associated with the PowerCenter worklet.
folder	Indicates the folder name associated with the PowerCenter worklet.
domain	Indicates the domain name associated with the PowerCenter worklet.
user_name	Indicates the name of the user who enforced a change to the PowerCenter worklet within the incremental time window.

The following table lists the properties for the pc_transforms topic:

Property	Description
mapping_id	Indicates the internal ID generated within PowerCenter for the mapping.
transform_type	Indicates the type of PowerCenter transformation. For example, type can be Source Definition or Target Definition.
last_saved	Indicates the time stamp when the PowerCenter transformation was last saved within the incremental time window.
transform_type_id	Provides the internal ID of the transformation type.
version_number	Indicates the version number of the modified PowerCenter transformation within the incremental time window.
transform_description	Provides the description of the PowerCenter transformation.
transform_name	Indicates the name of the PowerCenter transformation.
transform_id	Indicates the internal ID generated within PowerCenter for the transformation.
tstamp	Indicates the time stamp when the PowerCenter transformation was last saved within the incremental time window.
workflow_name	Indicates the workflow name associated with the PowerCenter transformation.
mapping_name	Indicates the mapping name associated with the PowerCenter transformation.

Property	Description
rs	Indicates the Repository Service name associated with the PowerCenter transformation.
folder	Indicates the folder name associated with the PowerCenter transformation.
domain	Indicates the domain name associated with the PowerCenter transformation.
user_name	Indicates the name of the user who enforced a change to the PowerCenter transformation within the incremental time window.

The following table lists the properties for the pc_mappings topic:

Property	Description
mapping_id	Indicates the internal ID generated within PowerCenter for the mapping.
mapping_is_valid	Indicates whether the mapping status is valid.
version_number	Indicates the version number of the modified PowerCenter mapping within the incremental time window.
tstamp	Indicates the time stamp when the PowerCenter mapping was last saved within the incremental time window.
workflow_name	Indicates the workflow name associated with the PowerCenter mapping.
mapping_name	Indicates the name of this PowerCenter mapping.
rs	Indicates the Repository Service name associated with the PowerCenter mapping.
mapping_last_saved	Indicates the time stamp when the PowerCenter mapping was last saved within the incremental time window.
folder	Indicates the folder name associated with the PowerCenter mapping.
domain	Indicates the domain name associated with the PowerCenter mapping.
mapping_description	Provides the description of the PowerCenter mapping.
user_name	Indicates the name of the user who enforced a change to the PowerCenter mapping within the incremental time window.

Property	Description
mapping_id	Indicates the internal ID generated within PowerCenter for the mapping.
mapping_is_valid	Indicates whether the mapping status is valid.
version_number	Indicates the version number of the modified PowerCenter mapping within the incremental time window.
tstamp	Indicates the time stamp when the PowerCenter mapping was last saved within the incremental time window.

Property	Description
workflow_name	Indicates the workflow name associated with the PowerCenter mapping.
mapping_name	Indicates the name of this PowerCenter mapping.
rs	Indicates the Repository Service name associated with the PowerCenter mapping.
mapping_last_saved	Indicates the time stamp when the PowerCenter mapping was last saved within the incremental time window.
folder	Indicates the folder name associated with the PowerCenter mapping.
domain	Indicates the domain name associated with the PowerCenter mapping.
mapping_description	Provides the description of the PowerCenter mapping.
user_name	Indicates the name of the user who enforced a change to the PowerCenter mapping within the incremental time window.

The following table lists the properties for the pc_workflows topic:

Property	Description
workflow_last_saved	Indicates the time stamp when the PowerCenter workflow was last saved within the incremental time window.
workflow_is_valid	Indicates whether the workflow status is valid.
workflow_is_runnable_service	Indicates whether the workflow is runnable, is valid, and is assigned to an Integration Service that is accessible.
version_number	Indicates the version number of the modified PowerCenter workflow within the incremental time window.
workflow_comments	Provides the comments of the PowerCenter workflow.
workflow_is_service	Indicates whether the workflow is a service workflow. You can only run a service workflow.
workflow_name	Indicates the name of the PowerCenter workflow.
tstamp	Indicates the time stamp when the PowerCenter workflow was last saved within the incremental time window.
rs	Indicates the Repository Service name associated with the PowerCenter workflow.
workflow_id	Indicates the internal ID generated within PowerCenter for the workflow.
folder	Indicates the folder name associated with the PowerCenter workflow.

Property	Description
domain	Indicates the domain name associated with the PowerCenter workflow.
user_name	Indicates the name of the user who enforced a change to the PowerCenter workflow within the incremental time window.

The following table lists the properties for the pc_command_tasks topic:

Property	Description
is_enabled	Indicates whether the command task is enabled.
task_name	Indicates the name of the PowerCenter command task.
version_number	Indicates the version number of the modified PowerCenter command task within the incremental time window.
workflow_name	Indicates the workflow name associated with the PowerCenter command task.
tstamp	Indicates the time stamp when the PowerCenter command task was last saved within the incremental time window.
type	Indicates the type of PowerCenter task. For example, task type can be Session, Command Task, or Start Task.
rs	Indicates the Repository Service name associated with the PowerCenter command task.
task_id	Indicates the internal ID generated within PowerCenter for the command task.
folder	Indicates the folder name associated with the PowerCenter command task.
attribute	Indicates the attribute name associated with the PowerCenter command task.
domain	Indicates the domain name associated with the PowerCenter command task.
user_name	Indicates the name of the user who enforced a change to the PowerCenter command task within the incremental time window.

The following table lists the properties for the pc_running_sessions_workflows_count topic:

Property	Description
is_name	Indicates the Integration Service name associated with the PowerCenter sessions and workflows that are running.
session_cnt	Indicates the number of sessions running within the Informatica domain.
tstamp	Indicates the snapshot time when the count of running sessions and workflows was extracted.
rs	Indicates the Repository Service name associated with the running PowerCenter sessions and worflows.

Property	Description
workflow_cnt	Indicates the number of workflows that run within the Informatica domain.
domain	Indicates the domain name associated with the running PowerCenter sessions and worflows.

APPENDIX C

Frequently Asked Questions

Does Proactive Monitoring solution support out-of-box reporting for alerts?

Yes. Proactive Monitoring solution supports number of out-of-box dashboards for current as well as historical reporting of alerts

What are the mechanisms available in Proactive Monitoring solution to send alerts?

You can use the Proactive Monitoring solution to send alerts as email, RTAM alerts, or SNMP traps or to send to all these systems.

If you use the Proactive Monitoring Management Console to add or remove PowerCenter monitored folders, will the updates appear in the PowerCenter Monitored Folders watchlist in RulePoint?

Yes. The updates made to PowerCenter Monitored Folders in Proactive Monitoring for PowerCenter Management Console will appear in the PowerCenter Monitored Folders watchlist in RulePoint.

Why I do not see data in the Reports dashboard?

Ensure that you schedule the workflows to populate data in Reports dashboard and clear the browser cache.

Why does an on-demand report does not populate data?

Ensure that you run the profile with correct attributes for the session, workflow, or transformation.

Is there any limit on the time period for alert history?

No. The History view will show all alert data that PMPC reports persists.

Does Proactive Monitoring for PowerCenter Governance support running best practice code checks on an on-demand basis?

Yes. You can use the Proactive Monitoring Management Console to create on-demand reports from the "On Demand Reports" view on the Governance tab in the Reports dashboard.

Why some columns do not display data even when all the services are running?

Ensure that you schedule the workflows to populate data in Reports dashboard and clear the browser cache.

How does the RulePoint communicate with the PowerCenter services or database servers?

The RulePoint communicates with the PowerCenter services or database servers through the Proactive_Monitoring user. The RulePoint connects to the PowerCenter repository through a JDBC connection and to the PowerCenter Integration Service through the Web Services Hub WSDL.

How do you determine the frequency of source services?

The alerting frequency of the sources must not be too high or too low. Each SQL source can have a different schedule based on your requirements. You can set the frequency for the SQL source services in the schedules. You can set the frequency of the PMPC SQL Source services in the source configuration.

Can Proactive Monitoring for PowerCenter monitor multiple Informatica domains?

No. You can monitor one domain with an instance of the Proactive Monitoring solution.

How do I configure the Proactive Monitoring sources to connect to the PowerCenter objects?

You can use the Proactive Monitoring Management Console to configure the solution to monitor an Informatica domain. You can use the Management Console to provide details of the nodes and the services that you want to monitor.

The administrator can use the Management Console to configure one or more PowerCenter services for monitoring. The user interface configuration screens in the Management Console replaced the command line utilities, Global Configuration Tool, and the Alert Recipient Tool from the earlier versions of the solution.

To monitor an Informatica domain, configuration through the Management Console is a prerequisite. The administrator provides configuration details of each host and node to the Management Console. To monitor PowerCenter Services, the administrator provides the configuration details of the services.

Why do I not see any alerts in RTAM even when the rules are activated?

You might not be able to receive alerts if the objects "PowerCenter Notification Responder" and "PowerCenter Notification Response" are not deployed. You need to deploy these objects to receive the alerts.

APPENDIX D

Glossary

Analytic

A service that implements a data processing function. An example of an Analytic is a match function that analyzes a set of input elements and returns a true or false if all elements match specific criteria. RulePoint offers a pre-defined set of Analytics. You can add additional Analytics to the system using the RulePoint SDK.

event

A piece of data that is pulled or pushed into RulePoint from a variety of sources. Events can be anything that you have deemed of interest, such as 911 dispatches, breaking news headlines, banking transactions, or persons of interest entering a predefined location.

event set

A grouping of multiple events into a single entity so that RulePoint can process the events at the same time.

event specific timestamp

This timestamp is used for events that have timestamp values as part of their source data. It does not pertain to event timestamp values that you create in the RulePoint database.

Informatica domain

A collection of nodes and services that define the Informatica platform. You group nodes and services in a domain based on administration ownership.

node

A logical representation of a machine or a blade. Each node runs a Service Manager that performs domain operations on that node.

PowerCenter resource

Any resource that may be required to run a task. PowerCenter has predefined resources and user-defined resources.

PowerCenter services

The services available in the PowerCenter domain. These consist of the Service Manager and the application services.

primary node

A node that is configured as the default node to run a service process. By default, the Service Manager starts the service process on the primary node and uses a backup node if the primary node fails.

repository domain

A group of linked repositories consisting of one global repository and one or more local repositories.

Repository Service

An application service that manages the PowerCenter repository. It retrieves, inserts, and updates metadata in the repository database tables.

Responder service

A service that invokes a response to an underlying service. An example of a Responder service is an email service that notifies specific users of events. RulePoint contains a number of pre-defined Responder Services.

response

A configurable action that is invoked by specific conditions set by a rule.

rule

Rules are used to analyze events based on specific conditions, and then invoke responses when conditions match. For example, when a service produces an event that matches a specific condition a specific response is invoked.

rule wizard

An easy-to-use application within RulePoint that guides users through each step of rule creation, such as define topics, define conditions, and select responses. The rule wizard then generates the rule.

Service

A service is a configurable program that connects to the outside world and pulls or pushes information into RulePoint or sends out information.

session

A task in a workflow that tells the Integration Service how to move data from sources to targets. A session corresponds to one mapping.

Source service

A service that has a configurable topic and can be scheduled to run at specific times. An example of a source service is a news reader that extracts events from a RSS or Atom news feed. RulePoint contains a number of pre-defined Source Services.

Template

A DRQL rule that uses substitution variables to enable users to create rules from a user interface form.

Topic

A category of events. topics are used to group incoming events into logical categories that are familiar to and defined by users. For example, World News, Transactions, or Stock.

transformation

A repository object in a mapping that generates, modifies, or passes data. Each transformation performs a different function.

Watchlist

Container that stores values as a single object with a unique name that you define. This name then can be referenced in a rule so that the rule can use the data stored in the object. You can modify the values within the watchlist at any time, and any rule referencing that watchlist will use those new values. For example, if you want to create several rules regarding your stock portfolio, you can create a watchlist containing symbols for all of the stocks that you currently own. When you create your rules, you would reference the watchlist instead of specifying each individual stock symbol in multiple rules. In the future, if your portfolio changes, you would simply modify the watchlist instead of individual rules.

Web Services Provider

The provider entity of the PowerCenter web service framework that makes PowerCenter workflows and data integration functionality accessible to external clients through web services.

workflow

A set of instructions that tells the Integration Service how to run tasks such as sessions, email notifications, and shell commands.

workflow instance

The representation of a workflow. You can choose to run one or more workflow instances associated with a concurrent workflow. When you run a concurrent workflow, you can run one instance multiple times concurrently, or you can run multiple instances concurrently.

INDEX

A

analytics
  predefined analytics 50
attribute values
  lookup table 39

G

governance alerts
  monitor 35

M

manage
  monitored folders watchlist 23
  PMPC SQL source service 21
monitor
  governance alerts 35
  operations alerts 33
  reports 30
monitored folders watchlist
  manage 23

O

on-demand reports
  create 37
  run 38
operations alerts
  monitor 33

P

PMPC SQL source service
  manage 21

R

reports
  monitor 30
responder
  predefined responder 52
response
  predefined response 81
rule
    advanced rule
      description 18
RulePoint
  responders 11
  rules 11
  sources 11
rules
  advanced rules 69
  predefined advanced rules 69
  types 17
run
  on-demand reports 38

S

SNMP
  alerts 42
  responder 42

T

template rules
  predefined template rules 61
templates
  predefined templates 53
topics
  predefined topics 46

W

watchlists
  predefined watchlists 44